



IAF SDR | SOFTWARE & DIGITAL | FIRST EDITION

AUDIT & RECOGNITION MANUAL

Twenty controlled procedures for competent assessment,
independent decisions and continuing confidence.

PREPARED FOR IAF ADOPTION

Version 1.0 | 16 September 2026

Software Developers & Digital Tools
Corporate Recognition | English master text

International Automotive Federation

iaf.com

Document control

Item	Controlled value
Programme	IAF Software and Digital Systems Recognition Programme (IAF SDR)
Document	Audit & Recognition Manual
Edition / version	First Edition Version 1.0
Prepared	16 September 2026
Status	Prepared for IAF adoption. Effective operation requires recorded adoption, validated pilots and an operational verification route.
Owner	International Automotive Federation
Master language	English
Public recognition wording	IAF Corporate Recognition - bounded to the approved legal entity, sites and activities.
Hierarchy	Standard including internal directives and normative annexes; adopted implementation notice within those rules; Status and Mark Rules; Audit and Software Lifecycle Manuals; Applicant Guide; controlled forms.
Authority boundary	Corporate implementation assurance. Corporate scope is separate from release approval; no blanket product certification, output endorsement or vehicle approval is conferred.
Control	Retain exact scope and criterion versions. Protect completed records, personal information and software evidence.

Purpose and use

Twenty controlled procedures for competent assessment, independent decisions and continuing confidence.

Shall denotes a requirement; should guidance; may permission. Examples are illustrative unless a normative provision expressly establishes a rule. No checklist score can compensate for failed safety, integrity, competence or an unsupported scope.

Contents

Document control	2
Roles and decision separation	4
Procedure map	4
OP01 Programme adoption and launch	6
OP02 Application and eligibility review	6
OP03 Team selection and impartiality	7
OP04 Scope, family coverage and assessment planning	8
OP05 Source-to-deployment evidence review	8
OP06 Hub assessment and technical demonstration	9
OP07 Classify findings and protect affected release/change events	10
OP08 Corrective action and effectiveness verification	10
OP09 Independent recognition-case technical review	11
OP10 Independent recognition decision	12
OP11 Annual surveillance and family rotation	12
OP12 Material change and scope extension	13
OP13 Incident and urgent interim suspension	14
OP14 Complaints, whistleblowing and fair investigation	14
OP15 Independent appeal	15
OP16 Registry, marks and public statements	16
OP17 Renewal, expiry, exit and restoration	16
OP18 Information, provenance and record lifecycle	17
OP19 Product family admission and support review	18
OP20 Controlled lifecycle and release assurance	18
Operating clocks and follow-up	19
Borderline cases	20

Roles and decision separation

Role	Responsibility	Boundary
IAF programme owner	Adopts rules, resources and launch readiness.	Cannot direct a favourable case result.
Programme manager	Controls intake, scope, coverage and deadlines.	Urgent interim protection needs independent technical lead concurrence.
Lead assessor	Plans and leads evidence collection and findings.	Does not make the independent recognition decision.
Technical assessor	Challenges software, tool and operational evidence.	Works within demonstrated technical competence.
Independent case reviewer	Checks scope, evidence and verified closure.	Uninvolved in assessment or applicant consultancy.
Decision panel	Three members participate; at least two reasoned votes.	All applicable gates remain mandatory for grant.
Appeal panel	Different three members review disputed decisions.	No original-case involvement; conflicts screened.
Registry/mark custodian	Publishes approved status and scope.	Cannot certify releases or alter technical decisions.
Organisation executive	Owns implementation, resources and customer duties.	Cannot override known unacceptable technical risk.
Technical/security authority	Controls consequence, holds and engineering adequacy.	Acts within demonstrated competence and lawful authority.
Independent release reviewer	Challenges consequential changes before delivery.	Did not create the work being independently verified.
Operator assurance reviewer	Audits programme integrity and decisions.	Independent of operation reviewed.

Procedure map

Code / procedure	Owner	Trigger
OP01 Programme adoption and launch	IAF programme owner	Before live recognition
OP02 Application and eligibility review	Programme manager	Initial, renewal or extension application
OP03 Team selection and impartiality	Programme manager and independent impartiality reviewer	Before each assignment and after material conflict information
OP04 Scope, family coverage and assessment planning	Lead assessor with independent reviewer	After eligibility acceptance

Code / procedure	Owner	Trigger
OP05 Source-to-deployment evidence review	Assessment team	Before and during technical assessment
OP06 Hub assessment and technical demonstration	Lead and technical assessors	Initial, annual, renewal or triggered review
OP07 Classify findings and protect affected release/change events	Lead assessor; programme manager for urgent protection	A supported failure, material uncertainty or serious risk
OP08 Corrective action and effectiveness verification	Organisation technical owner; independent verifier	Finding response or systemic technical failure
OP09 Independent recognition-case technical review	Uninvolved competent reviewer	Completed assessment and verified closure
OP10 Independent recognition decision	Three-person decision panel	Technically reviewed case
OP11 Annual surveillance and family rotation	Programme manager and assessment team	Annual cycle or additional risk review
OP12 Material change and scope extension	Programme manager with technical review and panel	Planned change, five-day unplanned notice or extension request
OP13 Incident and urgent interim suspension	Programme manager and independent technical lead	Credible serious risk, falsification or material loss of control
OP14 Complaints, whistleblowing and fair investigation	Uninvolved complaint owner	Customer, worker or public concern
OP15 Independent appeal	Appeal administrator and separate panel	Appeal received within 30 calendar days of decision notice
OP16 Registry, marks and public statements	Registry and mark custodian	Decision publication, claim request or verification inquiry
OP17 Renewal, expiry, exit and restoration	Programme manager and independent panel	Renewal, expiry, withdrawal or restoration request
OP18 Information, provenance and record lifecycle	IAF and organisation information owners	Routine operation, migration, compromise or disposal
OP19 Product family admission and support review	Organisation technical executive	New family, major change, acquisition or support exit
OP20 Controlled lifecycle and release assurance	Product owner, technical authority and independent reviewer	Every material software/service change

OP01 Programme adoption and launch

Owner: IAF programme owner. Trigger: Before live recognition.

1. Adopt controlled authority

Record programme ownership, exact editions, technical decision authority, impartial resources and accessible eligibility. Separate prepared documents from an operational scheme. Commercial or membership status shall not determine a technical result.

2. Prepare competent operation

Appoint assessors, independent reviewers, three-person panels, complaint owners and registry personnel against actual competence. Screen IAF case interests over at least 36 months and longer for residual risks. Test evidence protection and separation of commercial and technical roles.

3. Run representative pilots

Complete at least four pilots: small developer, engineering/test-tool supplier, vehicle update operation and cloud/AI service. Include a failed or contested case. Test real release evidence, remote-hub adequacy, duration, independent review, appeal and urgent protection.

4. Validate current verification

Test active, restricted, suspended, expired and unknown records with exact family/activity scope. Exercise outage and manual fallback. A product interface or saved certificate must not display stale status as current; preserve decision time separately from publication and retrieval.

5. Approve launch

Independently close essential pilot gaps and record adoption, effective operation and remaining nonessential improvements. Confirm sufficient technical and complaint capacity. Do not issue live recognition before the assurance and verification gates are demonstrably met.

Required record: F20 operator assurance; F21 pilot approval.

OP02 Application and eligibility review

Owner: Programme manager. Trigger: Initial, renewal or extension application.

1. Register the case

Assign case ID, record legal holder, authorised contact, route and submission version. Separate private readiness from recognition. Preserve original submissions and later changes; an accepted application is not an active status.

2. Validate accountability

Verify entity, lawful operation, contracting responsibility, lifecycle roles, hubs, suppliers and product families. Resolve unsupported ownership, licence or product-approval claims. A public repository or marketplace listing alone cannot bind an accountable holder.

3. Check implementation

Verify six months of implemented controls, completed internal audit and management review, and three real completed release/change events per family/responsible hub. Confirm genuine delivery or service operation and reject duplicated targets or invented trivial events. Governance-only functions provide actual oversight cases.

4. Assess access and resources

Confirm competent assessment, protected source/build review, required physical or approved remote-only office access, technical demonstrations and relevant staff availability. Identify language, confidentiality and supplier limitations. Defer unsupported scope rather than conceal missing essential evidence.

5. Record route acceptance

Issue reasoned acceptance, clarification, deferral or refusal with precise scope, missing items and process responsibilities. Explain recognition and release boundaries. Keep all pending scope outside active public claims.

Required record: F01 intake; application; scope schedule.

OP03 Team selection and impartiality

Owner: Programme manager and independent impartiality reviewer. Trigger: Before each assignment and after material conflict information.

1. Map competence

Translate profiles, technologies, vehicle classes, languages and local context into the required team skills. Appoint at least two competent assessors collectively covering the assignment, and arrange specialists where necessary. Allocate responsibilities rather than relying on an undifferentiated team résumé.

2. Screen interests

Obtain declarations covering the applicant, related entities and relevant commercial or personal interests. Exclude employment, consultancy, ownership or material commercial interests in the previous 36 months, and longer where residual risk remains. Review all assessors, reviewers and panel members.

3. Resolve and document

Have an uninvolved competent person determine whether a disclosed interest creates unacceptable risk. Replace personnel where exclusion applies; disclosure alone does not cure an excluded conflict. Record the rationale, restrictions and any additional safeguards for permissible residual risks.

4. Brief and authorise

Confirm task-specific competence, confidentiality, evidence rules and outputting boundaries. Ensure experts understand that advice to the audit team does not authorise applicant consultancy or an independent recognition decision. Notify the applicant of the team and a route to raise factual conflict concerns.

5. Monitor during the case

Require prompt declaration of new information, including unexpected prior relationships. Pause the affected assignment and preserve work already obtained while reviewing its validity. Reassign and repeat evidence collection where independence or technical reliability has been compromised.

Required record: F02 conflict declaration; F03 competence and team record.

OP04 Scope, family coverage and assessment planning

Owner: Lead assessor with independent reviewer. Trigger: After eligibility acceptance.

1. Reconcile the scope

Map legal entities, lifecycle roles, delivering hubs, families, support boundaries and external dependencies. Apply DEV and all relevant profiles/domains. Define family grouping by material architecture, controls and consequence; commercial similarity alone is insufficient.

2. Determine hub coverage

Assess every hub initially and at renewal and review every hub annually. Physically visit technical facilities handling vehicles, hardware or physical test work. A remote-only office may use secure live observation and original-source review only after uninvolved adequacy approval; otherwise visit or defer.

3. Determine family demonstrations

At initial/renewal demonstrate every family. Annually include all consequential, new/materially changed and adverse-case families plus $\text{ceil}(\sqrt{N})$ of remaining families, deduplicating mandatory groups. Rotate all families within three years; expand for risk and challenge relevant technical roles.

4. Calculate minimum effort

Initial/renewal: two central auditor-days plus one per hub up to ten technical personnel, two for 11-50 and three above 50. Add one hub-day per material factor: novel consequential software/AI, continuous multiregion operations, complex critical outsourcing and unresolved systemic risk. Annual: one central day plus one per physical facility and half a day per remote-only hub. Add necessary time; exclude travel and double-counted hours.

5. Approve evidence and safe access

Review at least three actual completed events per family/responsible hub. Expand for failed changes, dependencies and variant diversity. A physical visit spans a full operating day with at least half on-site time for observation, witnessing and interviews. Agree safe isolated challenges, protected access, dates, limitations and remote-route approval.

Required record: F04 plan; F24 hub/family review; scope schedule.

OP05 Source-to-deployment evidence review

Owner: Assessment team. Trigger: Before and during technical assessment.

1. Review controlled baselines

Check adopted requirements, scope, family definitions, roles, support commitments and additional IAF claim maps. Identify contradictions between contracts, marketing and actual capability. Do not infer implementation from policy volume.

2. Follow actual release events

Trace selected events from purpose and requirements through source/configuration, review, component inventory, build, original tests, release authority and actual deployed state. Preserve failures, overrides and superseded evidence. For operators, verify controlled supplier and operational interfaces rather than inventing code authorship.

3. Challenge authenticity

Check original timestamps, identities, source history, build evidence and delivered artifact identity. A hash proves byte identity, not trusted origin or correct behaviour. Investigate missing failures, copied approvals or inconsistent target populations fairly and expand samples where needed.

4. Protect confidential material

Use lawful controlled viewing and minimised extracts for source, credentials, customer data and proprietary models. Record sufficient facts to support conclusions without copying unnecessary secrets. If essential evidence cannot be lawfully verified, retain an unresolved result or defer scope.

5. Focus demonstrations

Select uncertain high-consequence paths and known-failure cases for safe live challenge. Policies and prerecorded demos cannot establish actual controls. Record test isolation and authorisation so assessment does not create unauthorised production or vehicle intervention.

Required record: F05 evidence log; R01-R16 lifecycle dossier.

OP06 Hub assessment and technical demonstration

Owner: Lead and technical assessors. Trigger: Initial, annual, renewal or triggered review.

1. Verify actual control

Reconcile hub, personnel, lifecycle role, environment access and family/event population. Physically observe relevant hardware/test facilities. For an approved remote-only office, verify identity, live workflow and original-source access under the adequacy plan.

2. Challenge the release chain

Ask responsible staff to reproduce a selected requirement-to-release trace and explain independent checks, failures and target compatibility. Use a bounded adverse case, such as missing input or failed deployment, to test stop and escalation behaviour. Do not introduce uncontrolled faults into customer production.

3. Evaluate competence and independence

Observe how relevant engineers, reviewers, operators and release owners reason about risks, assumptions and residual limits. Distinguish authorship from verification and supplier claims from applicant evidence. Credentials, tool access and confident presentation alone are insufficient.

4. Test continuing assurance

Review vulnerability intake, actual support cases, deployed inventories, corrective campaigns, end-of-support and recovery evidence. Reconcile customer-facing claims with actual service and version boundaries. Check whether an unavailable dependency invalidates the proposed assurance.

5. Conclude transparently

Record source evidence, witnessed behaviour, contrary facts, inaccessible material and limitations. Expand sampling or demonstrations where needed. Safe simulations support validation but cannot replace the actual three-event or six-month gates.

Required record: F05 observations; F24 hub review; checklist.

OP07 Classify findings and protect affected release/change events

Owner: Lead assessor; programme manager for urgent protection. Trigger: A supported failure, material uncertainty or serious risk.

1. State the requirement and fact

Record the exact requirement, original evidence, location, release/change event or population and the gap. Distinguish a missing record from evidence of unsafe work. Explain the scope and uncertainty; do not infer an organisation-wide failure solely from a local issue without investigating common causes.

2. Determine severity

Classify Critical for credible serious harm or severe integrity failure, Major for systemic or consequential breakdown, and Minor for an isolated lapse that does not invalidate essential assurance. Pending denotes unresolved evidence, not a passing result. Use technical consequences, not customer size, to determine severity.

3. Contain immediately

Require proportionate action to protect people, consequential release, data and affected customers. Trace potentially affected earlier release/change events and shared methods. Serious risk requires immediate protective review; root-cause investigation and factual-response periods must not delay necessary containment.

4. Set the applicable clock

Initial grant waits for complete effective closure. For active recognition, Minor is due within 90 calendar days; Major has immediate containment and a 30-day closure target with suspension review if unresolved. Critical prompts immediate protection. Record precise due dates and responsibility.

5. Preserve fairness

Communicate facts, reasons, scope and the response route. Reassess credible counter-evidence and correct mistakes transparently. Keep protective actions proportionate while uncertainty is resolved, and record why a wider restriction is or is not necessary.

Required record: F06 finding and action record; F11 interim protection.

OP08 Corrective action and effectiveness verification

Owner: Organisation technical owner; independent verifier. Trigger: Finding response or systemic technical failure.

1. Accept responsibility and contain

Identify the immediate affected work and a justified earlier-release population. Assign owners and prevent recurrence while investigation proceeds. A temporary additional check is containment and should not be mislabelled as permanent cause removal.

2. Investigate causes

Examine methods, competence, tools, workload, data, incentives and organisation interfaces. Seek evidence that distinguishes hypotheses. Avoid a default conclusion of human error when the process makes the mistake likely or fails to detect it before release.

3. Implement a coherent remedy

Correct the immediate defect, address cause and review customer remedies. Revise instructions, resources or authority where needed and communicate changes to affected delivering hubs. Training attendance alone is insufficient when the underlying failure involved unsuitable equipment or missing technical information.

4. Verify effectiveness

Use competent independent review for material failures and representative subsequent release/change events. Test the failure mechanism and potential side effects of the change. Preserve unsuccessful attempts. Where adequate actual evidence is not yet available, retain the finding as open rather than closing on a promise.

5. Authorise closure

Record the verified evidence, affected population disposition and closure rationale. Escalate unresolved Major or Critical conditions for protective decision. Initial recognition is not granted until all findings are effectively closed and every applicable requirement is Met.

Required record: F06 action; F07 verified closure; affected-release/change event register.

OP09 Independent recognition-case technical review

Owner: Uninvolved competent reviewer. Trigger: Completed assessment and verified closure.

1. Confirm independence and package

Verify your competence and conflict clearance, exact edition, scope version and evidence manifest. Reconcile requested, assessed and proposed families, hubs, roles and exclusions. Do not expand a conclusion beyond what was actually assessed.

2. Check mandatory gates

Verify implementation history, actual completed events, internal audit, management review, hub coverage, family demonstrations, technical competence and adequate effort. Review all essential gates and additional IAF claims. An attractive checklist total cannot replace source evidence.

3. Challenge reasoning and closure

Review contradictory results, NA decisions, severity, shared dependencies and prior-release effects. Confirm actual effectiveness and protection, not promises. Check that organisational finding deadlines have not been misused to postpone urgent software-risk response.

4. Resolve evidence gaps

Return documented queries for clarification or additional assessment without becoming the applicant's consultant or silently rewriting findings. Preserve material changes and responses. Unresolved essential facts prevent panel-ready grant recommendation.

5. Recommend bounded disposition

Record ready, defer or not supported, exact scope, limitations and surveillance focus. Independent technical review is separate from the three-person panel decision and from the applicant's own release approvals.

Required record: F08 case review and readiness recommendation.

OP10 Independent recognition decision

Owner: Three-person decision panel. Trigger: Technically reviewed case.

1. Confirm decision competence

Appoint three uninvolved competent members, screen conflicts and provide the same controlled case package. Identify the exact programme edition and scope version. All three must participate; commercial or membership representatives cannot predetermine the technical conclusion.

2. Evaluate the gates

Confirm every applicable requirement Met and all initial findings effectively closed. Evaluate eligibility, actual authorisation, approved hub coverage, evidence authenticity and release reliability explicitly. Do not offset a failed gate by strengths elsewhere or a high readiness score.

3. Record individual votes

Each member records grant, defer, refuse or another applicable disposition with reasons. Every disposition needs at least two reasoned votes; grant and restoration also require all applicable gates. Preserve dissent and resolve any evidence gap exposed by the panel before treating a majority as sufficient.

4. Define dates and conditions

Record legal entities, sites, technical activities, exclusions, maximum three-year term and annual surveillance dates. Clarify any retained scope under restriction. Do not backdate recognition to an application or audit date, or issue a conditional initial grant while findings remain open.

5. Issue and publish

Send a reasoned notice with appeal route and authorised claim wording. The registry custodian publishes the approved scope and status, then controls any mark licence. A draft statement or blank template must never be mistaken for an issued recognition record.

Required record: F09 panel votes and decision; F10 recognition statement template.

OP11 Annual surveillance and family rotation

Owner: Programme manager and assessment team. Trigger: Annual cycle or additional risk review.

1. Schedule coverage

Complete surveillance by months 12 and 24 and review every hub annually. Visit physical technical facilities annually; independently approve remote-only office alternatives. Allocate one central day plus one per physical facility and half a day per remote-only hub, adding time for adequate evidence.

2. Reconcile changes

Review current families, hubs, architecture, support, suppliers, consequences, incidents and claims. Identify all consequential, new/materially changed and adverse-case families for mandatory demonstration. Routine releases still need technical controls even when they do not require corporate scope extension.

3. Select remaining demonstrations

From remaining families select at least $\text{ceil}(\sqrt{N})$, in addition to deduplicated mandatory groups. Rotate so every family is demonstrated within three years and expand for risk. Record population, selection and actual coverage rather than silently substituting convenient demonstrations.

4. Review events and operations

Review at least three actual completed events per family/responsible hub plus current operating/support evidence. When no new event occurred, assess continuing control using existing events and current conditions; do not require artificial releases. Recheck adverse cases, independent gates and recovery.

5. Determine continuing confidence

Apply programme findings, immediate technical-risk protection and verified closure as appropriate. Preserve overdue dates and obtain independent review/panel decisions for material status or scope changes. Publish precise current scope and next coverage dates.

Required record: F12 surveillance; F24 hub/family review.

OP12 Material change and scope extension

Owner: Programme manager with technical review and panel. Trigger: Planned change, five-day unplanned notice or extension request.

1. Register the change

Capture what changed, when it became known, affected entities/sites/families and the technical or contractual reason. Planned material changes are notified before implementation; unplanned changes within five calendar days. Serious incidents remain subject to the separate 48-hour clock.

2. Determine effects

Assess authorisation, competence, equipment, technical methods, data, customer obligations and existing recognition claims. A change of owner or software platform can alter accountability even when the delivering hub address stays the same. Preserve a coherent boundary for unaffected scope.

3. Select evidence and assessment

Specify necessary records, appropriate hub review and technical checks. New delivering hubs or families require the initial six-month, three-event, internal-audit, management-review and hub-assessment and family-demonstration gates. Existing history may support unchanged operations only where continuity is actually demonstrated.

4. Hold unsupported claims

Keep the extension outside active listings and mark use until a valid decision. If the change undermines existing assurance, initiate restriction or suspension review. Customer continuity cannot justify presenting an unassessed technology as recognised.

5. Decide and update

Obtain independent technical review and panel decision where scope or status changes. Issue a versioned schedule with effective dates and exclusions, update registry and delivering hub communications, and verify implementation of any required continuing controls.

Required record: F13 change review; updated scope schedule.

OP13 Incident and urgent interim suspension

Owner: Programme manager and independent technical lead. Trigger: Credible serious risk, falsification or material loss of control.

1. Receive and triage

Record awareness time, facts, uncertainty, affected release/change events and immediate actions. Verify that the organisation's notice is within 48 hours without treating that limit as permission to delay emergency response. Preserve source material and identify the most urgent protection needed.

2. Assess proportionality

Examine whether the failure is local, technology-specific or systemic. Consider customer harm, evidence integrity, ongoing release and reach of shared controls. Seek competent technical input promptly; do not wait for a completed root-cause output to protect credible serious risk.

3. Impose interim protection

The programme manager and independent technical lead may authorise a proportionate interim suspension. Record reasons, exact scope, effective time and required immediate actions. Notify the organisation promptly with a response route and communicate urgent protective status through controlled channels.

4. Obtain panel review

A three-person independent panel reviews the interim measure within five business days. Consider new evidence, fairness and continuing risk, then maintain, amend or lift the measure with reasons. The interim route shall not become an indefinite substitute for independent decision.

5. Track resolution

Monitor containment, affected-release remedies, investigation and verified correction. Preserve customer duties and accurate public status. Restoration requires competent verification and an independent decision; an appeal or promised corrective plan does not automatically restore active claims.

Required record: F11 protection; F14 incident; F09 panel review.

OP14 Complaints, whistleblowing and fair investigation

Owner: Uninvolved complaint owner. Trigger: Customer, worker or public concern.

1. Make outputting accessible

Accept concerns through clear channels with reasonable language and accessibility support. Explain confidentiality limits and collect only necessary details. Permit good-faith outputting without retaliation; an anonymous output can still warrant investigation when credible supporting facts exist.

2. Triage and assign

Identify immediate safety or integrity risks and trigger protection where necessary. Separate technical remedy, recognition misuse and programme-conduct issues. Assign an investigator uninvolved in the disputed work and screen conflicts, including relationships with the local delivering hub or commercial team.

3. Investigate evidence

Seek relevant release/change event records, authorisations, communications and interviews, preserving both supporting and contrary facts. Give affected parties a fair opportunity to respond. Do not dismiss a complaint solely because a delivering hub is recognised or require a customer to abandon applicable rights.

4. Decide within remit

Record substantiated findings, uncertainty, responsible remedy and any programme action. IAF does not assume every commercial liability or adjudicate issues outside its remit. Where evidence reveals a wider control failure, expand review beyond the original complaint.

5. Communicate and verify

Explain progress, delays and the outcome within confidentiality limits. Verify completion of corrective action and watch for retaliation or recurrence. Close the administrative case only after recording what was remedied, what remains disputed and the available escalation route.

Required record: F15 complaint and investigation record.

OP15 Independent appeal

Owner: Appeal administrator and separate panel. Trigger: Appeal received within 30 calendar days of decision notice.

1. Check admissibility

Record the appealed decision, notice date, filing date, grounds and requested remedy. Acknowledge receipt and identify missing evidence. Explain that necessary protective action remains effective unless specifically changed; filing an appeal does not extend an expired term.

2. Appoint a separate panel

Select three competent conflict-free members uninvolved in the original assessment, review or decision. Provide the complete controlled record and a fair route for the appellant to submit relevant information. Protect confidentiality without withholding the substance needed for meaningful response.

3. Review facts and process

Examine the challenged evidence, requirement interpretation, proportionality and procedural fairness. Distinguish a new application or scope extension from correction of a prior error. Obtain independent technical clarification where necessary without turning the appeal into consultancy.

4. Decide with reasons

All three members participate and at least two votes establish the reasoned outcome. Record whether the original decision is upheld, amended, remitted for further assessment or corrected. Target completion within 45 calendar days after complete evidence; explain delay and provide updates.

5. Implement the result

Notify parties, correct registry and claims where required, and preserve the original decision and appeal history. Consider whether a revealed error affects other cases or programme instructions. Verify corrective action without backdating a status to conceal an actual interruption.

Required record: F16 appeal intake, votes and outcome.

OP16 Registry, marks and public statements

Owner: Registry and mark custodian. Trigger: Decision publication, claim request or verification inquiry.

1. Validate the source decision

Accept only an authenticated authorised decision with programme, entity, scope version, effective and expiry dates and status. Check that the proposed public record matches it exactly. The custodian may correct a transcription error but cannot expand scope or change technical findings.

2. Publish usable status

Make sites, technical activities, exclusions and current status understandable to a customer. Keep personal and confidential release/change event data out of public records. Publish protective changes normally within two business days, sooner for urgent risk, and retain the actual decision effective time.

3. Control artwork and placement

Record approved artwork, licence holder, permitted channels and scope wording. Review websites, premises and invoice contexts for misleading implications. The corporate mark shall not become a product seal, vehicle approval or claim that IAF performed or guaranteed an individual technical output.

4. Handle verification failure

For outages, unknown IDs, suspicious records or stale caches, output unavailable or unresolved with retrieval time. Use the controlled manual route against authoritative case records. Record the responder, evidence and bounded confirmation; do not infer active status from an old certificate image.

5. Correct misuse

Capture misleading content, require proportionate removal or correction and verify all affected channels, including departed delivering hubs. Escalate deliberate or repeated misuse for status review. Preserve evidence and protect customers from ongoing false claims while fair investigation proceeds.

Required record: F17 verification; F18 mark licence; F27 misuse record.

OP17 Renewal, expiry, exit and restoration

Owner: Programme manager and independent panel. Trigger: Renewal, expiry, withdrawal or restoration request.

1. Start renewal early

Invite or review the renewal application at least six months before expiry. Reconcile all changes, complaints, surveillance and authorisations. Apply initial/renewal audit floors, every-hub coverage and demonstrations of all families and challenge of relevant technical roles and actual-event review to the current scope.

2. Decide before expiry

Complete assessment, effective closure, independent technical review and panel decision in time. A pending application, commercial arrangement or appeal does not extend the stated term. If no valid renewal decision exists, record Expired and control active claims.

3. Manage orderly exit

For withdrawal, closure or organisation departure, identify unfinished work, continuing support obligations, customer complaints and record custody. Require removal of unsupported marks and directory claims. Recognition ending does not erase the organisation's continuing customer and legal obligations.

4. Verify restoration

For a restricted or suspended case, assess corrective action, affected-release disposition and demonstrated effectiveness. Use additional physical or independently approved remote-only office review where needed. A changed manager or new policy alone is not evidence that the technical or integrity failure has been corrected.

5. Record the new outcome

Obtain the independent panel's reasoned decision and publish exact retained or restored scope with effective dates. Keep interruption and prior-status history. A withdrawn or expired entity seeking a new recognition follows the applicable application route rather than assuming automatic restoration.

Required record: F19 renewal/exit; F09 decision; updated registry.

OP18 Information, provenance and record lifecycle

Owner: IAF and organisation information owners. Trigger: Routine operation, migration, compromise or disposal.

1. Define record classes

Separate public corporate scope from confidential source, build, validation, customer and operational data. Assign purpose, owner, access, retention and lawful transfer. Release assurance evidence remains ten years after last delivery or declared support end, whichever is later; IAF cases ten years after expiry/withdrawal, subject to binding limits and holds.

2. Minimise protected access

Use necessary extracts, controlled viewing and appropriate confidentiality rather than indiscriminate repository or raw telemetry copying. Restrict credentials and sensitive findings. Retain enough lawful source context for independent checking; privacy is not a reason to conceal a material contradiction.

3. Preserve provenance and corrections

Protect original results, identities, versions and material changes. Keep corrected decisions and outputs linked to originals. Authenticate consequential approvals and track migration; a typed name or copied signature is not by itself verified authority.

4. Test restoration and incidents

Recover source/build/release links, deployed state, evidence and authoritative status after outage or compromise. Preserve investigation evidence and notify affected parties under actual duties. Uncertain integrity must remain unresolved until independently reconciled.

5. Dispose and transfer responsibly

Apply documented retention limits, lawful holds and verified disposal or custody transfer. Minimise personal data and preserve essential lawful technical evidence. Closure, acquisition or support exit shall not silently abandon customer protection or necessary assurance records.

Required record: F22 records; F23 continuity; R06-R16 evidence.

OP19 Product family admission and support review

Owner: Organisation technical executive. Trigger: New family, major change, acquisition or support exit.

1. Identify responsibility and boundary

Define product/service family, architecture, lifecycle role, delivering hubs, intended use, consequence and dependencies. Distinguish supported release lines from prototypes and third-party offerings. Record technical justification for grouping.

2. Verify actual capability

Review competent roles, six-month implemented controls, three actual events per responsible hub and internal audit/review. Check original validation, provenance, independent release authority and operational evidence. A purchased codebase does not automatically bring valid history or support capability.

3. Review change and support

Assess compatibility, customer commitments, security maintenance, supplier support and end-of-life implications. Set support dates/resources and a tested exit or migration route appropriate to actual consequences. Do not invent a universal duration unrelated to obligations.

4. Obtain extension decision

Keep new scope outside active claims until assessment, independent review and panel decision are complete. A routine release within unchanged approved scope uses technical release control; a material change receives the notification and assessment required by its impact.

5. Maintain or retire responsibly

Review ongoing capability, critical dependencies, support promises and actual failures. Before support exit, protect users, communicate limitations, preserve necessary evidence and update scope/claims. Recognition ending does not erase existing support or correction duties.

Required record: F24 scope review; F25 support/configuration record; F28 extension.

OP20 Controlled lifecycle and release assurance

Owner: Product owner, technical authority and independent reviewer. Trigger: Every material software/service change.

1. Define change and consequence

Confirm authorised purpose, requirements, affected configurations/users, rights, data and safety/security implications. Set acceptance, evidence and stop criteria before testing. Separate prototype experiments from production authority and identify required independent reviewers.

2. Implement with traceability

Control source/configuration changes, access, code review, dependencies, toolchain and build provenance. Preserve exact artifacts and rights information. Generated code and external components require appropriate verification; a successful build or signed package alone is insufficient.

3. Verify intended behaviour

Retain original positive/adverse results, representative integration evidence, uncertainties, failed attempts and defect disposition. Validate consequential tool outputs and AI use within their limits. Independent reviewers challenge evidence and unresolved blockers before release.

4. Authorise safe deployment

Confirm every mandatory release gate, target compatibility, support, staged rollout and validated recovery. Authenticate the release decision and verify actual target/service state. Emergency work retains essential controls; retrospective paperwork cannot make a known unacceptable condition conforming.

5. Monitor and correct

Watch real outcomes, vulnerabilities, drift and support cases. Identify affected populations, contain serious risk and verify remedies and necessary notices. Preserve original and corrected versions, support/end-of-life duties and lessons for subsequent work.

Required record: R01-R16 lifecycle and release dossier; original attachments.

Operating clocks and follow-up

Finding deadlines run from written notice. Urgent protection starts when risk is known; incident notice runs from awareness. Record exact dates and time zones, and use the specified calendar or business-day basis.

Action	Time	Condition
Initial / new scope history	At least 6 months	Implemented controls by family/responsible hub; internal audit and review complete.
Completed event sample	At least 3 per family/hub	Real delivery or operation; no duplicate targets or invented trivial changes.
Internal audit / review	Before grant; annually	All hubs, families and relevant controls.
IAF conflict look-back	At least 36 months	Extend for residual risks; applies to IAF case personnel.
Factual response	15 calendar days	Reasoned extension possible without delaying protection.
Initial finding closure	Before grant	Every applicable requirement Met; all findings closed.
Active Minor finding	Within 90 calendar days	Essential assurance protected; from written notice.
Active Major finding	30-calendar-day target	Immediate containment; suspension review if unresolved.
Critical condition	Immediate protection	No finding clock permits delay of urgent software-risk response.
Interim suspension review	Within 5 business days	Independent three-person panel.
Serious notice to IAF	Within 48 hours of awareness	Earlier duties and emergency action take precedence.
Material changes	Planned: before; unplanned: 5 days	Calendar days; serious-incident clock also applies.
Surveillance	By months 12 and 24	Annual hub review and IR02 family demonstrations.
Family rotation	All within 3 years	Annual mandatory groups plus ceil square root of remaining families.
Term / renewal application	Max 3 years / 6 months early	No automatic extension beyond expiry.

Action	Time	Condition
Appeal filing	Within 30 calendar days	From decision notice.
Appeal outcome	45-calendar-day target	After complete evidence; explain delays.
Protective registry update	Normally within 2 business days	Sooner for urgent risk; preserve actual effective time.
Release assurance evidence	At least 10 years	After last delivery or declared support end, whichever later; binding limits/holds.
IAF case records	10 years after expiry/withdrawal	Binding limits/holds and minimised personal data.
Consequential release review	Before release	Competent independent challenge and all mandatory gates.
Operator assurance	Annual / independent every 3 years	Four diverse pilots and essential-gap closure before launch.

Borderline cases

A small developer lacks an independent reviewer

Arrange competent external verification and release challenge with protected access and outcome-independent fees. Self-approval cannot replace consequential independent review.

A remote-only office requests no physical visit

An uninvolved reviewer must approve secure live observation and original-source review adequacy. Physical vehicle/hardware/test facilities remain subject to physical visits.

One release was installed on one thousand targets

Count it as one event per family/hub, not one thousand. Review actual target outcomes separately and demonstrate each hub contribution where shared evidence is used.

A stable supported family has no new release this year

Review its existing completed events and current support, incidents, dependencies and operating state. Do not manufacture changes solely to satisfy a sample.

A critical vulnerability appears while a Minor finding is open

Protect affected systems immediately according to actual exposure. A programme finding deadline is not a grace period for uncontrolled critical exploitation.

Rollback would corrupt the new data schema

Retain the hold until a validated safe recovery route exists, such as coordinated roll-forward or isolation. A generic rollback policy is not sufficient.