



AF 9100:2026

Aerospace Quality Management System

TECHNICAL PROFILE BOOK

Organizational Management and Assurance — ORG Profile Book

AF-TP-9100-012

FIRST EDITION

30 September 2026 | English master text

Publication identity and application

Control	Publication value
Title	Organizational Management and Assurance — ORG Profile Book
Document code	AF-TP-9100-012
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	Management representative
Primary source anchors	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 22, A, B, D, V, W, AA, AB, AC, AD, AG
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	20
5 Interface records, decisions and continuing use	21
Appendix A — Controlling source and evidence	22
Source tables — complete field and decision payloads	59
Appendix B — Local implementation and release	73

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

The declared legal organization, its actual sites, functions and retained delivery responsibilities; not automatic conformity of all products or people.

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

Exact object and responsibility; intended use and operating domain; applicable activity modules; configuration and sites; criteria and methods; uncertainty or rubric; sampling and witnessed coverage; role independence; duration/instance; changes and claims

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

4.1 — Context, operating environment and emerging conditions

Source p. 14; complete conditions reproduced in Appendix A.

Implementation record: Context register; climate-relevance decision; assumptions; review minutes; resulting changes to objectives, hazards or controls.

Application check: Review every source clause and normative annex against actual activity and retained outsourced responsibility. Record affirmative triggers and reasoned exclusions; lack of resources, a small workforce or another certificate is not an exclusion rationale.

Review boundary: An undefined object, unjustified exclusion or unresolved essential criterion holds admission or acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

4.2 — Interested parties and public-interest interfaces

Source p. 14; complete conditions reproduced in Appendix A.

Implementation record: Interested-party register; obligation classification; communication responsibilities; conflict resolutions.

Application check: Review every source clause and normative annex against actual activity and retained outsourced responsibility. Record affirmative triggers and reasoned exclusions; lack of resources, a small workforce or another certificate is not an exclusion rationale.

Review boundary: An undefined object, unjustified exclusion or unresolved essential criterion holds admission or acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

4.3 — System scope, boundaries and responsibility

Source p. 14; complete conditions reproduced in Appendix A.

Implementation record: Scope statement and Annex A matrix; interface agreements; new-capability review; updated external claims.

Application check: Review every source clause and normative annex against actual activity and retained outsourced responsibility. Record affirmative triggers and reasoned exclusions; lack of resources, a small workforce or another certificate is not an exclusion rationale.

Review boundary: An undefined object, unjustified exclusion or unresolved essential criterion holds admission or acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

4.4 — Processes and their interactions

Source p. 15; complete conditions reproduced in Appendix A.

Implementation record: Process architecture; process-owner definitions; operating criteria; interaction records; process metrics and improvement actions.

Application check: Review every source clause and normative annex against actual activity and retained outsourced responsibility. Record affirmative triggers and reasoned exclusions; lack of resources, a small workforce or another certificate is not an exclusion rationale.

Review boundary: An undefined object, unjustified exclusion or unresolved essential criterion holds admission or acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

4.5 — Obligation and commitment register

Source p. 15; complete conditions reproduced in Appendix A.

Implementation record: Controlled obligation register; change assessments; authorized evidence-access arrangements.

Application check: Review every source clause and normative annex against actual activity and retained outsourced responsibility. Record affirmative triggers and reasoned exclusions; lack of resources, a small workforce or another certificate is not an exclusion rationale.

Review boundary: An undefined object, unjustified exclusion or unresolved essential criterion holds admission or acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

5.1 — Executive accountability and customer focus

Source p. 15; complete conditions reproduced in Appendix A.

Implementation record: Executive reviews; resource decisions; commitment reviews; balanced performance measures and escalations.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

5.2 — Policy and measurable commitments

Source p. 15; complete conditions reproduced in Appendix A.

Implementation record: Approved policy; communication records; observed application; linked objectives.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

5.3 — Roles, management representative and independence

Source p. 15; complete conditions reproduced in Appendix A.

Implementation record: Authority matrix; management-representative appointment; independence arrangements; delegation register.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

5.4 — Ethical behavior and quality culture

Source p. 16; complete conditions reproduced in Appendix A.

Implementation record: Behavior code; reporting channels; investigation records; incentive review; culture evaluation and actions.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

5.5 — Stop-work and release protection

Source p. 16; complete conditions reproduced in Appendix A.

Implementation record: Stop-work instruction; hold records; restart criteria and authorized decisions.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

5.6 — Governance of claims and external relationships

Source p. 16; complete conditions reproduced in Appendix A.

Implementation record: Claim-approval process; supporting evidence; conflict disclosures; correction records.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

6.1 — Risk planning and acceptance

Source p. 16; complete conditions reproduced in Appendix A.

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

Application check: 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.

Review boundary: Unsupported critical consequence, unverified protection or unacceptable residual risk prevents dependent progression. Record each source condition separately in the linked checklist and preserve approved exclusions.

6.2 — Opportunity planning as a distinct activity

Source p. 16; complete conditions reproduced in Appendix A.

Implementation record: Opportunity register; selected initiatives; benefit evaluations; associated risk assessments.

Application check: Allocate owner, resources, decision gates and evidence of success. Assess new safety, quality, security or continuity risks introduced by the proposal before implementation.

Review boundary: Undefined metrics or unassessed adverse effects prevent an achieved-benefit claim, not honest reporting of a shortfall. Record each source condition separately in the linked checklist and preserve approved exclusions.

6.3 — Objectives and execution plans

Source p. 17; complete conditions reproduced in Appendix A.

Implementation record: Objective plans; metric definitions; baseline data; progress reviews and decisions.

Application check: Allocate owner, resources, decision gates and evidence of success. Assess new safety, quality, security or continuity risks introduced by the proposal before implementation.

Review boundary: Undefined metrics or unassessed adverse effects prevent an achieved-benefit claim, not honest reporting of a shortfall. Record each source condition separately in the linked checklist and preserve approved exclusions.

6.4 — Management-system and operational changes

Source p. 17; complete conditions reproduced in Appendix A.

Implementation record: Change requests; impact assessments; approvals; training; implementation and post-change verification.

Application check: Use a difference matrix to justify every reused result. Define full or partial requalification and first-article work, relevant regression and actual receiving-site demonstration.

Review boundary: An unassessed essential difference, unsupported receiving capability or unapproved effectivity holds affected work. Record each source condition separately in the linked checklist and preserve approved exclusions.

6.5 — Resilience and continuity planning

Source p. 17; complete conditions reproduced in Appendix A.

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

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.

6.6 — Technology maturity and future readiness

Source p. 17; complete conditions reproduced in Appendix A.

Implementation record: Technology evidence dossier; experiment approvals; readiness gap list; transition-gate decisions.

Application check: Check material qualification, remaining life, contamination and protective consequences of repair, reuse or environmental improvement. A low-carbon claim does not establish technical interchangeability.

Review boundary: An omitted material category, failed essential human task or unqualified reused input blocks the related claim or release. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.1 — Resource and capacity assurance

Source p. 17; complete conditions reproduced in Appendix A.

Implementation record: Capacity reviews; staffing and equipment plans; constraint decisions; lifecycle-support commitments.

Application check: Link each tool, fixture, machine and controlling program to intended use, range, configuration and demonstrated output capability. Include failure behavior and unauthorized-edit prevention.

Review boundary: Missing protective-function evidence or insufficient actual capability prevents operational acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.2 — Competence, qualification and authorization

Source p. 17; complete conditions reproduced in Appendix A.

Implementation record: Role competence criteria; assessments; qualifications; task-authorization register; reassessment records.

Application check: Plan instruction and supervised work. Record the work actually performed and assistance received. Attendance and years of service are inputs, not automatic proof of current performance.

Review boundary: Unverified competence, a failed essential step or lack of actual task authority prevents independent task performance. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.3 — Awareness and human-performance conditions

Source p. 18; complete conditions reproduced in Appendix A.

Implementation record: Awareness evaluation; human-factor assessments; shift handover and error-prevention controls.

Application check: Plan instruction and supervised work. Record the work actually performed and assistance received. Attendance and years of service are inputs, not automatic proof of current performance.

Review boundary: Unverified competence, a failed essential step or lack of actual task authority prevents independent task performance. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.4 — Infrastructure, utilities and facility integrity

Source p. 18; complete conditions reproduced in Appendix A.

Implementation record: Infrastructure register; maintenance and commissioning records; utility limits; facility change reviews.

Application check: Link each tool, fixture, machine and controlling program to intended use, range, configuration and demonstrated output capability. Include failure behavior and unauthorized-edit prevention.

Review boundary: Missing protective-function evidence or insufficient actual capability prevents operational acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.5 — Work environment, cleanliness and contamination

Source p. 18; complete conditions reproduced in Appendix A.

Implementation record: Environmental specifications; monitoring logs; excursion investigations; cleanliness verification.

Application check: Register received tools, intellectual property, data, access credentials and physical items. Confirm permitted use, condition, custody and reporting obligations.

Review boundary: Unknown damaging exposure or incompatible preservation prevents routine acceptance of affected items. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.6 — Measuring equipment and metrological traceability

Source p. 18; complete conditions reproduced in Appendix A.

Implementation record: Equipment register; calibration chain; recall system; uncertainty suitability; impact and disposition records.

Application check: Use prospective performance criteria, representative specimens, relevant bias, precision, detection, range and robustness. Record transfer differences, failed trials and detection limitations.

Review boundary: Invalid inputs, wrong units, unavailable calibration, unsupported uncertainty or an indeterminate essential result prevent acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.7 — Measurement methods, uncertainty and decision rules

Source p. 18; complete conditions reproduced in Appendix A.

Implementation record: Method-validation records; uncertainty budgets; decision rules; automated inspection challenge results.

Application check: Use prospective performance criteria, representative specimens, relevant bias, precision, detection, range and robustness. Record transfer differences, failed trials and detection limitations.

Review boundary: Invalid inputs, wrong units, unavailable calibration, unsupported uncertainty or an indeterminate essential result prevent acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.8 — Organizational knowledge and technical continuity

Source p. 19; complete conditions reproduced in Appendix A.

Implementation record: Knowledge map; succession and transfer records; lessons database; reuse applicability reviews.

Application check: Assign custodians, lawful rights, readable formats, technical dictionaries and replacement expertise. Test whether receiving users can interpret the evidence without the original author.

Review boundary: Loss of essential support knowledge or source access holds the claim that depends on it until a valid alternative exists. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.9 — Communication and controlled information exchange

Source p. 19; complete conditions reproduced in Appendix A.

Implementation record: Communication matrix; notification and acknowledgement logs; approved information-sharing arrangements.

Application check: Use independently calculated known answers plus boundary, missing, malformed, wrong-unit and prohibited-state cases. Include attempts to approve with expired authority or open findings.

Review boundary: Failure of an essential known-answer, authority or relationship check blocks consequential use of the affected tool. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.10 — Document creation, approval and distribution

Source p. 19; complete conditions reproduced in Appendix A.

Implementation record: Document master list; approval workflow; distribution controls; point-of-use verification.

Application check: Record actual approval and effective events separately from the printed edition date. Publish a controlled master, identify authorized recipients and verify that the point of performance can retrieve the applicable version.

Review boundary: A missing applicable instruction, inaccessible essential evidence or unapproved technical amendment prevents dependent use. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.11 — Record integrity, retention and long-life readability

Source p. 19; complete conditions reproduced in Appendix A.

Implementation record: Retention schedule; signature controls; audit trails; migration and restore tests; authorized disposal records.

Application check: Record actual approval and effective events separately from the printed edition date. Publish a controlled master, identify authorized recipients and verify that the point of performance can retrieve the applicable version.

Review boundary: A missing applicable instruction, inaccessible essential evidence or unapproved technical amendment prevents dependent use. Record each source condition separately in the linked checklist and preserve approved exclusions.

7.12 — Technical software, spreadsheets and decision tools

Source p. 19; complete conditions reproduced in Appendix A.

Implementation record: Tool inventory; validation plan and known-answer tests; version records; review and revalidation triggers.

Application check: Use independently calculated known answers plus boundary, missing, malformed, wrong-unit and prohibited-state cases. Include attempts to approve with expired authority or open findings.

Review boundary: Failure of an essential known-answer, authority or relationship check blocks consequential use of the affected tool. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.1 — Integrated operational planning

Source p. 20; complete conditions reproduced in Appendix A.

Implementation record: Program assurance plan; work packages; control plans; integrated schedule; baseline consistency review.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.1.1 — Operational risk management

Source p. 20; complete conditions reproduced in Appendix A.

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

Application check: 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.

Review boundary: Unsupported critical consequence, unverified protection or unacceptable residual risk prevents dependent progression. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.1.2 — Configuration management

Source p. 20; complete conditions reproduced in Appendix A.

Implementation record: Configuration plan; item hierarchy; baselines; change board decisions; status accounting; configuration audits.

Application check: Use a difference matrix to justify every reused result. Define full or partial requalification and first-article work, relevant regression and actual receiving-site demonstration.

Review boundary: An unassessed essential difference, unsupported receiving capability or unapproved effectivity holds affected work. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.1.3 — Product safety and mission-critical controls

Source p. 20; complete conditions reproduced in Appendix A.

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

Application check: 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.

Review boundary: Unsupported critical consequence, unverified protection or unacceptable residual risk prevents dependent progression. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.1.4 — Counterfeit and unapproved-item prevention

Source p. 21; complete conditions reproduced in Appendix A.

Implementation record: Authenticity-risk assessment; approved sources; incoming verification; suspect-item records and disposition.

Application check: Record packaging, transport conditions, shelf or out-time, seals where relevant and receiving location. Maintain original-to-split links and account for sample consumption.

Review boundary: Unknown eligibility, incompatible material evidence or suspect authenticity holds affected inputs. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.1.5 — Temporary and permanent work transfer

Source p. 21; complete conditions reproduced in Appendix A.

Implementation record: Transfer plan; receiving-site readiness; qualification evidence; initial-output monitoring and closure.

Application check: Use a difference matrix to justify every reused result. Define full or partial requalification and first-article work, relevant regression and actual receiving-site demonstration.

Review boundary: An unassessed essential difference, unsupported receiving capability or unapproved effectivity holds affected work. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.2 — Requirements for products and services

Source p. 21; complete conditions reproduced in Appendix A.

Implementation record: Requirement lifecycle; agreed baseline; review and change records.

Application check: Obtain engineering, production, quality, supplier and service input. Verify personnel, equipment, capacity, evidence access and independent acceptance resources before promising delivery.

Review boundary: Unresolved safety obligation, unavailable essential data or unsupported capability holds the affected commitment. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.2.1 — Customer and user communication

Source p. 21; complete conditions reproduced in Appendix A.

Implementation record: Communication arrangements; technical clarifications; complaints; user-information distribution.

Application check: Obtain engineering, production, quality, supplier and service input. Verify personnel, equipment, capacity, evidence access and independent acceptance resources before promising delivery.

Review boundary: Unresolved safety obligation, unavailable essential data or unsupported capability holds the affected commitment. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.2.2 — Requirement determination and completeness

Source p. 21; complete conditions reproduced in Appendix A.

Implementation record: Requirements register; assumptions; applicable obligations; acceptance definitions; identified special requirements.

Application check: Obtain engineering, production, quality, supplier and service input. Verify personnel, equipment, capacity, evidence access and independent acceptance resources before promising delivery.

Review boundary: Unresolved safety obligation, unavailable essential data or unsupported capability holds the affected commitment. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.2.3 — Contract and commitment review

Source p. 21; complete conditions reproduced in Appendix A.

Implementation record: Multifunctional contract review; feasibility evidence; resolutions; approved deviations from the proposed offer.

Application check: Obtain engineering, production, quality, supplier and service input. Verify personnel, equipment, capacity, evidence access and independent acceptance resources before promising delivery.

Review boundary: Unresolved safety obligation, unavailable essential data or unsupported capability holds the affected commitment. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.2.4 — Changes to requirements

Source p. 22; complete conditions reproduced in Appendix A.

Implementation record: Requirement-change record; impact analysis; baseline update; implementation and acknowledgement evidence.

Application check: Use a difference matrix to justify every reused result. Define full or partial requalification and first-article work, relevant regression and actual receiving-site demonstration.

Review boundary: An unassessed essential difference, unsupported receiving capability or unapproved effectivity holds affected work. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.3 — Design and development

Source p. 22; complete conditions reproduced in Appendix A.

Implementation record: Design scope and responsibility; controlled inputs; review, verification, validation and changes.

Application check: Map local gates to the decision content of G0–G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.3.1 — Design and development governance

Source p. 22; complete conditions reproduced in Appendix A.

Implementation record: Design process; responsibility allocation; design-data acceptance; escalation of ambiguities.

Application check: Map local gates to the decision content of G0–G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.3.2 — Design planning and lifecycle controls

Source p. 22; complete conditions reproduced in Appendix A.

Implementation record: Design plan; interface agreements; review schedule; V&V strategy; required independence.

Application check: Map local gates to the decision content of G0–G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.3.3 — Design inputs and derived requirements

Source p. 22; complete conditions reproduced in Appendix A.

Implementation record: Approved input baseline; derivation rationale; assumption register; conflict resolutions.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.3.4 — Design review, verification and validation

Source p. 22; complete conditions reproduced in Appendix A.

Implementation record: Review records; requirements-to-evidence matrix; approved test plans; raw data; model credibility; anomaly dispositions.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.3.5 — Design outputs and release

Source p. 22; complete conditions reproduced in Appendix A.

Implementation record: Released design package; critical-characteristic list; approval; downstream usability review.

Application check: Map local gates to the decision content of G0-G9. Define input evidence, methods, representative configurations, uncertainty and independence before irreversible commitments.

Review boundary: Unresolved essential interface, unsafe residual condition or unsupported model use holds the dependent gate. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.3.6 — Design changes and continued validity

Source p. 23; complete conditions reproduced in Appendix A.

Implementation record: Change request; impact analysis; requalification decision; approvals; affected-item and implementation records.

Application check: Use a difference matrix to justify every reused result. Define full or partial requalification and first-article work, relevant regression and actual receiving-site demonstration.

Review boundary: An unassessed essential difference, unsupported receiving capability or unapproved effectivity holds affected work. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.4 — Externally provided products, processes and services

Source p. 23; complete conditions reproduced in Appendix A.

Implementation record: External-provider scope; approval, verification and flow-down evidence.

Application check: Review all relevant Annex AF contractual topics, transmit exact requirements and obtain important acknowledgements at the point of performance. Resolve conflicting commercial and technical instructions.

Review boundary: Missing critical flow-down, unassessed source change or unsupported site capability prevents dependent use. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.4.1 — External-provider selection and approval

Source p. 23; complete conditions reproduced in Appendix A.

Implementation record: Supplier evaluations; approval register; performance reviews; conditional approvals; sub-tier dependency map.

Application check: Review all relevant Annex AF contractual topics, transmit exact requirements and obtain important acknowledgements at the point of performance. Resolve conflicting commercial and technical

instructions.

Review boundary: Missing critical flow-down, unassessed source change or unsupported site capability prevents dependent use. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.4.2 — Verification of externally provided outputs

Source p. 23; complete conditions reproduced in Appendix A.

Implementation record: Incoming verification plans; report checks; delegated inspection controls; restricted-release and recall records.

Application check: Review all relevant Annex AF contractual topics, transmit exact requirements and obtain important acknowledgements at the point of performance. Resolve conflicting commercial and technical instructions.

Review boundary: Missing critical flow-down, unassessed source change or unsupported site capability prevents dependent use. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.4.3 — Purchasing information and flow-down

Source p. 23; complete conditions reproduced in Appendix A.

Implementation record: Purchase-order clauses; technical-data issue record; sub-tier acknowledgement; flow-down verification.

Application check: Review all relevant Annex AF contractual topics, transmit exact requirements and obtain important acknowledgements at the point of performance. Resolve conflicting commercial and technical instructions.

Review boundary: Missing critical flow-down, unassessed source change or unsupported site capability prevents dependent use. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5 — Production and service execution

Source p. 24; complete conditions reproduced in Appendix A.

Implementation record: Controlled work routes; actual execution; identity, preservation, support and change records.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.1 — Controlled production and service execution

Source p. 24; complete conditions reproduced in Appendix A.

Implementation record: Controlled route or work package; process records; in-process verification; quantity reconciliation; FOD and utility controls.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.1.1 — Equipment, tooling and production software

Source p. 24; complete conditions reproduced in Appendix A.

Implementation record: Tool and software qualification; controlled programs; maintenance; storage checks; revalidation records.

Application check: Link each tool, fixture, machine and controlling program to intended use, range, configuration and demonstrated output capability. Include failure behavior and unauthorized-edit prevention.

Review boundary: Missing protective-function evidence or insufficient actual capability prevents operational acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.1.2 — Special-process validation and control

Source p. 24; complete conditions reproduced in Appendix A.

Implementation record: Special-process qualification dossier; approved parameter ranges; operator qualifications; run records; requalification decisions.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.1.3 — Production-process and first article verification

Source p. 24; complete conditions reproduced in Appendix A.

Implementation record: First article record; characteristic accountability; material/process evidence; differences and repeat- verification rationale.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.2 — Identification, status and traceability

Source p. 24; complete conditions reproduced in Appendix A.

Implementation record: Identity scheme; genealogy records; status controls; signature register; forward and reverse trace exercises.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.3 — Customer and external-provider property

Source p. 25; complete conditions reproduced in Appendix A.

Implementation record: Property register; receipt checks; access controls; condition and incident records.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.4 — Preservation, packaging and transport

Source p. 25; complete conditions reproduced in Appendix A.

Implementation record: Preservation specifications; packaging qualification; environmental history; shelf-life controls; excursion dispositions.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.5 — Post-delivery support and field feedback

Source p. 25; complete conditions reproduced in Appendix A.

Implementation record: Support plan; service information; field reliability data; notifications; off-site work controls.

Application check: Record performer, event time, inputs, actual essential variables, results and deviations by output identity. Retain evidence of concealed or irreversible operations before they become unobservable.

Review boundary: An unverified essential operation, missing genealogy or out-of-window process remains held from acceptance. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.5.6 — Production and service changes

Source p. 25; complete conditions reproduced in Appendix A.

Implementation record: Process-change record; technical impact; approvals; temporary controls; changed-output verification.

Application check: Use a difference matrix to justify every reused result. Define full or partial requalification and first-article work, relevant regression and actual receiving-site demonstration.

Review boundary: An unassessed essential difference, unsupported receiving capability or unapproved effectivity holds affected work. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.6 — Acceptance and authorized release

Source p. 25; complete conditions reproduced in Appendix A.

Implementation record: Release checklist; acceptance results; closed or authorized issues; delivery dossier; release authorization.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

8.7 — Nonconforming outputs and escape control

Source p. 25; complete conditions reproduced in Appendix A.

Implementation record: NCR; material review decisions; population trace; notifications; repair/rework verification; scrap control.

Application check: Record correction, rework, repair, concession, return or scrap with competent design/customer/authority approval when required. Prevent suspect material returning uncontrolled to the supply chain.

Review boundary: An open in-scope nonconformity blocks initial attestation, renewal and extension even if an action plan is accepted. Record each source condition separately in the linked checklist and preserve approved exclusions.

9.1 — Monitoring strategy and data credibility

Source p. 26; complete conditions reproduced in Appendix A.

Implementation record: Monitoring plan; metric dictionary; source reconciliations; data-quality checks; action records.

Application check: Allocate owner, resources, decision gates and evidence of success. Assess new safety, quality, security or continuity risks introduced by the proposal before implementation.

Review boundary: Undefined metrics or unassessed adverse effects prevent an achieved-benefit claim, not honest reporting of a shortfall. Record each source condition separately in the linked checklist and preserve approved exclusions.

9.2 — Customer satisfaction and external feedback

Source p. 26; complete conditions reproduced in Appendix A.

Implementation record: Feedback records; segment analysis; improvement plans; effectiveness evaluations.

Application check: Use a distribution and dependence model suited to the actual mechanism. Separate process control from specification, and confidence bounds from point estimates or monitoring percentages.

Review boundary: An invalid model or unspecified denominator prevents the unsupported numerical claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

9.3 — Internal audit program

Source p. 26; complete conditions reproduced in Appendix A.

Implementation record: Risk-based audit program; competence and independence; plans; evidence trails; findings; closure verification.

Application check: Use actual outputs and adverse cases to connect requirements, sources, people, configuration, execution, release and feedback. Record population and sampling limits.

Review boundary: Uncovered mandatory scope or unsupported auditor competence prevents declaring the internal programme complete. Record each source condition separately in the linked checklist and preserve approved exclusions.

9.4 — Management review inputs

Source p. 26; complete conditions reproduced in Appendix A.

Implementation record: Review agenda and input pack; trend analyses; independent assurance concerns; status of prior actions.

Application check: Require comparable populations and original records for important trends. Distinguish isolated events from recurring mechanisms and consider missing data and reporting suppression.

Review boundary: Unaddressed essential capability or protective concern prevents treating review minutes as release authority. Record each source condition separately in the linked checklist and preserve approved exclusions.

9.5 — Management review decisions and follow-through

Source p. 27; complete conditions reproduced in Appendix A.

Implementation record: Recorded decisions; action ownership; resource commitments; follow-up and effectiveness evidence.

Application check: Require comparable populations and original records for important trends. Distinguish isolated events from recurring mechanisms and consider missing data and reporting suppression.

Review boundary: Unaddressed essential capability or protective concern prevents treating review minutes as release authority. Record each source condition separately in the linked checklist and preserve approved exclusions.

9.6 — Independent assurance and systemic challenge

Source p. 27; complete conditions reproduced in Appendix A.

Implementation record: Independent-review plan; challenge records; dissent resolution; release recommendations.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

10.1 — Response to nonconformity and containment

Source p. 27; complete conditions reproduced in Appendix A.

Implementation record: Response record; containment scope; trace results; effectiveness checks; preserved evidence.

Application check: Record correction, rework, repair, concession, return or scrap with competent design/customer/authority approval when required. Prevent suspect material returning uncontrolled to the supply chain.

Review boundary: An open in-scope nonconformity blocks initial attestation, renewal and extension even if an action plan is accepted. Record each source condition separately in the linked checklist and preserve approved exclusions.

10.2 — Cause analysis and corrective action

Source p. 27; complete conditions reproduced in Appendix A.

Implementation record: Evidence-based cause analysis; occurrence and escape controls; action plan; systemic extent; effectiveness results.

Application check: Record correction, rework, repair, concession, return or scrap with competent design/customer/authority approval when required. Prevent suspect material returning uncontrolled to the supply chain.

Review boundary: An open in-scope nonconformity blocks initial attestation, renewal and extension even if an action plan is accepted. Record each source condition separately in the linked checklist and preserve approved exclusions.

10.3 — Continual improvement and preventive learning

Source p. 27; complete conditions reproduced in Appendix A.

Implementation record: Improvement portfolio; baseline and outcome evaluation; change assurance; retained learning.

Application check: Allocate owner, resources, decision gates and evidence of success. Assess new safety, quality, security or continuity risks introduced by the proposal before implementation.

Review boundary: Undefined metrics or unassessed adverse effects prevent an achieved-benefit claim, not honest reporting of a shortfall. Record each source condition separately in the linked checklist and preserve approved exclusions.

10.4 — Learning across the lifecycle and network

Source p. 27; complete conditions reproduced in Appendix A.

Implementation record: Indexed lessons; applicability reviews; supplier communication; recurrence and uptake assessment.

Application check: Assign custodians, lawful rights, readable formats, technical dictionaries and replacement expertise. Test whether receiving users can interpret the evidence without the original author.

Review boundary: Loss of essential support knowledge or source access holds the claim that depends on it until a valid alternative exists. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.1 — Conformity evidence dossier

Source p. 40; complete conditions reproduced in Appendix A.

Implementation record: Object-specific dossier; applicable requirement set; evidence index; configuration and population coverage; limitations.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.2 — Evaluation, review and decision separation

Source p. 40; complete conditions reproduced in Appendix A.

Implementation record: Assignment matrix; competence and conflict checks; evaluation record; independent review and decision identities.

Application check: Examine ownership, finance, employment, consultancy, family relationships, referral incentives and shared resources. A signed declaration records inputs; an actual unmanageable conflict requires recusal, reassignment or refusal.

Review boundary: Unresolved conflicts, expired delegation or a failed essential protective control prevent the affected authorization. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.3 — Criteria, sampling and findings

Source p. 41; complete conditions reproduced in Appendix A.

Implementation record: Evaluation plan; sample rationale; objective evidence; requirement-linked findings; assessed limitations.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.4 — Decision conditions and release blockers

Source p. 41; complete conditions reproduced in Appendix A.

Implementation record: Requirement-by-requirement conclusion; finding closure; blocker check; reasoned and dated decision.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.5 — Statements, certificates and mark use

Source p. 41; complete conditions reproduced in Appendix A.

Implementation record: Approved claim text; certificate data; mark permission; actual recognition scope where claimed.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.6 — Continuing validity and changes

Source p. 41; complete conditions reproduced in Appendix A.

Implementation record: Change notifications; surveillance findings; renewal evidence; current and historical status records.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.7 — Complaints, appeals and corrective communication

Source p. 41; complete conditions reproduced in Appendix A.

Implementation record: Case records; independent reviewer appointment; reasoned outcomes; affected-population action and communication.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

22.8 — Scheme operation and competence attestations

Source p. 41; complete conditions reproduced in Appendix A.

Implementation record: Operator authority; body competence evaluation; written scope; independent decision; accurate accreditation and authorization claims.

Application check: Use the approved attribute or numerical rule and unrounded data. Check each essential characteristic independently; a favorable average cannot substitute for a required condition.

Review boundary: Unclosed release blocker, unsupported configuration or unavailable authority prevents release of the dependent claim. Record each source condition separately in the linked checklist and preserve approved exclusions.

4 Representative evaluation and adverse evidence

Scope, Context, Obligations and Applicability

Witness or trace: Map each applicable technical, customer and legal obligation to the current controlled data and responsible authority. Resolve conflicting obligations before the affected commitment; keep confidential review available through lawful access.

Synthetic challenge: A distributor starts repairing returned components. Keep distribution evidence but add actual repair, process, competence, technical-data and release duties. A former distribution certificate does not cover the new service.

Governance, Delegation, Impartiality and Stop Authority

Witness or trace: Specify delegated decisions, affected items, competence, duration, supervision and retained accountability. Confirm that supplier permissions and system access cannot enlarge the written delegation.

Synthetic challenge: The commercial director asks a reviewer to remove a finding to meet a delivery date. Retain the evidence-based finding, protect the release boundary and record the interference. Management may resource corrective work but cannot manufacture conformity.

Internal Audit and Requirement-Level Evaluation

Witness or trace: Combine current documents, interviews, witnessed work and original results. Resolve remote-access limitations through supplementary evidence or a bounded conclusion.

Synthetic challenge: All corporate procedures were reviewed but a night-shift critical process was never examined. Retain the coverage gap, resource the required observation and update the audit plan. Document presence is not evidence of that shift's implementation.

Management Review and Independent Assurance Challenge

Witness or trace: For high-consequence work apply Annex B independence and retain competing views. The designer or action owner cannot close a contested critical assumption solely by restating confidence.

Synthetic challenge: An overdue inspection-resource gap is repeatedly noted without action. Assign actual resource and restriction decisions and verify implementation. Repeated acknowledgement does not demonstrate an effective management response.

Scheme Admission, Participation Terms and Operator Authority

Witness or trace: For initial ORG assess actual internal audit, management review and sufficient implemented records. Do not impose a corporate audit on an individual PER candidate or request fabricated operating history.

Synthetic challenge: An applicant asks the operator to add an unfamiliar laboratory method to its offer. Classify it as scope development until technical criteria, competence, witnessing and authority are ready; do not infer capability from an existing organizational certificate.

Assessment Planning, Audit Time, Site Coverage and Remote Work

Witness or trace: Document identity, live evidence, confidentiality, configuration, access, recording permission and representation. Add physical witnessing where remote review cannot establish the required capability.

Synthetic challenge: Nine eligible low-consequence sites are proposed for surveillance using three sampled sites. The source formula requires five eligible sites, at least two random, plus central and separately

mandatory locations. Three is not sufficient under the uploaded rule.

Independent Decisions, Attestations, Claims and Registry

Witness or trace: For initial grant, renewal and extension require every applicable mandatory condition, adequate evidence and all in-scope nonconformities closed. Votes, payment and a high maturity score cannot supply a missing condition.

Synthetic challenge: All checks pass except one minor finding that has a promised future correction. Hold initial, renewed or extended attestation until verified closure. The bounded rule for an already existing minor does not permit a new certificate with open findings.

Surveillance, Renewal, Status, Transfer and Closure

Witness or trace: State scope, prohibited use, actions and the 90-day final resolution limit. Restore only on evidence, restrict independently unaffected scope or withdraw; preserve original expiry unless full renewal occurs.

Synthetic challenge: A suspended holder requests a new certificate number to restart the clock. Retain the original suspension and expiry history. A new number is not evidence of correction, renewal or restoration.

5 Interface records, decisions and continuing use

Record	Required implementation purpose
AF-FR-9100-001	Application and Scope
AF-FR-9100-002	Application Profile and Acceptance Schedule
AF-FR-9100-003	Competence, Independence and Assignment
AF-FR-9100-004	Audit and Evaluation Plan
AF-FR-9100-006	Nonconformity, Containment and Corrective Action
AF-FR-9100-007	Independent Review and Attestation Decision
AF-FR-9100-008	Surveillance, Renewal and Status
AF-FR-9100-013	Context, Processes, Obligations and Objectives
AF-FR-9100-028	Internal Audit, Management Review and Improvement

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.

1.1 Organizations and value chains covered

SOURCE p. 9 | Normative when applicable

1.1(a) This standard applies to organizations that design, develop, manufacture, assemble, integrate, test, inspect, procure, distribute, maintain, operate or support products and services for aviation, space, defense, heavy industry and mission-specific mobility. It includes prime contractors, equipment manufacturers, all supplier tiers, research organizations, engineering services, software providers, logistics providers and support facilities.

1.1(b) The scope includes civil and military aircraft, rotorcraft, unmanned systems, advanced air mobility, satellites, launch and ground systems, orbital and surface infrastructure, land and maritime defense platforms, industrial machinery, process plant and associated infrastructure. Automotive-derived products are included when used for defense missions, space exploration, launch-site support or other mission-specific applications. General-road homologation and specialized mission approval remain distinct responsibilities.

1.2 Products, services, processes and people

SOURCE p. 9 | Normative when applicable

1.2(a) Covered outputs include hardware, materials, electronics, embedded and application software, artificial-intelligence models, datasets, technical information, digital and professional services, training affecting competence, maintenance actions and integrated systems of systems. Covered delivery resources include personnel, special processes, subcontractors, sub-tier suppliers, laboratories, inspection and assessment providers.

1.2(b) The standard is technology-neutral. An unlisted material, energy source, computing paradigm, production method or autonomous capability shall be included in applicability and hazard analysis when its effects fall within scope. A technology not named in this edition is not exempt from assurance.

1.2(c) The conformity object shall be selected explicitly using Annex AA. Organizational conformity, product conformity, service conformity, process qualification, personnel certification, employer task authorization, supplier qualification and assessment-body competence are distinct conclusions. Evidence may be reused when its relevance and validity are established, but no conclusion automatically grants another.

Required evidence: Conformity-object register; product and service families; process and personnel scope; external-provider map; selected route and technical profile.

1.3 Scope statement and mandatory applicability decision

SOURCE p. 9 | Normative when applicable

1.3(a) An organization shall maintain a controlled scope identifying legal entities, sites, remote functions, products, services, processes, lifecycle responsibilities and exclusions. It shall complete Annex A before claiming conformity. Shared services and outsourced activities shall be included where responsibility remains with the organization.

1.3(b) The organizational route applies Clauses 1–10 and 22, with the relevant technical modules in Clauses 11–21 and object or provider controls in Clauses 23–28. A requirement may be excluded only where the activity and associated responsibility are genuinely absent and the exclusion cannot impair an assured outcome. Outsourcing, a small workforce or an existing certificate does not by itself justify exclusion.

1.3(c) For a product, service, process, person, supplier or assessment-provider route, Annex AA identifies the applicable evaluation boundary. A personnel applicant shall demonstrate the defined role competences, not ownership of a corporate management system. The body operating that route shall nevertheless fulfill its own governance, impartiality and evidence obligations.

1.3(d) Where product design responsibility is absent, supplied design data, manufacturing-process design, technical changes and error escalation shall remain controlled. Where only distribution occurs, authenticity, preservation, traceability and customer flow-down remain required. Incompatible obligations shall be escalated and the dependent work held until resolved.

Required evidence: Approved scope; object-route selection; Annex A matrix; exclusions with evidence; interface owners; review triggers and scope-change history.

1.4 Boundaries of conformity and authorization

SOURCE p. 10 | Normative when applicable

1.4(a) Conformity to this standard shall not be represented as a type certificate, airworthiness approval, launch license, defense authorization, vehicle homologation, marine class approval or statutory plant approval. Mandatory authorizations and program-specific technical requirements remain applicable. A product claim requires an evaluated product scope; an organizational certificate alone does not approve every output.

1.4(b) Membership, sponsorship, committee participation, awards and training attendance do not establish conformity. AF marks and AF-authorized scheme operation require actual written authorization. Annexes AA-AJ define this standard's assessment rules; their publication does not automatically authorize a body, accredit a laboratory or certify an applicant.

1.4(c) The designation AF 9100:2026 identifies an independent AF publication. Use of that identifier shall not imply adoption, sponsorship or recognition by another publisher, regional standards system or public authority.

Required evidence: Accurate claims and certificate scope; actual authorizations; mark permissions; separation of technical and statutory approvals.

1.5 System boundaries and hazardous domains

SOURCE p. 10 | Normative when applicable

1.5(a) The organization shall identify interactions among product safety, occupational safety, environmental protection, security, cybersecurity and mission effectiveness. Responsibilities shall cover both intended use and reasonably foreseeable misuse or abnormal conditions. Approval of one discipline shall not be interpreted as approval of the others.

1.5(b) For controlled defense technology, energetic materials, radiological sources or other restricted activities, this standard specifies governance and assurance responsibilities only. Detailed operating procedures, design criteria, access controls and approvals shall be established by appropriately authorized specialists under applicable obligations. No clause provides instructions for weapon construction or employment.

2.1 Self-contained AF requirement basis

SOURCE p. 10 | Normative when applicable

2.1(a) An AF 9100:2026 conformity decision shall evaluate all applicable requirements of this edition, including the triggered normative annexes and the approved object-specific application profile. A summary, checklist or training presentation shall not replace the complete applicable requirement set.

2.1(b) The responsible organization or scheme operator shall provide controlled access to this edition at the point of use. AF clauses shall not be represented as identical to an unevaluated external scheme. Compliance evidence shall be traced to the actual AF requirement and the actual evaluated object.

Required evidence: Controlled edition; applicable-requirement register; application profile; evidence mapping.

2.2 Controlled program and application profile

SOURCE p. 10 | Normative when applicable

2.2(a) Before evaluation or acceptance, the responsible technical authority shall approve an application profile defining the object, configuration, intended use, operational domain, applicable obligations, measurable criteria, verification methods, uncertainty treatment, sampling rationale and release limits. The profile shall be detailed enough for different competent evaluators to reach comparable conclusions.

2.2(b) Product tolerances, loads, environmental qualification levels, service performance limits and role-specific practical tasks shall be derived from the actual application. This standard does not invent one engineering limit for unrelated aircraft, spacecraft, vehicles, ships, plant or occupations. Absence of an adequate profile shall block a claim requiring that profile.

2.2(c) A controlled obligation register shall identify binding law, customer commitments, approved technical data, test procedures and authority decisions with their applicable editions, owners and change triggers. Such inputs may be legally or contractually necessary without becoming external normative references in this AF publication.

Required evidence: Approved application profile; technical rationale; criteria and methods; obligation register; change controls.

2.3 Precedence and conflict resolution

SOURCE p. 10 | Normative when applicable

2.3(a) Applicable law and competent-authority conditions shall not be waived by AF permission, customer agreement, risk acceptance or internal concession. Compatible binding requirements shall all be fulfilled. Where obligations cannot jointly be met, affected work and claims shall be held until a documented lawful resolution is approved by the responsible technical and contractual authorities.

2.3(b) The standard's requirements and triggered annexes shall be read together. Annex AD governs assessment decision rules; Annex AG governs scheme time limits; Annex AB governs assessor competence; Annex AE governs personnel assessment; Annex Y governs publication control. These rules cannot weaken safety, technical acceptance or legal obligations elsewhere in the standard.

2.3(c) An internal procedure, purchasing instruction, automated workflow or contract profile shall not remove an applicable AF requirement. More demanding program requirements may be added. A conflict shall be recorded, not resolved by silently selecting the less demanding provision.

Required evidence: Conflict register; affected scope; technical and contractual resolution; controlled amendments to working instructions.

2.4 Normative annexes and evidence conventions

SOURCE p. 11 | Normative when applicable

2.4(a) The status stated at each annex heading controls its use. Normative annexes impose requirements when triggered by activity or assessment route. Annex N has separately identified normative and informative portions. Other informative annexes explain methods and examples but do not create universal acceptance thresholds.

2.4(b) Equivalent record formats are permitted where every required field, relationship, approval and integrity control is retained. "Not applicable", "accepted risk" and "covered by supplier" are not evidence without a justified applicability or decision record. Synthetic example values shall never be copied into a real record as actual observations.

2.4(c) A compound requirement shall be assessed against every applicable condition. Checklist compression shall not remove conditions. A requirement is not satisfied merely because a document exists: appropriate implementation and outcome evidence are also required.

Required evidence: Annex applicability; complete evidence fields; evaluated conditions; justified non-applicability.

2.5 Edition, time and change control

SOURCE p. 11 | Normative when applicable

2.5(a) The publication identifier is AF 9100:2026; the edition is First Edition; the publication date is 29 September 2026. Amendments shall be uniquely identified and controlled under Annex Y. An edition designation does not attest that a particular organization, product or person has passed assessment.

2.5(b) Scheme time limits shall be interpreted under Annex AG. Adoption dates in contracts, transition dates in future amendments and effective dates of individual authorizations shall be recorded separately. No date shall be backdated to hide a gap in conformity status.

Required evidence: Edition and amendment register; adoption record; actual decision dates and status history.

2.6 Engineering judgment and reproducible decisions

SOURCE p. 11 | Normative when applicable

2.6(a) Where a requirement calls for proportionate controls, the organization shall record the consequence, uncertainty, selected method and technical rationale supporting that judgment. Competent discretion shall not be used to waive a defined minimum, omit an essential control or approve inaccessible evidence.

2.6(b) Calculations used for acceptance shall have verified inputs, compatible units, controlled algorithms and documented applicability assumptions. A successfully executed calculation or a digitally signed record does not by itself demonstrate a valid physical model or a true original observation.

Required evidence: Technical judgments; verified computations; assumptions and limitations; independent review when required.

3.1 Interpretation and evidence convention

SOURCE p. 14 | Normative when applicable

3.1(a) A requirement identifier consists of the subclause and its lettered paragraph, for example 8.1.3(a). The complete paragraph, including each condition joined within it, is applicable unless an approved scope decision establishes otherwise. Evidence notes identify minimum record content, not the only permissible proof of implementation.

3.1(b) “Documented” information may be digital, physical or a controlled combination. A database, model, signed workflow or automated log may satisfy a record requirement if identity, integrity, access, retention and retrievability are demonstrated. A screenshot without provenance is not sufficient evidence of the underlying transaction.

4.1 Context, operating environment and emerging conditions

SOURCE p. 14 | Normative when applicable

4.1(a) The organization shall determine internal and external conditions affecting its ability to deliver conforming and dependable outputs. The review shall include mission environments, technology maturity, human capability, infrastructure, supply dependencies, market changes, public-interest effects and applicable legal and contractual conditions. Material assumptions shall have owners and review triggers.

4.1(b) The organization shall explicitly assess whether climate change or climate-related disruption is relevant to product conformity, operational environments, infrastructure, supply continuity or interested-party requirements. It shall record the decision, evidence and necessary actions. The AF requirement extends this review to physical and transition effects without imposing a universal emissions target.

4.1(c) Context shall be reviewed at planned intervals and following a significant incident, acquisition, mission change, relocation, severe supply disruption or relevant change in obligations. A context review shall result in decisions affecting plans or controls where necessary, not only a static list of factors.

Required evidence: Context register; climate-relevance decision; assumptions; review minutes; resulting changes to objectives, hazards or controls.

4.2 Interested parties and public-interest interfaces

SOURCE p. 14 | Normative when applicable

4.2(a) The organization shall identify parties whose requirements or exposure can affect the system’s outcomes, including customers, end users, operators, workers, suppliers, authorities and persons exposed to credible product consequences. It shall determine which requirements are binding, which are adopted commitments and which are information to monitor.

4.2(b) Conflicting expectations shall be resolved through a documented decision process. Customer preference shall not override a binding safety or legal requirement. Community or user concerns relevant to product use shall be assessed on evidence, while access to sensitive or controlled information shall remain restricted to authorized recipients.

Required evidence: Interested-party register; obligation classification; communication responsibilities; conflict resolutions.

4.3 System scope, boundaries and responsibility

SOURCE p. 14 | Normative when applicable

4.3(a) The scope and applicability matrix shall reflect actual responsibilities at every lifecycle stage, including outsourced design, remote engineering, cloud services, off-site maintenance and customer-site work. Responsibility for an interface shall be assigned to a named role on each side; shared responsibility shall not leave an unowned decision.

4.3(b) Changes to scope shall undergo a documented capability and risk review before new work is accepted. The organization shall verify personnel, facilities, technical data, authorizations and assurance capacity for the changed scope. Public statements and any assessment certificate shall be updated when the controlled scope changes.

Required evidence: Scope statement and Annex A matrix; interface agreements; new-capability review; updated external claims.

4.4 Processes and their interactions

SOURCE p. 15 | Normative when applicable

4.4(a) The organization shall establish and maintain an integrated process model showing sequence, inputs, outputs, interfaces and feedback. For every process it shall assign an owner, determine resources, define operating and acceptance criteria, identify relevant risks and opportunities, and establish measures of both process performance and outcome effectiveness.

4.4(b) The organization shall control cross-functional handovers so that requirements, configuration, unresolved issues and acceptance responsibilities remain explicit. Process measures shall include failure and escape signals where relevant, rather than relying solely on activity counts or schedule achievement.

4.4(c) Documented operating information shall be maintained, and evidence of execution shall be retained. The organization may use a quality manual or equivalent navigable system; the chosen form shall allow personnel and assessors to locate current requirements, responsibilities and records without reconstructing them from personal knowledge.

Required evidence: Process architecture; process-owner definitions; operating criteria; interaction records; process metrics and improvement actions.

4.5 Obligation and commitment register

SOURCE p. 15 | Normative when applicable

4.5(a) The organization shall maintain an obligation register linking each applicable external obligation to affected products, sites, processes and accountable owners. The register shall identify evidence of fulfillment and the mechanism for detecting relevant changes. Subscription to an alert service alone shall not constitute an assessment of applicability.

4.5(b) Where access restrictions limit an assessor's ability to view evidence, the organization shall arrange an authorized alternative that preserves competence and traceability. Restricted information shall not be replaced by an unsupported statement of compliance. Unresolved access limitations shall be identified in the assessment outcome.

Required evidence: Controlled obligation register; change assessments; authorized evidence-access arrangements.

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.

5.3 Roles, management representative and independence

SOURCE p. 15 | Normative when applicable

5.3(a) Top management shall appoint a management representative with authority to coordinate the system, report performance and escalate unresolved quality or assurance issues directly to the accountable executive. Technical authorities for design, safety, production, software, cybersecurity and release shall be identified according to the organization's activities.

5.3(b) Personnel responsible for independent review or release shall have the competence, access and freedom necessary to challenge the work. For the criticality categories in Annex B, independence shall be demonstrated by the reporting or decision arrangement, not merely by a different job title. Conflicts of interest shall be recorded and managed.

5.3(c) Delegation shall specify scope, limitations, competence, duration and supervision. A delegated supplier or automated workflow shall not acquire authority beyond the documented delegation. The delegating organization shall monitor performance and retain the ability to suspend the delegation.

Required evidence: Authority matrix; management-representative appointment; independence arrangements; delegation register.

5.4 Ethical behavior and quality culture

SOURCE p. 16 | Normative when applicable

5.4(a) The organization shall establish behavioral expectations prohibiting falsification of test results, concealed rework, unauthorized substitutions, misleading claims and retaliation for good-faith reporting. Management incentives and production targets shall be reviewed for pressures that could undermine these expectations.

5.4(b) Personnel shall have accessible channels to raise concerns, including escalation outside the immediate production chain when necessary. The organization shall protect reporters within applicable requirements, investigate concerns impartially and communicate outcomes appropriately. An increase in reported concerns shall not automatically be interpreted as deteriorating culture.

5.4(c) Culture shall be evaluated using more than a survey score. The organization shall examine response to bad news, willingness to stop work, closure quality, recurrence, supplier treatment and management follow-through.

Required evidence: Behavior code; reporting channels; investigation records; incentive review; culture evaluation and actions.

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.

5.6 Governance of claims and external relationships

SOURCE p. 16 | Normative when applicable

5.6(a) The organization shall ensure that proposals, declarations, product literature, environmental claims and statements about certification or AF recognition are accurate, bounded and supported. A management-system assessment shall not be used as evidence of a product capability that was not evaluated.

5.6(b) Potential conflicts arising from investment, consultancy, training, supplier ownership or commercial sponsorship shall be disclosed to relevant decision makers. Any conformity decision shall remain independent of payments or membership status. Public corrections shall be made when a materially misleading claim is identified.

Required evidence: Claim-approval process; supporting evidence; conflict disclosures; correction records.

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.

6.2 Opportunity planning as a distinct activity

SOURCE p. 16 | Normative when applicable

6.2(a) The organization shall identify and evaluate opportunities for improved capability, customer value, reliability, resilience, resource efficiency and knowledge. Each selected opportunity shall have a benefit hypothesis, feasibility assessment, resources, accountable owner, implementation milestones and a method for evaluating achieved benefit.

6.2(b) Opportunity decisions shall be recorded separately from adverse-risk acceptance. An opportunity may generate new risks, which shall be evaluated through the risk process. The expected benefit of innovation shall not cancel a nonconformity or justify bypassing qualification.

Required evidence: Opportunity register; selected initiatives; benefit evaluations; associated risk assessments.

6.3 Objectives and execution plans

SOURCE p. 17 | Normative when applicable

6.3(a) Measurable objectives shall be established at relevant organizational, process and program levels. Each objective shall identify the outcome, baseline, measure definition, target rationale, owner, resources, due date and evaluation frequency. Safety and quality objectives shall include leading and lagging indicators where useful.

6.3(b) Denominators, exclusions and data sources shall be defined before reporting. Targets shall not encourage concealment, selective deletion, denominator changes or shipment before completion of acceptance. Failure to meet an objective shall trigger analysis and appropriate action, not retroactive redefinition without disclosure.

Required evidence: Objective plans; metric definitions; baseline data; progress reviews and decisions.

6.4 Management-system and operational changes

SOURCE p. 17 | Normative when applicable

6.4(a) Changes shall be planned with a stated purpose, affected requirements, risks, resources, competence needs, interfaces, implementation method and acceptance criteria. The organization shall identify the approved baseline, the proposed baseline and the evidence needed to authorize transition.

6.4(b) The change process shall cover organizational restructuring, relocation, outsourcing, supplier changes, digital- platform replacement, model updates, process-parameter changes and emergency changes. Temporary changes shall have explicit expiry or restoration criteria. Unintended changes shall be assessed and contained promptly.

Required evidence: Change requests; impact assessments; approvals; training; implementation and post-change verification.

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.

6.6 Technology maturity and future readiness

SOURCE p. 17 | Normative when applicable

6.6(a) The organization shall evaluate new technology against the actual intended environment and integration context. Readiness claims shall identify demonstrated functions, scale, duration, interfaces, limitations and unresolved gaps. A laboratory demonstration shall not automatically establish production, operational or mission readiness.

6.6(b) Programs involving AI, advanced autonomy, in-space manufacturing, new propulsion, quantum technologies or other emerging capabilities shall establish bounded experiments and explicit transition gates. Monitoring shall include new failure mechanisms and foreseeable misuse. Changes to assumptions shall reopen the relevant assurance decisions.

Required evidence: Technology evidence dossier; experiment approvals; readiness gap list; transition-gate decisions.

7.1 Resource and capacity assurance

SOURCE p. 17 | Normative when applicable

7.1(a) The organization shall determine and provide resources necessary for planned work and credible contingencies. Capacity reviews shall consider competent personnel, equipment availability, maintenance, inspection, independent review, supplier capacity and expected rework. Inspection capacity shall not be assumed unlimited when production volume increases.

7.1(b) Before accepting accelerated schedules or significant volume changes, the organization shall verify that resources and controls remain adequate. Unfunded assurance activities shall be escalated rather than silently removed. Resource plans shall include lifecycle support and retention of necessary technical knowledge.

Required evidence: Capacity reviews; staffing and equipment plans; constraint decisions; lifecycle-support commitments.

7.2 Competence, qualification and authorization

SOURCE p. 17 | Normative when applicable

7.2(a) Competence requirements shall be defined for roles affecting conformity and assurance, including temporary staff, contractors, reviewers, programmers, inspectors and release personnel. Competence shall be evaluated through suitable education, experience, supervised practice, demonstration or examination appropriate to the task.

7.2(b) Where a license or formal qualification is required, validity and scope shall be verified. Authorization shall identify the specific task, product or process and any limitations. Training attendance alone shall not establish competence. Reassessment shall follow significant technology change, extended inactivity or evidence of deficient performance.

7.2(c) Auditor and assessment-role competence shall meet Annex AB where those functions are performed. Personnel certification shall follow Clause 26 and Annex AE; employer task authorization shall remain specific to actual work. Contractors and temporary personnel shall meet the same relevant competence and authorization controls as employees.

Required evidence: Role competence criteria; assessments; qualifications; task-authorization register; reassessment records.

7.3 Awareness and human-performance conditions

SOURCE p. 18 | Normative when applicable

7.3(a) Personnel shall understand relevant policies, objectives, current instructions, their contribution to product safety and mission outcomes, ethical expectations and the consequences of nonconforming work. Communication shall be adapted to language, literacy, shift patterns and remote working.

7.3(b) The organization shall identify work conditions that increase error, including fatigue, interruption, confusing interfaces, inaccessible tools, time pressure and poor handovers. Controls shall address the system conditions as well as individual skill. Investigations shall not use “operator error” as a sufficient root-cause conclusion.

Required evidence: Awareness evaluation; human-factor assessments; shift handover and error-prevention controls.

7.4 Infrastructure, utilities and facility integrity

SOURCE p. 18 | Normative when applicable

7.4(a) Facilities, utilities, equipment, communication systems and supporting software shall be suitable for intended operations and maintained. Critical infrastructure shall have defined operating limits, inspection or maintenance requirements, condition monitoring and contingency arrangements.

7.4(b) Changes to foundations, equipment layout, utilities, environmental controls or network connections shall undergo impact review. Commissioning shall verify configuration and protective functions before production or service use. Where facility condition can influence measurement or process output, the condition shall be recorded or monitored.

Required evidence: Infrastructure register; maintenance and commissioning records; utility limits; facility change reviews.

7.5 Work environment, cleanliness and contamination

SOURCE p. 18 | Normative when applicable

7.5(a) The organization shall define necessary environmental conditions for work, storage, inspection and testing. Controls shall address relevant temperature, humidity, vibration, lighting, electromagnetic disturbance, cleanliness, electrostatic discharge, contamination and biological or chemical exposure.

7.5(b) Clean zones, sensitive assemblies and contamination-critical processes shall have controlled entry, materials, cleaning methods and verification. Excursions shall trigger an assessment of exposed products and evidence, including material already transferred downstream. Restoration of room conditions alone shall not close the product-impact assessment.

Required evidence: Environmental specifications; monitoring logs; excursion investigations; cleanliness verification.

7.6 Measuring equipment and metrological traceability

SOURCE p. 18 | Normative when applicable

7.6(a) Measurement systems used to demonstrate conformity shall be suitable for the measurand, range, environment and decision risk. The organization shall maintain a register containing equipment identity, location, owner, range, calibration or verification method, interval, status and acceptance criteria.

7.6(b) Where traceability is required or necessary for confidence, calibration shall be linked through a documented chain to appropriate measurement references. Where an established reference does not exist, the technical basis of verification shall be documented. Equipment shall be protected from unauthorized adjustment and damage.

7.6(c) Out-of-tolerance, damaged, overdue or otherwise unsuitable equipment shall be removed or restricted from use. The organization shall assess the validity of prior results and trace affected outputs. An equipment recalibration certificate shall not, by itself, resolve the product disposition.

Required evidence: Equipment register; calibration chain; recall system; uncertainty suitability; impact and disposition records.

7.7 Measurement methods, uncertainty and decision rules

SOURCE p. 18 | Normative when applicable

7.7(a) Test and inspection methods shall be validated or verified as appropriate for their intended use. The organization shall establish an uncertainty model and decision rule where measurement uncertainty can affect conformity. Personnel shall understand the distinction between specification limits, instrument resolution, uncertainty and process-control limits.

7.7(b) Automated inspection, machine vision and in-process probing shall be evaluated against representative defects, surfaces, geometries and environmental conditions. False acceptance and false rejection shall be considered. Revalidation shall follow material changes to optics, algorithms, fixtures, software or decision thresholds.

7.7(c) Annex AD shall govern conformity decisions relying on measurement uncertainty. The informative examples in Annex H shall not be used to select favorable acceptance criteria after results become known. The decision rule and treatment of an indeterminate result shall be fixed before evaluation.

Required evidence: Method-validation records; uncertainty budgets; decision rules; automated inspection challenge results.

7.8 Organizational knowledge and technical continuity

SOURCE p. 19 | Normative when applicable

7.8(a) The organization shall identify knowledge necessary for current and future obligations, including tacit process knowledge, field experience, design rationale and failure mechanisms. It shall preserve critical knowledge

when personnel retire, suppliers exit or technology changes.

7.8(b) Lessons learned shall be indexed so that relevant programs can retrieve and evaluate them. Reuse of a lesson or legacy design shall include an applicability check; similarities in name or appearance shall not establish equivalence of mission, materials or environment.

Required evidence: Knowledge map; succession and transfer records; lessons database; reuse applicability reviews.

7.9 Communication and controlled information exchange

SOURCE p. 19 | Normative when applicable

7.9(a) The organization shall define what information is communicated, by whom, to whom, when and through which controlled channels. Urgent information affecting released products shall have an escalation path and acknowledgement mechanism. Supplier and customer changes shall reach the functions that use the affected data.

7.9(b) Sensitive, proprietary, personal or controlled technical information shall be shared only through authorized arrangements. Meeting attendance or federation membership shall not itself grant access. Communication restrictions shall be reconciled with required hazard and conformity reporting through an approved process.

Required evidence: Communication matrix; notification and acknowledgement logs; approved information-sharing arrangements.

7.10 Document creation, approval and distribution

SOURCE p. 19 | Normative when applicable

7.10(a) Documented information shall have a unique identity, title, revision, owner, approval status and effective date as appropriate. Review shall verify technical accuracy, clarity, consistency and suitability before issue. Instructions shall distinguish mandatory steps, hold points, permitted alternatives and acceptance criteria.

7.10(b) Current information shall be available at the point of use. Obsolete versions shall be removed from unintended use or clearly restricted for historical purposes. Personal copies, local spreadsheets and cached digital files shall be controlled when they influence conformity decisions.

Required evidence: Document master list; approval workflow; distribution controls; point-of-use verification.

7.11 Record integrity, retention and long-life readability

SOURCE p. 19 | Normative when applicable

7.11(a) Records shall preserve the identity of the subject, performer, reviewer and applicable configuration, together with time, results, units and disposition. Changes to recorded evidence shall retain the original value, reason, author and approval where relevant. Electronic signatures and acceptance media shall be individual, protected and revocable.

7.11(b) Retention periods shall consider law, contract, product life, latent defects, liability, material traceability and long- duration missions. No universal short retention period is prescribed. Digital preservation shall address format obsolescence, cryptographic validity, migration verification, backup, recovery and readable access after supplier or platform failure.

7.11(c) The organization shall test retrieval of selected legacy and current records, including restoration from backup. Destruction shall be authorized, recorded and suspended when subject to a relevant investigation, claim or preservation obligation.

Required evidence: Retention schedule; signature controls; audit trails; migration and restore tests; authorized disposal records.

7.12 Technical software, spreadsheets and decision tools

SOURCE p. 19 | Normative when applicable

7.12(a) Software, scripts, spreadsheets and computational tools that influence design, inspection, acceptance or assurance decisions shall be identified and controlled. Validation shall be proportionate to the consequence of an undetected error and shall include known-answer tests, boundary conditions, unit consistency and independent review where required.

7.12(b) Inputs, algorithms, dependencies, versions and output interpretation shall be documented. Formula cells and approved parameters shall be protected where appropriate. An AI-generated calculation or report shall undergo competent review; fluent language or successful execution shall not constitute verification of technical

correctness.

Required evidence: Tool inventory; validation plan and known-answer tests; version records; review and revalidation triggers.

8.1 Integrated operational planning

SOURCE p. 20 | Normative when applicable

8.1(a) The organization shall translate requirements into an executable program or order plan covering responsibilities, resources, lifecycle stages, work packages, suppliers, verification, validation, acceptance and delivery. Planning shall address producibility, inspectability, reliability, maintainability, safety, software, obsolescence, preservation and end-of-life obligations as relevant.

8.1(b) Critical items, key characteristics and special requirements shall be identified early and connected to control plans. The plan shall identify required evidence and hold points before the affected work begins. Changes in schedule or resources shall trigger a review of the continuing adequacy of the plan.

8.1(c) The organization shall verify consistency among the contract, technical baseline, purchasing requirements, manufacturing or service instructions and acceptance plan. A discrepancy shall be resolved before the affected activity proceeds. Work shall not be released merely because each department has approved a different interpretation.

Required evidence: Program assurance plan; work packages; control plans; integrated schedule; baseline consistency review.

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.

8.1.2 Configuration management

SOURCE p. 20 | Normative when applicable

8.1.2(a) The organization shall establish configuration identification, baseline control, change control, status accounting and configuration verification across hardware, software, models, manufacturing data and service information. The configuration structure shall identify relevant interfaces and distinguish as-designed, as-planned, as-built, as-tested, as-delivered and as-maintained states.

8.1.2(b) Changes shall be assessed for effects on fit, form, function, safety, interchangeability, qualification, maintenance, cybersecurity, traceability and customer obligations. The affected population and implementation point shall be identifiable. Mixed configurations shall be prevented unless their compatibility is specifically justified.

8.1.2(c) Configuration audits shall reconcile physical and digital evidence against approved baselines. Unauthorized substitutions or unexplained version differences shall be treated as nonconformities. A digital twin or model of record shall not conceal a discrepancy in the physical item.

Required evidence: Configuration plan; item hierarchy; baselines; change board decisions; status accounting; configuration audits.

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.

8.1.4 Counterfeit and unapproved-item prevention

SOURCE p. 21 | Normative when applicable

8.1.4(a) The organization shall assess counterfeit and unapproved-item risk for materials, parts, electronic components, software licenses, calibration records and certificates. Procurement preference, source approval, authenticity checks and testing shall be proportionate to consequence and supply risk.

8.1.4(b) Source identity, authorized-channel evidence, original manufacturer information and chain of custody shall be verified where relevant. A certificate alone shall not be accepted without evaluation of its origin, scope, consistency and credibility. Brokers and obsolete components shall receive additional controls when risks justify them.

8.1.4(c) Suspect items shall be segregated and positively controlled to prevent use or re-entry into the supply chain. Investigation, notification, preservation of evidence and disposition shall follow applicable obligations. Returning suspect material to the supplier without controls shall not be the default disposition.

Required evidence: Authenticity-risk assessment; approved sources; incoming verification; suspect-item records and disposition.

8.1.5 Temporary and permanent work transfer

SOURCE p. 21 | Normative when applicable

8.1.5(a) The organization shall plan transfer of work between sites, suppliers, equipment, production lines or service locations. The transfer plan shall identify baseline data, process capability, competence, tooling, environmental conditions, technical support, traceability and delivery-continuity risks.

8.1.5(b) Transferred work shall undergo appropriate first article, process requalification or service-capability verification before unrestricted release. The receiving source shall demonstrate actual capability; the sending source's records alone shall not establish equivalence. Early production shall be monitored against defined exit criteria.

Required evidence: Transfer plan; receiving-site readiness; qualification evidence; initial-output monitoring and closure.

8.2 Requirements for products and services

SOURCE p. 21 | Normative when applicable

8.2(a) The organization shall control customer communication, requirement definition, commitment review and changes through the complete sequence in 8.2.1–8.2.4. The approved requirements shall remain traceable to the product, service, process, performer and acceptance decision they affect.

Required evidence: Requirement lifecycle; agreed baseline; review and change records.

8.2.1 Customer and user communication

SOURCE p. 21 | Normative when applicable

8.2.1(a) The organization shall establish channels for enquiries, proposals, orders, changes, technical questions, complaints, customer property and contingency communication. Information supplied to customers shall accurately state capabilities, limitations, dependencies and required user actions.

8.2.1(b) Safety, service-life and configuration information shall reach the intended operator or maintainer, not only the purchasing contact where this would be insufficient. Relevant feedback shall be reviewed and connected to engineering, supplier and process decisions.

Required evidence: Communication arrangements; technical clarifications; complaints; user-information distribution.

8.2.2 Requirement determination and completeness

SOURCE p. 21 | Normative when applicable

8.2.2(a) Before committing to an output, the organization shall identify customer requirements, applicable obligations and requirements necessary for the intended use when known. The assessment shall cover performance, interfaces, environment, reliability, safety, cybersecurity, maintenance, delivery, documentation and retirement.

8.2.2(b) Special requirements and assumptions shall be visible. Claims in quotations, marketing materials or demonstrations that become commitments shall be included in the review. Requirements shall be unambiguous and verifiable, with measurable acceptance criteria or an approved qualitative evaluation method.

Required evidence: Requirements register; assumptions; applicable obligations; acceptance definitions; identified special requirements.

8.2.3 Contract and commitment review

SOURCE p. 21 | Normative when applicable

8.2.3(a) The organization shall review its ability to fulfill requirements before accepting a contract or order, including repeat orders when relevant conditions have changed. The review shall involve affected technical, quality, production, supply, service and commercial functions.

8.2.3(b) Differences from prior proposals or agreements shall be resolved. Missing written requirements shall be confirmed through an appropriate controlled record. Where requirements cannot be fully met, the organization shall obtain an authorized revised agreement before commitment; it shall not rely on later concessions.

8.2.3(c) Review shall include liability boundaries, data rights, access restrictions, support duration, source dependencies and customer approval points. Unresolved safety or legal obligations shall prevent acceptance of the affected commitment.

Required evidence: Multifunctional contract review; feasibility evidence; resolutions; approved deviations from the proposed offer.

8.2.4 Changes to requirements

SOURCE p. 22 | Normative when applicable

8.2.4(a) Changes shall be uniquely identified, reviewed, approved and communicated to all affected functions and external providers. The organization shall evaluate impacts on completed work, purchased material, qualification evidence, delivered products, software compatibility and maintenance information.

8.2.4(b) The change implementation point shall be controlled. Obsolete requirements shall be removed from unintended use, and affected verification shall be repeated where necessary. The organization shall confirm that downstream recipients have incorporated changes requiring their action.

Required evidence: Requirement-change record; impact analysis; baseline update; implementation and acknowledgement evidence.

8.3 Design and development

SOURCE p. 22 | Normative when applicable

8.3(a) The organization shall apply 8.3.1–8.3.6 to its actual product, service and process design responsibilities, including outsourced design for which it remains responsible. Supplied design shall be controlled and deficiencies escalated even where the organization does not own the product design.

Required evidence: Design scope and responsibility; controlled inputs; review, verification, validation and changes.

8.3.1 Design and development governance

SOURCE p. 22 | Normative when applicable

8.3.1(a) The organization shall establish a design and development process appropriate to the complexity, novelty and consequence of the output. It shall define technical authority, independent review, design responsibility and interfaces with customer or externally provided design.

8.3.1(b) Design assurance shall include hardware, software, interfaces, manufacturing methods, operational procedures and maintenance assumptions. Build-to-print work shall still assess the adequacy and controlled use of supplied data and shall escalate defects or ambiguities to the design authority.

Required evidence: Design process; responsibility allocation; design-data acceptance; escalation of ambiguities.

8.3.2 Design planning and lifecycle controls

SOURCE p. 22 | Normative when applicable

8.3.2(a) The design plan shall define stages, work breakdown, resources, reviews, verification, validation, configuration controls and transition criteria. Planning shall address ability to manufacture, inspect, integrate, test, operate, maintain, repair and retire the design.

8.3.2(b) Interfaces among disciplines and organizations shall be explicitly managed. Customer and user involvement shall be planned where necessary to validate intended use. Independence and specialist competence shall be matched to criticality and uncertainty.

Required evidence: Design plan; interface agreements; review schedule; V&V strategy; required independence.

8.3.3 Design inputs and derived requirements

SOURCE p. 22 | Normative when applicable

8.3.3(a) Design inputs shall identify functions, performance, constraints, operating environments, applicable obligations, lessons learned, failure consequences, materials, lifecycle limits and obsolescence risks. The organization shall review inputs for completeness, consistency and testability before baselining.

8.3.3(b) Derived requirements shall have a documented technical rationale and a traceable parent need or analysis. Safety-related derived requirements shall be reviewed by the appropriate authority. Conflicts shall be resolved rather than propagated into competing design assumptions.

Required evidence: Approved input baseline; derivation rationale; assumption register; conflict resolutions.

8.3.4 Design review, verification and validation

SOURCE p. 22 | Normative when applicable

8.3.4(a) Reviews shall evaluate whether the design can fulfill requirements and whether evidence and unresolved issues justify progression. Verification shall demonstrate that outputs satisfy specified inputs; validation shall demonstrate suitability for intended use in a representative context. These activities shall not be treated as interchangeable.

8.3.4(b) Test plans shall identify the test item and configuration, objectives, methods, environment, equipment, uncertainty, data to retain, acceptance criteria and anomaly handling. Test readiness shall be approved before execution. Deviations from the plan shall be recorded and evaluated for their effect on validity.

8.3.4(c) Analysis and simulation used as evidence shall have a justified model, validated range, input provenance, sensitivity analysis and uncertainty treatment. Completion of design shall require evidence covering identified operating conditions and interfaces; untested or unanalyzed conditions shall be explicitly bounded or resolved.

Required evidence: Review records; requirements-to-evidence matrix; approved test plans; raw data; model credibility; anomaly dispositions.

8.3.5 Design outputs and release

SOURCE p. 22 | Normative when applicable

8.3.5(a) Design outputs shall define the product or service sufficiently for procurement, manufacture, integration, verification, use and support. They shall identify characteristics, interfaces, materials, software versions, critical items, key characteristics, acceptance criteria and necessary handling or maintenance information.

8.3.5(b) Outputs shall be approved by authorized technical personnel before release. Where a model is authoritative, its role, exchange format, revision and interpretation rules shall be explicit. Manufacturing and inspection shall use consistent definitions of geometry, units, coordinate systems and tolerances.

Required evidence: Released design package; critical-characteristic list; approval; downstream usability review.

8.3.6 Design changes and continued validity

SOURCE p. 23 | Normative when applicable

8.3.6(a) Design changes shall be identified, reviewed, verified or validated as necessary and approved before implementation. Impact shall be assessed on interchangeability, interfaces, hazards, software, process capability, qualification, service instructions and the affected delivered population.

8.3.6(b) The organization shall identify when customer or competent-authority approval is required. A change that appears physically small shall not be presumed low risk. Changes to materials, manufacturing routes, model

training data or timing behavior shall receive a consequence-based assessment.

Required evidence: Change request; impact analysis; requalification decision; approvals; affected-item and implementation records.

8.4 Externally provided products, processes and services

SOURCE p. 23 | Normative when applicable

8.4(a) The organization shall apply 8.4.1–8.4.3 to selection, approval, verification and communication for external provision. Clause 27 and Annex AF additionally control actual performers, further tiers and retained responsibility. Customer nomination of a source shall not remove these obligations.

Required evidence: External-provider scope; approval, verification and flow-down evidence.

8.4.1 External-provider selection and approval

SOURCE p. 23 | Normative when applicable

8.4.1(a) The organization shall evaluate, select and approve external providers according to their ability to fulfill the assigned requirements. Controls shall consider technical capability, criticality, past performance, authenticity risk, capacity, financial continuity where relevant and sub-tier dependencies.

8.4.1(b) An approved-provider register shall identify status, scope, conditions, limitations and review dates. Customer nomination or an external certificate shall not remove the organization's responsibility to verify suitability for the actual supplied scope. Conditional approval shall have defined controls and closure criteria.

8.4.1(c) Provider performance shall be monitored using conformity, delivery, responsiveness, change discipline and corrective-action effectiveness. Approval shall be restricted, suspended or withdrawn when justified. Single-source and long-lead risks shall be addressed without relaxing required assurance.

Required evidence: Supplier evaluations; approval register; performance reviews; conditional approvals; sub-tier dependency map.

8.4.2 Verification of externally provided outputs

SOURCE p. 23 | Normative when applicable

8.4.2(a) The organization shall determine verification appropriate to the output and source risk, including inspection, testing, source surveillance, document review and periodic revalidation where necessary. It shall verify that supplied evidence corresponds to the correct item, lot, revision and test method.

8.4.2(b) External test reports shall be evaluated for consistency, adequacy and authenticity. For significant-risk raw material or critical items, a defined method shall validate report accuracy. Delegated supplier inspection shall have a controlled scope, qualified personnel, a delegation register and periodic oversight.

8.4.2(c) Limited release for further processing before verification is complete shall be specifically authorized, uniquely traceable and recoverable. It shall not permit irreversible consumption or final customer release of an output whose required conformity evidence remains unresolved.

Required evidence: Incoming verification plans; report checks; delegated inspection controls; restricted-release and recall records.

8.4.3 Purchasing information and flow-down

SOURCE p. 23 | Normative when applicable

8.4.3(a) Purchasing requirements shall communicate the exact technical baseline, acceptance criteria, critical characteristics, required processes, competence, approvals, verification and evidence. Requirements shall be reviewed for adequacy before transmission and flowed down to relevant sub-tier providers.

8.4.3(b) The organization shall specify change notification and approval requirements, nonconformity notification, disposition authority, counterfeit prevention, records retention, authorized access and required test specimens where relevant. Rights of access shall be implemented within applicable confidentiality and security restrictions, not omitted without resolution.

8.4.3(c) Providers shall be informed of their contribution to conformity, safety and ethical conduct. The organization shall verify that important requirements reached the point of performance rather than only the first-tier purchasing office.

8.4.3(d) Subcontracting and sub-tier flow-down shall also meet Clause 27 and Annex AF. An organization may use common contractual clauses, but it shall verify their applicability to the actual performer, including outsourced

engineering, cloud services, laboratories and personnel agencies.

Required evidence: Purchase-order clauses; technical-data issue record; sub-tier acknowledgement; flow-down verification.

8.5 Production and service execution

SOURCE p. 24 | Normative when applicable

8.5(a) The organization shall apply 8.5.1–8.5.6 to the controlled execution, identification, preservation, support and modification of its outputs. Special processes and first article verification shall be triggered by the actual work rather than omitted because a supplier or customer performs part of the activity.

Required evidence: Controlled work routes; actual execution; identity, preservation, support and change records.

8.5.1 Controlled production and service execution

SOURCE p. 24 | Normative when applicable

8.5.1(a) Production and service work shall use approved instructions, suitable equipment, competent personnel and defined environmental conditions. Instructions shall identify required characteristics, sequence, workmanship criteria, inspection points, process limits and authorized alternatives.

8.5.1(b) The organization shall maintain accountability for quantities and configuration through split lots, rework, scrap and partial completion. Critical items and key characteristics shall be controlled at points where their conformity can be established. A later inspection shall not be presumed to detect every earlier process failure.

8.5.1(c) Evidence shall show completion of required operations and acceptance activities. Utilities, consumables, tools and software affecting output shall be controlled. Error prevention, FOD prevention and identification of work awaiting verification shall be integrated into the process.

Required evidence: Controlled route or work package; process records; in-process verification; quantity reconciliation; FOD and utility controls.

8.5.1.1 Equipment, tooling and production software

SOURCE p. 24 | Normative when applicable

8.5.1.1(a) Equipment, tooling, fixtures and software used to create, control, inspect or measure outputs shall be verified or validated before release for use. The assessment shall include the actual application, configuration, interfaces, failure behavior and ability to maintain required characteristics.

8.5.1.1(b) Maintenance, storage, preservation and periodic condition checks shall be defined. Tool repairs, software updates, relocation and changes to compensation parameters shall trigger an impact-based revalidation decision. Access to editable machine programs shall be restricted and changes traceable.

Required evidence: Tool and software qualification; controlled programs; maintenance; storage checks; revalidation records.

8.5.1.2 Special-process validation and control

SOURCE p. 24 | Normative when applicable

8.5.1.2(a) Special processes shall have approved methods, qualified personnel, suitable equipment, validated parameter windows and defined acceptance and monitoring criteria. Qualification shall demonstrate that relevant output characteristics can be achieved reproducibly under the proposed operating conditions.

8.5.1.2(b) The organization shall define conditions for maintaining approval, monitoring essential variables, retaining records and requalification. Changes to material, geometry, equipment, software, consumables or location shall be evaluated. Final visual inspection alone shall not replace control of hidden or irreversible characteristics.

Required evidence: Special-process qualification dossier; approved parameter ranges; operator qualifications; run records; requalification decisions.

8.5.1.3 Production-process and first article verification

SOURCE p. 24 | Normative when applicable

8.5.1.3(a) The organization shall verify that the planned production route, documentation, equipment and tooling can produce an item meeting requirements. Verification shall use a representative item or other justified approach and account for every applicable characteristic, including material, process, software and interface requirements.

8.5.1.3(b) Repeat verification shall be considered after design, process, source, tooling or location changes, significant interruption or evidence that previous results no longer represent production. Partial verification shall identify and justify the unaffected portion. Approval of first article evidence shall not authorize later process drift.

Required evidence: First article record; characteristic accountability; material/process evidence; differences and repeat-verification rationale.

8.5.2 Identification, status and traceability

SOURCE p. 24 | Normative when applicable

8.5.2(a) Outputs shall be identified sufficiently to establish their configuration and acceptance status throughout the lifecycle. Where traceability is required, identity shall link material origin, lots, serials, processing, personnel, inspection, software versions and disposition as relevant to consequence and obligations.

8.5.2(b) Traceability shall survive splitting, combining, packaging changes, repairs and movement between systems. Acceptance stamps, passwords and electronic signatures shall be controlled. The organization shall periodically demonstrate that a suspect source or process event can be traced to the affected population and that an item can be traced back to its evidence.

Required evidence: Identity scheme; genealogy records; status controls; signature register; forward and reverse trace exercises.

8.5.3 Customer and external-provider property

SOURCE p. 25 | Normative when applicable

8.5.3(a) Property under the organization's control shall be identified, protected and used only as authorized. This includes physical items, tooling, intellectual property, technical data, software, personal information and access credentials.

8.5.3(b) Loss, damage, unsuitable condition or unauthorized use shall be reported to the owner through the agreed channel and recorded. The organization shall preserve evidence and assess product or service impact rather than treating the issue solely as an administrative property loss.

Required evidence: Property register; receipt checks; access controls; condition and incident records.

8.5.4 Preservation, packaging and transport

SOURCE p. 25 | Normative when applicable

8.5.4(a) The organization shall preserve conformity during handling, storage, packaging and transport. Controls shall address cleanliness, FOD, humidity, temperature, corrosion, ESD, shock, shelf life, material compatibility, hazardous conditions and stock rotation as applicable.

8.5.4(b) Packaging methods shall be qualified for the actual route and exposure where risk warrants. Excursions or damaged packaging shall trigger a product assessment. Expired, life-limited or environmentally exposed material shall not be returned to normal stock without an authorized disposition based on technical evidence.

Required evidence: Preservation specifications; packaging qualification; environmental history; shelf-life controls; excursion dispositions.

8.5.5 Post-delivery support and field feedback

SOURCE p. 25 | Normative when applicable

8.5.5(a) The organization shall define support responsibilities for installation, operation, training, maintenance, repair, warranty, spare parts, software updates and obsolescence within the agreed lifecycle. Technical information shall be controlled and updated when experience changes safe or effective use.

8.5.5(b) Field performance and failures shall be collected and analyzed with exposure and configuration context. A detected problem shall trigger investigation, communication and appropriate containment of the affected population. Off-site work shall meet the same applicable controls as equivalent work at the main facility.

Required evidence: Support plan; service information; field reliability data; notifications; off-site work controls.

8.5.6 Production and service changes

SOURCE p. 25 | Normative when applicable

8.5.6(a) Production and service changes shall be reviewed and authorized by competent persons with defined authority. The review shall consider changes to output characteristics, process capability, hidden features,

qualification, measurement, configuration and contractual approvals.

8.5.6(b) Emergency changes shall have temporary limits, additional checks and an expiry or conversion decision. The organization shall retain the baseline, change rationale, approval and verification of the changed output. A change implemented to restore delivery shall not bypass required design approval.

Required evidence: Process-change record; technical impact; approvals; temporary controls; changed-output verification.

8.6 Acceptance and authorized release

SOURCE p. 25 | Normative when applicable

8.6(a) Before release, the organization shall verify completion of the agreed acceptance plan, disposition of nonconformities, configuration consistency and availability of required documentation. Acceptance evidence shall identify actual results, applicable criteria and the authorized release person or controlled function.

8.6(b) Open issues shall be evaluated against explicit release-blocking criteria. A concession may address only a specifically authorized and lawful departure; it shall not waive a mandatory safety approval or conceal missing verification. Products awaiting required evidence shall remain controlled.

8.6(c) Where qualification evidence is required, it shall demonstrate the correct configuration and intended conditions. Delivery documentation shall state approved deviations, restrictions, service-life status and required user actions. Electronic release shall preserve individual accountability and tamper evidence.

8.6(d) The release authority shall identify whether it is releasing a product, a service event, a process for use or a person for a task. Release is not equivalent to third-party certification. Conformity attestation shall additionally follow Clause 22 and Annexes AA and AD; a lifecycle conditional progression decision shall not be presented as a conditional certificate.

Required evidence: Release checklist; acceptance results; closed or authorized issues; delivery dossier; release authorization.

8.7 Nonconforming outputs and escape control

SOURCE p. 25 | Normative when applicable

8.7(a) The organization shall identify and control nonconforming or suspect outputs to prevent unintended use or delivery. The response shall address severity, exposure, affected populations and consequences, including outputs already delivered or incorporated into higher assemblies.

8.7(b) Disposition authority shall be defined. Repair or use-as-is decisions affecting design requirements shall obtain design-authority approval and customer approval where the contract requires it. Reworked or repaired outputs shall undergo appropriate verification. Scrap shall be positively controlled until re-entry into the supply chain is prevented.

8.7(c) The organization shall notify relevant customers and other required recipients promptly within applicable deadlines, preserve evidence and initiate corrective action appropriate to the issue. The record shall describe the nonconformity, containment, affected population, disposition, concessions, approvals and verified outcome.

Required evidence: NCR; material review decisions; population trace; notifications; repair/rework verification; scrap control.

9.1 Monitoring strategy and data credibility

SOURCE p. 26 | Normative when applicable

9.1(a) The organization shall define what will be monitored, why it matters, how it is measured, when it is evaluated and who acts on the result. Measures shall connect process performance to product conformity, delivery, reliability, safety, customer experience and evidence integrity.

9.1(b) Data shall retain configuration, exposure, time period and denominator information needed for interpretation. Automated dashboards shall be reconciled to source records. Missing, delayed or selectively excluded data shall be visible. Leading indicators shall be evaluated against outcomes to confirm their usefulness.

Required evidence: Monitoring plan; metric dictionary; source reconciliations; data-quality checks; action records.

9.2 Customer satisfaction and external feedback

SOURCE p. 26 | Normative when applicable

9.2(a) The organization shall monitor customer and relevant user perceptions through suitable methods, including complaints, delivery experience, acceptance issues, service performance and corrective-action requests. Absence of complaints shall not be the sole evidence of satisfaction.

9.2(b) Trends shall be analyzed by meaningful product, site, supplier or configuration groups. Improvement plans shall address identified weaknesses and assess whether the customer or user experience actually improved. Contractual acceptance and user satisfaction shall be distinguished.

Required evidence: Feedback records; segment analysis; improvement plans; effectiveness evaluations.

9.3 Internal audit program

SOURCE p. 26 | Normative when applicable

9.3(a) The organization shall maintain an audit program covering the full applicable system, sites, shifts, remote activities and relevant external interfaces. Frequency and depth shall reflect criticality, changes, performance, prior findings and the maturity of controls. The program shall include process implementation and evidence integrity, not only procedure presence.

9.3(b) Auditors shall be competent and sufficiently independent of the work assessed. Audit criteria and sampling rationale shall be defined. A sampled audit shall not be described as verification of every item. Critical controls and unresolved high-consequence issues shall receive explicit attention.

9.3(c) Findings shall identify the requirement, objective evidence and the nature of the gap. The organization shall correct and address causes, verify effectiveness and escalate overdue or ineffective action. Remote auditing shall be used only where evidence reliability and access are adequate.

9.3(d) The complete applicable internal audit program shall be completed at intervals not exceeding 12 months. C2 and C3 critical-control implementation shall additionally be examined at intervals not exceeding six months, using targeted audits where suitable. These are organizational internal-audit duties, separate from third-party surveillance under Annex AG.

Required evidence: Risk-based audit program; competence and independence; plans; evidence trails; findings; closure verification.

9.4 Management review inputs

SOURCE p. 26 | Normative when applicable

9.4(a) Top management shall review the system at planned intervals and when major changes or incidents require it. Inputs shall include previous actions, context and obligation changes, objectives, process outcomes, product conformity, delivery, customer feedback, supplier performance, audits, nonconformities, risks, opportunities and resource adequacy.

9.4(b) Review shall also consider culture, reporting behavior, emerging technology, cybersecurity, resilience, climate-related relevance, field reliability and lifecycle support. The review shall distinguish recurring patterns from isolated events and examine whether assurance independence is functioning under commercial pressure.

9.4(c) The interval between complete management reviews shall not exceed 12 months. An immediate serious concern shall be escalated when detected rather than deferred until the next scheduled review. More frequent focused reviews shall be used where criticality, rapid change or adverse performance warrants them.

Required evidence: Review agenda and input pack; trend analyses; independent assurance concerns; status of prior actions.

9.5 Management review decisions and follow-through

SOURCE p. 27 | Normative when applicable

9.5(a) Review outputs shall include decisions on priorities, resources, risk treatment, opportunities, process changes, capability gaps and improvement. Each action shall have an accountable owner, due date, expected result and verification method.

9.5(b) Top management shall follow up actions and unresolved risks. Repeated deferral of an issue shall trigger escalation and an explicit decision about continued operations. Minutes stating “reviewed and accepted” without a basis or action on adverse evidence shall not establish effectiveness.

Required evidence: Recorded decisions; action ownership; resource commitments; follow-up and effectiveness evidence.

9.6 Independent assurance and systemic challenge

SOURCE p. 27 | Normative when applicable

9.6(a) For high-consequence programs, the organization shall obtain independent challenge of the assurance strategy and major release decisions at the level specified in Annex B. The review shall examine assumptions, common-cause dependencies, missing evidence and the credibility of residual-risk acceptance.

9.6(b) The independence arrangement may use qualified internal or external personnel. It shall not be weakened by allowing the designer to approve their own contested evidence without the required review. Dissenting technical opinions shall be recorded and resolved through the defined authority structure.

Required evidence: Independent-review plan; challenge records; dissent resolution; release recommendations.

10.1 Response to nonconformity and containment

SOURCE p. 27 | Normative when applicable

10.1(a) When a nonconformity or credible concern is detected, the organization shall protect affected users and outputs, determine the immediate extent and assign a response owner. Initial containment shall cover related stock, work in progress, delivered configurations and digital artifacts as relevant.

10.1(b) Containment effectiveness shall be checked. A correction to the first detected item shall not close the investigation of the wider population. Evidence shall be preserved so that cause analysis remains possible, including raw data, software versions, material samples and process conditions.

Required evidence: Response record; containment scope; trace results; effectiveness checks; preserved evidence.

10.2 Cause analysis and corrective action

SOURCE p. 27 | Normative when applicable

10.2(a) The organization shall determine causes using evidence appropriate to the problem. Analysis shall consider requirement quality, design assumptions, process conditions, human factors, tooling, suppliers, management pressures, software and detection failures. Unsupported labels such as “carelessness” shall not be accepted as completed analysis.

10.2(b) Corrective action shall address both occurrence and escape causes where relevant. Actions shall be assigned, implemented and verified against a pre-defined effectiveness measure. The organization shall assess whether similar conditions exist in other products, sites, suppliers or processes and extend action where necessary.

10.2(c) Where an external provider is responsible, corrective requirements shall be flowed down and their effectiveness verified. Repeated or late ineffective action shall be escalated. Risk assessments, technical data, control plans and training shall be updated when the findings change their basis.

Required evidence: Evidence-based cause analysis; occurrence and escape controls; action plan; systemic extent; effectiveness results.

10.3 Continual improvement and preventive learning

SOURCE p. 27 | Normative when applicable

10.3(a) The organization shall select improvement opportunities using performance evidence, user experience, lessons learned, technology developments and strategic needs. Improvement shall address system effectiveness, not only cost or administrative simplification.

10.3(b) Changes introduced as improvements shall undergo the same appropriate assurance as other changes. Benefits shall be verified against the baseline, while unintended adverse effects shall be monitored. Knowledge from unsuccessful experiments shall be retained without representing an unproven benefit as achieved.

Required evidence: Improvement portfolio; baseline and outcome evaluation; change assurance; retained learning.

10.4 Learning across the lifecycle and network

SOURCE p. 27 | Normative when applicable

10.4(a) The organization shall make relevant lessons available to affected functions and suppliers through controlled channels. Significant lessons shall be considered at new-program initiation, design review, supplier approval and process change.

10.4(b) Lessons shall identify conditions of applicability and evidence, rather than only a slogan or narrative. The organization shall periodically test whether the lessons are being used and whether repeated events indicate ineffective knowledge transfer.

Required evidence: Indexed lessons; applicability reviews; supplier communication; recurrence and uptake assessment.

22.1 Conformity evidence dossier

SOURCE p. 40 | Normative when applicable

22.1(a) The applicant shall maintain an indexed dossier linking the defined object, approved scope, applicability decisions, application profile, technical modules, implementation evidence, internal evaluations and corrective actions. Evidence shall permit a competent reviewer to follow a requirement to the relevant activity, result and decision.

22.1(b) The dossier shall identify missing, inaccessible, obsolete or unrepresentative evidence. Procedures and questionnaires alone shall not establish implementation. Confidentiality shall be protected through authorized access; a secrecy claim shall not convert unsupported assertions into verified evidence.

Required evidence: Object-specific dossier; applicable requirement set; evidence index; configuration and population coverage; limitations.

22.2 Evaluation, review and decision separation

SOURCE p. 40 | Normative when applicable

22.2(a) The scheme operator shall appoint evaluators competent for the object, sector, criticality and methods involved. Technical expertise shall be added where an auditor's competence does not cover the evaluated activity. Assignment, competence and conflicts shall be checked before work begins.

22.2(b) For third-party attestation, the decision maker shall not have performed that evaluation or supplied the relevant consultancy. A competent independent person may combine evidence review and the decision, but shall not certify their own evaluation. Internal release and internal audit independence shall follow their applicable role and criticality rules, not an inappropriate assumption that every employee is independent.

Required evidence: Assignment matrix; competence and conflict checks; evaluation record; independent review and decision identities.

22.3 Criteria, sampling and findings

SOURCE p. 41 | Normative when applicable

22.3(a) The evaluation plan shall identify criteria, locations, periods, methods and sampling limitations. Audits shall examine process implementation and actual outputs; product, service, process and personnel evaluations shall additionally apply the relevant object criteria.

22.3(b) Each nonconformity shall identify a requirement, objective evidence and the gap. Classification and decision consequences shall follow Annex AD. Audit-time planning shall follow Annex AC; personnel examinations shall follow Annex AE. A sampled review shall not be claimed to verify every item or person.

Required evidence: Evaluation plan; sample rationale; objective evidence; requirement-linked findings; assessed limitations.

22.4 Decision conditions and release blockers

SOURCE p. 41 | Normative when applicable

22.4(a) Initial grant, renewal and scope extension shall require closure of all nonconformities in the proposed scope and satisfactory independent review. Missing critical evidence, unresolved major breakdowns, falsified evidence and unfulfilled mandatory criteria shall prevent a positive decision. A percentage score shall not offset such a blocker.

22.4(b) For an existing attestation, a localized minor finding may be handled through a bounded continuation decision only under Annexes AD and AG. That decision is not a new certificate with open findings. Technical product holds, personnel restrictions and legal reporting shall be applied independently of certificate administration.

Required evidence: Requirement-by-requirement conclusion; finding closure; blocker check; reasoned and dated decision.

22.5 Statements, certificates and mark use

SOURCE p. 41 | Normative when applicable

22.5(a) A conformity statement shall identify AF 9100:2026, First Edition, the route, evaluated object, applicable profile, scope, sites or configurations, issuer, decision date, status and limitations. Self-declaration, customer assessment and independent third-party attestation shall be clearly distinguished.

22.5(b) AF marks shall require written permission for the exact use. An organizational mark shall not be placed so that it implies unevaluated product approval. No claim of official recognition, legal equivalence, accreditation or global acceptance shall be made without an actual supporting authorization or arrangement.

Required evidence: Approved claim text; certificate data; mark permission; actual recognition scope where claimed.

22.6 Continuing validity and changes

SOURCE p. 41 | Normative when applicable

22.6(a) The attestation holder shall report changes that can affect conformity, including new sites, ownership or legal identity, product configuration, service architecture, essential process variables, competence, critical subcontractors and serious incidents. Changes shall be evaluated before the affected extended claim is used.

22.6(b) Surveillance, renewal, suspension, restoration, expiry and withdrawal shall follow Annex AG. Status records shall preserve dates and scope history. Reissue of a document, payment of a fee or filing an appeal shall not extend an expired or suspended authorization.

Required evidence: Change notifications; surveillance findings; renewal evidence; current and historical status records.

22.7 Complaints, appeals and corrective communication

SOURCE p. 41 | Normative when applicable

22.7(a) A transparent complaint and appeal process shall be available under Annex AI. Persons deciding an appeal shall be independent of the contested decision and its evaluation. Good-faith complaints shall not result in retaliation or reduced access to fair assessment.

22.7(b) A substantiated concern shall trigger correction of affected outputs, evidence or public claims. Confidential information shall remain protected, while necessary safety communication shall not be suppressed to avoid reputational harm.

Required evidence: Case records; independent reviewer appointment; reasoned outcomes; affected-population action and communication.

22.8 Scheme operation and competence attestations

SOURCE p. 41 | Normative when applicable

22.8(a) Bodies operating AF assessment routes shall fulfill Clause 28 and Annex AH, in addition to the route-specific rules. A laboratory, inspection body or certification body seeking a CAB competence attestation shall undergo evaluation of its actual technical activities, not merely an organizational audit.

22.8(b) Accreditation and AF authorization shall not be self-awarded by a body using this publication. They require the separately identified authorized decision described in Annex AH. Organizations without that authorization may use the standard internally or contractually but shall describe the basis accurately.

Required evidence: Operator authority; body competence evaluation; written scope; independent decision; accurate accreditation and authorization claims.

A.1 Required applicability process

SOURCE p. 50 | Normative when applicable

A.1(a) The organization shall identify each product or service family, site and lifecycle role; assess the activities and effects below; select all triggered clauses and normative annexes; and record exclusions with evidence. A module applies when an activity is performed directly or when the organization retains responsibility for an externally performed activity.

A.1(b) The matrix shall be approved by the management representative and relevant technical authorities. It shall be reviewed at least within management review and whenever scope, configuration, technology, suppliers or obligations materially change. Applicable legal and contractual obligations remain binding; AF tailoring shall not remove them.

A.1(c) For a PER route, the individual scope record shall select Clause 26 and Annex AE, plus Annex AB for an assessor credential and the relevant technical competences from the job profile. The individual is not required to operate the organizational core. The scheme operator is assessed separately for its organizational and provider duties.

Required evidence: Versioned activity matrix; product/site coverage; reasons for exclusions; technical approval; review triggers.

A.2 Minimum scope-record fields

SOURCE p. 51 | Normative when applicable

A.2(a) Each matrix row shall contain entity, site, product or service, customer or mission, lifecycle responsibility, triggered clause, applicability decision, reason, evidence reference, accountable owner and approval date. Remote

functions and critical suppliers shall be linked to the relevant row.

A.2(b) An exclusion shall not be accepted when the activity is merely subcontracted. For a design exclusion, the record shall identify the actual design authority and demonstrate controls over supplied design data, change requests and escalation of errors.

Required evidence: Completed matrix with each mandatory field and approved interface responsibilities.

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.

D.1 Requirement-record integrity

SOURCE p. 55 | Normative when applicable

D.1(a) Every controlled product or service requirement shall have an identifier, statement, source, owner, revision, rationale, applicability, verification method and acceptance criteria. Derived and safety-related requirements shall include their parent link and approving authority.

D.1(b) The organization shall maintain traceability through allocation, implementation, verification, anomaly resolution and release. Traceability completeness shall be evaluated for meaning and validity, not only the presence of hyperlinks. Broken or circular links shall be investigated.

D.2 Identifiers, versioning and time

SOURCE p. 55 | Normative when applicable

D.2(a) Identifiers shall remain unique within the defined repository and resolvable after migration. Revision and status shall be distinct; an approved obsolete version shall not appear current. Time records shall identify the relevant time basis and sequence sufficient to reconstruct events.

D.2(b) Units, coordinate systems, reference frames and data encodings shall be explicit where misinterpretation could affect conformity. Imported supplier data shall be checked for mapping errors, truncated precision and semantic differences. Automated exchange shall retain validation results.

D.3 Evidence provenance and tamper indication

SOURCE p. 55 | Normative when applicable

D.3(a) An evidence record shall identify the source system or person, acquisition method, processing, transformations and approvals. Cryptographic hashes or signatures may support integrity but shall not be treated as proof that the original observation was correct.

D.3(b) Corrections shall preserve the prior evidence and explain why it changed. Access and modification logs shall be protected in accordance with consequence and obligations. Migration shall verify relationships as well as files; a readable PDF without its underlying configuration links may be insufficient. The filled chain demonstrates structure only. It deliberately does not supply a universal stopping-time value, load or speed; those values require a valid system-specific safety basis.

V.1 Assessment planning and evidence sampling

SOURCE p. 87 | Normative when applicable

V.1(a) The assessor shall establish the object, scope, applicable requirements, sites, functions, products, periods and authorized evidence access. Sampling shall consider criticality, changes, poor performance, process diversity and potential systemic failure. Sample limitations shall be recorded and shall constrain the resulting claim.

V.1(b) Assessment shall combine documented arrangements, interviews, observed work and retained results. The reviewer shall test whether records agree across the lifecycle. A completed questionnaire, certificate or policy statement alone shall not demonstrate implementation.

V.1(c) Organizational evaluation time and coverage shall follow Annex AC. The selected object route shall additionally follow Annex AA, and the actual decision shall follow Annex AD. Confidential evidence shall remain accessible to suitably authorized reviewers; unresolved absence of necessary evidence blocks the dependent conclusion.

Required evidence: Scope and route; approved plan; sample rationale; combined evidence; actual limits and access.

V.2 Findings and requirement-level conclusions

SOURCE p. 87 | Normative when applicable

V.2(a) Each finding shall identify the exact requirement, objective evidence, affected scope and gap. Classification shall follow Annex AD. A technical release hold shall be applied where needed irrespective of an administrative grade. Opportunities for improvement shall not conceal nonconformities.

V.2(b) The conclusion shall state conforming, nonconforming, not applicable with approved rationale or not yet demonstrated for each relevant requirement. Aggregate scores shall not offset missing mandatory evidence. The final decision shall identify unresolved issues and the precise scope that the evidence can support.

Required evidence: Requirement-level findings; classification; technical holds; evaluated applicability; clear conclusion. For Annex N, only N.1–N.3 and their required record tables are normative; the numerical worked examples are informative. For Annex AJ, required record fields and controls are normative, while filled sample values are informative.

V.3 Integrated audit trail and sample expansion

SOURCE p. 95 | Normative when applicable

V.3(a) An assessor may select a delivered serial, service event or task authorization and trace it backward through release, requirements, configuration, process, competent performer, measurement and external source. The assessor shall then trace relevant changes, field issues or complaints forward through population identification and corrective action.

V.3(b) When records disagree, the assessor shall expand the trail according to the potential extent and consequence. One successfully traced item does not verify the whole population. An apparent completeness score shall not conceal absent actual measurements, unverified qualifications or unresolved configuration changes.

Required evidence: Complete backward/forward trail; consistency checks; expanded samples; evaluated population limitations.

W.1 Required corrective-action sequence

SOURCE p. 96 | Normative when applicable

W.1(a) The organization shall record the detected issue, protect affected outputs, determine the extent, preserve evidence, establish causes, implement actions and verify effectiveness. The response shall address both the occurrence of the defect and the failure of controls to prevent escape.

W.1(b) Closure shall not be based solely on training attendance, a revised procedure or the action owner's statement. The organization shall define evidence showing that causes were addressed and controls remain effective under representative conditions.

W.2 Completed synthetic case — measurement offset

SOURCE p. 96 | Definition, explanation or informative example; no new universal limit

W.2(a) Case NCR-026 concerns a dimensional characteristic measured using an automated fixture. A periodic independent check identifies a 0.012 mm offset after fixture maintenance. The applicable procedure required a reference check after maintenance, but the work-order system did not trigger it. The issue is not closed by recalibrating the fixture.

W.2(b) Containment holds 240 items measured since maintenance; 90 remain on site and 150 are traceable to two customers. The responsible team preserves raw measurements, fixture settings and maintenance records and notifies recipients according to the assessed consequence and applicable obligations. No assumption is made that all 240 items are defective.

W.3 Recurrence and ineffective action

SOURCE p. 97 | Normative when applicable

W.3(a) Recurrence or failure of an effectiveness check shall reopen the analysis and trigger review of related assumptions, resource decisions and management controls. A new due date alone shall not be treated as corrective action.

W.3(b) The organization shall identify whether earlier closures relied on inadequate evidence, narrow population scope or untested human-factor assumptions. Lessons shall be incorporated into new-program and change reviews.

AA.1 Object selection and the scope tuple

SOURCE p. 103 | Normative when applicable

AA.1(a) Before accepting an application, the scheme operator shall select one or more routes from Table AA-1. Each route shall have a separate evaluation boundary and conclusion. A combined assessment may share relevant evidence, but shall not merge different conformity objects into an ambiguous certificate.

AA.1(b) The scope tuple shall identify object type; applicant and responsible legal entity; product, service, process, person or provider identity; sites and remote functions; configuration or role version; lifecycle responsibilities; criticality; technical modules; application profile; evaluated period; and exclusions or restrictions. Empty fields shall be justified rather than omitted silently.

Required evidence: Application review; selected routes; completed scope tuple; responsibility and applicability matrix.

AA.2 Application profile requirements

SOURCE p. 103 | Normative when applicable

AA.2(a) The profile shall define the evaluated object, version, intended use, operating or task domain, characteristics or competences, acceptance criteria, methods, samples, uncertainty or scoring rules, required evidence, critical failures, surveillance and change triggers. The technical profile owner shall be identified and competent to approve those criteria.

AA.2(b) A PRD profile shall state relevant performance, environmental, safety, interface and life criteria. A SVC profile shall state delivery outcomes and observation windows. A PRC profile shall state essential variables and qualified ranges. A PER profile shall state tasks, prerequisites, knowledge and practical demonstration. SUB and CAB profiles shall state the actual work or assessment capability.

AA.2(c) The profile shall be approved before evaluation. It may add requirements but shall not waive AF minima or mandatory obligations. Where methods or limits are missing, the application shall be held until competent technical definition is available; broad references to "good quality" or "all aerospace uses" are not adequate

criteria.

Required evidence: Approved profile with technical criteria; method and decision matrix; critical-failure list; profile change history.

AA.3 Evaluation sequence and admission controls

SOURCE p. 104 | Normative when applicable

AA.3(a) The operator shall review eligibility, scope, competence resources, impartiality, evidence access and evaluation feasibility before contracting. It shall agree the profile and explain fees independently of outcome. An application shall not be accepted for a scope the operator cannot competently assess.

AA.3(b) The evaluation shall establish readiness, verify implementation or technical performance, record findings, verify correction and submit the complete evidence for independent review. ORG evaluation shall include readiness and implementation stages. Other routes shall use object-appropriate stages without imposing an organizational audit on an individual candidate.

AA.3(c) For an initial ORG assessment, the applicant shall have completed an internal audit covering the applicable scope and a management review, with sufficient implemented records to show operation. A new organization may be assessed when adequate actual evidence exists; artificial backdated records or a fixed unsubstantiated history shall not be requested or accepted.

Required evidence: Admission decision; contract; approved evaluation plan; readiness evidence; evaluation results and independent review.

AA.4 Evaluation evidence by route

SOURCE p. 104 | Normative when applicable

AA.4(a) For PRD, evaluation shall verify product identity, representative qualification and applicable unit or lot evidence. For an ongoing family claim it shall also verify that manufacturing and change controls maintain the evaluated properties. A one-time sample test shall not support indefinite production claims.

AA.4(b) For SVC and PRC, evaluation shall include actual delivery or witnessed execution under representative conditions. For PER, it shall include verified identity, prerequisites and the required knowledge and practical assessments. For SUB, it shall examine the actual performer and supplied scope, not merely a purchasing intermediary.

AA.4(c) For CAB, evaluation shall cover the technical methods and decisions the body intends to perform, including representative witnessed activities. A general quality audit without technical witnessing and competence evidence shall not be treated as a completed CAB route.

Required evidence: Route-specific results; representative work; witnessed evidence; limits of reused or sample evidence.

AA.5 Independent review, decision and permitted outcomes

SOURCE p. 104 | Normative when applicable

AA.5(a) The independent reviewer shall confirm scope completeness, criteria validity, evaluator competence, method suitability, adequate evidence, findings and closure. A reviewer shall return an incomplete dossier rather than infer missing results. Technical disagreements shall be recorded and resolved through competent authority.

AA.5(b) The authorized decision shall grant, refuse, maintain, restrict, suspend, restore, renew or withdraw a defined attestation. Initial grant, renewal and extension require closure of all nonconformities in the granted scope under Annex AD. A refusal shall identify the relevant unmet conditions without implying that unrelated scopes were evaluated.

AA.5(c) An applicant may correct deficiencies and reapply with actual evidence. The operator shall control repeat evaluations and configuration changes so that rejected results are not discarded. Payment, membership or seniority shall not determine the outcome.

Required evidence: Independent review checklist; reasoned decision; finding closure; precise scope and actual decision date.

AA.6 Attestation content and separate claims

SOURCE p. 104 | Normative when applicable

AA.6(a) An attestation shall contain a unique identifier, issuer, applicant or holder identity, full publication identifier, First Edition, route, application-profile ID and revision, evaluated scope and sites, configuration or role, decision and issue dates, applicable expiry or instance boundary, restrictions, status-verification method and

authorized signatory.

AA.6(b) Multiple routes may be presented in one document only where the separate route, criteria, evaluation, decision and status are clear for each object. Suspension of one route shall not be concealed by the continued validity of another. Product markings shall be controlled separately from organizational publicity.

AA.6(c) A supplier's own declaration shall be labeled as a self-declaration. A customer's assessment shall be labeled as such. Neither shall be represented as an independent AF-authorized attestation unless that independent process and authorization actually exist.

Required evidence: Issued statement; separate route conclusions; mark permission; status record; accurate self-declaration labeling.

AA.7 Scheme ownership, authorization and changes

SOURCE p. 105 | Normative when applicable

AA.7(a) AF shall control the published AF rule set and written permissions to operate its scheme or use its marks. The operator shall retain responsibility for its evaluations and decisions within the granted scope. The applicant shall retain responsibility for its products, services and representations.

AA.7(b) A scheme operator shall not expand its authorized sector, object or technical scope without the required competence evaluation and written approval. Scheme changes shall follow Annex Y; changes to individual attestations shall follow Annex AG. An AF designation does not establish governmental delegation or recognition in another scheme.

Required evidence: Scheme governance; actual written operator authorization; authorized scope; controlled changes.

AA.8 Illustrative combined-scope example

SOURCE p. 105 | Definition, explanation or informative example; no new universal limit

AA.8(a) Illustrative example: an organization manufactures ground-support carts, provides maintenance and employs inspectors. ORG evaluates its management and assurance system. PRD evaluates a stated cart configuration and technical profile. SVC evaluates the maintenance service. PER evaluates an inspector's defined competence. Employer task authorization permits that inspector to work on the specified cart family.

AA.8(b) A positive ORG decision cannot close missing cart braking evidence, failed service recovery tests or a failed practical inspector assessment. Each route retains its own evidence, decision, status and limitations. The example describes scheme logic, not an actual AF approval.

AB.1 Role definition and competence domains

SOURCE p. 106 | Normative when applicable

AB.1(a) The provider shall define competence separately for auditor, lead auditor, technical expert, application reviewer, technical reviewer, decision maker and appeal reviewer. Authorization shall state the routes, sectors, methods, criticality limits, languages and any supervision requirements. One role shall not automatically confer the others.

AB.1(b) Required competence shall include interpreting AF requirements and application profiles; process and lifecycle understanding; evidence integrity; sampling; measurement and statistical limitations; configuration and traceability; risk and criticality; human factors; ethics; interview and observation; reporting; finding classification; and recognition of work beyond personal competence.

AB.1(c) Domain-specific competence shall cover the hazards, materials, technologies, operational conditions and approval interfaces relevant to the assignment. For C2 or C3 work, the team shall include a verified technical specialist with relevant recent practice or demonstrated equivalent current competence. Merely adding a specialist's name to the plan shall not satisfy actual participation.

Required evidence: Role competence profiles; sector and method criteria; authorization limits; assigned technical coverage.

AB.2 Knowledge examination and practical evaluation

SOURCE p. 106 | Normative when applicable

AB.2(a) A third-party auditor shall achieve at least 80% in a controlled written examination covering AF interpretation, evidence, scope, findings and decisions, and at least 85% in the practical assessment. Every predefined essential safety, integrity and independence step shall be passed. A high total shall not compensate for falsified evidence, unsupported critical acceptance or failure to escalate an essential hold.

AB.2(b) The practical assessment shall include planning, interviews, observation, sampling, tracing actual or controlled simulated evidence, writing findings and presenting a reasoned conclusion. Competence evaluators shall record observed strengths, deficiencies and authorization limits. Assessment shall be independently reviewed before authorization.

AB.2(c) Assessment questions and case criteria shall be mapped to the competence profile, technically reviewed, secured and periodically evaluated for validity. Reassessment following failure shall use corrected competence and an equivalent controlled assessment, not memorized answers to an unchanged disclosed case.

Required evidence: Examination blueprint; secured questions; scores; essential-step results; practical observations; authorization decision.

AB.3 Experience equivalence and initial assessor development

SOURCE p. 107 | Normative when applicable

AB.3(a) An experience-equivalence route may recognize comparable prior professional audit or technical practice where identity, scope, dates, duration, role and performance are verified. It shall not waive the AF knowledge assessment, witnessed practical demonstration, impartiality or essential competence requirements.

AB.3(b) For the initial development of an AF assessor population, a panel of at least two independent competent professionals shall evaluate each candidate against this annex. Their own relevant technical and assessment competence shall be documented. Reciprocal self-approval, honorary appointments and automatic recognition based on membership shall not be accepted.

AB.3(c) The equivalence record shall identify each criterion satisfied by prior evidence, each remaining gap, the evaluated scope and the reason for the final decision. Unknown or unverifiable audit logs shall not be counted toward the required mentored experience.

Required evidence: Verified experience log; equivalence matrix; independent panel competence; witnessed demonstration; remaining restrictions.

AB.4 Assignment and technical coverage

SOURCE p. 107 | Normative when applicable

AB.4(a) Before each assignment, the provider shall verify role authorization, current competence, sector and criticality coverage, language, methods, physical or remote access and independence. The team shall be able to evaluate each relevant critical process and technical interface; no individual is presumed competent in all sectors covered by this standard.

AB.4(b) A technical expert shall work within a defined assignment and communicate evidence and limitations to the auditor and reviewer. The lead auditor shall integrate the result without overruling a specialist on a technical matter outside the lead auditor's competence. Unresolved disagreement shall be escalated and recorded.

AB.4(c) Classified or otherwise controlled work shall be assigned only to appropriately authorized personnel. Lack of permitted access or competence shall lead to resourcing changes, scope restriction or refusal, not acceptance on the strength of an unsupported management statement.

Required evidence: Assignment review; team coverage matrix; specialist work record; access and conflict checks; disagreement resolution.

AB.5 Impartiality and incompatible activities

SOURCE p. 107 | Normative when applicable

AB.5(a) For third-party evaluation, review and decision, personnel shall not be assigned to a client for which they provided relevant consultancy or held employment within the preceding 24 months. The provider shall also evaluate ownership, financial dependence, family or close relationships and other conflicts that may remain after that period.

AB.5(b) The 24-month rule is not an internal-audit ban on employees. Internal auditors shall instead be independent of the work they evaluate, with suitable reassignment or external support where separation is not feasible. A product release reviewer may be internal, subject to the technical independence required by Annex B.

AB.5(c) An evaluator shall not promise a favorable decision, design the corrective action they will independently certify, accept outcome-linked compensation or suppress evidence at the applicant's request. General explanation of a requirement is permitted; client-specific system design that undermines independence is not.

Required evidence: Conflict declarations; prior-work screening; compensation controls; reassignment decisions; internal independence arrangements.

AB.6 Continuing authorization and observed performance

SOURCE p. 107 | Normative when applicable

AB.6(a) All authorized assessment-role personnel shall complete at least 16 hours of relevant continuing professional development in each 12-month period. Independent auditors shall additionally perform at least four auditor-days across at least two assignments in that period. A lead auditor shall lead at least two complete assignments in each 24-month period.

AB.6(b) Reviewers and decision makers shall complete at least three substantive file reviews or decisions in each 12-month period. Technical experts shall demonstrate current relevant practice and review changes affecting their technical scope. Providers shall assess performance using witnessed work, report quality, decisions, complaints and recurrence of errors.

AB.6(c) An independent auditor shall undergo a witnessed performance review at least once every 24 months. More frequent observation shall be required for a new sector, C2/C3 expansion, significant adverse evidence or deficient performance. Training hours shall not substitute for the required observed competence.

Required evidence: Development and activity logs; witnessed reviews; report-quality checks; ongoing role authorizations.

AB.7 Inactivity, restriction and reactivation

SOURCE p. 107 | Normative when applicable

AB.7(a) When the applicable activity minimum is not met, independent authorization for that role shall be suspended until a competence review and supervised reactivation demonstrate current capability. After more than 12 months without relevant audit practice, an auditor shall complete updated AF learning and a satisfactory witnessed assignment before independent work resumes.

AB.7(b) A serious competence or integrity concern shall trigger immediate assessment of the authorization and earlier affected work. Reinstatement shall require evidence proportionate to the cause, including reassessment where necessary. The original authorization expiry shall not be extended merely by restoration.

AB.7(c) Changes to the standard, sector technology, methods or legal access shall trigger targeted updates. An assessor shall decline tasks outside their authorization and request appropriate technical support. Automated tools may support work but shall not replace the accountable human evaluator or decision maker.

Required evidence: Restriction and inactivity records; reactivation plan; witnessed results; prior-work assessment; restored scope.

AB.8 Competence dossier and approval record

SOURCE p. 108 | Normative when applicable

AB.8(a) The provider shall retain the role profile, verified experience, training, examination and practical results, mentored assignments, competence decisions, technical scope, witnessed performance, development, conflicts and status history. The record shall identify who evaluated, reviewed and authorized each role.

AB.8(b) Certificates or authorization letters shall disclose limitations and shall not imply that a person can audit every AF sector. Evidence of technical competence may be confidential, but the provider shall retain sufficient authorized access to substantiate assignments and respond to complaints.

Required evidence: Complete competence dossier; role and scope register; approval identity; current and historical restrictions.

AC.1 Planning inputs and effective personnel

SOURCE p. 109 | Normative when applicable

AC.1(a) The plan shall identify sites, shifts, functions, product and service families, technical modules, criticality, languages, external work, past performance, changes and access conditions. The provider shall review scope before determining time, rather than deriving scope from a fee quotation.

AC.1(b) Effective personnel N shall include employees and externally provided people whose work falls within the assessed organizational scope, including relevant temporary and seasonal staff. Part-time work may be converted using documented full-time-equivalent hours; each unique critical role shall nevertheless count as at least one person. Peak relevant staffing and actual shift diversity shall be considered. After the FTE calculation, N shall be

rounded upward to the next whole person, with a minimum of one, before selecting the Table AC-1 band.

AC.1(c) Personnel shall not be excluded solely because they work remotely, are employed by an agency or support production indirectly. The provider shall document any consolidation of equivalent roles and shall avoid counting the same shared-service staff more than once.

Required evidence: Scope and staffing basis; FTE calculation; sites and shifts; critical-role coverage; planning rationale.

AC.2 Criticality, complexity and site modifiers

SOURCE p. 109 | Normative when applicable

AC.2(a) The multiplier K shall use the highest relevant criticality in the assessed scope: C0 = 1.00; C1 = 1.15; C2 = 1.35; C3 = 1.60. Where genuinely separate technical scopes are evaluated independently, their separate time allocations shall be recorded; a critical function shall not be diluted by averaging personnel across lower- criticality work.

AC.2(b) The additive complexity factor f shall include 0.15 for special-process qualification in scope, 0.15 for assured software/AI or digitally controlled acceptance, and 0.15 for materially novel technology without representative operating history. These are distinct triggers; a trigger shall be counted once. Other complexity requiring more time shall be added through a documented plan adjustment.

AC.2(c) Let S_v be the number of physical sites to be visited, with a minimum value of one for calculation. Let H be the number of additional materially different operating shifts requiring separate observation beyond the primary shift. The site/shift addition is $0.5(S_v - 1) + 0.5H$ auditor-days. This addition does not remove the coverage floor in AC.3.

Required evidence: Criticality selection; triggered complexity factors; site and shift additions; additional-resource decisions.

Source calculation note: (AC-1) $T_{calc} = \text{ceil}(2 \times [B(N) \times K \times (1 + f) + 0.5(S_v - 1) + 0.5H]) / 2$ ceil means rounding upward to the next integer. T_{calc} is rounded upward to a half auditor-day. One auditor-day is eight hours of actual evaluation; time is additive across competent evaluators, not merely elapsed calendar days.

AC.3 Total time, stages and exclusions

SOURCE p. 109 | Normative when applicable

AC.3(a) Initial evaluation time T shall be at least T_{calc} and at least one auditor-day per visited physical site, with additional time for the central function and remote activities where needed. For a wholly digital single-location organization, the physical-site floor shall be treated as one evaluation location, not an obligation to invent a physical visit.

AC.3(b) Readiness-stage time T1 shall be at least 0.5 auditor-day and the upward half-day rounding of 25% of T. Implementation-stage time T2 shall be the remainder and at least 1.5 auditor-days. If these minima cannot both be met, total time shall be increased. Readiness shall verify scope, documents, internal evaluation, implemented evidence and readiness for technical examination.

AC.3(c) Travel, meal breaks, commercial administration, final report production, interpretation delays, independent review and decision time shall not count as evaluation time. Trainees and observers shall not be counted as fully productive auditors. Separate technical expert time shall be counted only for the actual evaluation task and not double-counted against simultaneous auditor activity on the same task.

Required evidence: Time calculation; stage allocation; site/shift schedule; productive-time records; separate review and decision resources.

Source calculation note: (AC-2) $T1 = \max[0.5, \text{ceil}(2 \times 0.25T)/2]$; $T2 = T - T1 \geq 1.5$ The equation gives the minimum readiness allocation. Increase total time where the readiness or implementation evidence requires more time.

AC.4 Surveillance and renewal time

SOURCE p. 110 | Normative when applicable

AC.4(a) For the current scope, the operator shall recalculate the initial time T when material scope or risk changes. Each surveillance evaluation shall use at least half of T, rounded upward to a half-day, and at least one auditor-day. Renewal shall use at least three quarters of T, rounded upward to a half-day, and at least two auditor-days.

AC.4(b) The site coverage and critical-control requirements remain additional floors. The provider shall increase time where these percentages cannot cover required sites, shifts, technical processes or unresolved concerns. No reduction shall be granted merely for AF membership, another certificate, a low fee or long customer history.

AC.4(c) Frequency is governed by Annex AG. Time allocated to one surveillance visit shall not be borrowed from a future visit to cover a missed required activity. Extra follow-up to verify nonconformity closure shall be planned according to the nature of the issue.

Required evidence: Current T calculation; surveillance and renewal schedules; required-site coverage; added follow-up time.

AC.5 Multisite coverage and controlled sampling

SOURCE p. 110 | Normative when applicable

AC.5(a) Every physical site included in an initial or renewal ORG scope shall be evaluated. The central management function, shared critical activities and remote functions shall also be covered. Site selection shall consider actual processes rather than addresses alone; a legal address with no operational activity shall not be represented as a production site.

AC.5(b) For surveillance only, homogeneous C0/C1 sites under one centrally controlled system may be sampled when equivalent activities, methods and controls are demonstrated. From S eligible sites, at least $m = \max(\text{ceil}(\sqrt{S}), \text{ceil}(S/2))$ shall be evaluated at each annual surveillance. Selection shall rotate to cover all eligible sites within 24 months. At least one quarter of selected sites, rounded upward, shall be chosen randomly; the remainder shall be risk-selected.

AC.5(c) C2/C3 sites, unique activities, materially different processes, sites with significant unresolved issues and newly added sites shall not enter that reduced homogeneous pool. Relevant C2/C3 critical-control sites shall be evaluated at each required surveillance interval. The central function shall be evaluated at every surveillance. These selections are coverage rules, not statistical confidence claims.

AC.5(d) A systemic finding at one site shall trigger review of all potentially affected sites and expansion of the sample. Removing the failing site from the certificate shall not be accepted as correction where the central system or remaining sites share the deficiency.

Required evidence: Eligibility analysis; site pool; random and risk selection; rotation history; expanded sampling and systemic review.

Source calculation note: (AC-3) $m = \max[\text{ceil}(\sqrt{S}), \text{ceil}(S/2)]$ Applies only to the eligible homogeneous C0/C1 surveillance pool. Mandatory central, critical and otherwise ineligible sites are added separately.

AC.6 Remote evaluation and access limitations

SOURCE p. 110 | Normative when applicable

AC.6(a) Remote methods may be used when identity, confidentiality, live observation, configuration, provenance and access provide evidence equivalent for the stated purpose. The provider shall document the suitability decision and limitations. Remote record review alone shall not replace necessary observation of a physical special process or safety-critical activity.

AC.6(b) Where reliable physical evidence cannot be obtained remotely, on-site evaluation or an appropriately controlled witnessed method shall be used. Restricted access shall be resolved through authorized arrangements. If necessary evidence remains unavailable, the corresponding conformity conclusion shall not be granted.

AC.6(c) Recording, screen capture and transfer of sensitive data shall be authorized. Live feeds shall be protected against selective or prerecorded presentation. Network failure or incomplete observation shall be recorded and the affected activity repeated or supplemented rather than marked complete.

Required evidence: Remote-method suitability review; authorized access; witnessed records; limitations and completed supplementary work.

AC.7 Audit execution, sample expansion and reporting

SOURCE p. 110 | Normative when applicable

AC.7(a) The audit shall include an opening review of scope and access, examination of actual process interactions, vertical traceability through selected outputs, observation of critical controls and a closing review of evidence-based findings. The sample shall include unfavorable results, changes, rework, complaints and unsuccessful tests where relevant.

AC.7(b) Samples shall identify populations, selections and limitations. Judgmental sampling shall not be described as a statistical assurance level. An inconsistency or suspected systemic issue shall trigger an expanded trail proportionate to consequence. The final report shall be issued within 14 calendar days after the evaluation closes, unless a documented exceptional delay is communicated without postponing protective action.

AC.7(c) The report shall identify actual evaluation time, participants, scope, criteria, methods, locations, sample, findings, unresolved limitations and the evaluator's recommendation. The independent decision shall remain distinct from that recommendation.

Required evidence: Audit plan; time log; evidence and sample trails; expanded checks; final report and separate decision.

AC.8 Worked time and sampling examples — illustrative

SOURCE p. 111 | Definition, explanation or informative example; no new universal limit

AC.8(a) For $N = 80$, one physical site, one observed shift, C2 criticality and two complexity triggers, $B = 5$, $K = 1.35$ and $f = 0.30$. The calculation gives $5 \times 1.35 \times 1.30 = 8.775$ auditor-days, rounded upward to $T = 9.0$. The minimum readiness stage is 2.5 days and implementation is 6.5 days. Surveillance is at least 4.5 days; renewal is at least 7.0 days. Independent review and decision require additional time.

AC.8(b) For nine eligible homogeneous C0/C1 sites, $m = \max(3, 5) = 5$ sites at annual surveillance, plus the central function and any separately mandatory locations. The selection rotates to cover every eligible site within 24 months. At least two of the five selected sites are random. This does not mean the unvisited sites are known to conform.

AC.8(c) For an optional statistical detection study, independent random observations with a true issue rate $p = 0.10$ need $n = \text{ceil}(\ln(0.05)/\ln(0.90)) = 29$ to have at least 95% probability of observing one or more issues. This model does not validate judgmental audit sampling, dependent records or a claim that the whole system is 95% conforming.

Source calculation note: (AC-4) $n_{\text{detect}} = \text{ceil}[\ln(1 - C)/\ln(1 - p)]$ C is the desired probability of detecting at least one issue when independent observations each have issue probability p. This is a detection-planning model, not a universal audit sample requirement.

AD.1 Decision basis and non-compensable conditions

SOURCE p. 112 | Normative when applicable

AD.1(a) Before evaluation, the responsible authority shall define the object, applicable requirements, criterion for each characteristic or competence, evidence needed, uncertainty treatment, required independence and permitted outcomes. Criteria shall not be selected retrospectively to obtain a favorable result.

AD.1(b) Every applicable mandatory criterion shall be fulfilled for a positive initial conformity attestation. No aggregate score, favorable delivery performance, commercial benefit or passing result in an unrelated area shall compensate for an unmet mandatory requirement, missing critical evidence or unresolved unacceptable risk.

AD.1(c) A technical release may include a lawful, explicitly approved concession for a bounded departure where the underlying technical and contractual framework permits it. The record shall identify that departure; it shall not falsely state that the original requirement was fulfilled. A concession cannot waive a mandatory legal approval or alter the AF requirements for an attestation.

Required evidence: Pre-agreed decision basis; complete criterion register; blocker review; concession and release distinctions.

AD.2 Measurement decision preparation

SOURCE p. 112 | Normative when applicable

AD.2(a) The measurement decision shall use the corrected result, applicable specification, validated method, justified uncertainty model and pre-agreed rule. Known significant systematic effects shall be corrected or otherwise treated through an approved model; an uncertainty allowance shall not conceal an ignored known bias.

AD.2(b) The record shall distinguish specification limits, control limits, resolution, uncertainty and acceptance limits. Units, significant figures, confidence or coverage interpretation and treatment of correlation shall be stated. The uncertainty shall be appropriate to the actual result and conditions, not copied from an unrelated calibration capability.

AD.2(c) Decisions shall use sufficient unrounded precision. Rounding is applied to reported values after the decision and shall not turn a failing or indeterminate result into a pass. When both lower and upper limits apply, both shall be evaluated; one favorable characteristic shall not substitute for another.

Required evidence: Measurement model; corrections; uncertainty budget; specification and acceptance limits; recorded rule and precision.

AD.3 DR-A — Full-interval decision rule

SOURCE p. 112 | Normative when applicable

AD.3(a) For a two-sided numerical specification $[L, H]$, DR-A shall conclude “conformity demonstrated” only when the entire stated uncertainty interval lies within the inclusive specification limits. It shall conclude “nonconformity demonstrated under DR-A” when the entire interval lies outside one specification limit. All other results are indeterminate and shall be held from acceptance pending valid disposition.

AD.3(b) For C2 or C3 acceptance characteristics whose uncertainty can materially change the decision, DR-A shall be the default unless a documented alternative is approved under AD.5 by the metrology and relevant independent technical authorities. Applicable binding rules take precedence where they mandate another lawful rule.

AD.3(c) A one-sided specification shall use the corresponding single bound. For asymmetric uncertainty, the actual lower and upper coverage endpoints shall replace $y - U$ and $y + U$. The interpretation remains conditional on the stated measurement model and coverage; it is not an absolute guarantee of physical truth.

Required evidence: Declared DR-A application; actual result and coverage endpoints; criterion-by-criterion disposition; independent alternative approval where used.

Source calculation note: (AD-1) Conform: $y - U \geq L$ and $y + U \leq H$. Nonconform: $y + U < L$ or $y - U > H$. Otherwise: indeterminate. y is the corrected result and U the justified expanded uncertainty for the symmetric case. Equality at a specification boundary is inside the limit. An interval overlapping a limit is not automatically a proven physical defect, but conformity has not been demonstrated by this rule.

AD.4 DR-B — Simple acceptance with disclosed decision risk

SOURCE p. 112 | Normative when applicable

AD.4(a) Simple acceptance compares the corrected result directly with the specification limits. It may be used for C0 or C1 characteristics only where the rule is agreed before evaluation, the method is suitable, uncertainty and decision risk have been reviewed, and no binding obligation requires a more protective rule.

AD.4(b) The report shall disclose that acceptance does not use a guard band and that uncertainty can create false acceptance or false rejection near a limit. The operator shall not describe simple acceptance as zero risk. C2 or C3 use requires the independent alternative-rule approval in AD.5; it shall not be selected solely to accept a result that failed DR-A.

Required evidence: Prior agreement; uncertainty and risk review; scope and criticality; clearly disclosed acceptance rule.

AD.5 DR-C — Risk-targeted or other justified alternative

SOURCE p. 113 | Normative when applicable

AD.5(a) An alternative rule shall define the decision objective, allowable risks, statistical or physical model, prior information where used, distribution, dependence, measurement uncertainty, acceptance region and validation. Consumer and producer risks shall be distinguished. Approval shall occur before results are evaluated.

AD.5(b) A posterior probability of nonconformity conditional on a result shall be reported only when the underlying prior and likelihood are specified and justified. A coverage interval shall not automatically be reinterpreted as that posterior probability. Likewise, a sampling plan’s operating characteristic shall not be interpreted as the probability that an accepted particular lot is conforming.

AD.5(c) For a C2/C3 alternative, the independent technical reviewer shall evaluate consequences, model limitations, sensitivity and whether the rule provides the required protection. The metrology authority, relevant safety or mission authority and contractual authority where required shall approve its exact scope. The rule shall be reviewed after a material model or process change.

Required evidence: Alternative-rule model; risk constraints; validation and sensitivity; independent approvals; application limits.

AD.6 Indeterminate results, repeat testing and multiple criteria

SOURCE p. 113 | Normative when applicable

AD.6(a) An indeterminate result shall remain held until a validated improved measurement, relevant additional evidence or a lawful technical disposition resolves it. Repeating observations until a favorable reading appears is prohibited. A repeat or pooled-result method shall be specified in advance or independently justified with the original results retained.

AD.6(b) Where a guard band leaves an empty acceptance region, the method cannot demonstrate conformity under that rule. The response shall improve the method or obtain an approved technically justified alternative, not quietly widen the product specification. Known nonconforming material shall remain controlled under Clause 8.7.

AD.6(c) For many characteristics or repeated decisions, the plan shall consider cumulative false-decision risk, dependence and the consequences of multiple comparisons. A nominal interval for each characteristic shall not be represented as the same confidence for all characteristics jointly without a justified analysis.

Required evidence: Hold and disposition record; repeat-test plan; retained original results; cumulative-risk review.

AD.7 Finding classification and immediate action

SOURCE p. 113 | Normative when applicable

AD.7(a) A finding shall identify the exact requirement, objective evidence, affected scope and gap. The evaluator shall classify the finding using Table AD-2 and separately decide whether an immediate technical hold or protective action is necessary. Administrative classification shall never delay protection.

AD.7(b) Related localized findings shall be reviewed together for evidence of systemic breakdown. An opportunity for improvement shall not replace a nonconformity where a requirement is unmet. A mere preference for a different method, where the actual requirement is fulfilled, shall not be raised as a nonconformity.

Required evidence: Requirement-evidence-gap statement; classification rationale; systemic extent; immediate technical action.

AD.8 Attestation decisions and open findings

SOURCE p. 114 | Normative when applicable

AD.8(a) Initial grant, renewal and extension shall require all nonconformities in the granted scope to be closed, adequate evidence for all mandatory criteria and independent review. A restricted scope may be granted only where its boundary is real, independently evaluated and unaffected by unresolved systemic deficiencies; it shall not conceal the failed scope.

AD.8(b) An existing attestation may be maintained with a localized minor finding only when immediate correction or containment is adequate, cause and extent are reviewed, a corrective plan is accepted within the Annex AG time limit, and no essential control or mandatory output criterion is compromised. The decision maker shall record why continued status is justified and verify closure within the required period.

AD.8(c) An existing major finding shall trigger an immediate assessment of continuing conformity. Where the underlying ability to meet requirements is not demonstrated, the affected status shall be suspended. Limited continuation is permitted only for a specifically evidenced unaffected scope, through a documented restriction decision. A planned future correction alone is not evidence of current conformity.

AD.8(d) A conditional lifecycle gate or conditional supplier-development approval may permit bounded non-dependent work. Neither is a conditional conformity certificate. Annex AG controls closure, suspension and restoration deadlines; an expired deadline shall not be reset by reissuing the same finding.

Required evidence: Independent grant or continuation decision; closed findings; real scope boundaries; verified corrections and corrective action.

Source calculation note: (AD-2) Grant = scope valid AND all applicable criteria fulfilled AND evidence adequate AND findings closed AND independent decision authorized This is a logical conjunction, not a weighted score. "Findings closed" refers to nonconformities in the scope being granted; observations do not create a mandatory failure.

AD.9 Decision record and challenge

SOURCE p. 114 | Normative when applicable

AD.9(a) The record shall identify the applicant and object, route, profile, evidence package, evaluator and reviewer, findings and closure, independence, limitations, decision, reasons, actual date and signatory. Automated workflow may enforce checks, but an accountable authorized person shall approve the conformity decision.

AD.9(b) Technical dissent shall remain in the record with its resolution. An appeal shall follow Annex AI. A revised decision shall preserve the earlier decision and explain the new evidence or corrected interpretation. No record shall be backdated or altered to make the earlier basis appear stronger than it was.

Required evidence: Complete decision record; documented dissent; accountable signatory; preserved history and appeal disposition.

AG.1 Time interpretation and recorded dates

SOURCE p. 120 | Normative when applicable

AG.1(a) Unless explicitly stated otherwise, “days” means calendar days. A period starts when the holder or responsible operator is first formally informed of the relevant finding, decision or event; final report production shall not postpone an already communicated finding. A deadline measured in months falls on the corresponding calendar date, or the last day of that month if no corresponding date exists.

AG.1(b) A validity record shall specify its time basis and exact expiry date. Certificate issue date and conformity decision date shall be recorded separately when they differ. No document shall be backdated to conceal an expired, suspended or unassessed period. A later correction shall preserve the actual history.

Required evidence: Time basis; notification timestamps; decision, issue and expiry dates; preserved amendments.

AG.2 Ongoing versus instance attestations

SOURCE p. 121 | Normative when applicable

AG.2(a) An ongoing attestation remains valid only while required surveillance, criteria and conditions are fulfilled. A holder with mixed criticality shall follow the shortest interval triggered by the attested scope unless genuinely separate scopes and records justify different surveillance arrangements.

AG.2(b) A lot, serial, one-time test, service-event or other instance attestation shall identify the exact evaluated instance and conditions. It does not authorize future production or continuing services. Its historical result does not acquire a universal 24-month technical validity; later evidence that invalidates the result shall nevertheless trigger correction or withdrawal of the claim.

AG.2(c) A process qualification or personnel task authorization may lose validity before its scheduled review because conditions or competence have changed. A certificate period shall not extend an equipment life limit, calibration validity, operator license or qualified process window.

Required evidence: Ongoing/instance classification; appropriate expiry or event boundary; monitored conditions; linked technical limits.

AG.3 Surveillance planning and completed coverage

SOURCE p. 121 | Normative when applicable

AG.3(a) The operator shall plan surveillance using current scope, criticality, changes, performance, complaints, prior findings and technical dependencies. Annex AC sets organizational time and site-coverage minima. Other routes shall use the profile’s appropriate tests, observation or competence checks within the intervals in Table AG-1.

AG.3(b) Completed surveillance shall verify that the attestation basis remains valid, not merely that documents have not changed. Missed surveillance by the applicable deadline shall trigger suspension of the affected ongoing attestation. Scheduling an audit, paying an invoice or issuing a reminder shall not count as completion.

AG.3(c) A serious event or material change shall trigger special evaluation before the routine due date where necessary. Recovery from an interruption shall verify actual competence, configuration and controls before the affected status is restored.

Required evidence: Risk-based surveillance plan; completed evidence; missed-deadline decisions; special evaluations and restoration checks.

AG.4 Finding closure and overdue action

SOURCE p. 121 | Normative when applicable

AG.4(a) The finding owner shall implement immediate correction or containment, determine extent and cause, implement corrective action and provide evidence of effectiveness. The operator shall verify closure by a method appropriate to the finding; a revised procedure alone is insufficient for an implementation failure.

AG.4(b) If a major or minor closure deadline is missed, the operator shall suspend or further restrict the affected ongoing scope unless it is already suspended or withdrawn. A new finding number or revised action plan shall not restart the original deadline. The deadline for a critical finding shall be set by the necessary protective action and relevant technical basis, not by the minor or major timetable.

AG.4(c) For initial grant, renewal and extension, no open nonconformity may remain within the requested scope at the decision. Corrective-action periods are time allowed to remedy deficiencies, not a permission to issue a certificate before those deficiencies are closed.

Required evidence: Correction and cause evidence; verified effectiveness; original due dates; overdue status decisions.

AG.5 Suspension, restriction, restoration and withdrawal

SOURCE p. 121 | Normative when applicable

AG.5(a) Suspension shall state the affected object, scope, reason, prohibited claims, required action and final resolution deadline. The holder shall cease the affected claim and mark use immediately. Product or service containment obligations remain separate and shall be implemented where the technical issue requires them.

AG.5(b) Restoration shall require verification that the cause is resolved, affected outputs have been addressed and the attestation basis is again valid. The original expiry shall remain unchanged unless a complete renewal decision is also made. Restoration shall not retrospectively validate the suspended interval.

AG.5(c) Restriction shall be allowed only where the remaining scope is independently demonstrated to be unaffected and adequately controlled. At the end of 90 days of suspension, the operator shall restore, formally restrict to such a scope or withdraw. Suspension shall not be prolonged by repeated administrative resets.

Required evidence: Reasoned status decisions; required action; verified restoration; unaffected-scope analysis; complete history.

AG.6 Renewal and continuity of claims

SOURCE p. 121 | Normative when applicable

AG.6(a) The operator and holder shall plan renewal sufficiently before expiry to complete evaluation, corrective action, independent review and decision. Initiating the process at least 90 days before expiry is recommended; it does not guarantee completion or extend validity.

AG.6(b) Renewal shall evaluate the complete current basis, performance over the preceding period, changes, complaints, competence and surveillance effectiveness. The operator shall not rely solely on the prior certificate. All nonconformities in the renewed scope shall be closed before the new decision.

AG.6(c) If the decision is completed after expiry, the new attestation shall begin no earlier than its actual decision date. The gap shall remain visible. The holder shall not use the expired claim while waiting for a decision.

Required evidence: Renewal plan; complete evaluation; closed findings; actual decision dates; disclosed gaps.

AG.7 Scope change, transfer and provider closure

SOURCE p. 122 | Normative when applicable

AG.7(a) Expansion to new products, services, roles, technical methods, critical processes or sites shall require competence, profile and evidence review before the expanded claim is used. Legal identity, ownership and key resource changes shall be assessed for their effect on responsibility and continuing control.

AG.7(b) Transfer to another operator shall not be automatic. The receiving operator shall verify authenticity, actual scope, decision history, open findings, surveillance and competence evidence and perform additional evaluation where necessary. A suspended or unsupported claim shall not be made valid by transfer.

AG.7(c) If an operator ceases operation, the owner and authorized parties shall preserve records, status and outstanding cases, and arrange any lawful transfer. Holders shall be informed of effects on surveillance and claims. Record transfer alone does not transfer accreditation or AF operating authority.

Required evidence: Scope-change evaluation; transfer review; unresolved findings; provider closure and holder notification.

AG.8 Status register, records and historical integrity

SOURCE p. 122 | Normative when applicable

AG.8(a) The scheme operator shall maintain a current register identifying attestation ID, holder, route, scope, profile, issue and decision dates, expiry or instance boundary, status and restrictions. Public verification shall disclose sufficient information to prevent misleading use while protecting personal and controlled technical data.

AG.8(b) Assessment and decision records shall be retained for at least seven years after the last relevant decision, or longer where applicable obligations, product life or investigations require. Sensitive personnel information shall be minimized, access controlled and lawfully disposed of when retention is no longer justified. Legal constraints requiring a different handling arrangement shall be documented without falsifying or concealing the decision basis.

AG.8(c) Corrections, restrictions, suspension, expiry and withdrawal shall preserve historical dates. A record may be archived but shall not be deleted to imply that an adverse status never existed. The operator shall test retrieval

and continuity of status information.

Required evidence: Current and historical register; privacy controls; justified retention; tested retrieval and continuity.

Source tables — complete field and decision payloads

Table 3-1 — Core terms

Source p. 11, 12, 13 | Illustrative or explanatory source table

Term	Meaning within this standard
Accountable executive	Person with authority to allocate resources and accept organizational responsibility for the system; delegating tasks does not remove accountability.
Assurance case	Structured argument linking a specific claim, operating context, reasoning, evidence, limitations and residual risks.
Assurance independence	Freedom and authority to challenge or decide without being subordinate to the delivery pressure or work being assessed; the necessary degree depends on criticality.
Baseline	Approved set of identifiable requirements, designs, process definitions, data or configurations under change control.
Critical item	Item, function, characteristic, software element or process whose failure or variation requires special controls because of its consequence.
Key characteristic	A measurable attribute whose variation materially affects fit, function, performance, life or producibility and therefore requires controlled variation.
Special requirement	A requirement with elevated difficulty or risk of fulfillment, such as immature technology, demanding tolerance or constrained delivery.
Safety-critical characteristic	A characteristic connected to a hazardous consequence and therefore requiring an explicit safety-related control and verification rationale.
Operational domain	Defined environment, mission, users, interfaces, modes, timing and constraints within which a function is intended to operate.
Mission assurance	Coordinated activities supporting justified confidence that mission objectives and associated constraints can be achieved.
Residual risk	Risk remaining after implemented controls, with stated assumptions, evidence, owner and acceptance authority.
Risk acceptance	Authorized decision about a stated residual risk; not the absence of information or a substitute for a mandatory requirement.
Opportunity	Potential beneficial outcome considered through a deliberate feasibility and benefit assessment, distinct from an adverse-risk register.
Special process	Process for which all relevant output characteristics cannot be adequately verified by subsequent inspection alone.
First article verification	Documented verification that the intended production configuration and route can produce an item satisfying its specified characteristics.
Configuration status accounting	Recorded history and current status of baselines, approved changes, deviations and actual item or service configurations.
Concession	Authorized permission for a specifically bounded departure, without waiving applicable legal obligations or unapproved safety constraints.
Counterfeit or suspect item	Item or record whose claimed identity, origin, condition or approval is intentionally misrepresented, or for which credible evidence raises that concern.
Traceability	Ability to connect an output with its applicable requirements, origin, processing, evidence, configuration and authorized disposition.

Term	Meaning within this standard
Digital thread	Controlled connections among lifecycle information; a particular software architecture or vendor platform is not mandated.
Digital twin	A model linked to an identified physical or operational entity and maintained for a defined decision purpose, with validated limits of credibility.
Model of record	Controlled model version authorized as an authoritative input for a stated purpose; not necessarily valid outside that purpose.
Out-of-distribution condition	Input or context insufficiently represented in a model's demonstrated operating basis, potentially invalidating expected performance.
Software bill of materials	Structured inventory of software components and relevant versions, dependencies, provenance and identification.
Measurement uncertainty	Parameter characterizing the dispersion of values reasonably attributable to a measurand under an identified model.
Decision rule	Pre-agreed method describing how measurement uncertainty and risk are considered when determining conformity.
Nonconformity	Failure to fulfill an applicable requirement; an improvement suggestion alone is not a nonconformity.
Containment	Immediate action to prevent further impact or escape while the extent and causes of a problem are being determined.
Correction	Action addressing a detected nonconformity in a particular output or situation.
Corrective action	Action addressing substantiated causes to prevent recurrence or occurrence elsewhere, with effectiveness verification.
Release authority	Identified competent person or controlled function authorized to release an output against defined acceptance conditions.
Service-life limit	Approved bound on time, cycles, exposure or condition that shall not be exceeded without an authorized engineering disposition.
Technology readiness evidence	Documented demonstration of a capability in a specified environment; a readiness label alone is not sufficient evidence.
Foreseeable misuse	Use or behavior reasonably predictable in the intended context even though not intended by the designer.
AF criticality category	Internal tailoring category C0 to C3 in Annex B; not an equivalence to any external design assurance or safety integrity classification.
Conformity object	Precisely identified organization, product, service, process, person, supplier scope or assessment-provider capability to which an evaluation and claim apply.
Application profile	Approved definition of an object, intended use, scope, technical or competence criteria, evaluation methods and limitations required by Annex AA.
Scheme owner	AF, responsible for the controlled rule set and governance of the AF scheme; not necessarily the body performing evaluations.
Scheme operator	Body with actual written authority to operate a stated AF assessment route and responsibility for its implementation.
Evaluation	Examination of evidence by audit, inspection, testing, observation, interview, examination or analysis against specified requirements.
Review	Competent examination of the sufficiency and consistency of evaluation evidence before the conformity decision.

Term	Meaning within this standard
Conformity decision	Accountable determination to grant, refuse, maintain, restrict, suspend, restore, renew or withdraw a bounded attestation.
Auditor / lead auditor	Person authorized to conduct audits / person additionally authorized to lead and integrate an audit team's work.
Technical expert	Person providing verified domain expertise who does not automatically possess audit leadership or conformity decision authority.
Personnel certification	Independent attestation that a person has demonstrated specified role competence within a defined scope and period.
Task authorization	Employer or responsible technical authority permission to perform a defined task on specified work; distinct from certification or a statutory license.
Subcontractor / sub-tier provider	External performer of assigned work / a further provider used by that performer; retained accountability does not disappear through these tiers.
Accreditation	A distinct, authorized competence attestation for a conformity-assessment body's defined activities, following the CAB route; not organizational certification or membership.
Indeterminate measurement decision	A result for which the selected uncertainty-aware rule demonstrates neither conformity nor nonconformity; acceptance is held unless valid further evidence resolves it.
Critical / major / minor finding	Finding classifications defined in Annex AD; they do not replace the separate technical hold decision.
Suspension / withdrawal	Temporary prohibition on use of an attestation / termination of that attestation; both retain an auditable status history.
Restriction	A formally evaluated reduction or limitation of scope; not a means of concealing a systemic failure affecting the remaining scope.
Ongoing attestation / instance attestation	A time-limited claim maintained through surveillance / a claim confined to an identified lot, serial, service event or evaluated instance.

Table 3-2 — Abbreviations

Source p. 13, 14 | Illustrative or explanatory source table

Abbreviation	Meaning
AI / ML	Artificial intelligence / machine learning
BOM / SBOM	Bill of materials / software bill of materials
CAPA / NCR	Corrective action management / nonconformity record
COTS	Commercial off-the-shelf
EMC / EMI / ESD	Electromagnetic compatibility / interference / electrostatic discharge
FAI / FMEA / FTA	First article inspection or verification / failure mode and effects analysis / fault tree analysis
FOD	Foreign object debris or damage, as specified by context
MRO	Maintenance, repair and overhaul
MBSE	Model-based systems engineering
MTBF / MTTR	Mean time between failures / mean time to repair

Abbreviation	Meaning
NDT	Non-destructive testing
ODD	Operational design domain
OT	Operational technology
QMS	Quality management system
RAM	Reliability, availability and maintainability
RPO / RTO	Recovery point objective / recovery time objective
SPC	Statistical process control
UAS	Unmanned aircraft system
V&V	Verification and validation

Table A-1 — Module selection rules

Source p. 50, 51 | Required structure when applicable

Activity or effect	Required AF coverage	Additional evidence focus
All organizations	Clauses 1–10; 22; relevant 23–28; Annexes A, B, D, V, W	Scope, processes, competence, evidence integrity, evaluation and claims.
System design or integration	11; relevant parts of 8.3; Annex C	Requirements allocation, interfaces, lifecycle gates and assurance case.
Software or programmable hardware	12; 13; Annexes N, O	Controlled digital lifecycle, configuration, verification and security.
AI in product, inspection or engineering	12.4–12.7; Annex N	Use case, data lineage, independent evaluation and bounded authority.
Connected product, OT or remote service	13; Annex O	Trust boundaries, identity, updates, incident response and recovery.
Space mission or space-purpose equipment	14; Annex P	Mission environment, ground/space interfaces, end-of-life and remote assurance.
Aircraft, UAS, aviation equipment or services	15; Annex Q	Approval interfaces, installation, operational domain and continued support.
Defense land, maritime, air or multi-domain work	16; Annex R	Contract obligations, controlled information, integration and lifecycle support.
Defense automotive or mission vehicles	16.3; relevant 12–13, 18–21; Annex R	Duty cycle, modified-platform effects, road/mission approval boundaries.
Lunar or planetary mobility	14.7; relevant 11–13, 18–21; Annex P	Space-environment qualification; terrestrial qualification limitations.

Activity or effect	Required AF coverage	Additional evidence focus
Industrial machinery, plant or infrastructure	17; Annex S	Design basis, code interfaces, installation, commissioning and integrity.
Materials, manufacture or special processing	18; 8.5; Annexes K, L	Process qualification, essential variables, genealogy and first article evidence.
Energy storage, fuel or propulsion	19; relevant sector annex	Coupled hazards, operating limits, degradation and emergency interfaces.
External provision or supply responsibility	8.4; Annex J	Source approval, flow-down, delegated verification and authenticity.
Test, calibration or inspection service	7.6–7.7; 8.3.4; Annex M	Method validity, uncertainty, traceability and decision rules.
Maintenance, overhaul, distribution or logistics	21; Annex T	Capability, current data, life status, custody and authorized release.
Lifecycle environmental or human-system effects	20; relevant sector requirements	Impact boundaries, human factors, credible claims and retirement controls.
Novel or previously unlisted activity	6.6; 11; 20.6; applicable existing modules	Hazard-driven extension; evidence gaps; approved technical basis.
Product or integrated-system claim	23; Annexes AA, AD, AG; relevant K–S	Exact configuration/family and technical profile; qualification versus instance acceptance.
Service conformity claim	24; Annexes AA, AD, AG; relevant T	Service boundary, outcomes, capacity, continuity and observed delivery.
Process qualification claim	25; Annexes AA, AD, AG; relevant L	Qualified process window, site, equipment, essential variables and monitoring.
Personnel competence or task authorization	26; Annex AE; AB for assessment roles	Role and task criteria, demonstrated competence and bounded authorization.
Subcontracted or multi-tier work	27; Annexes AF, J	Accountability, actual performer, flow-down, changes, evidence and exit.
Assessment, inspection or laboratory operation	28; Annexes AB, AH; applicable AA–AI	Body competence, impartiality, valid methods and independent decisions.

Table A-2 — Illustrative scope decisions, not actual AF approvals

Source p. 51 | Illustrative or explanatory source table

Organization example	Decision	Reason and retained controls
Build-to-print aircraft bracket manufacturer	Own product design not performed; manufacturing process design remains applicable.	Customer holds design authority. Apply 8.3 data controls, 8.4, 8.5, 15 and 18; escalate drawing errors and unauthorized changes.
Satellite battery supplier	Space, software/security and energy modules apply.	Product includes embedded control and contributes to mission hazards. Apply 11–14, 18–20 and relevant normative annexes.
Defense vehicle integrator using a commercial chassis	Vehicle and defense modules apply to the modified configuration.	Chassis evidence does not establish payload integration or mission-duty suitability. Apply 16.3 and energy/software modules as triggered.
Stockist splitting sealed fastener lots	Distribution and authenticity controls apply; no manufacturing claim.	Preserve source/lot identity, certificate linkage, quantity and storage. Any rework would trigger additional manufacturing controls.
Software-only inspection-service provider	Digital and measurement-method controls apply.	No physical manufacture, but algorithms influence acceptance. Apply 7.7, 7.12, 12, 13 and verification-service controls.

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.
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 D-1 — Required lifecycle data entities

Source p. 55 | Required structure when applicable

Entity	Minimum fields	Required relationships
Requirement	ID; revision; statement; source; rationale; criticality; owner; acceptance criterion; status.	Parent need; allocated item/function; verification case; applicable obligation.
Configuration item	ID; type; revision; physical/software identity; owner; baseline; approved use.	Requirements; BOM; interfaces; change history; as-built or deployed instances.
Material or component lot	Source; manufacturer; lot/batch; quantity; condition; certificate; received date.	Incoming verification; process route; consumed serials; split/merge history.
Verification case	ID; method; requirement; configuration; procedure; environment; uncertainty; acceptance rule.	Test article; equipment; raw data; result; anomaly and disposition.

Entity	Minimum fields	Required relationships
Process execution	Route revision; operation; performer; date/time; equipment; parameters; material; result.	Lot/serial; qualified procedure; inspection; nonconformity; next authorized step.
Change	ID; reason; baseline before/after; impact; approvals; effectivity; verification.	Affected requirements/items; delivered population; suppliers; support information.
Hazard or risk	ID; scenario; consequence; likelihood basis; exposure; controls; owner; residual decision.	Requirements; mitigations; verification evidence; operational limitations.
Release	ID; configuration; scope; acceptance evidence; concessions; restrictions; authorized identity; date.	Requirements baseline; product serial/lot; delivery dossier; service-life status.
Digital artifact	Artifact ID; version; source/build; dependencies; hash; signature; provenance; access class.	Requirements; verification; release; deployment instances; vulnerabilities.
Retirement	Asset identity; condition; hazardous inventory; reuse restrictions; disposition; verifier.	Life history; disposal evidence; retained records; remaining obligations.

Table D-2 — Filled illustrative trace chain

Source p. 55, 56 | Illustrative or explanatory source table

Record	Example value	Connection
Need	NEED-GSC-01: controlled motion during payload handling.	Allocated to SYS-GSC-R12.
Requirement	SYS-GSC-R12 rev B: stop response within a program-defined limit under stated load and speed.	Hazard H-GSC-02; verification V-GSC-12.
Configuration	Controller CTRL-07 rev C; firmware 2.4.1; cart serial GSC-004.	Build manifest BM-241; interface ICD-09 rev D.
Verification	V-GSC-12 rev 3; test article GSC-004; report TR-012.	Raw records RAW-012; calibrated timer TM-08; approved decision rule DR-03.
Disposition	Anomaly AN-04 closed after independent retest.	NCR-026; verified corrective action CA-026.
Release	REL-GSC-004 rev 1; approved operating- domain restriction attached.	Release authority RA-02; receiving acknowledgement ACK-004.

Table V-1 — Audit and assessment record fields

Source p. 87 | Required structure when applicable

Field	Minimum required content
Identity and scope	Evaluation ID, date, assessor, object route, entity/person, site, configuration, profile and period.
Requirement	Exact clause and lettered paragraph, normative table condition or profile criterion.
Sample	Records, items, people, sites and periods observed; selection method and limitations.

Field	Minimum required content
Evidence	Objective observations, actual results, traceable records and confidentiality controls.
Conclusion	Conforming, nonconforming, approved non-applicability or not yet demonstrated.
Finding and action	Requirement–evidence–gap, grade, extent, protection, cause, actions, owner and original deadline.
Closure and decision	Verified implementation and effectiveness; independent reviewer and decision; actual status and date.

Table W-1 — Complete NCR/CAPA record requirements

Source p. 96 | Required structure when applicable

Stage	Required record content
Identification	NCR ID, date, reporter, requirement, item/process, configuration, actual evidence and initial consequence.
Containment	Affected population, immediate controls, stock/delivery status, responsible person, notifications and effectiveness.
Extent	Related lots/serials/sites/suppliers/configurations; trace method; uncertainty and expanded search.
Disposition	Correction, rework, repair, return, concession or scrap; design/customer/authority approvals as applicable.
Cause	Evidence-supported occurrence and escape causes; tested hypotheses; human/system factors; rejected explanations.
Actions	Action tied to each cause, owner, due date, resources, affected documents/tools/suppliers and change approval.
Verification	Implementation evidence, pre-defined effectiveness criterion, sample/exposure, results and adverse side effects.
Systemic learning	Risk updates, similar processes, supplier flow-down, knowledge transfer and recurrence monitoring.
Closure	Independent review where necessary, residual limitations, final authority and reopened conditions.

Table W-2 — Filled corrective-action case

Source p. 96, 97 | Illustrative or explanatory source table

Step	Recorded result
Requirement and evidence	Post-maintenance reference check required by WI-MET-08 rev D; no check record for event M-114; independent comparison shows 0.012 mm offset.
Containment	Hold 90 on-site items; notify two recipients of 150 shipped items; identify exact serial range and related jobs.
Extent assessment	Trace confirms 240 potentially affected items. Independent remeasurement finds 8 outside the actual product limit; remaining results are assessed under the approved decision rule.
Occurrence cause	Fixture datum was reset incorrectly during maintenance; the setup allowed an undetected offset.

Step	Recorded result
Escape cause	Maintenance event classification did not generate the mandatory metrology hold; production release checked only calendar calibration status.
Correction/disposition	Restore and verify fixture datum; disposition 8 nonconforming items through authorized technical review; record customer actions and remeasurement evidence.
Corrective action 1	Interlocked reference verification required after the relevant maintenance event before measurement results can support release.
Corrective action 2	Maintenance classifications and release checks revised; challenge test confirms that a missing check blocks release.
Corrective action 3	Review similar fixtures and maintenance workflows; extend controls to two additional affected process families.
Effectiveness plan	Independently observe the next 10 relevant maintenance events and 100 post-maintenance measurements; verify hold behavior and measurement validity.
Example effectiveness outcome	All 10 events generated the required hold and valid reference check; 100 independent comparisons met the pre-approved method criterion; no bypass observed.
Closure and limitation	Technical and quality reviewers approve closure; continued trend monitoring remains active. The sample does not prove recurrence is impossible.

Table AA-1 — AF conformity objects and decision boundaries

Source p. 103 | Required structure when applicable

Route / object	Applicable evaluation basis	Permitted conclusion and boundary
ORG — Organization	Clauses 1-10 and 22; triggered 11-21 and 23-28; organizational implementation and outcomes.	Defined management and assurance system. Does not approve every product or certify every employee.
PRD — Product / system	Clause 23; product profile; relevant technical, qualification and acceptance requirements; controlled production where ongoing.	Identified product, configuration, family, lot or serial against stated criteria. No implied statutory approval.
SVC — Service	Clause 24; defined outcomes, delivery boundary, period, interfaces, competence and continuity.	Specified service or service event, not an unrestricted approval of the provider's other services.
PRC — Process	Clause 25; relevant Annex L; essential variables, qualification, scope, monitoring and output relationship.	Process capability within the qualified conditions. Not automatic acceptance of all output.
PER — Person	Clause 26 and Annex AE; approved job profile; Annex AB for assessment-role credentials.	Demonstrated competence for a defined role. Employer task authorization and required licenses remain separate.
SUB — External provider	Clause 27; Annexes J and AF; actual site, supplied work and sub-tier controls.	Qualification for a defined supply scope. Conditional development status is not a conformity certificate.

Route / object	Applicable evaluation basis	Permitted conclusion and boundary
CAB — Assessment provider	Clause 28 and Annex AH; role-specific competence, methods, witnessing, impartiality and independent decisions.	Defined assessment capability under actual AF authorization. ORG certification is not accreditation.

Table AA-2 — Minimum profile fields

Source p. 103, 104 | Required structure when applicable

Field group	Required information
Identity and ownership	Profile ID, revision, route, owner, technical approver, issue date and affected claims.
Object and domain	Exact object/configuration, sites, relevant users, operating or task conditions and exclusions.
Obligations and criteria	Requirement IDs, quantitative limits or defined attributes, legal and customer constraints, essential controls.
Evaluation design	Methods, test conditions, samples, representativeness, uncertainty, validity checks, required independence.
Decision	Pre-agreed passing rules, critical failures, treatment of unavailable evidence and nonconformities, decision authority.
Continuing basis	Surveillance, expiry or instance boundary, change triggers, renewal and retained support obligations.
Records and claims	Required reports, retention, authorized public statement, privacy and mark restrictions.

Table AB-1 — Minimum entry evidence for assessment roles

Source p. 106 | Required structure when applicable

Role	AF entry and demonstration requirements	Authorization limitation
Internal auditor	Task-relevant experience; at least 16 hours of AF/process-audit learning; one complete witnessed internal audit; satisfactory evidence-based reporting.	May audit internally within demonstrated competence; shall not independently audit their own work.
Third-party auditor	At least three years of relevant professional experience, including two years in quality, assurance or the intended technical domain; at least 40 hours of AF audit training; knowledge and practical assessment under AB.2; four mentored complete audits totaling at least 20 auditor-days.	Independent assignments only after witnessed approval and defined route/sector authorization.
Lead auditor	Qualified third-party auditor; additionally three complete audits led under supervision totaling at least 10 auditor-days; demonstrated planning, team direction, conflict handling and integrated reporting.	May lead only within authorized scope; technical gaps require participating specialists.
Technical expert	At least three years of relevant technical practice, normally including two years within the preceding five; verified task demonstration and sufficient AF scheme orientation.	Provides technical conclusions; not automatically an auditor or independent decision maker.

Role	AF entry and demonstration requirements	Authorization limitation
Technical reviewer	Demonstrated AF interpretation and evidence-review competence; technical coverage for the assigned scope; five satisfactorily mentored complete file reviews.	Shall not independently review an evaluation they performed. May combine review and decision if separately authorized.
Decision maker	Verified knowledge of routes, scope, decision rules, impartiality, status and appeals; five satisfactorily mentored complete conformity decisions; access to required technical expertise.	Shall not have performed the evaluation being decided or supplied the relevant consultancy.
Application / appeal reviewer	Demonstrated competence for scope determination and resource review / fair case analysis, AF requirements and independence; observed satisfactory performance.	Appeal reviewer shall be independent of the original evaluation and decision.

Table AC-1 — Base initial organizational evaluation time

Source p. 109 | Required structure when applicable

Effective personnel N	Base B(N), auditor-days	Application
1-10	2.0	Readiness and implementation evaluation combined, before modifiers.
11-25	3.0	Same scope and time definition.
26-75	4.0	Same scope and time definition.
76-150	5.0	Same scope and time definition.
151-300	7.0	Same scope and time definition.
301-600	9.0	Same scope and time definition.
Above 600	$9 + \text{ceil}((N - 600)/300)$	Add one base auditor-day for each additional block of up to 300 effective personnel.

Table AD-1 — Illustrative DR-A outcomes for the Annex H example

Source p. 113 | Illustrative or explanatory source table

Corrected result y, mm	Expanded uncertainty U, mm	Outcome under the stated example rule
50.0240	0.00444522	Conformity demonstrated: the full interval is inside [49.970, 50.030] mm.
50.0280	0.00444522	Indeterminate: nominal result is inside the specification, but the interval overlaps the upper limit. Hold acceptance.
50.0360	0.00444522	Nonconformity demonstrated under DR-A: the full interval is above the upper limit.

Corrected result y, mm	Expanded uncertainty U, mm	Outcome under the stated example rule
50.02555478	0.00444522	Upper interval endpoint equals 50.03000000 mm: inside the inclusive limit using these stated numbers. Actual decisions use unrounded inputs.

Table AD-2 — Finding categories and minimum consequences

Source p. 113, 114 | Required structure when applicable

Class	Decision definition	Required consequence
Critical	Evidence of an uncontrolled unacceptable safety/mission risk, deliberate material falsification, serious compromise of essential evidence, or another condition requiring immediate protection.	Stop or contain the affected activity immediately. Block grant/renewal. For an existing affected attestation, suspend or impose an effective evaluated restriction without delay; apply Annex AG notifications.
Major	Absence or breakdown of a required control, or a group of deficiencies, materially undermining the ability to fulfill requirements; not necessarily an immediate hazard.	Block initial grant/renewal/extension until verified closure. Assess existing scope promptly; suspend when continuing conformity cannot be demonstrated.
Minor	Localized failure to fulfill a requirement where evidence does not show a material system breakdown or loss of essential control.	Correct and address cause. No open minor at initial grant, renewal or extension. Existing status may continue only under the bounded AD.8 decision.
Observation / improvement	No demonstrated failure of an applicable requirement; a documented possibility to improve effectiveness.	May support improvement. Shall not be used to conceal nonconformity or require uncontracted consultancy.

Table AG-1 — Controlling AF scheme intervals and deadlines

Source p. 120 | Required structure when applicable

Activity / status	Maximum interval or deadline	Decision condition
Ongoing ORG, PRD-family, SVC, PRC, SUB or CAB attestation	24 months from the conformity decision	Renewal decision completed before expiry; no automatic extension. Route-specific instance limits remain separate.
PER credential	24 months from the conformity decision	Continued competence and renewal under Annex AE.
Employer task authorization review	12 months	Earlier reassessment after change, inactivity or adverse evidence; not a statutory license period.
C0/C1 ongoing surveillance	12 months between decision/last surveillance and next completed surveillance	First surveillance completed no later than 12 months after initial decision.

Activity / status	Maximum interval or deadline	Decision condition
C2/C3 ongoing surveillance	6 months between decision/last surveillance and next completed surveillance	First surveillance completed no later than six months after initial decision; relevant critical-control sites included.
Corrective-action plan for a nonconformity	30 days after finding notification	Immediate protection is separate; initial grant and renewal still require actual closure.
Major nonconformity verified closure	60 days after finding notification	No presumption of continued status during correction; AD.8 controls suspension or evaluated restriction.
Minor nonconformity verified closure	90 days after finding notification	Bounded continuation only for an existing attestation under AD.8.
Critical concern: protective action	Immediately upon recognition	Stop/contain the affected work; do not wait for an administrative deadline.
Holder notification to its scheme operator of a critical attestation-related concern	Within 24 hours after awareness	Earlier legal/customer notification duties still apply; continue updates as scope becomes known.
Operator action on a substantiated critical concern	Suspend or impose an effective evaluated restriction within 24 hours	The decision cannot wait for root-cause completion. Notify AF where AF authorization is involved.
Registry update after a status decision	Within two days	Holder informed immediately; public record accurately identifies affected scope.
Suspension duration	90 days from suspension decision	Restore on verified evidence, formally restrict to a demonstrably unaffected scope, or withdraw; no rolling reset.
Final evaluation report	14 days after evaluation close	Exceptional delay communicated under AC.7; protection and finding clocks unaffected.
Complaint/appeal acknowledgement	Five days after receipt	Assign case and provide process information.
Appeal submission	30 days after notification of the contested decision	A justified exceptional late submission may be admitted under AI.3.
Ordinary complaint/appeal determination	60 days after receipt	Necessary exceptional extensions require reasons and progress communication at least every 30 days.

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.