



AF-SM-9200-001

Safety and Operational Assurance Manual

Space / Aviation / Defense

FIRST EDITION

AF 9200 SUPPORTING DOCUMENT

Document identity and use

Field	Declared position
Code	AF-SM-9200-001
Title	Safety and Operational Assurance Manual
Family	Manuals
Organization	Aerospace Federation
Edition	FIRST EDITION
Relationship	Supporting material for AF 9200 - Aerospace Safety & Operational Assurance
Status	Prepared for publisher review; approval and effective dates not assigned
Language	English master text

Use and precedence

The AF 9200 standard contains the proposed requirements. This supporting document supplies guidance, model controls or records within its stated purpose. Complete the local scope, parameters, roles and authority before operational use. A completed template does not establish conformity or permission.

Applicable legal and competent-authority obligations remain independently binding. No AF recognition, accreditation, statutory approval or operational authorization is created by this document. Codes in this set are proposed identifiers for the newly prepared supporting collection.

Record completion

Where fillable fields are provided, use a PDF reader that supports interactive forms. Blank fields remain unresolved. Attach controlled evidence by identifier where space is insufficient. Typed names are not certificate-based digital signatures. Preserve the completed record and its history under the local retention rules.

Implementation control	Allocation
Responsible function	Safety-system owner
Primary AF 9200 anchors	0-28; Annexes A-R, Y
Catalogue	AF-ML-9200-001; coverage: AF-CM-9200-001

Contents - clauses and annexes

Entries are clickable. PDF bookmarks also locate subclauses and technical examples. Page numbers refer to this file.

1 Manual purpose and local adoption	4
2 Procedure P01 - Scope, obligations and planning	5
3 Procedure P02 - Hazard identification and risk control	6
4 Procedure P03 - Evidence and safety-case review	7
5 Procedure P04 - Operational readiness and release	8
6 Procedure P05 - Execution, impairment and handover	9
7 Procedure P06 - Emergency, recovery and restart	10
8 Procedure P07 - Management of change	11
9 Procedure P08 - Reporting, investigation and corrective action	12
10 Procedure P09 - Suppliers and shared services	13
11 Procedure P10 - Monitoring, audit and management review	14
12 Procedure P11 - Records, access and recovery	15
13 Local adoption and validation	16

1 Manual purpose and local adoption

This model manual defines the operating processes needed to implement AF 9200. It is a supporting document, not evidence that an organization has already implemented the system. Before use, the organization shall complete its local scope, roles, authorities, criteria and record locations through AF-TP-9200-001 and approve the resulting local procedure baseline.

The manual uses role names rather than invented individual appointments. The local authority schedule shall identify actual eligible people and deputies. A combined role is permitted only where competence and required independence are preserved.

Table MN-1. Process ownership

Role	Retained responsibility
Accountable executive	Resources, policy, authority, systemic conflict resolution and executive risk decisions
Safety-system owner	Programme coordination, hazard register, performance and escalation
Technical authority	Technical criteria, control adequacy, configuration and evidence acceptance
Operational owner	Planning, readiness, execution, monitoring and protective action
Independent reviewer	Competent challenge and finding closure within assigned scope
Record custodian	Identity, access, history, retention and recovery of records
Assessor/decision authority	Evaluation and bounded conformity conclusions where authorized

2 Procedure P01 - Scope, obligations and planning

Trigger: New activity, new site, major change, revised responsibility or scheduled scope review.

The operational owner describes the object, lifecycle, configuration, environment, exposure and interfaces. The safety-system owner maps activities to AF 9200 and identifies retained outsourced duties. Technical authorities identify obligations, safety objectives and necessary methods. The accountable executive confirms resources and resolves responsibility gaps.

Table MN-2. P01 control points

Step	Owner	Output
Define actual activity	Operational owner	Scope and system description
Determine applicability	Safety-system owner with technical authorities	Clause and module matrix
Establish criteria	Technical authority	Completed AF-TP-9200-001 parameters
Assign work and gates	Programme owner	Safety programme and evidence schedule
Approve baseline	Eligible local authority	Controlled scope, profile and plan

Exit: The scope and decision criteria are sufficiently complete to support analysis. Any unresolved essential boundary remains HOLD. Records: AF-TP-9200-001, local obligation register and safety programme.

3 Procedure P02 - Hazard identification and risk control

Trigger: Initial analysis, changed state, occurrence, new evidence or periodic review.

The safety-system owner convenes competent participants from design, operations, maintenance, suppliers and human performance as relevant. The team examines functions, states, transitions, energy, data, human tasks and shared services. It records scenarios and uncertainty without replacing causes with generic labels.

The technical authority allocates verifiable requirements and selects controls. Control owners define performance standards and verification methods. The analyst evaluates residual risk using the approved profile, preserving common causes and uncertainty. The eligible authority accepts residual risk only after required controls and evidence are established.

Table MN-3. P02 hold conditions

Condition	Required response
Essential hazard owner absent	Escalate ownership and protect affected activity.
Risk criterion missing	Complete and approve the profile before acceptance.
Credited control unverified	Remove credit or complete verification.
Independence assumption unsupported	Reanalyze dependency and controls.
Severe uncertainty remains unbounded	HOLD or demonstrably protective restriction.

Records: AF-FR-9200-001 to AF-FR-9200-004. Exit: Each significant scenario has a maintained control and decision basis; open actions remain linked to blocked transitions.

4 Procedure P03 - Evidence and safety-case review

Trigger: Lifecycle gate, operational release basis, significant change or challenged claim.

The evidence producer identifies the method, configuration, raw source, competence, equipment, uncertainty and intended purpose. The technical reviewer accepts, rejects or limits the evidence. The safety-case owner explains the relationship between claims and evidence using AF-IG-9200-002.

The independent reviewer challenges completeness, assumptions, common causes, human reliance, test representativeness and recovery. Findings are recorded against specific claims or requirements. The author proposes correction; the eligible reviewer verifies closure. The decision authority records the bounded conclusion and unresolved limitations.

Exit: The case supports the intended transition, or its unsupported portions remain explicitly HOLD/FAIL. A review signature alone is insufficient without the technical disposition. Records: Evidence acceptance, claim register, independent review and decision record.

5 Procedure P04 - Operational readiness and release

Trigger: Each operation or each execution covered by a standing authorization.

The operational owner verifies the actual configuration, personnel, equipment, environment, interfaces, residual-risk acceptance and emergency capability. Variable conditions are checked for each execution. Temporary controls and deferred defects are reviewed together.

The release authority confirms that every prerequisite and no-go condition is resolved. The record states the permitted activity, restrictions, duration or completion condition, monitoring roles and invalidation triggers. Personnel receive the applicable instructions and handover information before exposure begins.

Table MN-4. Operational decision rules

Result	Action
All prerequisites met	Release within the defined envelope.
Narrower separable activity fully supported	Issue explicit restricted release.
Essential evidence or authority incomplete	HOLD affected activity.
Active unsafe condition	Stop or enter the defined protective state.
Activity complete	Record resulting state and continuing obligations.

Records: AF-FR-9200-005 and AF-FR-9200-006. Exit: A current authorized decision is available at the point of use.

6 Procedure P05 - Execution, impairment and handover

During execution, assigned personnel monitor the envelope and barrier health. Any exceedance, abnormal behavior or loss of monitoring is assessed immediately against the predefined protective rules. Personnel may raise a good-faith safety concern and request a pause without retaliation.

A barrier impairment is recorded with time, affected scenario, remaining controls, immediate protection and responsible owner. Continued operation requires a valid decision for the actual degraded state. An expired temporary control cannot be renewed by silence.

At handover, the sender and receiver reconcile configuration, work in progress, hazards, restrictions, bypasses, pending decisions and monitoring duties. Unclear responsibility remains with the current accountable owner until a valid transfer is confirmed; urgent protective action is not delayed by administrative disagreement.

Records: Barrier impairment, operational log and handover. Exit: The operation remains within a supported state or is protected and escalated.

7 Procedure P06 - Emergency, recovery and restart

Trigger: Emergency condition, protective stop, major disruption or loss of an essential service.

The designated command role initiates the emergency plan, protects life, controls the hazardous state and coordinates assistance. Evidence collection follows when safe. The response uses the approved communication and command succession arrangements, including alternate channels.

The recovery owner defines the target state, restoration sequence, inspections, tests, data reconciliation, personnel readiness and external clearances. A competent reviewer checks that the initiating defect and restoration-induced hazards are addressed. Restart requires a fresh release decision.

Table MN-5. Restart prerequisites

Prerequisite	Evidence
Hazard controlled	Cause addressed or uncertainty bounded with justified protection
Configuration restored	Actual baseline verified
Barriers effective	Inspection and test results current
People and support ready	Competence, staffing, services and emergency capability
Records reconciled	Correct status, restrictions and evidence history
Authority valid	Required local and external permissions

Records: Emergency log, recovery dossier and restart release. Exit: Verified safe and usable condition with current authorization.

8 Procedure P07 - Management of change

Trigger: Any change that can affect a hazard, control, assumption, evidence or authority condition.

The change owner describes the old and proposed baselines. Technical and operational owners identify the impact set, including people, suppliers, interfaces and transition states. The reviewer evaluates concurrent temporary conditions and rollback feasibility. Required approvals precede live implementation.

Verification demonstrates the changed behavior. The implementation record identifies actual configuration and completed training. Enhanced monitoring checks the assumptions during stabilization. The change closes only when its acceptance and effectiveness criteria are satisfied.

Records: AF-FR-9200-007 change dossier and updated profile, hazard register, safety case and release.

Exit: The actual changed state has a supported assurance basis.

9 Procedure P08 - Reporting, investigation and corrective action

Trigger: Occurrence, near miss, hazard report, evidence concern or repeated weak signal.

The intake owner preserves the report and triages potential consequence, urgency, containment and notifications. The investigation authority assigns competent independent investigators. Analysis examines technical, human, organizational, interface and assurance conditions, preserving alternative hypotheses and uncertainty.

Action owners implement corrections and systemic measures. The verifier distinguishes implementation from effectiveness and reviews similar exposure. The safety-system owner updates affected hazards, controls, competence and procedures and provides feedback to reporters where permitted.

Records: Occurrence, investigation, action and effectiveness records. Exit: Verified learning and control improvement; residual limitations remain visible.

10 Procedure P09 - Suppliers and shared services

Before reliance, the commissioning owner defines safety requirements, evidence, interfaces, change notifications and access. Technical acceptance confirms applicability to the actual configuration. The supplier owner monitors changes, performance, escapes and support continuity.

A supplier escape triggers affected-population analysis and review of prior decisions. Commercial acceptance does not replace safety acceptance. Where evidence is proprietary, an authorized competent review route is required; an inaccessible assertion is not accepted as proof.

Records: Supplier qualification, interface agreement, acceptance and surveillance records. Exit: Essential outsourced dependencies remain supported and owned.

11 Procedure P10 - Monitoring, audit and management review

The safety-system owner maintains an indicator dictionary and validates data quality. Thresholds trigger assigned responses. Internal assurance samples actual operations, adverse cases, changes and outsourced interfaces. Findings remain linked to requirement states and affected operational decisions.

Management reviews control effectiveness, resources, competence, reporting culture, significant changes, overdue actions and the validity of continuing acceptance. Decisions identify owners, resources, deadlines and effectiveness checks. The organization verifies that the assurance system itself can detect material deficiencies.

Records: Performance review, audit findings and management-review actions. Exit: Current decisions and funded corrective priorities.

12 Procedure P11 - Records, access and recovery

The record custodian maintains unique identities, compatible configurations, authorized states, access rights and immutable history appropriate to the system. Authors, reviewers and approvers remain distinguishable. Retention follows the approved profile and applicable obligations.

Automated workflows are tested for prohibited transitions, expired authority, missing links, concurrent edits and recovery. Backup restoration is followed by semantic reconciliation of record identity, relationships, states and restrictions. Operational use resumes only after the required recovery decision.

13 Local adoption and validation

The organization shall record the scope of adoption, completed profile, assigned roles, local procedure identifiers, trained personnel and first-case validation. This supporting manual is not itself local approval. Uncompleted local criteria remain HOLD, and no approval or recognition by Aerospace Federation is implied by use of the model.