



IAF PPR | PROFESSIONAL PRACTICE | 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

Independent Experts & Professionals
Corporate Recognition | English master text

International Automotive Federation

iaf.com

Document control

Item	Controlled value
Programme	IAF Professional Practice Recognition Programme (IAF PPR)
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 Professional Practice Manuals; Applicant Guide; controlled forms.
Authority boundary	Corporate implementation assurance. Individual role authorisation is separate; no transferable personal licence, report endorsement or vehicle approval is conferred.
Control	Retain exact scope and criterion versions. Protect completed records, personal information and professional 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, personnel coverage and assessment planning	8
OP05 Desk review and evidence authenticity	8
OP06 Hub observation and professional technical challenge	9
OP07 Classify findings and protect affected engagements	10
OP08 Corrective action and effectiveness verification	10
OP09 Independent technical review	11
OP10 Independent recognition decision	12
OP11 Annual surveillance and continuing confidence	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 security and record lifecycle	17
OP19 Professional roster admission and role control	18
OP20 Engagement, expert opinion and report control	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 individual decision.
Programme manager	Controls intake, scope, deadlines and records.	Urgent interim protection needs independent technical lead concurrence.
Lead assessor	Plans evidence, coverage and findings.	Does not make the independent recognition decision.
Technical assessor	Challenges relevant professional competence and methods.	Works within demonstrated discipline competence.
Independent technical reviewer	Checks the recognition case and closure.	Uninvolved in its assessment or applicant consultancy.
Decision panel	Three uninvolved members; at least two reasoned votes.	All participate; every gate remains mandatory for grant.
Appeal panel	Different three members review the challenged decision.	No original-case involvement; conflicts screened.
Registry and mark custodian	Publishes approved status and scope.	Cannot create competence or alter technical decisions.
Practice executive / proprietor	Owns implementation, resources and role control.	Cannot override unsupported technical conclusions.
Independent engagement lead	Owns instructions, analysis and bounded opinion.	Acts only within authorised disciplines and competence.
Case technical reviewer	Independently challenges consequential work before issue.	Did not create/direct the conclusion; ordinary review fees allowed.
Operator assurance reviewer	Audits programme integrity and performance.	Independent of the operation reviewed.

Procedure map

Code / procedure	Owner	Trigger
OP01 Programme adoption and launch	IAF programme owner	Before public recognition
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
OP04 Scope, personnel coverage and assessment planning	Lead assessor with technical reviewer	After eligibility review

Code / procedure	Owner	Trigger
OP05 Desk review and evidence authenticity	Assessment team	Before and during hub and professional assessment
OP06 Hub observation and professional technical challenge	Assessment team	Initial, annual, renewal or triggered assessment
OP07 Classify findings and protect affected engagements	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 professional 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 Annual surveillance and continuing confidence	Programme manager and assessors	Annual cycle and risk triggers
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 Professional roster admission and role control	Practice executive and competence authority	Admission, new discipline, departure or concern
OP20 Engagement, expert opinion and report control	Independent lead and independent technical reviewer	Every scoped engagement

OP01 Programme adoption and launch

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

1. Record authority

Adopt the exact edition, accountable governance, funding, competence and conflict controls. Separate programme development from an issued status. Publish intelligible eligibility, costs and review routes without promising universal acceptance or predetermined decisions.

2. Prepare impartial operation

Appoint at least two competent assessors for a case, an uninvolved technical reviewer and three uninvolved decision members. Test access controls, evidence preservation, role separation and impartiality screening over at least 36 months for IAF case personnel.

3. Complete representative pilots

Run at least four pilots covering a sole practice, multidisciplinary firm, disputed physical investigation and remote/digital practice. Include a failed or contested case. Test technical challenge, source review, duration, safe witnessing, an appeal and an urgent protective measure.

4. Test verification

Test active, restricted, suspended, expired and unknown records, including scope versions, individual role boundaries and manual fallback. An outage must produce unavailable or unresolved rather than a stale active confirmation. Keep private client and personnel evidence out of public records.

5. Approve operation

Close essential pilot weaknesses, independently verify readiness and record the adoption and effective operating date. Retain residual improvement actions with owners. Do not issue live recognition until competent operation and reliable public verification are demonstrably available.

Required record: F20 operator review; F21 pilot and launch approval.

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, required professional permissions and permitted activities. Identify the actual contracting entity and each delivering hub. Resolve unsupported personal credentials or discipline claims; 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 engagements per discipline/hub. Verify each independent lead's 24-month relevant experience and three representative assignments in the preceding 36 months per discipline. 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, required physical or independently approved remote-only office access, original records and lawful information review are feasible for every requested hub. 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, personnel coverage and assessment planning

Owner: Lead assessor with technical reviewer. Trigger: After eligibility review.

1. Reconcile scope

Identify every contracting entity, delivering hub, professional discipline, named lead and material external reviewer. Apply PRC and each triggered profile/domain. Separate advisory services from regulated activities and future capabilities. Do not treat one person's specialist competence as that of the whole firm.

2. Determine hub coverage

Assess every delivering hub at initial and renewal stages and review every hub annually. Physical facilities handling subjects require physical initial, renewal and annual assessment. A remote-only office may use secure live observation and original-source review only where an uninvolved reviewer approves adequacy; otherwise arrange a physical visit or defer.

3. Determine personnel coverage

At initial and renewal directly interview and technically challenge every named independent lead in each authorised discipline. Annually cover all new or materially changed leads and adverse cases, plus the ceiling of the square root of remaining leads. Rotate this additional selection so every lead is covered within three years; enlarge it for risk.

4. Calculate effort

Initial/renewal minimum is two central auditor-days plus one per hub up to ten professionals, two for 11-50 and three above 50. Add one hub-day for each material factor: novel consequential method, hazardous/destructive activity, complex critical outsourcing and unresolved systemic risk. Annual minimum is one central day plus one per physical technical facility and half a day per remote-only hub. Add time needed for all coverage; exclude travel and double-counted hours.

5. Approve evidence plan

Select at least three completed engagements per discipline/hub and expand for adverse facts, methods and personnel diversity. Physical assessment spans at least one full operating day, with at least half on-site time on observation, interviews and witnessing. Record dates, secure access, interpreters, limitations and independent approval of any remote-only office route.

Required record: F04 plan; professional roster; F24 hub review.

OP05 Desk review and evidence authenticity

Owner: Assessment team. Trigger: Before and during hub and professional assessment.

1. Review controlled texts

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

2. Follow actual engagements

Trace selected engagements through instructions, conflicts, authority, evidence collection, methods, analysis, independent review, issue and subsequent correction. Compare original timestamps with the actual sequence. Include adverse facts, failed methods, review disagreement and superseded conclusions rather than the final summary alone.

3. Test source integrity

Check who created and changed material records, how attachments link to the engagement 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 client 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 E01-E16 engagement dossiers.

OP06 Hub observation and professional technical challenge

Owner: Assessment team. Trigger: Initial, annual, renewal or triggered assessment.

1. Verify actual operation

Reconcile the included hub, people, equipment, original case population and controlled methods. Observe physical technical work safely where relevant. Do not stage dangerous work solely for an audit or accept a promotional demonstration as proof of sustained practice.

2. Challenge professional reasoning

Ask each selected independent lead to explain an actual assignment, competence boundary, contradictory evidence, method choice, uncertainty and limits. Use a relevant changed assumption or alternative scenario to test understanding. A memorised answer, credential or years-of-service claim alone is insufficient.

3. Trace the complete case

Follow instructions, conflict clearance, evidence acquisition, analysis, review, issued report and subsequent correction. Distinguish personal authorship from team participation. Identify actual independent review and unresolved queries. Inspect original material through a lawful protected route if copying is inappropriate.

4. Verify special boundaries

For a remote-only hub test live identity, source access, actual workflow and evidence integrity under the approved plan. For disputed or privileged work obtain authorised redacted context or protected review; do not demand unlawful disclosure. Where essential evidence cannot be verified, defer or exclude the unsupported scope with reasons.

5. Conclude with limits

Document evidence, adverse facts, technical challenge results and remaining uncertainty. Expand cases or interviews where discrepancies arise. Safe simulations supplement competence review but do not replace the three real completed engagements or demonstrated professional history.

Required record: F05 evidence log; F24 hub review; named professional roster.

OP07 Classify findings and protect affected engagements

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, engagement or population and the gap. Distinguish a missing record from evidence of unsafe work. Explain the scope and uncertainty; do not infer a practice-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, consequential report issue, data and affected clients. Trace potentially affected earlier engagements 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 professional failure.

1. Accept responsibility and contain

Identify the immediate affected work and a justified earlier-engagement 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 practice 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 report issue.

3. Implement a coherent remedy

Correct the immediate defect, address cause and review client 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 engagements. 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-engagement 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 delivering hubs and underlying professional permissions. 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-engagement and individual experience floors, approved hub coverage and named-lead challenge, 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-engagement impact and effectiveness of closure. Challenge unsupported NA decisions and coherent exclusions. Require clear reasons where different delivering hubs 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, approved hub coverage, evidence authenticity and report 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, professional 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 continuing confidence

Owner: Programme manager and assessors. Trigger: Annual cycle and risk triggers.

1. Schedule before deadlines

Complete surveillance by months 12 and 24 and review every hub annually. Physically assess technical facilities handling subjects annually; approve any remote-only office alternative independently. Allocate at least one central day, one per physical facility and half a day per remote-only hub, then add time for full evidence and personnel coverage.

2. Reconcile people and changes

Review the current roster, authority limits, departures, capability changes, external reviewers, complaints, corrected reports and material incidents. Identify new and materially changed independent leads and adverse cases for direct challenge. Hold unsupported role and scope extensions outside active claims.

3. Select remaining leads

From remaining leads select at least the ceiling of the square root, in addition to mandatory changed/adverse selections. Record the remaining population and selection rationale. Rotate so every lead receives direct challenge within three years and expand for risk. A small numerical sample cannot conceal an unreviewed consequential discipline.

4. Review real work

Review at least three completed engagements per discipline/hub, choosing independently from the complete population. Follow consequential opinions to independent review and actual recipients. Check CPD effectiveness, method changes, custody and correction control. Low volume does not waive evidence adequacy.

5. Resolve status

Apply active finding clocks and proportionate protection; preserve overdue dates. Complete independent review and any required panel decision for changed scope or status. Record next due dates, full personnel-cycle coverage and current public claims.

Required record: F12 coverage; F24 hub review; F25 professional role record.

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/disciplines 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, client 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 disciplines require the initial six-month, three-engagement, internal-audit, management-review and hub-assessment and named-lead 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. Client 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 engagements 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 client harm, evidence integrity, ongoing report issue 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-engagement remedies, investigation and verified correction. Preserve client 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 professional 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 engagement 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 delivering hub is recognised or require a client 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, professional activities, exclusions and current status understandable to a client. Keep personal and confidential engagement 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 professional report.

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 delivering hubs. Escalate deliberate or repeated misuse for status review. Preserve evidence and protect clients 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 direct challenge of all independent leads and actual-engagement 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 practice departure, identify unfinished work, continuing reliance obligations, client complaints and record custody. Require removal of unsupported marks and directory claims. Recognition ending does not erase the organisation's continuing client and legal obligations.

4. Verify restoration

For a restricted or suspended case, assess corrective action, affected-engagement 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 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 engagement data and personal identifiers. Assign purpose, access roles, retention and disposal basis. IAF case records are retained ten years after expiry/withdrawal; professional case records at least ten years after final issue or case closure, whichever is later, 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 engagement 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 Professional roster admission and role control

Owner: Practice executive and competence authority. Trigger: Admission, new discipline, departure or concern.

1. Verify identity and history

Confirm identity lawfully, authentic qualifications and relevant work history. For an independent lead verify at least 24 months of relevant practice and three representative completed assignments within the preceding 36 months per authorised discipline. Equivalent demonstrated learning may support competence; neither a degree nor membership alone establishes it.

2. Evaluate actual contribution

Review original work, references and a structured technical challenge. Distinguish authorship, supervised contribution and independent responsibility. Record discipline, vehicle/technology limits, permitted role and restrictions. A trainee may contribute under competent supervision without being listed as an independent lead.

3. Control review independence

Appoint competent reviewers who did not create or direct the conclusions. External paid review is permissible if fees do not depend on the desired outcome and material interests are controlled. Screen repeated reciprocal arrangements for ineffective challenge; a sole practice needs a functioning independent route.

4. Maintain capability

Plan continuing development from actual gaps and future work, and verify learning through work review or challenge. Reassess after prolonged inactivity, serious error or material technical change. Confirm local permissions where required; programme recognition is not a transferable individual licence.

5. Respond to departure or failure

Remove obsolete role authority and affected public claims promptly, assign qualified replacements and protect open engagements and record custody. Notify IAF of material changes and obtain scope approval where needed. Preserve individual history without transferring the former firm's recognition to the departing person.

Required record: F25 professional role record; scope and credential schedule.

OP20 Engagement, expert opinion and report control

Owner: Independent lead and independent technical reviewer. Trigger: Every scoped engagement.

1. Accept an appropriate assignment

Verify client authority, purpose, intended users, professional role, local duties, competence, capacity and conflicts. Reject unmanageable self-review, outcome-contingent independent opinions or demands for a predetermined result. Record terms, reliance limits and lawful evidence access before starting.

2. Plan and preserve evidence

Define questions, competing explanations, required observations, safe methods and acceptance limits. Identify subjects and source provenance. Obtain specific permission for destructive or digital activity and preserve originals, custody, configuration and relevant timestamps. Do not fill gaps with invented facts.

3. Analyse transparently

Separate observations, assumptions, measured values and opinion. Challenge alternatives, adverse facts, model sensitivity and measurement uncertainty. Identify authentic technical materials actually relied upon in the report. The programme's self-contained drafting does not forbid source citations in professional opinions.

4. Review and issue

Obtain competent independent technical review before every consequential output. Resolve material queries, maintain holds and issue only a bounded supported conclusion under authenticated authority. State unique report ID/version, intended reliance, limitations and what may change the conclusion; an IAF mark does not endorse that report's result.

5. Monitor reliance and correction

Retain the issued version and recipients, review onward-use requests and correct material errors promptly through a lawful route. Preserve the original, reason and replacement links. Do not withhold a necessary protective correction because of a fee dispute. Close custody and retention records while maintaining continuing duties.

Required record: E01-E16 engagement and expert report 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 / extension history	At least 6 months	Implemented controls for each discipline/hub; internal audit and management review complete.
Actual engagement sample	At least 3 per discipline/hub	Real completed work; enlarge sample for risk and diversity.
Independent lead experience	At least 24 months	Relevant practice plus 3 verified assignments in prior 36 months per discipline.
Internal audit and review	Before initial grant; annually	All included hubs and applicable scope.
IAF conflict look-back	At least 36 months	Extend for residual risk; not a ban on ordinary independent case-review fees.
Factual response	15 calendar days	Reasoned extension possible without delaying protection.
Initial finding closure	Before grant	All applicable requirements Met; no open findings.
Active Minor	Within 90 calendar days	Essential assurance protected; clock from written notice.
Active Major	30-calendar-day closure target	Immediate containment; suspension review if unresolved.
Critical risk	Immediate protective review	Act from awareness; do not await formal notice.
Interim suspension review	Within 5 business days	Independent three-person panel.

Action	Time	Condition
Serious notice to IAF	Within 48 hours of awareness	Earlier applicable duties and emergency action take precedence.
Material changes	Planned: before; unplanned: 5 days	Calendar days; serious-incident clock also applies.
Surveillance / personnel	By months 12 and 24	Annual hub review; physical technical visits; all leads challenged within 3 years.
Maximum term / renewal	3 years / apply 6 months early	No automatic extension past expiry.
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; retain actual effective time.
Professional case retention	At least 10 years	After final issue or case closure, whichever is later; binding limits and lawful holds.
IAF case retention	10 years after expiry/withdrawal	Binding limits and lawful holds; minimise personal information.
Consequential technical review	Before issue	Independent competent challenge; no retrospective rubber stamp.
Operator assurance	Annual / independent every 3 years	Four representative pilots and essential-gap closure before launch.

Borderline cases

A sole practice lacks an independent reviewer

Arrange a competent conflict-free external reviewer before consequential issue. Ordinary review fees are allowed; self-review or retrospective signatures do not meet the requirement.

A remote-only office requests no physical visit

An uninvolved reviewer must approve the adequacy of secure live observation and original-source review. Physical technical facilities handling subjects do not qualify for this alternative.

A qualified lead has no recent verified portfolio

Defer independent role authorisation until the required actual assignments and technical challenge are satisfied. Supervised contribution may remain appropriate within a controlled role.

One Minor remains open at initial review

Defer initial recognition until effective closure. Active-status deadlines do not relax initial gates.

A client prohibits any disclosure of a material report error

Determine the actual lawful protective communication route and preserve the reasoning. Do not silently overwrite the report or use confidentiality as a blanket excuse for known misleading reliance.

The only authorised specialist leaves

Review and restrict affected capability promptly, protect open cases and correct claims. The departing person does not take the corporate status to a new firm.