



AF-FAQ-9500-001

Interpretation Questions and Boundary Cases

Space / Aviation / Defense

FIRST EDITION

AF 9500 SUPPORTING DOCUMENT

Document identity and use

FIRST EDITION MANUSCRIPT - Prepared for Aerospace Federation review

Field	Controlled identity
Document	AF-FAQ-9500-001 - Interpretation Questions and Boundary Cases
Parent standard	AF 9500 - Aerospace Digital Systems, Software & Cybersecurity
Edition / language	FIRST EDITION / English master text
Family	Companions
Primary source anchors	0-40; informative Annex S
Suggested local owner	Technical authority
Authority	Publisher approval and effective date are not assigned. Local use requires authorized adoption and completed parameters.

Use with the main standard

This document implements the identified AF 9500 clauses and annexes. Read the complete applicable requirements in the main standard. The source anchors are navigation references; a template does not replace technical judgement, evidence, permission or eligible approval.

AF-ML-9500-001 lists the complete supporting set. AF-CM-9500-001 maps the main clauses and annexes to working documents. AF-TP-9500-001 establishes the common local parameter baseline; add the relevant discipline profiles.

Record control

Identify the object, configuration, record owner and dates. Reference attachments by stable identifier and version. Keep superseded evidence and decisions traceable. Use the approved local retention, access and authentication arrangements. No technical limit, numerical limit, interval or acceptance value is assigned by a blank template.

Implementation model: Translate the stated responsibilities and controls into the actual organization. Informative examples remain explanatory; use approved programme-specific values for operational decisions.

1 Use of this companion

This companion explains recurrent interpretation questions. Answers do not waive applicable requirements or supply missing programme parameters. Read the exact source clause before making a decision.

2 Questions and decision boundaries

Status: Informative. Answers explain recurring boundaries and do not supply missing local parameters or waive applicable requirements.

1 Does a valid signature make software safe?

No. It supports a defined authenticity claim under the trust policy. Correct behavior, target compatibility, current signer authority and permitted use require separate evidence.

2 Does 100% code coverage prove correctness?

No. Executed code may still implement an incorrect requirement or produce a wrong result. Coverage needs valid requirements-based tests, meaningful expected outcomes and review of uncovered or excluded behavior.

3 Can an SBOM establish absence of vulnerabilities?

No. It identifies components and relationships within its declared scope. Completeness, vulnerability applicability, configuration and ongoing threat information require separate assessment.

4 Can an urgent patch bypass safety checks?

Urgency changes response priority, not the need for eligible authority and a justified technical transition. Interim restrictions and compensating controls may be necessary while a safe update route is established.

5 Is fail-closed always the secure answer?

The required protective behavior depends on consequence and operating mode. Blocking access can itself remove an essential control function. The safety-security interaction must be assessed and verified.

6 Does restoring a backup close an incident?

No. Trust, persistence, identities, data relationships, pending actions and affected outputs must be assessed. Return to service and incident closure are distinct decisions.

7 Can a generic vulnerability score decide aircraft operation?

It is one input. Actual installed state, exposure, functional effects, protective controls, uncertainty and operating authority determine the bounded decision.

8 Does a cloud provider's approval cover our application?

No. The configured service and retained user responsibilities require evidence. Application behavior, identity, data, integration and recovery may remain the customer's duties.

9 Does a human reviewer make an AI function acceptable?

Only when the reviewer's information, competence, time, workload and ability to intervene are demonstrated for the relevant conditions. Nominal human presence is not an effective safeguard by itself.

10 Can old software remain in service without source code?

Only within a justified continued-use argument that addresses evidence limitations, current exposure, support, controls and withdrawal conditions. Previous successful operation alone is insufficient.

11 Can an agent approve its own deployment?

Only authority explicitly established in a validated workflow can permit an action, and required independent or human decisions remain mandatory. A generated completion message cannot grant new authority.

12 Does this set confer AF recognition or operating permission?

No. Publication, organizational adoption, technical acceptance, recognition and operating permission are separate decisions made by their eligible authorities on the required evidence.