



FIRST EDITION / CORPORATE GOVERNANCE

REMOTE ASSESSMENT POLICY

Aerospace Federation

TRUSTED DIGITAL EVIDENCE

VALIDATED REMOTE METHODS

INDEPENDENT HUMAN DECISIONS

Publication identity and use

Control field	Controlled value
Title / document code	Remote Assessment Policy / AF-PL-015
Edition / revision / language	First Edition / Revision 00 / English master text
Edition date	30 September 2026
Document owner	Assurance Programme Manager
Operating interface	P06-P08 and P17; other approved evaluation activities
Publication type	Corporate and scheme delivery policy
Scope	The whole AF federation and its relevant delivery, oversight and partner interfaces.
Approval and effective use	Record the actual competent approval, effective date and implementation conditions in AF-FR-001 and AF-ML-001.
Relationship to existing files	Separate expanded publication. Existing AF documents and the final AF 9100:2026 files are not silently replaced or amended.

Authority. AF-CON-001 controls governance when lawfully operative; mandatory law and controlling formation instruments remain superior. Applicable technical standards and AF-SR-001 control their own assessment scope. This publication implements those boundaries, not a new public regulatory power.

Reading rule. Shall denotes an AF requirement after valid adoption; should denotes guidance; may denotes permission. Annexes specify whether their controls are mandatory, model records or informative examples. A blank form is not an executed approval.

Source distinction. The final annex identifies inherited AF requirements, new operating detail and implementation dependencies. New controls are authored for this publication; they are not represented as rules already adopted in earlier files. Completed examples, where used, are synthetic.

Contents

Section	Page
1 Purpose and remote-assessment commitment	4
2 Authority, hierarchy and effective use	4
3 Definitions and assessment modes	4
4 Responsibilities and independent decisions	5
5 Eligibility and the remote-method decision	5
6 Risk, consequences and mandatory physical evidence	6
7 Agreement, participant information and fair access	6
8 Personnel competence, independence and local support	7
9 Platform, endpoint and provider controls	7
10 Technical rehearsal and readiness	8
11 Assessment planning, time and site coverage	8
12 Identity, liveness and evidence integrity	9
13 Execution, interviews and technical witnessing	9
14 Recording, data minimization and confidentiality	10
15 Interruptions, integrity concerns and safe resumption	11
16 Findings, supplementary work and decision readiness	11
17 Reporting, notification and public claims	12
18 Surveillance, change and reliance on earlier evidence	12
19 Future technology and inaccessible environments	12
20 Monitoring, audit and public-benefit review	13
Annex A — Remote feasibility and go/no-go record	14
Annex B — Activity and evidence matrix	15
Annex C — Plan, rehearsal and session record modules	16
Annex D — Interruptions, incidents and supplementary work	17
Annex E — Worked resource and coverage calculations	18
Annex F — Independent review and decision-readiness checklist	19
Annex G — Future-method validation and performance review	20
Annex H — Source alignment and implementation record	21

Clause and annex numbers are the controlling references. Page numbers identify the beginning of each section.

1 Purpose and remote-assessment commitment

1.1 Evidence equivalence, not reduced requirements

AF may use remote and hybrid assessment methods where they provide sufficient trustworthy evidence for the specific requirement being evaluated. Location and technology shall not lower competence, independence, technical criteria, required witnessing, scope coverage or decision safeguards. A video call, document upload or functioning platform is not by itself a completed assessment.

1.2 Whole-federation scope

This policy covers remote elements of internal audit, recognition, accreditation, conformity evaluation, supplier assessment, personnel and learning assessment, and other approved reviews within the AF portfolio. It includes relevant corporate, regional, partner and outsourced delivery. Aviation, space, all defense-industrial domains, heavy and advanced industry, and defense- or space-purpose mobility remain within the Federation's remit.

1.3 Distinct activities remain distinct

An online committee meeting is not a technical assessment. A webinar is not a personnel certification examination; a grant review is not accreditation; a remote tour is not laboratory witnessing. Ordinary meetings retain their own quorum and voting rules. A program shall identify its actual output, authority and criteria before applying this policy to its remote evidence process.

2 Authority, hierarchy and effective use

2.1 Controlling AF instruments

AF-CON-001 controls governance, independent decisions, protected information and public claims when lawfully operative. AF-SR-001 Clauses 15–19 and 24–28 control applicable assurance cases. AF 9100:2026 retains its own Annexes AA–AJ and all triggered technical requirements. Corporate procedures govern the remaining processes. Mandatory law and actual controlling instruments prevail.

2.2 No amendment by modality

This policy does not reopen the finalized AF 9100 files, reduce their audit-time or site-coverage floors, extend validity, change examination thresholds or waive an essential technical observation. It provides the remote delivery controls supporting existing obligations. A genuine conflict shall be recorded and the affected claim held until resolved through the appropriate formal process.

2.3 Source distinction and adoption

Inherited AF requirements and new remote operating detail are identified in Annex H. The request to develop these detailed policies is not evidence of an executed approval or an active remote service. Before reliance, record the competent adoption, actual effective date, responsible operators, tested systems and implementation conditions in AF-FR-001 and AF-ML-001.

3 Definitions and assessment modes

3.1 Modes

On-site assessment uses an assessor physically present at the relevant activity. **Synchronous remote assessment** uses real-time communication and observation. **Asynchronous assessment** examines records or observations produced at another time. **Hybrid assessment** deliberately combines physical and remote methods. A remotely participating specialist and a local assessor are distinct assigned roles; neither shall be described as physically present where they were not.

3.2 Evidence and observation

Source evidence is the attributable original record or authoritative system record supporting the conclusion. **Witnessing** is competent observation of the required activity under a controlled method. **Liveness** is evidence that the observed activity or participant is present and current rather than a substituted recording. **Evidence equivalence** means fitness for the stated assessment purpose; it is not a blanket equivalence between all remote and on-site methods.

3.3 Completion, interruption and restriction

An activity is complete only when the required scope and evidence have been obtained and evaluated. A connection failure is an interruption, not proof of nonconformity. It may nevertheless prevent a favorable conclusion when necessary evidence remains unavailable. A restricted scope is legitimate only where its boundary is real and the remaining work is independently supportable; it shall not conceal a systemic failure.

4 Responsibilities and independent decisions

4.1 Program owner and assignment authority

The program owner shall identify permitted assessment modes, contractual access, applicable technical profiles, security requirements and the competent authority approving remote suitability. The assignment function shall verify personnel scope, currency, language, independence, lawful access and workload before assigning work. Commercial staff may explain options but shall not promise remote approval or remove necessary physical work to lower a fee.

4.2 Lead assessor and participating specialists

The lead assessor shall prepare the requirement-to-method plan, sampling, live observation and contingency arrangements; conduct the assessment; preserve evidence and limitations; and recommend the appropriate outcome. Specialists shall actively examine their assigned technical scope. A listed expert who did not participate cannot supply missing competence or retrospectively authenticate an observation.

4.3 Information, legal and safety functions

Information and security personnel shall approve the platform and evidence controls for the actual data and locations. The relevant legal or controlled-technology function shall confirm permissions and transfers. The local operator or host retains responsibility for safe physical work. An assessor does not become the equipment operator or acquire authority to command a mission merely by watching it remotely.

4.4 Reviewer and decision maker

The independent reviewer shall examine remote suitability, actual completion, provenance, sampling, competence, unresolved limitations and technical adequacy. The authorized decision remains independent of evaluation. Where AF-SR-001 requires a three-person accreditation decision panel, remote delivery does not change that requirement. Appeal reviewers remain independent of the original evaluation, review and decision.

4.5 Applicant, host and local witness

The applicant shall provide accurate scope, authorized participants, reliable evidence access and disclosure of restrictions. A host may operate a camera or retrieve records, but shall not select only favorable evidence, coach confidential interview answers or hide failed activities. A local witness contributing independent technical evidence shall have a verified assignment, competence, impartiality and report; the applicant's own camera operator is not automatically an independent witness.

5 Eligibility and the remote-method decision

5.1 Decide by requirement and task

Suitability shall be determined for each material task, not solely by organization size, location or an overall remote percentage. The plan shall identify which requirements can be assessed through documents, interviews, live observation, validated telemetry or local independent witnessing, and which require physical attendance. A general statement that the applicant is digitally mature is insufficient.

5.2 Essential feasibility gates

Before remote work, confirm lawful access, identity, information protection, competent personnel, suitable observation detail, representative scope, safe execution, reliable records and a viable interruption remedy. Annex A contains the gate record. A failed essential gate shall prevent the affected remote activity until corrected or moved to another valid mode. A score averaging these gates is not permitted.

5.3 Outcomes of suitability review

The documented decision shall authorize remote work for specified tasks, authorize a bounded hybrid plan, defer pending evidence or require an on-site/other valid method. It shall state limitations, conditions, approval identity and change triggers. It does not determine final conformity. The applicant shall receive understandable reasons and the relevant challenge route without a promise that every preference can be accommodated.

5.4 No universal remote allowance

This policy establishes no universal percentage cap or entitlement, automatic remote-only first assessment, country-based waiver or fee-based reduction. A fully remote assessment is permissible only where the complete required scope can lawfully and competently be evaluated that way under the controlling scheme. Where physical conditions cannot be adequately verified remotely, physical or other valid controlled witnessing is required.

6 Risk, consequences and mandatory physical evidence

6.1 Consequence and evidence risk

Review the highest credible consequence, novelty, configuration complexity, special processes, human factors, critical characteristics, prior findings, evidence fraud, access and data sensitivity. AF 9100 C0–C3 categories remain technical tailoring categories, not public-authority approvals. Corporate risk prioritization shall not dilute a safety or integrity failure by averaging it with low-risk work.

6.2 Physical and high-consequence activity

A physical special process, test, inspection or safety-critical operation requires observation capable of establishing the relevant variables and actual performance. A remote feed may support the task only where validated detail, continuity, context and competent witnessing are sufficient. If touch, access, field of view, instrumentation, environmental conditions or independent sample handling cannot be adequately established, obtain the necessary local/on-site evidence.

6.3 Exceptional access constraints

Travel restrictions, conflict, remote geography or inaccessible deployed systems may justify a different evidence plan, not assumed conformity or automatic certificate extension. Determine whether an authorized local assessor, protected review facility or validated technical method can close the actual gap. If not, defer, restrict, suspend or refuse as the applicable decision rules require.

6.4 No hazardous demonstration for the camera

Do not request unsafe fault insertion, bypassed interlocks, live unauthorized penetration testing, prohibited disclosure or operation beyond a permitted envelope to improve a remote view. Use a safe validated representative demonstration where the technical profile allows it and state its limits. The responsible operator may stop unsafe work; a stop shall not be punished as non-cooperation merely because assessment becomes less convenient.

7 Agreement, participant information and fair access

7.1 Agreed assessment arrangements

Before the activity, communicate the scope, criteria, modes, participants, dates and time zones, evidence access, tools, language, recording conditions, costs, interruptions, supplementary work, confidentiality and complaint route. Identify technical activities that may still require an on-site visit. A remote quote shall not imply that additional necessary evidence has been waived.

7.2 Privacy basis and recording permissions

The responsible data owner shall establish the actual lawful processing basis and notices. Consent, where required or chosen, shall be specific and meaningful; it is not a universal substitute for legal review. Recording, screenshots, transcription, biometric checks and third-party access require separate justification and controls. Do not bundle unnecessary publicity consent into necessary assessment participation.

7.3 Accessibility and alternatives

Consider captioning, interpretation, accessible documents, assistive technology, breaks, scheduling and suitable alternatives to unnecessary intrusive monitoring. An adjustment shall preserve the essential competence and evidence being assessed. A person shall not be disadvantaged merely because an equally valid lower-bandwidth or accessible arrangement is needed. Record reasons where an alternative cannot satisfy an essential criterion.

7.4 Candidate and employee protection

Explain who will observe, what information will be retained and how concerns may be raised. Avoid needless searches of private living spaces, collection of identity copies or monitoring of unrelated personal activity. For young or vulnerable participants, apply the actual safeguarding, supervision and permission arrangements. An assessment interest does not authorize surveillance unrelated to its scope.

8 Personnel competence, independence and local support

8.1 Existing competence requirements

Internal auditors retain the corporate minimum of relevant experience, at least 16 hours of audit learning and one satisfactory complete witnessed audit. Third-party, technical, examiner, reviewer and decision roles retain the applicable AF 9100 Annex AB, Annex AE and AF-SR-001 Annex F requirements. Remote skill is additional to technical competence, not an alternative to it.

8.2 Remote-method demonstration

Before independent remote assignment, personnel shall demonstrate suitable use of the approved platform, identity checks, evidence selection, confidentiality, live observation, interruption handling and reporting. This is a new operating requirement introduced here. The record shall identify actual observed competence and limitations; attendance at a platform demonstration alone is insufficient.

8.3 Assignment conflicts

Check current and relevant prior employment, consultancy, financial dependence and personal relationships. Apply the 24-month third-party exclusion where required by the controlling scheme, with continuing conflict review beyond that interval. It is not a prohibition on employees internally auditing other work. Do not let a person who designed the client's remote corrective solution independently certify its effectiveness where that compromises independence.

8.4 Host, interpreter and local witness controls

Identify hosts, camera operators, interpreters and witnesses and their relationship to the applicant. Interpreters shall preserve meaning and confidentiality without answering for the interviewee. A local witness shall report actual location, method, conditions, evidence and restrictions. Verify authorization to transfer the resulting information; an employment title or a nondisclosure agreement alone does not establish such permission.

9 Platform, endpoint and provider controls

9.1 Platform approval

Use a platform approved for the actual information classification, locations, participants and purpose. Review identity management, access permissions, encryption appropriate to the risk, session controls, data storage, logs, retention, subcontractors, support access, recovery and exit. Do not assume every consumer account has the controls of an approved enterprise configuration.

9.2 Session and endpoint configuration

Use attributable accounts, appropriate multifactor authentication for sensitive or privileged access, controlled invitations, restricted sharing and verified participants. Avoid public meeting links and shared privileged credentials. Configure recording, downloads, transcription, file transfer and AI assistants deliberately. The host shall prevent unauthorized late joiners or observer access to protected material.

9.3 Third-party and cross-border processing

Identify the assessor's, host's and relevant provider's access locations, storage locations and subprocessors where material. Review controlled-technology, privacy, contractual and security restrictions before transfer. Participation through an encrypted connection does not itself make a transfer lawful. A change of participant or hosting location shall trigger re-review where it affects permissions.

9.4 Separation from operational control

Remote assessment access should be read-only or otherwise limited to the verified task. Do not grant an assessor routine control of production machinery, aircraft, spacecraft, defense systems or safety-critical settings. Any separate authorized operational action requires its own competent operator, safe-work controls and permission; this policy does not supply them.

9.5 Supplier continuity and retirement

Record provider obligations for incidents, access withdrawal, data return and deletion. Material system, model, hosting or security changes require review. Decommissioned accounts and integrations shall be revoked while retaining required evidence. Critical evidence shall not depend on a private user account or an expired software subscription without an approved continuity arrangement.

10 Technical rehearsal and readiness

10.1 Representative pre-session test

Before consequential remote observation, test the actual or equivalent setup for identity, audio, video detail, document viewing, access, safe camera positioning, measurement legibility and permitted evidence capture. Include the bandwidth and lighting conditions likely during the task. A successful administrative call does not establish capability to witness a fine measurement or complex physical process.

10.2 Detail and measurement fitness

The rehearsal shall demonstrate that required characteristics, identifiers, displays, timestamps, environmental data and essential variables can be read and linked to originals. Zoom, frame rate, compression, glare and latency shall not conceal a condition that determines conformity. Do not prescribe a universal camera resolution or network speed as sufficient for every technical method.

10.3 Contingency test

Verify the fallback contact route, safe pause, alternative evidence access and reconnection procedure. Determine what must be repeated after a break in observation. Test restoration of necessary records rather than merely confirming a backup exists. An unresolved essential readiness failure prevents the affected assessment task from starting.

10.4 Readiness record

Record tested configuration, participants, locations, results, limitations and approval. Annex C provides the module. Rehearse again when the setup materially changes or performance is unreliable. A prior successful session for another method does not automatically establish the current method's readiness.

11 Assessment planning, time and site coverage

11.1 Requirement-to-method matrix

The plan shall map every applicable requirement or justified requirement group to a method, responsible assessor, location, evidence source, expected observation and completion criterion. Identify critical tasks separately. Plan backward and forward traces through actual outputs, source records, changes and complaints. Annex B provides route-specific prompts and Annex C provides the record.

11.2 Productive time

Use sufficient competent evaluation time. Travel savings do not establish a technical time reduction. Platform setup, avoidable connection waiting, breaks, commercial administration, final report production, independent review and decision remain separate from productive evaluation. Where concurrent assessors perform distinct necessary work, record their individual time; do not double-count the same task as fully productive for multiple observers without justification.

11.3 Applicable AF time floors

AF 9100 organizational assessments retain Annex AC's staffing, criticality, complexity, site/shift, stage, surveillance and renewal minima. Do not apply its headcount formula to a personnel examination, calibration or destructive test. Other AF-SR-001 recognition and CAB activities use an adequate task-based plan. Necessary follow-up and incomplete remote tasks require actual additional resources.

11.4 Sites and method families

Every included physical operating site shall be evaluated at initial grant and renewal under AF-SR-001. The physical or remote mode must be justified for its actual work; identifying an address on a call is not site evaluation. AF 9100 ORG surveillance alone may use its eligible homogeneous C0/C1 site-sampling provisions. Those provisions do not authorize omitted CAB method witnessing, unique processes or critical sites.

11.5 Representative scheduling

Include actual relevant shifts, operations, users, subcontractors and adverse cases. Do not accept a staged demonstration as routine production without identifying it. Where a permitted representative simulation is used, record its validity and remaining real-work evidence. An applicant may identify availability and safety limits but shall not control the evidence population solely to exclude unfavorable records.

12 Identity, liveness and evidence integrity

12.1 Participant and location authentication

Verify participant identity and role proportionately using trustworthy organizational or personal evidence and an independent confirmation route where needed. Confirm the actual location and function being assessed without collecting unnecessary personal information. Recheck a substituted host, witness, candidate or assessor before accepting their contribution.

12.2 Live observation safeguards

For live tasks, use proportionate methods such as a contemporaneous session reference, assessor-selected records or item identifiers, safe changes of viewpoint and correlation with original operating logs. These methods support but do not guarantee authenticity. A suspected prerecorded loop, substituted participant or synthetic feed requires a hold, corroboration and competent review; automated deepfake detection shall not be the sole decision basis.

12.3 Evidence manifest

Each accepted evidence item shall have an ID, source, actual creation or observation time, time zone where material, creator or custodian, object/configuration, method/version, transfer/access location, integrity reference and relevant limitation. Distinguish source originals, exports, extracts, translations, recordings and assessor notes. Preserve adverse and replaced versions with reasons.

12.4 Limits of digital proof

A hash proves consistency with a particular reference byte sequence, not truth of a measurement. A timestamp is meaningful only with its clock, time zone and provenance. A signed document may identify a signatory or integrity relationship but does not prove competence, permission or independent judgment. The assessor shall correlate consequential digital records with their actual technical and authority basis.

12.5 Redacted and restricted evidence

Redaction or controlled local viewing may protect information if sufficient relevant evidence remains available to the competent assessor and reviewer. Record what was examined, by whom, under what permission and what could not be verified. An unsupported management assurance shall not replace withheld critical evidence. Do not copy protected data merely to make a dossier appear complete.

13 Execution, interviews and technical witnessing

13.1 Opening control

Confirm identities, scope, criteria, locations, approved mode, safety stop, confidentiality, recording choices, evidence rules, schedule and contingencies. Identify changes since planning and obtain necessary approval

before continuing. Confirm that the applicant understands the distinction between a finding, recommendation and independent decision.

13.2 Interviews and record selection

Interview appropriate people without unnecessary supervision that inhibits truthful answers. Provide a lawful private channel where sensitive issues require it. Ask for original records selected from the defined population and trace both successful and unsuccessful cases. An interpreter, manager or host shall not replace the knowledge or response of the person being assessed.

13.3 Physical task observation

Observe the required setup, item identity, equipment status, essential variables, execution, actual results and report linkage. A camera tour showing equipment ownership is not proof of competent use. Where sample handling, measurement detail or process continuity is decisive, establish suitable independent observation and source-data access. Repeat or supplement a missed essential portion rather than marking it complete.

13.4 Personnel and learning assessment

Remote examinations shall protect identity, question security, permissible aids, scoring, independence and equivalent access. Practical skills require direct suitable demonstration; a knowledge test cannot replace an essential physical task. AF 9100 PER passing and renewal conditions remain unchanged. A candidate shall not be failed for an unproven technology fault, but an incomplete required assessment cannot support a pass.

13.5 Closing review

Communicate factual findings, evidence gaps, completed scope, interruptions, required follow-up and proposed next steps. The applicant may correct factual errors, not negotiate away a valid requirement. Record dissent and unresolved technical issues. Do not describe a closing-meeting recommendation as the final grant or renewal decision.

14 Recording, data minimization and confidentiality

14.1 Recording is not the default proof of completion

An assessment may be evidenced through competent notes, source references and signed records without recording every participant or the entire session. Record only what is justified and permitted. Where a task's reliability depends on a retained recording, approve its scope, access, retention and technical adequacy beforehand. A refusal of unnecessary recording is not automatically refusal of all assessment access.

14.2 Controls for recorded material

State when recording starts and stops and identify authorized recipients. Disable unapproved local copies, cloud recording, automated transcription and AI meeting agents. Keep sensitive recordings separate from general meeting files. Protect authentication data, exam content, personal documents, confidential trade information and officially controlled material according to their actual needs.

14.3 Retention and deletion

Retain necessary assessment evidence under the relevant scheme and AF-SC-001. Assessment and decision evidence normally requires at least seven years after the last relevant decision where AF 9100 or AF-SR-001 applies. Separable incidental personal material and raw recordings shall have a justified schedule, not automatic seven-year retention merely because recording was easy. Material evidence under a lawful hold shall not be destroyed to avoid scrutiny.

14.4 Disclosure and review access

Confidentiality shall enable necessary independent evaluation, lawful inspection and fair case review. Do not promise absolute anonymity, universal secrecy or an unconditional right to delete all evidence. Where disclosure is limited, document the basis and a sufficient lawful alternative; if no adequate route exists, the affected conclusion remains limited or held.

15 Interruptions, integrity concerns and safe resumption

15.1 Stop triggers

Pause the affected task for unsafe activity, unauthorized participation, unapproved recording, illegible evidence, lost critical observation, disputed identity, suspected manipulation, compromised confidentiality or a material system failure. The pause is a protection and evidence decision, not automatically a disciplinary finding. Preserve the actual timeline and the last reliable evidence point.

15.2 Partial completion

Identify which tasks remain supportable, which must be repeated and which cannot proceed remotely. A later recording cannot silently be described as an earlier live observation. Where continuity is part of the technical criterion, an unobserved interval may invalidate the whole relevant run; the technical authority shall determine that effect.

15.3 Resumption

Resume only after the relevant identity, security, safety, evidence and method conditions are restored and recorded. Reconfirm participants and recording status. Move to hybrid, on-site or another valid controlled method if the remote setup remains inadequate. Do not repeat unsafe work merely to reproduce a feed.

15.4 Deadlines and public status

Interruption does not automatically stop finding clocks, extend surveillance deadlines or renew an expiring credential. Apply AF-SR-001 Annex I and AF 9100 Annex AG where relevant. Missed required completion triggers the applicable status decision. Communicate reasonable scheduling remedies without concealing a lapse or promising a grace period not present in the governing rules.

15.5 Incidents and notifications

Suspected data or security incidents follow AF-PR-015 and the actual legal notification clocks. Critical attestation-related concerns retain immediate protection and the applicable 24-hour holder/operator actions. Technical status updates remain due within two calendar days of a status decision. No generic platform-incident target shall delay these duties.

16 Findings, supplementary work and decision readiness

16.1 Finding basis

Record the requirement, objective evidence, gap, affected scope and classification. Differentiate a demonstrated nonconformity, an evidence limitation and a technical disagreement. A poor connection alone need not prove a failed technical control; it may establish that the assessment cannot conclude. Deliberate falsification or concealed failed work requires integrity review and appropriate protection.

16.2 Supplementary assessment

Define the missing task, required method, responsible competent person, location, evidence and time. Preserve earlier results and explain the new evidence. Supplementary remote work is permitted only if it can actually close the gap. A favorable unrelated test or a general pledge shall not close a missing essential observation.

16.3 Independent review

The reviewer shall verify the complete requirement-to-evidence matrix, actual productive time, site and method coverage, verified identities, source integrity, restrictions, findings, corrections and prospective claim. A remote-suitability approval is not sufficient proof that the executed session met its conditions. Unresolved essential limitations prevent a positive conclusion for the affected scope.

16.4 No conditional conformity by convenience

Initial grant, renewal and extension require closure of all in-scope nonconformities and adequate evidence under the controlling rules. A conditional project gate or supplier-development arrangement is not a conditional conformity certificate. Continuing-status decisions, including bounded minor continuation and critical suspension, follow their existing requirements; remote delivery does not create a new exception.

17 Reporting, notification and public claims

17.1 Required report content

Identify the evaluated object, criteria/profile version, sites, actual physical and remote locations, team roles, mode by task, productive time, tools, evidence sources, sampling, witnessing, interruptions, limitations, findings and follow-up. Distinguish live observation from recorded or simulated evidence. Sensitive location details may be held in a protected annex while retaining enough information for independent scrutiny.

17.2 Timing and handover

Applicable AF-SR-001 and AF 9100 final evaluation reports are due within fourteen calendar days after evaluation closure, subject to their documented exceptional-delay provisions. Earlier communicated finding clocks and protective duties are not postponed by report production. Corporate internal audit follows AF-HB-009 and its separately identified reporting target. Other programs retain their approved service rules.

17.3 Accurate conclusions

A public credential shall state its real route, object, issuer, scope, limitations and current/instance boundary. Remote delivery does not confer a new higher status or an inferior label by itself. Where method limitations materially affect the claim, disclose them sufficiently; do not advertise physical inspection or witnessing that did not occur. Logo and public verification use follow AF-PL-014 and the applicable scheme.

18 Surveillance, change and reliance on earlier evidence

18.1 Continuing scrutiny

Reassess remote suitability before each materially different assignment and after significant change, adverse results or compromised evidence. Prior remote acceptance is not a perpetual waiver. Surveillance shall evaluate continuing implementation, not only confirm that a policy file is unchanged.

18.2 Reuse of evidence

Reuse earlier reports only after confirming object, configuration, method, period, scope, issuer competence, authenticity and continuing relevance. Record the work legitimately avoided and any remaining AF requirement. A previous certificate, local witness statement or partner recognition arrangement does not automatically substitute for all current witnessing.

18.3 Transfer and closure

A change of operator or platform shall preserve original findings, status, access rights, records and actual authority. A suspended or unsupported claim cannot become valid through transfer. On provider closure, arrange lawful custody and verification continuity; transfer of files is not transfer of accreditation or AF operating permission.

19 Future technology and inaccessible environments

19.1 Digital twins and telemetry

A digital twin or live telemetry source shall identify its intended decision, physical reference, configuration, sensor provenance, validation domain, uncertainty, drift and missing-data treatment. Continuous evidence may supplement but shall not cancel periodic assessment, independent witnessing or renewal. Modeled output shall not be presented as measured reality without its actual basis and limitations.

19.2 AI-assisted evidence

Approved AI may assist search, anomaly detection, transcription, translation or preliminary analysis. Assessors shall treat document-embedded instructions and untrusted input as evidence content, not commands to change their criteria, disclose data or alter a decision. Verify consequential outputs against original evidence. Automated scores, synthetic reconstructions or deepfake-detection results shall not become the sole authority for an independent outcome.

19.3 Immersive and robotic observation

Augmented-reality, remotely piloted cameras or robotic inspection may support observation within approved safe and lawful operation. Validate actual field of view, scale, positioning, image processing, operator control and retained source data. An attractive virtual tour does not establish access to hidden features, instrument validity or material condition outside the method's detection capability.

19.4 Space, marine and long-life assets

For deployed spacecraft, planetary systems, offshore or other inaccessible assets, separate event time from receipt time, account for communication delay and identify what can only be inferred. Validate onboard logs, telemetry and ground processing for the intended conclusion. Do not require impossible real-time interaction, but do not disguise delayed or incomplete evidence as live complete witnessing. Operational permissions and mission responsibility remain with the actual operator and competent authorities.

19.5 Validation before adoption

A novel remote method shall have an approved purpose, representative validation including adverse and edge conditions, independent technical challenge, security review and controlled release. Where it introduces substantive scheme requirements, follow the applicable consultation and approval process. A pilot may demonstrate feasibility without issuing unrestricted production credentials.

20 Monitoring, audit and public-benefit review

20.1 Measures and denominators

Track required tasks completed, essential evidence gaps, repeated interruptions, supplementary visits, report correction, adverse scope decisions, incidents, accessibility barriers, complaints and actual remote/physical effort. State populations, time periods and limitations. High remote utilization, lower travel or a high grant rate is not by itself proof of reliable assessment.

20.2 Assurance over the method

Include remote practices in annual active-process audit and quarterly performance review under AF-HB-009. Sample accepted and refused remote methods, significant interruptions, restricted evidence and outsourced witnesses. Verify the approval-to-execution trail and whether pressure to reduce travel or fees compromised evidence.

20.3 Review and change

The policy owner shall review this policy at least annually and after material method, security, legal or performance change. This is a new policy-maintenance control. Preserve existing source files and transition contracts and tools through actual approval. An improved platform feature is not a self-executing change to technical criteria.

Annex A — Remote feasibility and go/no-go record

Status: mandatory task-level controls and blank model record. Complete within AF-FR-013 and AF-FR-015, or AF-FR-023 for internal audit. No score may compensate for a failed essential gate.

Gate	Required decision evidence	Failure response
A01 Authority and mode	Actual scheme/program permission, task scope and approving role.	Hold the unapproved task.
A02 Lawful access	Parties, locations, confidentiality, controlled technology and processing basis reviewed.	Resolve permission or use a lawful alternative.
A03 Competence	Current technical, remote-method and language coverage; independent roles.	Reassign, support or defer.
A04 Identity	Participant, role, object and location adequately authenticated.	Reverify before accepting evidence.
A05 Observation	Detail, context, continuity and essential variables observable by a validated method.	Add local/on-site evidence or restrict.
A06 Scope coverage	Every required site, method family, shift and critical task addressed.	Complete missing coverage; no automatic remote exception.
A07 Security	Approved platform, endpoints, permissions, storage and provider controls.	Correct configuration or use another approved route.
A08 Recording and privacy	Necessary collection, notices, permissions and retention established.	Do not record or process beyond the lawful basis.
A09 Safe execution	Local operator, safe boundaries, stop route and necessary permissions.	Stop unsafe or unauthorized work.
A10 Original evidence	Source records, provenance, selection and adverse results accessible.	Hold unsupported conclusions.
A11 Rehearsal and fallback	Representative test passed; interruption/repeat method defined.	Rehearse or use another mode.
A12 Fair participation	Accessible equivalent arrangement and candidate/participant information.	Resolve avoidable barriers without weakening competence.
Decision field		Actual entry
Case/task ID; profile; criteria; date and mode requested		
Gate results, evidence references and unresolved limitations		
Approved remote tasks; physical/local tasks; conditions		
Technical, security and access reviewers; actual approving authority		
Reassessment triggers, contingency and participant notification		

Annex B — Activity and evidence matrix

Status: mandatory interpretation of route boundaries; methods remain subject to task-specific validation. A remote mode is not approved simply because an activity appears in this table.

Activity	Suitable remote contribution to evaluate	Evidence that shall not be silently omitted
Corporate internal audit	Source records, interviews, workflow demonstration and implemented case trails.	Independence, every active-process cycle and actual delivery evidence.
ORG assessment	Controlled system access, readiness, interviews, record tracing and suitable live observation.	Required implementation, physical-site evaluation, critical processes, time and stage floors.
PRD assessment	Configuration, engineering records, traceable test data and valid witnessing.	Actual representative product, required physical tests, sample identity and acceptance criteria.
SVC assessment	Actual service observation, user interactions, outcome records and recovery evidence.	Defined service window, real delivery and essential continuity criteria.
PRC assessment	Essential-variable logs, equipment records and suitable witnessed execution.	Qualified range, physical conditions and validation of a special process.
PER assessment	Identity, secure knowledge assessment and valid practical demonstration.	Essential practical skills, passing gates, examiner competence and independent decision.
SUB assessment	Actual performer and sub-tier records, controlled work-package tracing.	Source capability, required witnessing and flow-down to the point of performance.
CAB accreditation	Methods, competence dossiers, report trails and qualified live/local witnessing.	Each distinct method family/route, technical capability and independent competence decision.
Testing and calibration	Raw data, instrument status, method setup and readable measurement displays.	Sample custody, traceability, actual uncertainty and method validity.
Education and learning	Accessible participation and approved learning-assessment evidence.	Distinction between attendance, assessed learning and personnel certification.
Awards and grants	Secure submission review, interviews and permitted demonstrations.	Published merit criteria, independent jurors, adverse evidence and no-award/refusal option.
Research and project review	Versioned data, milestones, peer analysis and funded-work records.	Real results, rights, ethics, restrictions and differences between models and measurements.
Event or partner readiness	Permits, plans, venue/platform walkthroughs and contractual deliverables.	Actual operator safety duties and evidence not visible through the selected mode.
Corporate meetings	Identity, accessible papers and secure participation.	Constitutional notice, quorum, voting and consent rules; this is not an assessment route.

Annex C — Plan, rehearsal and session record modules

Status: mandatory minimum fields; blank templates. Store under the originating case and form version. Add continuation pages where needed.

C.1 Requirement-to-method plan

Field	Actual entry
Case ID; object/route; profile and criteria versions	
Requirement/task; essential status; completion criterion	
Physical and remote locations; sites/shifts/method families	
Assigned assessor, specialist, host and independent local witness	
Mode; population/sample; original evidence expected	
Productive evaluation time; reporting/review time separately	
Access, recording, data transfer and retention permissions	
Rehearsal result; known limitations; fallback and repeat conditions	
Actual suitability approval and participant agreement reference	

C.2 Session and evidence log

For each session record start/end with time zone; authenticated attendees and roles; actual location and mode; platform/configuration; recording status; task IDs; evidence selected by whom; observed results; interruptions and re-verification; productive hours; safety or integrity holds; incomplete tasks; and closing communication. The evidence manifest shall link original creation time, configuration, source custodian and authorized transfer or viewed-only access.

C.3 Minimum rehearsal checklist

Confirm protected invitations and identity; permissions; sound and interpretation; ordinary and close-up detail; readable measurement values; safe camera position; live-reference test; access to selected original records; recording/transcription settings; authorized downloads; session interruption; and fallback contact. Each necessary item needs a result, reviewer and evidence. A simple declaration “platform works” is inadequate.

Annex D — Interruptions, incidents and supplementary work

Status: mandatory minimum control record and illustrative decision examples. Do not treat every interruption as misconduct or every restored connection as recovered evidence.

Record item	Actual entry
Case/task; actual detection time; observer and location	
Failure or concern; affected evidence; last reliable observation	
Immediate safety, security or claim protection; authority	
Tasks still supported; tasks invalidated or incomplete	
Required repeat/local/on-site work and competent owner	
Notification clocks, original due dates and status effects	
Restored conditions; re-verification; resumption approval	
Final supplementary evidence, remaining limits and closure	

D.1 Measurement-display failure

A live connection remains active but the displayed calibration result cannot be read reliably. The assessor shall not transcribe a guessed value or accept a typed chat message as if it were the observed display. Obtain a validated readable view and source record, or use a suitable authorized local observation. If the missing evidence cannot be recovered, the relevant conclusion remains incomplete.

D.2 Surveillance deadline during an outage

A scheduled session fails before required coverage is completed and the surveillance due date arrives. Booking, payment and partial attendance do not constitute completed surveillance. Apply the controlling status rule, preserve the lapse and plan the remaining evidence. An administrative rescheduling message cannot extend validity.

D.3 Suspected synthetic feed

A material inconsistency suggests a substituted recording. Pause the affected task, preserve the observations, confirm identity through an independent route and seek relevant source corroboration. Do not declare fraud solely from an automated detector result. A substantiated falsification and an unresolved evidence gap have different findings, but neither supports an unsupported positive decision.

Annex E — Worked resource and coverage calculations

Status: informative synthetic examples; controlling AF time and scope requirements remain unchanged. Use unrounded values for decisions and show units.

E.1 Organizational floor is unchanged by remote delivery

For the existing AF 9100 Annex AC example, $N = 80$ effective personnel gives $B = 5$ auditor-days. C2 gives $K = 1.35$ and two complexity triggers give $f = 0.30$. With one site and no additional observed shift, calculated time is $5 \times 1.35 \times 1.30 = 8.775$ days, rounded upward to the half-day floor $T = 9.0$ days, or 72 productive auditor-hours. Minimum readiness time is 2.5 days and implementation 6.5 days. Review and decision time are additional. A justified plan containing 24 productive remote auditor-hours and 48 productive on-site auditor-hours totals 72. The reported remote share is $24 / 72 \times 100 = 33.33\%$. This arithmetic does not establish that the task mix or coverage is adequate. Extra setup, connection loss, travel, final reporting and independent decision work are not used to inflate those 72 hours.

E.2 Personnel and witnessing are not headcount audits

A personnel task requiring a secure knowledge examination and observed practical demonstration uses its actual task profile. It does not obtain a nine-day organizational floor merely because the candidate's employer has 80 personnel. Equally, a laboratory with a small headcount cannot avoid a distinct method family requiring actual competent witnessing.

E.3 Coverage is not a pass score

A plan has ten mandatory tasks. Seven have sufficient evidence, two need local observation and one lacks essential source data. Administrative completion is $7 / 10 \times 100 = 70\%$. That number is a progress measure, not 70% conformity or permission to grant. All mandatory tasks in the granted scope must have adequate evidence and the other decision conditions must be satisfied.

E.4 Eligible site sampling remains narrowly bounded

For nine genuinely homogeneous C0/C1 sites in an AF 9100 ORG annual-surveillance pool, $m = \max(\text{ceil}(\sqrt{9}), \text{ceil}(9/2)) = 5$. At least $\text{ceil}(5/4) = 2$ selected sites are random, with rotation and separately mandatory coverage retained. This is not permission to omit four sites at initial evaluation, sample five of nine unrelated CAB methods, or infer statistical confidence from judgmental selection.

E.5 Clock preservation

A six-month surveillance deadline from 31 August 2026 falls on 28 February 2027 using the corresponding-date/month-end rule. A status decision on 30 September 2026 requires a two-calendar-day registry update no later than 2 October 2026 under the stated date basis. A later report or restored connection does not restart either trigger.

Annex F — Independent review and decision-readiness checklist

Status: mandatory minimum review coverage for applicable cases. This checklist does not replace the independent decision or actual scheme requirements.

Review area	Required check
Actual authority	Scheme, route, operator and remote-method approval are valid for the case.
Scope	Object, profile, configuration, sites and exclusions are precise.
Competence	Current remote and technical competence, specialists and role separation established.
Access	Lawful locations, permissions and sufficient original evidence were available.
Rehearsal	Actual setup was suitable for the task; material changes were rechecked.
Execution	Required work was observed/evaluated; live, recorded and simulated methods distinguished.
Sampling	Actual population, selection, adverse evidence and expanded trails are recorded.
Time	Productive work meets applicable floors without double counting or hidden reduction.
Integrity	Identity, provenance, originals, failed runs and changed evidence are traceable.
Interruptions	Last reliable evidence, repetitions, supplementary work and safe resumption are documented.
Findings	Requirement–evidence–gap, severity, containment and verified closure are adequate.
Critical gates	No missing essential observation, unresolved unacceptable risk or false-record concern remains.
Decision	Correct independent authority/panel, exact permitted outcome and actual dates.
Publication	Scope and limitations match the claim; registry and mark controls preserved.
Retention	Necessary dossier and incidental data schedules, holds and access are defined.

Annex G — Future-method validation and performance review

Status: mandatory validation principles with informative metrics. No future technology is approved solely by inclusion in this Annex.

G.1 Validation dossier

Record intended decision and users; real-world reference; scope and limits; sensor, software and model versions; rights and permissions; representative and adverse-condition tests; accuracy, detection and uncertainty relevant to the task; missing/stale data; security and manipulation threats; human review; independent challenge; pilot constraints; and the authorized release or refusal. Revalidate after material change.

G.2 Performance measures

Measure	Definition and interpretation
Remote task completion	Supported planned remote tasks divided by required planned remote tasks for the defined period; missing evidence is not a pass.
Supplementary work rate	Cases needing unplanned supplementary physical/local work divided by completed assessed cases; examine planning adequacy, not pressure to avoid visits.
Evidence-integrity events	Number, consequence and affected population of substantiated events, with unsubstantiated reports separate.
Productive remote share	Credited remote evaluation hours divided by all credited evaluation hours; excludes waiting and administrative time.
Method-related corrections	Reports or decisions corrected due to remote-method defects divided by the relevant reviewed population.
Accessibility response	Justified requests resolved and unresolved, with reasons and preserved essential requirements.
Deadline failures	Required surveillance, reporting or notification events missed, by actual original trigger.

A zero denominator shall be reported as Not applicable or Not measured with reasons, not an invented 100% success. Samples are not automatically representative of all AF cases. Review actual effects on access, burden, reliability and public benefit, not remote volume alone.

Annex H — Source alignment and implementation record

Status: source-to-control map, proposed Master List entry and blank release record. Earlier files remain unchanged.

Source	Inherited requirement	Expansion in this policy
AF-CON-001 Articles 18, 22–28	Competence, independence, lawful access, records, fair remedies and audit/review.	Remote-role allocation, permission flow and protected participant handling.
AF 9100 Annexes AA–AJ	Exact routes, technical evidence, time/coverage, passing rules, status clocks and independent decisions.	No amendment; task-specific remote implementation and examples.
AF-SR-001 16.1–16.6 and 17–19	Resources, all-site/method coverage, reliable remote evidence, witnessing and independent review.	Binary feasibility gates, readiness rehearsal and execution records.
AF-SR-001 24–27; AF-PL-005/006	Truthful verification, provenance, privacy, secure systems and human accountability.	Liveness checks, scoped recording, platform configuration and novel-method validation.
AF-PR-015 and AF-SC-001	Incident, continuity, recovery and justified retention controls.	Task interruption, partial completion and resumption trace.
New operating detail	No earlier universal remote percentage or camera specification is asserted.	Remote-method demonstration, gate checklist, task matrix and annual policy review.

H.1 Connected documents

AF-QM-001, AF-ML-001, AF-CON-001, AF-SR-001, AF-GD-003, AF-PL-003, AF-PL-004, AF-PL-005, AF-PL-006, AF-PL-008, AF-PR-001, AF-PR-004, AF-PR-007 through AF-PR-011, AF-PR-014 through AF-PR-020, AF-SC-001, AF-SC-004 and AF-FR-001, AF-FR-003, AF-FR-005, AF-FR-006, AF-FR-013 through AF-FR-017, AF-FR-021 through AF-FR-024, AF-FR-027 and AF-FR-031 provide the principal interfaces. Companion AF-HB-009, AF-PL-013 and AF-PL-014 supply audit, conduct and brand controls.

H.2 Proposed Master List entry

AF-PL-015 | Remote Assessment Policy | Corporate and scheme delivery policy | Owner: Assurance Programme Manager | Processes: P06–P08 and P17; applicable other evaluation activities | First Edition | Revision 00 | Edition date: 30 September 2026 | R01 publication lineage; completed cases R06/R12 and related classes | Actual approval/effectivity recorded through AF-FR-001. This entry does not itself update the earlier workbook.

Release dependency	Actual entry
Competent approving authority, exact publication and actual effectivity	
Applicable program/profile modes, criteria and lawful access constraints	
Named technical, remote, security and independent decision personnel	
Approved platforms, provider terms and representative rehearsal evidence	
Live records, incident/fallback channels and tested retrieval arrangements	
User communication, contract transition and first policy/audit review	