



IAF SDR | SOFTWARE & DIGITAL | FIRST EDITION

APPLICANT GUIDE

Preparing authentic software lifecycle evidence and a precise corporate scope.

PREPARED FOR IAF ADOPTION

Version 1.0 | 16 September 2026

Software Developers & Digital Tools
Corporate Recognition | English master text

International Automotive Federation

iaf.com

Document control

Item	Controlled value
Programme	IAF Software and Digital Systems Recognition Programme (IAF SDR)
Document	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 Recognition - bounded to the approved legal entity, sites and activities.
Hierarchy	Standard including internal directives and normative annexes; adopted implementation notice within those rules; Status and Mark Rules; Audit and Software Lifecycle Manuals; Applicant Guide; controlled forms.
Authority boundary	Corporate implementation assurance. Corporate scope is separate from release approval; no blanket product certification, output endorsement or vehicle approval is conferred.
Control	Retain exact scope and criterion versions. Protect completed records, personal information and software evidence.

Purpose and use

Preparing authentic software lifecycle evidence and a precise corporate scope.

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 The programme and its promise	4
G02 Bound the organisation and product families	4
G03 Show real implementation	4
G04 Build the claim-to-evidence map	5
G05 Establish effective technical authority	5
G06 Protect releases and users	5
G07 Submit the controlled application	6
G08 Prepare for assessment and challenge	6
G09 Understand decisions and deadlines	6
G10 Maintain support and truthful scope	7
G11 Use recognition and resolve disputes fairly	7
G12 Use the complete document suite	7

G01 The programme and its promise

IAF SDR connects a software organisation's quality claim to implemented evidence, competent assessment, independent Corporate Recognition and continuing accountability. It covers the exact legal holder, delivering hubs, software/service families and lifecycle responsibilities in the approved schedule. The organisation remains accountable for its products, services and customer commitments.

Corporate recognition is not a certificate for every release or an assurance that software has no defects. A product-facing claim must identify the corporate meaning and current scope. Vehicle approval, customer integration acceptance, individual report validity and permission for automated driving remain separate decisions supported by their own evidence.

This First Edition is prepared for IAF adoption. Before live recognition the operator must adopt the rules, appoint competent impartial personnel, complete representative pilots and test current verification. International use is an objective; actual acceptance by customers or authorities must be demonstrated separately.

G02 Bound the organisation and product families

Identify the contracting entity, development/integration/operation roles, delivering hubs, critical suppliers and distribution channels. Record whether each family is embedded software, engineering or test tooling, cloud, fleet/mobility application, update system, AI, security tool or data platform. DEV is mandatory for all applicants, including operators and distributors.

A family groups products or services with materially common architecture, lifecycle controls, competence and consequence. Do not combine unrelated products merely to satisfy an evidence floor. Record supported configurations, versions or release lines, deployment modes, intended use, support commitments and exclusions.

Every responsible hub must demonstrate its actual contribution and control. A customer installation is not automatically a recognised hub. A supplier or open-source community is not recognised because its component appears in an inventory; the applicant must demonstrate the supplier interfaces and acceptance controls it owns.

G03 Show real implementation

Initial and new family/hub scope need at least six months of implemented controls, completed internal audit and management review, and three real completed release/change events per family/responsible hub. Events may be software releases, substantive maintenance, configuration or service changes with actual delivery or operation and complete relevant assurance.

Count an event once within a family/hub, not once for each replicated target or pipeline run. Do not manufacture trivial changes to meet the gate. A shared event may demonstrate several hubs only when each hub's real responsibility and evidence are shown. Governance-only functions demonstrate real oversight cases.

At surveillance, review existing events plus current support and operating evidence when no new release was appropriate; the programme does not require needless production changes. Simulations and safe demonstrations support competence and failure testing but do not replace the completed-event or implemented-history gates.

G04 Build the claim-to-evidence map

Adopt the exact SDR edition and map requirements to implemented practice, owners, original evidence and effectiveness. List additional claimed IAF quality texts by exact edition and approval status with separate clause maps. Recognition under SDR does not automatically confer other IAF programme outcomes.

Trace a consequential requirement to design, code/configuration, review, build, original test results, release approval, distribution and actual target or service state. Include failures, overrides, rollback attempts and support incidents. A green dashboard is an index, not the source evidence.

Use NA only where a requirement's inherent trigger is absent from the bounded scope, with reasoned acceptance. Outsourcing, confidentiality, cost or missing records do not themselves justify NA. IAF operator duties require separate independent operator evidence rather than applicant declarations.

G05 Establish effective technical authority

Assign competent owners for architecture, development, verification, security, safety interfaces, privacy, AI and operations according to actual activity. Verify capability through representative work and practical challenge. Give technical owners authority to stop unsupported releases and protect good-faith dissent.

Consequential creation and verification/release challenge must be independent. Small firms may use competent external reviewers with controlled access and outcome-independent fees.

Automated tools assist evidence gathering; they do not replace required human judgment or cure a reviewer's material conflict.

Keep IAF assessment roles separate from applicant engineering. At least two competent assessors collect evidence, an uninvolved reviewer checks the case and three uninvolved panel members decide. IAF case personnel undergo at least a 36-month conflict look-back, extended where residual risk remains.

G06 Protect releases and users

Define acceptance and stop criteria before testing. Preserve source/build provenance, component composition, original failures, compatibility and support readiness. No executive waiver, emergency deadline or customer acceptance makes a known uncontained serious-harm or uncontrolled critical-exploitation condition acceptable.

Validate staged deployment and target-side state, including partial failure and recovery. Rollback is not always safe when physical states or data schemas changed; document and validate rollback, roll-forward, isolation or another suitable recovery route. Do not equate a successful download with a safe functional update.

Provide truthful limitations, support horizons and customer responsibilities. Maintain accessible vulnerability intake and risk-based response deadlines. The programme's 48-hour serious-incident notice to IAF is not a vulnerability-patching grace period and does not postpone emergency or earlier applicable duties.

G07 Submit the controlled application

Complete the Corporate Recognition Application, Product and Service Scope Schedule and Self-Assessment Dossier. Attach legal authority, adoption, six-month history, actual event populations, internal audit, management review, competence, supply-chain controls and original release evidence. Sign through a person able to bind the applicant.

Index evidence by ID, title, version, date, owner and lawful access route. Prepare protected source/build review where copying is inappropriate. State missing or restricted evidence and material incidents honestly; if essential facts cannot be verified, the affected scope must be deferred or narrowed coherently.

Applications, membership, fees, pilots and private readiness reviews do not grant active status. Keep pending products and proposed capabilities outside active claims and preserve submitted versions. Typed form names require authority and supporting signature or authentication, not merely a copied signature image.

G08 Prepare for assessment and challenge

Every delivering hub is assessed initially and at renewal and reviewed annually. Physical technical facilities receive physical visits. A remote-only office route requires uninvolved approval of secure live observation and original-source review adequacy; otherwise arrange physical access or defer. Cloud hosting alone does not determine the applicant hub model.

Demonstrate every family at initial/renewal. Annually demonstrate all consequential, new/materially changed and adverse-case families, plus a rotating ceiling-square-root selection of remaining families, covering all within three years. Review at least three completed events per family/responsible hub and expand for risk.

Initial/renewal effort starts at two central auditor-days plus hub-size and risk additions in IR02. Physical visits span at least a full operating day with at least half on-site time for observation, witnessing and interviews. Safe isolated demonstrations should challenge failures without disrupting customer production.

G09 Understand decisions and deadlines

Initial grant requires every applicable requirement Met and every finding effectively closed. Pending is not a pass; no weighted score compensates for a failed gate. The independent reviewer checks the evidence and three panel members participate, with at least two reasoned votes for every disposition.

For an active holder, an isolated Minor may remain open up to 90 calendar days with essential assurance protected. Major requires immediate containment, a 30-day closure target and suspension review if unresolved; Critical requires immediate protective review. These rules concern programme findings and do not delay urgent defect or security response.

Recognition lasts at most three years, with surveillance by months 12 and 24 and renewal application at least six months before expiry. A pending assessment or appeal does not extend the term. Factual response is normally 15 calendar days; appeal filing is within 30 days of decision notice.

G10 Maintain support and truthful scope

Notify planned material changes before implementation, unplanned material changes within five calendar days and serious incidents within 48 hours of awareness. Changes in support, suppliers, consequence, lifecycle responsibility or production architecture may be material even if the marketing product name is unchanged.

Keep release approval separate from corporate status and keep new capabilities outside active scope until extension gates are met. A routine release inside an already approved family need not become a new corporate application, but still requires complete technical change control and notification when the change is material.

Maintain supported versions, customer notices, vulnerability response, exit and migration. Retain necessary assurance evidence for ten years after last delivery or declared support end, whichever is later, subject to binding limits and lawful holds. This does not justify retaining unnecessary personal telemetry indefinitely.

G11 Use recognition and resolve disputes fairly

Use exact legal-holder, scope, status and verification information with licensed corporate artwork. A logo beside a software interface, AI answer or test report must not imply IAF endorsed the particular output. Current verification concerns corporate status, not the correctness of a specific computation.

For verification outages or unknown records, report unavailable or unresolved and use the controlled manual route; a cached certificate is not current confirmation. Correct misleading claims after restriction, suspension, expiry or scope change, including distributor and marketplace contexts under the holder's control.

Complaints and appeals receive uninvolved review. A different three-person appeal panel targets a decision within 45 calendar days after complete evidence, with no automatic stay of necessary protection. Restoration requires verified correction and a dated independent decision preserving status history.

G12 Use the complete document suite

The Standard, internal directives and normative annexes establish requirements. The Applicant Guide explains preparation; the Software Lifecycle and Evidence Manual explains implementation; the Audit and Recognition Manual controls evaluation. Status and Mark Rules govern public claims within the Standard.

The six fillable PDFs cover application, scope, self-assessment, all 204 checklist requirements, 28 governance records and 16 lifecycle/release records. Attach original evidence rather than copying confidential repositories wholesale. Form space does not limit the required explanation; use controlled continuation records and attachments.

The master language is English. Shall indicates a requirement, should guidance and may permission. Repeated interactive pages need separate filenames or unique field names to avoid synchronised values. Preserve versions across the suite; a form label or example cannot waive a normative gate.