



AF-HB-9300-002

Digital Test Evidence and Records Manual

Space / Aviation / Defense

FIRST EDITION

AF 9300 SUPPORTING DOCUMENT

Document identity and use

FIRST EDITION MANUSCRIPT - Prepared for Aerospace Federation review

Field	Controlled identity
Document	AF-HB-9300-002 - Digital Test Evidence and Records Manual
Parent standard	AF 9300 - Aerospace Testing, Verification & Qualification
Edition / language	FIRST EDITION / English master text
Family	Manuals
Primary source anchors	6, 10-12, 15, 17, 26, 29-32; Annex H
Suggested local owner	Data owner
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 9300 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-9300-001 lists the complete supporting set. AF-CM-9300-001 maps the main clauses and annexes to working documents. AF-TP-9300-001 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 Keep superseded evidence and decisions traceable.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 test level, 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 Define the evidence object

The evidence package is more than the measured values. It includes object and article identity, requirement and method baselines, facility and fixture configuration, channel map, timestamps, units, validity states, event log, software and processing versions, raw files, derived outputs, review and decisions. Assign a stable package identifier and owner.

1.1 Record relationships and states

Use AF-RG-9300-008 to relate each run, article, requirement, anomaly, processing result and report. Distinguish planned, executed, incomplete and invalid execution from accepted evidence and from PASS, FAIL, HOLD or approved N/A. A single database status field shall not silently collapse these different decisions.

1.2 Baseline and access design

Approve naming, object identifiers, roles, change records and retention values. Protect native observations against unrecorded alteration. Permit controlled correction without erasing the original. Separate user authority to acquire, transform, review and issue where required by the programme's independence rules.

2 Configure and validate acquisition

2.1 Channel and time design

Use AF-FR-9300-008. Identify physical input, sensor, conditioning, range, correction, units, sign, sample rate, anti-aliasing, synchronization and expected bandwidth. State absolute and relative timing needs. Preserve clock adjustments and discontinuities. Document channel validity when clipping, dropout or saturation occurs.

2.2 End-to-end challenge

Stimulate or otherwise verify the complete chain with a suitable known input. Check scaling, polarity, cross-channel identity, timing and failure behavior. Demonstrate what happens to missing input, over-range, full storage, interrupted power and network loss as applicable. Do not assess a chain solely from a nominal software setting.

2.3 Configuration at execution

Capture the released channel map, software, firmware, script and parameter versions before the run. Reconcile the actual configuration and article at start. Changes during execution are event records with their time, authority and impact. A restart uses the new actual baseline and an appropriate release.

3 Preserve raw evidence and derive results

3.1 Acquisition closeout

Use AF-WI-9300-006. Complete the event log; verify expected file count, duration, identity, sizes and available integrity checks. Identify partial files rather than silently treating their absence as no event. Transfer through the approved route and verify the receiving copy before disposition of the acquisition source.

3.2 Processing lineage

Store processing code or executable identity, dependencies, parameters, units, corrections, exclusions and output references. Explain filtering, resampling, alignment and interpolation where they affect a conclusion. Preserve the mapping from each reported value to the raw data and relevant time interval. Uncertainty includes relevant processing effects.

3.3 Controlled exclusions and missing data

For each excluded sample or interval, retain the selection rule and technical reason. Predefined rules are preferable; later changes require review for selective bias. Mark invalid and unknown data distinctly from measured zeros. A missing channel cannot become PASS through a default software branch.

4 Review, recovery and incidents

4.1 Technical reproducibility

An eligible reviewer checks the object, criteria, units, conditions and data route, then independently reproduces material results or performs an equivalent effective challenge. Use AF-FR-9300-013 and AF-WI-9300-009. Confirm that the implemented decision rule handles equality, rounding, invalid input and uncertainty as approved.

4.2 Recovery demonstration

Recover a representative complete package in a controlled location. Verify file content and the links among article, run, requirement, anomaly, report and approval state. Confirm access permissions and that superseded data are not promoted to current status. Record discrepancies and approve recovery only for demonstrated capabilities.

4.3 Integrity or security event

Restrict affected evidence, preserve logs and identify the time/configuration/population potentially affected. Evaluate whether the event changes observations, attribution, processing or decision state. Notify eligible owners of dependent reports and claims. Restore reliance only after technical validity and records relationships are demonstrated.

5 Reports, amendments and retention

5.1 Report package

Use AF-FR-9300-019 and AF-RG-9300-012. Each issued report identifies its evidence package, scope, limitations and issue authority. Store the exact issued representation. Receiving recipients must be able to distinguish current, amended, superseded and withdrawn issues without losing historical traceability.

5.2 Amendment

State what changed, why, which result or conclusion is affected, who approved the change and which recipients require notice. Re-evaluate dependent qualification or acceptance decisions where needed. A corrected document must not imply that the earlier issue never existed.

5.3 Retention and disposal

Apply locally approved retention periods and triggers rather than a universal duration. Consider unresolved disputes, investigations, live claims and contract duties before disposal. Test retrievability during retention and after platform migration. Record eligible disposal authority and the exact scope removed.

6 Adoption and practical implementation

Start with a single representative campaign. Build its evidence graph using stable IDs and approved record states, then test acquisition failure, processing error, report amendment and restore scenarios. Resolve weaknesses before scaling the workflow. Train operators on contemporaneous recording and analysts on traceable transformations; train reviewers to challenge relationships as well as individual files.

Required evidence: Data plan, validation challenges, native package, transformation lineage, recovery tests, access/change history, review, exact report issue, amendment notifications and approved retention/disposal decisions.

Decision control: An intact file whose origin, configuration, meaning or approved state is unknown remains insufficient for the affected technical conclusion.