IAF CRP | CORPORATE RECOGNITION | FIRST EDITION

AUDIT & RECOGNITION MANUAL

Independent assessment, physical site evidence, recognition decisions, surveillance and fair remedies.

PREPARED FOR IAF ADOPTION

Version 1.0 | 16 September 2026

OEMs | Manufacturers | Assemblers
Corporate Recognised | English master text

International Automotive Federation

iaf.com

Document control

Item	Controlled value
Programme	IAF Corporate Recognition Programme (IAF CRP)
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 Recognised - 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 Implementation Manuals; Applicant Guide; controlled forms.
Authority boundary	Corporate implementation assurance. Separate product approvals, market permissions and other IAF programme decisions remain distinct.
Control	Retain exact scope and criterion versions. Protect completed records, personal information and industrial evidence.

Purpose and use

Independent assessment, physical site evidence, recognition decisions, surveillance and fair remedies.

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 separation of authority 4
Case lifecycle and decision gates 4
OP01 Intake, eligibility and version control 5
OP02 Competence, independence and appointments 5
OP03 Document and IAF adoption review 6
OP04 Risk, site, shift and duration planning 6
OP05 Physical audit and evidence triangulation 7
OP06 Outsourced manufacture and group interfaces 8
OP07 Findings and factual response 8
OP08 Corrective action and closure verification 9
OP09 Independent recognition decision 9
OP10 Publication, recognition record and mark licence 10
OP11 Annual surveillance and performance review 10
OP12 Scope change and renewal 11
OP13 Serious incidents and field-action oversight 11
OP14 Suspension, withdrawal and restoration 12
OP15 Complaints and protected concerns 13
OP16 Appeals and independent review 13
OP17 Digital verification, access and continuity 14
OP18 Programme launch, calibration and future revision 14
Operating deadlines and clock controls 15
Borderline cases and consistent decisions 16

Roles and separation of authority

Role	Responsibility
Governing authority	Adopts rules, appoints independent oversight and authorizes operational launch; does not direct favourable case outcomes.
Programme manager	Controls editions, competence resources, implementation, consistency and annual performance review.
Case manager	Coordinates intake, scope versions, access, deadlines and communication without changing technical conclusions.
Lead auditor	Owns the evidence plan, site and shift coverage, team coordination, findings and reasoned recommendation.
Technical auditor/expert	Evaluates manufacturing and technology evidence within documented competence; declares limitations.
Independent technical reviewer	Checks evidence sufficiency, applicability, closure and scope consistency before panel review.
Decision panel	Three uninvolved competent members participate; grant requires at least two reasoned affirmative votes and all initial gates.
Appeal panel	Three different competent reviewers examine the challenged decision and record reasons independently.
Impartiality/ethics oversight	Reviews structural conflicts, protected concerns and separation from membership and commercial influence.
Registry/mark custodian	Publishes authorized scope/status, controls licences and preserves current and historical verification.
Applicant executive	Accepts legal-entity accountability, resources, truthful declarations and continuing duties.
Site/product owners	Demonstrate actual controls, provide original evidence and implement containment and verified improvement.

Case lifecycle and decision gates

Intake and eligibility -> adoption/scope review -> conflict and competence clearance -> risk/site/shift plan -> original-record and physical audit -> findings and response -> verified closure -> independent decision -> scope/status publication -> annual surveillance -> renewal or controlled exit.

Use one controlled case manifest. The case manager coordinates administrative work; the technical team evaluates evidence; the independent panel decides. Commercial staff, membership recruiters and sponsors shall not determine technical outcomes. A readiness review remains private and grants no public recognition rights.

OP01 Intake, eligibility and version control

Owner: Case manager | Trigger: New application or scope request

1. Register

Create a case ID and preserve the exact submission version. Confirm the legal applicant, authority and confidentiality needs. Acknowledge receipt and distinguish administrative receipt from eligibility or recognition.

2. Classify

Select all actual activity profiles and technology modules. Separate manufacturing scope, related services, outsourced controls and excluded entities. Resolve whether a private readiness route is needed because the operating-history gate is not met.

3. Check

Verify the adoption schedule, six months of operation, initial internal audit/review and three completed cases per family/site. Request missing information through a dated list; do not recast unavailable evidence as NA.

4. Assign

Check technical capacity and conflicts before accepting the assessment. State languages, access needs, proposed roles and any limitations. Refer unsupported technologies for expert capability review.

5. Control

Lock the accepted scope and criterion versions for planning. Record subsequent changes and their effect on time and evidence. Explain decision, complaint and appeal routes to the applicant.

Required record: F01 intake and scope acceptance

OP02 Competence, independence and appointments

Owner: Programme manager | Trigger: Team, expert or panel appointment

1. Define

Identify required industrial, quality, safety and technology knowledge against the actual scope. Include regional and language competence needed for original evidence. Specify tasks that an expert may advise on without deciding.

2. Screen

Review each person employment, consultancy, ownership and material commercial connections for the preceding 36 months and longer where risk persists. Document other relationships, gifts and conflicts; applicant agreement alone cannot cure a serious threat.

3. Authorize

Assign at least two competent auditors and bounded expert roles. Maintain a separate uninvolved technical reviewer and three-person decision panel. Keep appeal reviewers independent of the original audit, advice and decision.

4. Observe

Monitor audit conduct and technical judgments through witnessed work and file review. Withdraw or narrow authorization where competence is not demonstrated. Protect workers and customers from coached interviews.

5. Record

Retain individual competence evidence, conflict declarations, authorizations and substitutions. Recheck conflicts when the scope, ownership or team changes and before the final decision.

Required record: F02 competence and conflict clearance

OP03 Document and IAF adoption review

Owner: Lead auditor and technical reviewer | Trigger: Accepted application

1. Map

Read the scope and adoption schedule against the complete CRP matrix and every additional claimed IAF text. Confirm whether texts are adopted or draft and which claims require a separate programme decision.

2. Follow

Trace a sample of requirements to actual process records, responsible people and results. Distinguish a policy from evidence of implementation and verify that records belong to the proposed site and product family.

3. Challenge

Test exclusions, outsourced interfaces and technical-family grouping. Identify missing original data, contradictory claims and gaps in six-month operation or completed cases. Document unresolved questions for physical audit.

4. Protect

Agree lawful confidential review and necessary copies. Record redactions and how the evidence remains sufficient. Escalate access restrictions that prevent a defensible conclusion.

5. Plan

Issue a readiness conclusion for audit planning, not a grant recommendation. Where fundamental eligibility is absent, defer the audit or offer a clearly private readiness assessment with no public status.

Required record: F03 criteria and evidence review

OP04 Risk, site, shift and duration planning

Owner: Lead auditor | Trigger: Initial, surveillance, renewal or special audit

1. Calculate

For initial audit add two central auditor-days to the manufacturing site floor of two, three or four days for up to 100, 101-500 or over 500 effective workers. Effective workers include relevant temporary/contract staff and equivalent distributed shifts. Apply each specified one-day risk addition once per affected site.

2. Cover

Identify every included factory, critical process family, release route and relevant contractor. Allocate at least one full operating day physically at each factory and at least half on-site time to observation, witnessing and interviews. Do not count travel or report-writing as on-site audit.

3. Select

Choose at least three completed cases per family/site from the available population, including change and adverse cases where available. Add cases and time for differences, failures and uncertainty. Observe at least two shifts when multiple shifts operate and schedule remaining shifts within the annual programme.

4. Adapt

For surveillance plan at least one central auditor-day plus at least one auditor-day per included factory, keeping the full operating-day visit and two-auditor team rules. Increase effort to meet actual coverage; the numerical floor never caps time. Renewal uses the full initial planning rules and all sites.

5. Approve

Obtain independent approval of the coverage plan and retain assumptions and additions. Resolve access, safety, interpreters and real production availability. A duration change shall preserve mandatory floors and evidence sufficiency.

Required record: F04 audit programme and duration calculation

OP05 Physical audit and evidence triangulation

Owner: Lead auditor | Trigger: Approved audit plan

1. Open

Confirm the scope, criteria, access and current operational changes with management. Reaffirm stop-work safety rules, confidentiality and independent interview access. Record whether planned production and shifts are actually available.

2. Observe

Follow work from incoming requirements and material through critical operations, tests, release and shipment. Witness normal and relevant abnormal controls without creating unsafe conditions. Review actual nonconforming stock, rework, bypass and maintenance evidence.

3. Trace

Select an actual delivered case and trace backward to design, material, process and approvals, then forward to potentially affected customers. Reconcile quantities, configurations and software. Record retrieval times and unexplained gaps.

4. Corroborate

Compare observations with original digital records, interviews, customer outcomes and adverse cases. Ask for source data behind dashboards. Document contradictions and expand the sample when assurance weakens.

5. Close

Explain evidenced findings and limitations with affected scope. Invite factual correction without negotiating requirements. Record incomplete activities and follow-up; the audit team recommends but does not issue recognition.

Required record: F05 witnessed audit and evidence trail

OP06 Outsourced manufacture and group interfaces

Owner: Technical auditor | Trigger: Group, contract factory or critical provider in scope

1. Bound

Identify the exact applicant entity and the activities controlled externally. Separate a supplier evaluated as evidence from a separately recognised company. Record design, manufacturing, release and field responsibilities.

2. Access

Verify contracts permit necessary original-record review, physical observation and technical interviews. If access is insufficient, defer or exclude the affected scope. A supplier certificate or secrecy clause cannot replace missing essential evidence.

3. Evaluate

Review flow-down, change notification, incoming acceptance, capacity, traceability and adverse performance. Witness critical operations necessary to establish the applicant controls. Confirm whether parent-level processes actually operate at the local site.

4. Reconcile

Trace product identity, quantities, tooling rights, software and customer ownership across handovers. Look for unapproved substitution, excess production and unclear field-action authority.

5. Conclude

State the applicant control demonstrated, remaining limits and any additional direct evidence required. Prevent a recognition statement from presenting all contract factories or affiliates as approved merely through association.

Required record: F06 group and external-operation assessment

OP07 Findings and factual response

Owner: Lead auditor | Trigger: Evidence of unmet or unverified requirement

1. State

Record the requirement ID, objective facts, evidence references and exact affected site/activity. Separate observed failure from inference and identify unresolved information. Missing evidence is Pending, not NA.

2. Classify

Assess consequence, recurrence, systemic scope and current protection. Use Minor for an isolated lapse without demonstrated essential loss, Major for systemic/consequential failure and Critical for serious harm or severe integrity failure. Do not let a score override the classification.

3. Protect

Require immediate containment for serious risks and notify the IAF status authority. Assess prior-output impact and necessary public protection. Do not wait for the ordinary response clock to act on a credible threat.

4. Hear

Allow 15 calendar days for factual response and preserve the applicant evidence and disagreement. Correct a finding when facts warrant it; document the reason. Keep the original audit trail.

5. Route

Set closure evidence and deadlines, then refer the final finding set for independent review. Explain available appeal rights after decision and maintain any proportionate protective action.

Required record: F07 finding and response record

OP08 Corrective action and closure verification

Owner: Independent competent verifier | Trigger: Submitted action evidence

1. Confirm

Check that containment covers all potentially affected configurations and recipients. Review whether delivered output or public claims require correction. Verify that the original evidence has been preserved.

2. Examine

Evaluate technical, organizational and detection causes. Challenge unsupported operator-blame conclusions and actions limited to retraining. Identify other sites or products sharing the cause.

3. Verify

Use new operating evidence, re-performance or a follow-up visit to test predefined closure criteria. Material findings require independent competent verification; a revised procedure alone is insufficient.

4. Time

For initial grant close all applicable findings. For active recognition enforce the 90-day Minor maximum and 30-day Major target with suspension review for unresolved affected scope. Treat Critical findings through urgent protection and a separate restoration decision.

5. Record

State effectiveness, residual limits and the recommendation. Reopen a finding when recurrence disproves closure and assess whether prior recognition decisions or other scopes require review.

Required record: F08 corrective action and effectiveness verification

OP09 Independent recognition decision

Owner: Decision panel | Trigger: Complete audit and closure dossier

1. Review

The independent technical reviewer checks eligibility, all applicable results, scope, competence, conflicts, physical coverage and evidence limitations. Return incomplete cases for further work without implying likely grant.

2. Convene

Three uninvolved competent panel members review the same controlled dossier. Each records an independent vote and reasons. Grant needs all three participating and at least two affirmative votes, with every initial gate satisfied.

3. Decide

Grant, defer, refuse or approve a technically coherent reduced scope. Do not issue conditional initial recognition with open findings. Explain excluded activities and ensure that common unresolved causes do not undermine retained scope.

4. Authorize

Set effective and expiry dates within the three-year maximum, surveillance deadlines and the exact recognition schedule. Approve the public wording and licence separately from commercial administration.

5. Notify

Issue the reasoned decision, scope and appeal deadline to the authorized applicant. Transfer only authorized data to the registry custodian and verify publication before public mark use.

Required record: F09 independent decision and votes

OP10 Publication, recognition record and mark licence

Owner: Registry custodian | Trigger: Authorized decision or status change

1. Check

Verify the decision signature or authenticated authority, scope version, legal names, dates and restrictions. Reject ambiguous wording and unapproved product-certification implications.

2. Publish

Create or update the stable recognition ID and current/historical record. Include covered sites, activities, family boundaries and verification time. Minimize personal and confidential data.

3. Test

Confirm public lookup and controlled manual verification return the same status and scope. Test copied or superseded records, outage behaviour and unauthorized amendments. Do not issue a live badge before the service is operational.

4. License

Issue only approved artwork and permitted placements, with stop-use and correction obligations. Corporate use must remain visibly scope-bound; no implication of product-by-product approval is allowed.

5. Monitor

Review public samples and reported misuse. Preserve historical status events and notify affected parties of material corrections. Publish protective changes normally within two business days.

Required record: F10 recognition record and mark licence

OP11 Annual surveillance and performance review

Owner: Case manager and audit team | Trigger: Annual due date or adverse trend

1. Collect

Obtain the annual scope, indicator, change, incident, complaint, internal-audit and review package. Reconcile important results to source records and identify material changes since the last decision.

2. Plan

Schedule a physical audit of each included manufacturing/assembly site at least annually and review central/support controls. Surveillance is due by months 12 and 24. Use risk to add effort, not to remove mandatory coverage.

3. Evaluate

Verify continuing implementation, past actions, critical process performance and truthful claims. Include changed and adverse cases, relevant shifts and support/recall outcomes. Expand scope review when common causes emerge.

4. Decide

Independently confirm continuation, restriction or protective action. Enforce active-finding limits and address missed surveillance through suspension review. A current certificate copy cannot override changed status.

5. Update

Record the annual conclusion, next due dates and revised risk profile. Refresh public scope only through an authorized decision and retain evidence of notifications.

Required record: F11 annual surveillance and continuation

OP12 Scope change and renewal

Owner: Programme manager and audit team | Trigger: Material change or approaching expiry

1. Classify

Determine whether the change affects legal identity, ownership, sites, design responsibility, family, process, technology or support. Apply the prior-notification rule for planned changes and five-day rule for unplanned changes; use 48 hours for serious incidents.

2. Assess

Identify evidence, competence and physical audit needed before extension. New families/sites must satisfy the operating-history and completed-case gate. Existing scope does not authorize unreviewed expansion.

3. Renew

Begin renewal from an application at least six months before expiry. Use the full initial planning and site-coverage rules, review performance throughout the term and verify all applicable gates before the new decision.

4. Control

Complete the decision before expiry and set the new bounded term. If evidence or access is incomplete, let affected recognition expire or apply a lawful protective restriction; do not backdate or silently extend.

5. Communicate

Update schedules, status and approved claims, including historical continuity and any gap. Notify users of material restrictions through appropriate routes.

Required record: F12 change and renewal assessment

OP13 Serious incidents and field-action oversight

Owner: Programme manager with technical lead | Trigger: Serious incident or credible integrity concern

1. Protect

Act immediately on credible danger or material evidence compromise. Bound affected sites, configurations and public claims, preserve records and consider protective suspension. The organization retains its own safety and notification duties.

2. Register

Record the awareness time and 48-hour IAF notice compliance, known facts, uncertainty and containment. Coordinate required external notifications without assuming IAF replaces any authority or customer channel.

3. Investigate

Use independent technical competence to test the cause, population and prior-output impact. Obtain original data and evaluate whether information has been concealed, altered or selectively reported.

4. Verify remedy

Assess practical completion and effectiveness of physical or software remedies, including unreachable products. Review other sites and products sharing the failure mechanism and the continued ability to support users.

5. Resolve

Issue a reasoned status decision, corrective requirements and communication plan. Preserve the event and correction history. Restoration requires demonstrated control and an independent authorized decision.

Required record: F13 serious incident and field-action record

OP14 Suspension, withdrawal and restoration

Owner: Decision authority | Trigger: Loss of control, missed monitoring or voluntary exit

1. Bound

Identify affected scope and whether shared causes invalidate other activities. Select proportionate restriction, suspension or withdrawal. The programme manager with an independent technical lead may issue an urgent interim suspension for a credible serious safety/integrity threat; a three-person independent panel shall review it within five business days.

2. Notify

Give reasons, effective time, claim restrictions and appeal rights. Require preservation of records and customer-remedy capability. Necessary urgent protection can precede complete factual resolution.

3. Publish

Update verification and stop misleading mark use. Preserve history and distinguish inactive scope from coherent unaffected activity. Notify known affected users where proportionate and necessary.

4. Verify

For restoration, require new evidence, effective correction and any necessary physical audit. Check that support obligations and information corrections were fulfilled. A promise or elapsed suspension period is not proof of restoration.

5. Decide

Use an independent three-person panel with recorded votes and reasons. Restoration cannot backdate status or extend the original maximum term; renewal requires its own completed assessment and decision.

Required record: F14 protective status and restoration

OP15 Complaints and protected concerns

Owner: Independent complaint handler | Trigger: Complaint, whistleblowing or alleged misuse

1. Receive

Provide accessible confidential contact routes and normally acknowledge within five business days. Record subject, available evidence, requested remedy and immediate safety needs without demanding unnecessary personal data.

2. Protect

Review retaliation risk, conflicts and confidentiality. Route urgent technical threats to protective action. Keep commercial disputes distinguishable while investigating any credible quality or integrity allegation.

3. Investigate

Assign competent uninvolved personnel, seek relevant original evidence and allow a fair response. Do not disclose reporter identity unnecessarily or let the subject control the investigation.

4. Conclude

Record facts, uncertainty, reasons, actions and remaining review rights. Communicate an appropriate outcome to the parties while protecting confidential data. A complaint outcome does not silently amend recognition scope.

5. Learn

Track timeliness, recurrence and systemic implications. Feed confirmed weaknesses into surveillance and programme improvement and verify any required remedy.

Required record: F15 complaint and protected-concern record

OP16 Appeals and independent review

Owner: Appeal panel | Trigger: Appeal within 30 calendar days

1. Register

Verify the challenged decision, notification date, grounds, evidence and requested outcome. Record completeness and explain any missing information. Maintain necessary proportionate protection while review proceeds.

2. Appoint

Select three competent reviewers uninvolved in the original audit, advice and decision. Document conflicts and access rights. The original decision-makers may provide facts but shall not determine the appeal.

3. Review

Examine the criteria, evidence, procedure, scope and reasons, allowing a fair response. Obtain independent technical advice where required and preserve the original record rather than rewriting history.

4. Determine

Target a reasoned outcome within 45 calendar days after a complete appeal. Uphold, amend or remit the decision with clear instructions. Any grant or restoration must still satisfy the applicable evidence gates.

5. Implement

Notify the parties, authorize any status correction and retain the appeal record. Review lessons for consistency, competence and fair process; do not penalize a good-faith appellant.

Required record: F16 appeal and determination

OP17 Digital verification, access and continuity

Owner: Registry and information custodian | Trigger: System operation, incident or migration

1. Control

Restrict creation, approval and publication by role and separate incompatible duties. Use stable IDs and versioned data with recoverable event history. Protect signing and privileged credentials.

2. Validate

Test entity matching, scope versions, effective dates, inactive states and manual lookup against authorized decisions. Verify that a copied record cannot be mistaken for current status without a fresh check.

3. Recover

Test backup restoration and safe outage operation. Return unavailable or unresolved with retrieval time rather than an unjustified valid status. Provide an authenticated manual response and reconcile later changes.

4. Retain

Apply the IAF ten-year post-expiry/withdrawal retention clock, holds and minimization. Maintain interpretability after migration and preserve evidence of corrections and authorized deletions.

5. Audit

Review access logs, anomalies, data exports and correction requests. Investigate integrity incidents and their effect on past decisions and public reliance.

Required record: F17 registry event and verification record

OP18 Programme launch, calibration and future revision

Owner: Governing authority and programme manager | Trigger: First adoption or material programme change

1. Prepare

Approve scope, rules, competent roles, impartiality controls, resources, contact routes and operational responsibilities. Validate forms, decisions, appeal channels and status verification before any public grant.

2. Pilot

Run representative OEM/outsourcing, vehicle/assembly, component/material and digital/emerging cases. Include a failed case and a contested decision. Compare auditor judgments and test whether time floors and evidence gates are sufficient.

3. Correct

Resolve pilot weaknesses, authorize personnel by demonstrated competence and verify protective status and remedy workflows. Record the launch decision and exact edition effective date.

4. Review

Audit operation annually and independently review effectiveness at least every three years. Monitor consistency, adverse outcomes, complaints and actual acceptance arrangements, publishing accurate aggregate information.

5. Develop

Use technical review, consultation and further pilots for new modules and revisions. Publish prospective transition rules and scope effects. Preserve historical decisions and prevent speculative technology claims from bypassing validation.

Required record: F18 programme assurance and transition

Operating deadlines and clock controls

Action	Time	Condition
Administrative acknowledgement	Target 5 business days	Complete intake; not recognition.
Initial implemented operation	At least 6 months	Also one internal audit and one management review.
Completed initial cases	At least 3 per family/site	Actual release/traceability evidence; no simulation substitution.
Factual response	15 calendar days	From finding notification; urgent action continues.
Initial grant	All applicable Met	No open initial finding or conditional public recognition.
Active isolated Minor	Maximum 90 calendar days	Only where safety, validity and integrity remain protected.
Active Major	Target 30 calendar days	Immediate containment; unresolved scope enters suspension review.
Critical finding	Immediate protection	Urgent protective-suspension review.
Interim suspension review	Within 5 business days	Three-person panel reviews urgent manager/independent technical-lead action.
Serious incident notice	Within 48 hours	From awareness; earlier binding notices prevail.
Planned material change	Before implementation	Expanded scope needs prior independent approval.
Unplanned material change	Within 5 calendar days	Use 48-hour rule where incident is serious.
Recognition term	Maximum 3 years	From grant; no automatic extension.
Surveillance	By months 12 and 24	Annual physical audit of each manufacturing/assembly site.
Renewal application	At least 6 months before expiry	Reassessment and decision before expiry.

Action	Time	Condition
Appeal submission	Within 30 calendar days	From decision notification.
Appeal determination	Target 45 calendar days	From complete appeal; necessary protection continues.
Protective status publication	Normally within 2 business days	Preserve actual effective date/time and affected scope.
Organization quality records	At least 10 years	After last supply or end of promised support, whichever is later.
IAF case records	At least 10 years	After recognition expiry or withdrawal; holds/longer duties prevail.

Borderline cases and consistent decisions

A mature group adds a new plant

The new plant and each family/site must meet the initial history, case and physical-audit gates before extension. Existing group status does not cover the new location.

A technically strong applicant has an open Minor

Do not grant initial public recognition. Verify effective closure or exclude only a coherent scope that the lapse does not affect.

A contract factory refuses original-record access

Seek a lawful protected review arrangement. If essential evidence remains unavailable, defer or exclude the affected scope; do not replace evidence with a confidentiality assertion.

A serious incident occurs during appeal

Maintain necessary proportionate protection while the independent appeal panel reviews facts and fairness. Appeal does not automatically restore active claims.

A production dashboard reports perfect quality

Reconcile first-pass results, rework, rejects, returns and denominator definitions. A polished summary cannot establish the absence of concealed adverse outcomes.

The registry is unavailable

Report unavailable or unresolved with retrieval time and use the controlled manual route. Do not present an old cached record as current status.