



IAF SNR | SERVICE NETWORKS | 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

Authorised Service Networks
Corporate Recognition | English master text

International Automotive Federation

iaf.com

Document control

Item	Controlled value
Programme	IAF Service Network Recognition Programme (IAF SNR)
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 Service Operations Manuals; Applicant Guide; controlled forms.
Authority boundary	Corporate implementation assurance. Manufacturer service appointments, vehicle approvals and other IAF programme decisions remain distinct.
Control	Retain exact scope and criterion versions. Protect completed records, personal information and service 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, families and audit planning	8
OP05 Desk review and evidence authenticity	8
OP06 Physical outlet and mobile assessment	9
OP07 Classify findings and protect affected jobs	10
OP08 Corrective action and effectiveness verification	10
OP09 Independent technical review	11
OP10 Independent recognition decision	12
OP11 Surveillance and continuing confidence	12
OP12 Material change and scope extension	13
OP13 Incident and urgent interim suspension	13
OP14 Complaints, whistleblowing and fair investigation	14
OP15 Independent appeal	15
OP16 Registry, marks and public statements	15
OP17 Renewal, expiry, exit and restoration	16
OP18 Information security and record lifecycle	17
OP19 Outlet authorisation and network enforcement	17
OP20 Service job authorisation and release assurance	18
Operating clocks and follow-up	19
Borderline cases	20

Roles and decision separation

Role	Responsibility	Boundary
IAF programme owner	Adopts controlled rules, resources and launch gates.	Cannot direct a favourable case outcome.
Programme manager	Controls intake, coverage, deadlines and case administration.	May impose urgent interim protection only with independent technical lead.
Lead assessor	Plans and leads evidence collection and findings.	Does not make the independent recognition decision.
Technical assessor / expert	Verifies relevant service technology and competence.	Works within authorised technical scope; discloses conflicts.
Independent technical reviewer	Checks evidence, scope, findings and closure.	Was not involved in the assessment or applicant consultancy.
Decision panel	Three members decide with recorded individual votes.	All participate; at least two affirmative votes plus all gates for grant.
Appeal panel	Different three members review contested decisions.	No involvement in the original case; conflicts screened.
Registry and mark custodian	Publishes authorised status and controls artwork/licences.	Does not alter the technical decision or invent effective dates.
Network executive	Owns quality adoption, resources and enforceable outlet control.	Cannot waive technical safety or customer rights.
Outlet manager / technical lead	Controls local jobs, competence, evidence and release.	Does not extend recognised scope without decision.
Independent release checker	Verifies safety-critical work and holds.	Did not perform the critical steps being checked.
Operator assurance reviewer	Audits IAF programme operation and consistency.	Independent of the operational work reviewed.

Procedure map

Code / procedure	Owner	Trigger
OP01 Programme adoption and launch	IAF programme owner	Before live recognition or material relaunch
OP02 Application and eligibility review	Programme manager	New application, renewal or extension
OP03 Team selection and impartiality	Programme manager and independent impartiality reviewer	Before each assignment and after material conflict information

Code / procedure	Owner	Trigger
OP04 Scope, families and audit planning	Lead assessor with technical reviewer	After eligibility acceptance and before fieldwork
OP05 Desk review and evidence authenticity	Assessment team	Before and during physical audit
OP06 Physical outlet and mobile assessment	Lead assessor and technical assessors	Initial, annual, renewal or triggered visit
OP07 Classify findings and protect affected jobs	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 service failure
OP09 Independent technical review	Uninvolved competent reviewer	After assessment and verified closure
OP10 Independent recognition decision	Three-person decision panel	Technically reviewed case
OP11 Surveillance and continuing confidence	Programme manager and assessment team	Annual cycle or additional risk-triggered 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 security and record lifecycle	IAF information owner and organisation record owners	Routine operation, migration, incident or disposal
OP19 Outlet authorisation and network enforcement	Network executive and outlet technical lead	Outlet admission, permission change or enforcement issue

Code / procedure	Owner	Trigger
OP20 Service job authorisation and release assurance	Outlet manager, technician and independent checker	Every included service job

OP01 Programme adoption and launch

Owner: IAF programme owner. Trigger: Before live recognition or material relaunch.

1. Establish authority

Record programme ownership, decision authority, controlled editions, resources and accessible operating information. Identify the exact claim the programme will support. Keep prepared documents separate from adopted operating rules and do not issue live recognition before the launch gates are closed.

2. Build competent operation

Appoint assessors, reviewers, panels, complaint handlers and registry staff against role-specific competence. Screen conflicts and test separation of commercial and technical functions. Verify confidential evidence access, case security and the ability to preserve original decisions.

3. Run representative pilots

Complete at least four pilots covering owned, franchise, mobile/remote and high-technology service operations, including a failed or contested case. Test real scope boundaries, duration, critical findings, independent review, appeal and an urgent protective-status update. Label pilot outputs clearly as such.

4. Validate public verification

Test a valid, restricted, suspended, expired and unknown record, effective dates, scope versions and manual fallback. Simulate an outage and an altered record. Confirm that neither the portal nor staff present unresolved or stale information as active confirmation.

5. Authorise launch

Review pilot weaknesses and close essential gaps. Approve adoption and effective operation through the authorised programme owner, with independent operator-assurance evidence. Publish the operating edition and scope limits; retain a reasoned record of readiness and unresolved nonessential improvement actions.

Required record: F20 programme review; F21 pilot and launch record.

OP02 Application and eligibility review

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

1. Register the case

Assign a unique case reference, identify all legal applicants and capture submission version, contact and requested route. Separate readiness review from recognition assessment and explain that application does not grant public status. Preserve original submissions and later changes.

2. Validate identity and authorisation

Check legal authority, entity undertakings, underlying service authorisations and permitted activities. Distinguish the centre from the customer-contracting outlet. Resolve false or ambiguous authorised-service claims before accepting a recognition scope; do not assume group branding proves legal control.

3. Check minimum evidence

Confirm six months of implemented operation, completed internal audit and management review, and three actual jobs per service family/site. Review the full proposed roster and unsupported technologies. If the gates are absent, defer recognition assessment or agree a clearly private readiness route.

4. Assess access and competence

Check whether competent assessment, safe physical access, original records and lawful information review are feasible for every requested site. Identify languages, technical specialisms and restrictions. Define a narrower coherent scope if necessary; do not obscure an evidence gap through vague wording.

5. Record acceptance

Issue a reasoned acceptance, clarification, deferral or refusal of the requested assessment route. Identify the accepted scope version, missing items, proposed responsibilities and expected process. Acceptance of the application remains distinct from a favourable recognition decision.

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 reporting 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, families and audit planning

Owner: Lead assessor with technical reviewer. Trigger: After eligibility acceptance and before fieldwork.

1. Freeze the planning boundary

Reconcile entity, outlet, mobile-unit, remote-hub and family lists against actual operations and authorisations. Identify support functions and critical external work. Define family grouping by methods, competence and release controls; do not group fundamentally different repairs solely to reduce samples.

2. Calculate the effort

Use two central auditor-days plus site floors of two, three or four days by effective workforce bands up to 100, 101-500 and above 500. Add one site-day per defined material risk factor. Annual surveillance starts at one central plus one per operational site. Record necessary additions.

3. Allocate real coverage

Physically assess every included operational site and unit. Provide at least a full operating day per site, with at least half on-site time for observation, witnessing and interviews. Observe at least two shifts where multiple shifts operate. Shared staff or a combined visit shall not double-count assessment hours.

4. Select evidence

Obtain complete job populations and independently select at least three completed jobs per family/site, including adverse, changed and repeat cases where available. Schedule relevant live critical work and trace outsourced interfaces. More cases or time may be necessary for diversity, weak evidence or failure patterns.

5. Confirm the plan

Agree practical access, safety induction, languages, customer-data protection and working hours without allowing the applicant to select only favourable evidence. Record unavailable activities and how they will be addressed. Unverified essential scope is deferred rather than marked Met by assumption.

Required record: F04 plan and duration; scope schedule; F24 outlet control.

OP05 Desk review and evidence authenticity

Owner: Assessment team. Trigger: Before and during physical audit.

1. Review controlled texts

Check adoption, editions, requirement maps, authorisation instruments and scope versions. Identify contradictions between policy, contracts, booking claims and actual capability. Map additional IAF claims separately and avoid treating this recognition as automatic certification of other programmes.

2. Follow actual jobs

Trace selected jobs through intake, authority, diagnosis, estimate, consent, parts, work, tests, release and handover. Compare system timestamps with original records and the actual sequence. Include failed tests and revised estimates rather than using the final summary alone.

3. Test source integrity

Check who created and changed material records, how attachments link to the job and whether originals can be retrieved. Distinguish later reconstruction from contemporaneous evidence. Investigate copied signatures, repeated photographs, unexplained perfect results or missing adverse records without presuming guilt from one anomaly.

4. Protect information

Use minimised extracts, controlled viewing and authorised interpretation where necessary. Preserve enough information to support the conclusion while avoiding unnecessary customer identifiers. Document limitations and a lawful review route; essential facts that cannot be verified remain unresolved.

5. Prepare focused fieldwork

Identify high-risk uncertainties, weak interfaces and cases requiring observation or interviews. Update the sampling plan with reasons. Policies and desk evidence can focus a visit, but cannot replace the required physical assessment or demonstrate tasks never actually performed.

Required record: F05 evidence log; self-assessment; indexed job dossiers.

OP06 Physical outlet and mobile assessment

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

1. Open the visit

Confirm actual scope, authorisations, workforce, shifts, available jobs and safety arrangements. Explain independent interviews, stop rules and evidence protection. Resolve material differences from the approved plan before treating the visit as complete.

2. Observe the service chain

Witness intake, customer approval, technical preparation, work, independent critical checks and release as relevant. Ask workers to explain actual decisions and limitations. For mobile units observe base controls and a real or safely arranged representative job setting, preserving the actual-job evidence distinction.

3. Challenge critical interfaces

Check parts identity, tool suitability, technical method versions, remote-provider access and handovers. Trace an adverse result to its disposition and ask how a release hold prevents handover or dispatch. Observe the relevant shifts and variations instead of repeating the same low-risk task.

4. Verify central and local control

Compare outlet practice with centre requirements and contractual authority. Interview staff without coaching, review a local complaint and trace its escalation. An effective headquarters process cannot substitute for a local inability to perform an included service safely and competently.

5. Close with facts

Present supported findings, affected scope and unresolved evidence. Record the applicant's factual comments without bargaining away requirements. Explain response, containment and next steps. A closing meeting recommendation is not the independent recognition decision.

Required record: F05 evidence; F24 outlet review; checklist.

OP07 Classify findings and protect affected jobs

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, job or population and the gap. Distinguish a missing record from evidence of unsafe work. Explain the scope and uncertainty; do not infer a network-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 client size, to determine severity.

3. Contain immediately

Require proportionate action to protect people, vehicle release, data and affected customers. Trace potentially affected earlier jobs 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 service failure.

1. Accept responsibility and contain

Identify the immediate affected work and a justified earlier-job 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 network 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 outlets. 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 jobs. 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-job register.

OP09 Independent technical review

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

1. Check independence and scope

Confirm your competence and conflict clearance. Reconcile the requested, assessed and proposed scope, including excluded outlets and underlying authorisations. Verify that the applicant's claimed public wording matches the conclusion the evidence can actually support.

2. Check mandatory gates

Verify six months of implementation, internal audit, management review, completed-job floors, physical site coverage, duration and relevant witnessing. Review every essential gate and additional IAF claim map. A checklist total is not a substitute for the substantive evidence.

3. Review findings and reasoning

Confirm classifications, contradictory evidence, prior-job impact and effectiveness of closure. Challenge unsupported NA decisions and coherent exclusions. Require clear reasons where different outlets or configurations receive different conclusions.

4. Resolve gaps

Return queries to the assessment team without providing applicant consultancy or silently changing the evidence. Require additional work where essential facts remain unsupported. Retain the query and response trail so the decision panel can understand material changes.

5. Recommend a bounded decision

Record ready, defer or not supported, with exact scope, evidence manifest, residual nonessential limitations and proposed surveillance focus. The reviewer checks the case and does not bypass the three-person independent panel.

Required record: F08 technical review and panel-readiness record.

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, physical coverage, evidence authenticity and release safety 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, services, 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 Surveillance and continuing confidence

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

1. Plan before the due date

Schedule surveillance by months 12 and 24 and annual physical coverage of every operational site. Start with one central auditor-day plus one per site and add time for actual risk. Include mobile units, remote hubs and changed critical operations.

2. Review changes and adverse facts

Reconcile directory, authorisations, services, competence, complaints, repeat repairs, incidents and public claims since the last decision. Check that proposed extensions remain outside active scope. Follow up previous weaknesses without limiting review to the same familiar samples.

3. Verify ongoing operation

Review at least three actual jobs per family/site, expand for failures and witness relevant critical work. Check implementation of network actions and independent release controls. Observe at least two shifts where multiple shifts operate and document unavailable essential activity.

4. Act on findings

Apply active Minor, Major and Critical rules with containment and verified closure. Protect affected scope proportionately and examine systemic effects. An overdue visit or incomplete essential review is not resolved by silently changing the due date.

5. Maintain or change status

Complete technical review and any required independent decision for a change of status or scope. Record continuing confidence and next review focus when status remains supported. Publish protective changes promptly and preserve original deadlines and effective dates.

Required record: F12 surveillance plan; F24 outlet review; checklist.

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 outlet address stays the same. Preserve a coherent boundary for unaffected scope.

3. Select evidence and assessment

Specify necessary records, physical review and technical checks. New outlets or service families require the initial six-month, three-job, internal-audit, management-review and physical-assessment 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 service 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 outlet 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 jobs 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 report 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-job 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 reporting accessible

Accept concerns through clear channels with reasonable language and accessibility support. Explain confidentiality limits and collect only necessary details. Permit good-faith reporting without retaliation; an anonymous report 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 service remedy, recognition misuse and programme-conduct issues. Assign an investigator uninvolved in the disputed work and screen conflicts, including relationships with the local outlet or commercial team.

3. Investigate evidence

Seek relevant job 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 an outlet 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, services, exclusions and current status understandable to a customer. Keep personal and confidential job 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 repair.

4. Handle verification failure

For outages, unknown IDs, suspicious records or stale caches, report 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 outlets. 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-site physical coverage and actual-job 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 network departure, identify unfinished work, warranties, 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-job disposition and demonstrated effectiveness. Use additional physical 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 security and record lifecycle

Owner: IAF information owner and organisation record owners. Trigger: Routine operation, migration, incident or disposal.

1. Define record classes

Distinguish public status, confidential case evidence, technical job data and personal identifiers. Assign purpose, access roles, retention and disposal basis. IAF case records are retained ten years after expiry/withdrawal; service technical records at least ten years after job closure, subject to binding limits.

2. Minimise and protect

Use necessary identifiers, protected transfer and restricted access. Separate or pseudonymise personal information when no longer needed and document lawful holds. Do not interpret the technical-retention rule as permission to keep unnecessary raw telematics, contact or location data indefinitely.

3. Preserve integrity and continuity

Maintain material version history, authenticated authorisations and access logs. Test backup restoration and reconcile records after outage or migration. A successful file copy is not enough if job links, timestamps or scope decisions are corrupted.

4. Respond to compromise

Contain suspected unauthorised access or altered records, preserve evidence and assess affected parties and decisions. Notify under applicable duties and re-establish authoritative information. Treat questionable public status as unresolved until independently verified.

5. Dispose and assure

Delete or irreversibly de-identify records when their purpose and lawful retention end, with documented approval. Audit retrieval, access revocation and disposal periodically. Preserve only the evidence needed for continuing obligations and explain material limitations in future reviews.

Required record: F22 information control; F23 continuity exercise.

OP19 Outlet authorisation and network enforcement

Owner: Network executive and outlet technical lead. Trigger: Outlet admission, permission change or enforcement issue.

1. Verify the underlying appointment

Check the actual issuer, legal entity, location, brand, service activities, territory and validity of every claimed authorisation. Retain reliable confirmation and any restrictions. A logo, parts account or training attendance is not sufficient proof of a service appointment.

2. Bind responsibilities

Execute participation undertakings covering quality controls, record access, corrective action, customer remedies, incident reporting and claim removal. Identify who contracts with the customer and how the centre can enforce compliance. Resolve gaps before proposing outlet inclusion.

3. Monitor validity and capability

Track authorisation expiry and conditions, competence, equipment, technical access and actual service performance. Reconcile the public directory and booking system with approved scope. Investigate whether an outlet continues to sell a service after losing the means or permission to perform it.

4. Enforce proportionately

Stop unsupported authorised-service claims, restrict affected work and arrange responsible customer handover when necessary. Notify IAF under change or serious-incident rules. Do not assume that losing one brand appointment automatically proves every independent service unsafe; assess the exact affected scope.

5. Control departure

Remove departed outlets from active listings, revoke network assets and identify record, warranty and complaint responsibilities. Verify removal of marks from local channels and preserve necessary evidence. Record any surviving independent service scope separately and only after the applicable decision.

Required record: F24 outlet review; F25 authorisation register; scope schedule.

OP20 Service job authorisation and release assurance

Owner: Outlet manager, technician and independent checker. Trigger: Every included service job.

1. Accept and authorise

Create a unique job, verify vehicle and customer authority, record condition and concern, and agree a clear diagnostic or repair scope. Preserve estimate versions and actual consent. Confirm capability before work, including specialist referrals and access to current technical methods.

2. Diagnose and plan

Record initial symptoms, tests, cause reasoning and uncertainty. Define actual repair instructions, critical steps, parts, tools, competence and acceptance criteria. Obtain approval for material changes. A sales target or insurer instruction does not replace technical validity and necessary customer consent.

3. Execute with evidence

Record work, parts identity, changed configuration, hold points and unexpected findings. Preserve failures and interruptions. Use the relevant technology supplement for electrical, structural, calibration or software activity and keep the original technical results, not merely a final green indicator.

4. Verify and release

Complete job-specific checks and independent verification of safety-critical work. Resolve essential anomalies before technical release. Plan any test drive lawfully and safely. If a customer declines work, record the evidence, risk explanation and lawful safe disposition without presenting the signature as a safety waiver.

5. Handover and learn

Explain completed work, invoice, warranty and remaining limitations; return records and property appropriately. Link repeat visits, complaints and incidents back to the job. Verify remedies and feed actual failures into outlet and network improvement, protecting customer information throughout.

Required record: J01-J16 service job dossier and original technical 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 / extension history	At least 6 months	Real operation for each included outlet/family; actual evidence, not plans.
Completed jobs	At least 3 per family/site	Initial, renewal and audit sampling floor; expand for risk and diversity.
Internal audit and review	Before initial grant; annually	Cover all included outlets and applicable scope.
Conflict look-back	36 months minimum	Longer if residual impartiality risk remains.
Draft finding response	15 calendar days	Reasoned extension possible; urgent protection need not wait.
Initial finding closure	Before grant	Every applicable requirement Met; no open findings.
Active Minor closure	Within 90 calendar days	Essential assurance protected; verified effective closure.
Active Major closure	30-calendar-day target	Immediate containment; unresolved case requires suspension review.
Critical risk	Immediate protective review	Protect people, evidence and affected scope immediately.
Interim suspension review	Within 5 business days	Three-person independent panel reviews the interim measure.
Serious incident notice	Within 48 hours of awareness	Earlier emergency or applicable reporting duties take precedence.
Planned material change	Before implementation	Extension claims wait for applicable independent decision.
Unplanned material change	Within 5 calendar days	48-hour clock applies if it is also a serious incident.
Surveillance	By months 12 and 24	Every operational site physically visited annually; adequate added time.
Recognition term	Maximum 3 years	No automatic extension beyond stated expiry.
Renewal application	At least 6 months before expiry	Decision must precede expiry to maintain continuity.
Appeal filing	Within 30 calendar days	Measured from decision notice.
Appeal outcome	45-day target after complete evidence	Calendar days; explain delays and provide updates.

Action	Time	Condition
Protective registry update	Normally within 2 business days	Sooner for urgent risk; preserve effective decision time.
Technical service records	At least 10 years after job closure	Binding retention limits apply; minimise personal identifiers.
IAF case records	10 years after expiry/withdrawal	Binding limits and lawful holds; protect personal information.
Operator assurance	Annual; independent review every 3 years	Launch pilots and essential-gap closure before live operation.

Borderline cases

A large franchise network requests sampled outlets

This edition requires physical coverage of every included operational site. Agree a smaller accurately bounded scope or sufficient resources; a sampling shortcut is not an adopted option.

A competent outlet has one open Minor at initial review

Defer initial recognition until effective closure. Active-status closure allowances do not apply to an initial grant.

The manufacturer appointment ends during the term

Remove the affected authorised-service claim and evaluate technical access, permissions and scope. Do not assume automatic extension of the appointment or automatically condemn unrelated competent independent services.

An annual visit is overdue

Review status promptly and impose proportionate restriction or suspension where essential assurance is unsupported. Preserve the original due date; do not silently reset the clock.

A declined repair includes a material safety concern

Document the evidence, customer communication and lawful safe disposition. A disclaimer cannot create a conforming unsafe repair or a general right to detain the vehicle.

A remote programming ticket closes but the vehicle remains faulty

Retain the technical release hold, verify actual configuration and required local checks, and investigate the discrepancy before handover.