



IAF PSR | SUPPLIER RECOGNITION | FIRST EDITION

APPLICANT GUIDE

From an industrial quality claim to a complete evidence dossier, independent audit and continuing recognition.

PREPARED FOR IAF ADOPTION

Version 1.0 | 16 September 2026

Product & System Suppliers
Corporate Recognised | English master text

International Automotive Federation

iaf.com

Document control

Item	Controlled value
Programme	IAF Product & System Supplier Recognition Programme (IAF PSR)
Document	Applicant Guide
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

From an industrial quality claim to a complete evidence dossier, independent audit and continuing recognition.

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
G01 Understand supplier corporate recognition	4
G02 Choose responsibility, family and operational sites	4
G03 Create the IAF requirement adoption schedule	4
G04 Establish actual history and completed cases	5
G05 Build the supplier evidence and approval dossier	5
G06 Make the internal audit meaningful	5
G07 Submit and agree the audit boundary	6
G08 Support physical and digital evidence review	6
G09 Respond to findings and verify closure	6
G10 Use the status accurately	7
G11 Maintain recognition and report change	7
G12 Build enduring trust and future capability	7
Submission pack and final readiness review	8

G01 Understand supplier corporate recognition

IAF Corporate Recognised under PSR means that independent assessment has established implemented corporate quality and trust controls for the named supplier and exact scope. The record identifies product/system responsibilities, sites, families and relevant technologies. It supports an informed supplier-selection decision without promising defect-free products or successful transactions.

The ten profiles cover systems, components, electronics, materials, digital products, special processes, production technology, energy systems, circular products and controlled distribution. Engineering, installation and support services may be included when directly accountable to the supplied output. A sourcing introduction or unverified brokerage operation is not sufficient.

The prepared edition requires formal adoption and validated operation before live recognition. Application, membership, nomination by a customer, private readiness work and planned investments do not confer status. Other IAF recognition programmes retain separate scope and decision records; common wording does not create automatic transfer.

G02 Choose responsibility, family and operational sites

List the legal entity and every proposed operational site. State whether each site manufactures, processes, configures, warehouses, engineers or releases digital products. Name the controlled operating centre for remote personnel and show how distributed work is supervised. A website, registered address or cloud-hosting contract alone is not a demonstrated operating site.

Select every relevant profile. A battery controller supplier may need ELE, SWD and ENE; a module integrator with purchased mechanical parts may need SYS and CMP; a distributor that loads firmware needs DST and the relevant digital controls. Technology modules add application-specific evidence rather than replacing the common baseline.

Define technically coherent families by responsibility, process, source, technology, critical characteristics and risk. Distinguish source manufacturers and critical contractors from separately recognised applicants. Keep customer programme, design authority, intended integration, excluded activities and planned capability visible in the scope schedule.

G03 Create the IAF requirement adoption schedule

Adopt the PSR baseline through an authorized executive decision. If you claim conformity with additional IAF quality texts, identify each exact title, edition and approval status and provide the complete requirement-level map. The PSR checklist is a navigation tool for its own 216 requirements, not a substitute for assessing another text in full.

For each applicable requirement connect the responsible process, actual practice, evidence location and evaluation result. A single authentic record may support several requirements if the links are clear. Keep an exclusion rationale for genuinely absent responsibilities; outsourced activity and lack of resources are not grounds to mark a requirement NA.

Do not translate a working draft or pilot result into an approved-standard claim. Where another IAF programme requires a separate test, rating or certificate, follow that programme independently and link only the actual decision. Resolve contradictions through technical review before making a public conformity statement.

G04 Establish actual history and completed cases

Initial recognition requires six months of implemented operation, one internal audit and one management review. Each included responsibility-family/site needs at least three distinct completed cases. A case connects a real requirement or order to execution, acceptance, release and traceability; it is not a single isolated test or a duplicate copy of another delivery record.

For manufacturing, use actual completed batches or production/delivery cases; for a process provider, completed customer loads; for software, distinct controlled releases, customer deliveries or deployments with their own acceptance evidence; for distribution, completed supply lots with source and receipt linkage. The case definition must match the supplier responsibility and avoid counting copies or download events as independent evidence.

Provide the most recent twelve months available, with at least six months for initial review. Auditors select cases, including adverse and changed cases when available. Low-volume or new suppliers may need longer to meet the floor. Simulations and pilots support learning but do not replace actual required cases.

G05 Build the supplier evidence and approval dossier

Use a controlled evidence index with identity, version, date, source, owner, site, confidentiality class and requirement links. Preserve original test records, raw results, build histories and corrections. Connect the self-assessment to product/system approval dossiers and to customer dispositions where required.

For each assessed family show the path from quotation and requirement review through design responsibility, sub-tier controls, process readiness, acceptance and delivered configuration. Include capacity, material/software provenance, warranties, change decisions and actual customer outcomes. Keep negative evidence and unapproved assumptions visible.

Agree protected access early. A technically competent reviewer may examine source code or proprietary material records in a controlled environment without unrestricted copying. Record what was verified and the limitations. If necessary evidence cannot be lawfully verified, the affected recognition scope remains unsupported.

G06 Make the internal audit meaningful

Use competent reviewers who can challenge the process rather than only confirm the presence of procedures. Follow actual orders through design, production, release, shipment and field feedback. Trace an output backward and forward, interview people privately and examine at least one relevant failure or change.

Write each finding with the requirement, original evidence, affected scope and consequence. Distinguish a missing document from a failed process or a serious safety risk. Assign containment, cause analysis, actions and independent verification. A corrected form does not automatically prove that the underlying process now works.

Present management with unresolved risks, resource needs and customer effects. Record decisions and follow-up. The internal review should reveal the same adverse facts that will be available to IAF; rehearsed answers and selective samples undermine the trust the programme is designed to establish.

G07 Submit and agree the audit boundary

Submit the application, scope schedule, adoption matrix, self-assessment and evidence manifest together, with authorized declarations accepting the identified IAF Constitution and programme edition. Use the agreed administrative channel and protect confidential attachments.

IAF checks eligibility, completeness, conflicts and available technical competence. The audit plan identifies sites, shifts, process families, witnesses, case samples, time allocation and access restrictions. The initial duration floor is a planning minimum; complexity, risk and evidence weaknesses can require more time.

Challenge a factual error in the plan and disclose a genuine conflict promptly. You may not select only favourable samples or insist on excluding a competent auditor for refusing a preferred outcome. Ensure that critical outsourced processes can be accessed where necessary to verify your claim.

G08 Support physical and digital evidence review

Every included operational site receives a physical initial and renewal audit and an annual physical surveillance visit. This includes accountable software engineering/release and warehouse/configuration centres as well as factories. Central/support work can use justified remote evidence; remote participation does not remove the operational-site visit.

Prepare actual process and release activities for witnessing, relevant shifts and original data. For digital suppliers this may include source-to-build trace, release signing, configuration control, incident handling and deployment recovery. For distribution it includes source authenticity, storage, identity, release and recipient trace. Auditors choose the cases and shall not rely only on a staged demonstration.

Provide competent access to critical outsourced operations where necessary to verify the claim. Distinguish supplier process controls from IAF approval of the upstream entity. At closing, review facts and limitations; only the independent decision process can grant corporate recognition.

G09 Respond to findings and verify closure

You have 15 calendar days for factual response to audit findings. Submit objective corrections if facts are wrong and explain the affected scope. A response period does not suspend immediate containment or urgent reporting duties. Record remaining disagreement and use the appeal route after the decision where appropriate.

Before initial grant every applicable requirement must be Met and every finding effectively closed. For an active recognition, only an isolated Minor may remain open within the 90-day maximum when safety, validity and integrity are protected. Major findings require immediate containment and a 30-day closure target; Critical findings trigger immediate protective suspension review.

Provide evidence of cause removal, affected-population control and new operation under the changed process. The independent verifier may require re-performance, observation or further records. Do not label a promise, training attendance or an unsigned revised procedure as verified effectiveness.

G10 Use the status accurately

After grant, use IAF Corporate Recognised with the recognition ID and exact scope. The certificate or recognition statement is accompanied by the approved schedule and verification route. Check both current status and historical effective dates; a downloaded copy may no longer reflect a restricted or suspended activity.

Use only authorized artwork under the mark licence. Corporate stationery, an appropriate website page or facility display may carry the bounded corporate claim. Product labels, packaging and test reports must not suggest product certification through the corporate mark. Separate independently issued product approvals from this status.

Do not claim global legal acceptance, blanket supplier approval, guaranteed product safety or creditworthiness. Customers may use the record as evidence in their own qualification process and must still check applicability to the actual purchase, site, product and market.

G11 Maintain recognition and report change

Recognition lasts at most three years. Surveillance is due by months 12 and 24 and each included operational site requires an annual physical audit. Maintain current indicators, complaints, changes, audit results and corrective actions. Plan the next audit before the due date so operational constraints do not create a lapse.

Notify IAF before planned material changes; report unplanned material changes within five calendar days of awareness. Serious safety, falsification, scope failure or evidence-compromise incidents require notice within 48 hours, alongside immediate containment and any earlier binding notice. Unapproved expansion remains outside recognition.

Apply for renewal at least six months before expiry. Complete reassessment and an independent decision before the end date. A renewal application or appeal does not extend the term, and historical recognition must not be presented as active after expiry.

G12 Build enduring trust and future capability

Use the programme to connect operational decisions with customer outcomes. Demonstrate that failure data reaches engineering, supplier development and leadership; show that recalls and remedies work in practice. Publish accurate scope and useful aggregate information while protecting personal data and technical secrets.

Future technologies belong in controlled development until evidence supports their intended application. Apply the technology modules to automation, batteries, connected services, digital twins and circular products where relevant. A promising pilot is an opportunity for learning, not an unrestricted public recognition claim.

Keep acceptance claims specific. Confidence can grow through transparent criteria, consistent auditing and documented customer arrangements, but worldwide acceptance cannot be created by a sentence in a standard. Contribute evidence and lessons to controlled programme revisions without weakening current essential gates.

Submission pack and final readiness review

Folder	Contents
01 Identity and scope	Legal undertakings; entities/sites; profiles; product/service families; exclusions.
02 Adoption	PSR adoption; additional IAF titles/editions; requirement applicability and evidence map.
03 Governance	Responsibilities; safety/quality policy; risks; competence; integrity and obligations.
04 Technical operation	Design, supply, production, measurement, release, software and support evidence.
05 Actual history	Six-month operating record; case populations; adverse/changed cases; traceability exercise.
06 Assurance	Internal audit, management review, performance, findings and effectiveness.
07 Access and application	Audit availability, secure evidence access, translation, application and authorized declarations.

Executive check

Confirm that the scope describes actual work, every critical responsibility has an owner, every claim leads to verifiable evidence and every material adverse fact is disclosed. The application is ready for assessment when these links can be independently tested; it is ready for recognition only after all applicable gates and the independent decision are complete.