



QUALITY MANUALS | FIRST EDITION

IAF AUTOID OPERATIONS AND IMPLEMENTATION MANUAL

Procedures for application, identity, assessment,
issuance, change control and continuing assurance.

PROPOSED FOR IAF ADOPTION

Version 1.0 | Prepared for IAF adoption

Applications, identity and evidence verification
Independent assessment and controlled publication
Lifecycle monitoring, changes and operational assurance

International Automotive Federation

English master text | 15 September 2026

iaf.com

Document control

This manual converts the standard into 18 operational procedures with accountable roles, inputs, actions, records and stop conditions. It also defines the adoption gates and practical case examples. The companion fillable checklist contains forms F01 to F08.

Control	Value
Programme	IAF AUTOID
Document	IAF AUTOID Operations Manual First Edition Version 1.0
Status	Proposed for adoption; operational effect requires the recorded IAF authorization
Prepared	15 September 2026
Accountable owner	AUTOID Programme Manager
Publication authority	Presidential Council under the effective Constitution
Adoption record	Resolution reference, authorized scope and effective date recorded in the controlled master list
Review	At least annual maintenance; immediate review on material legal, safety or integrity change
Control	English master; printed and downloaded copies checked against the current controlled edition

Use of this document

This package defines an IAF scheme and its implementation. It does not represent existing regulatory delegation, external acceptance or a live database. Pilot and operational records must be distinguished. The accountable operator shall activate only the markets, categories and functions approved through the release gate.

Contents

Document control	2
Contents	3
Operating model and responsibilities	4
Time rules and service targets	5
P01 Establish and authorize the programme	6
P02 Develop and maintain a jurisdiction profile	7
P03 Receive an application and verify the applicant	8
P04 Resolve identity and allocate the object hierarchy	9
P05 Capture and authenticate the evidence dossier	10
P06 Assess the configuration and applicable requirements	11
P07 Review decide and notify	12
P08 Publish and verify the issued record	13
P09 Bind individual production vehicles	14
P10 Control product changes and software updates	15
P11 Monitor sources and maintain current statements	16
P12 Handle production deviations and supplier issues	17
P13 Respond to a safety or integrity incident	18
P14 Handle privacy requests and controlled disclosure	19
P15 Handle complaints and appeals	20
P16 Operate secure interfaces and recover the service	21
P17 Manage external acceptance and ecosystem adoption	22
P18 Audit improve and expand the programme	23
Worked implementation cases	24
Adoption and rollout roadmap	26
Form and register index	27

Operating model and responsibilities

A case proceeds through intake, identity resolution, evidence authentication, assessment, independent review, independent decision and controlled publication. Identity-only records have a separate limited meaning. After release, configuration changes, source updates, recalls and appeals can change the scoped result without changing the permanent identity.

Function	Accountability	Boundary
Presidential Council	Programme authority, budget, policy, publication and launch	Does not direct case merits
Technical committee	Requirements, consultation, technical recommendations	Does not confer statutory authority
Programme Manager	Service delivery, providers, adoption and maintenance	Cannot waive decision gates
Registrar	Organization checks, scope, identity allocation and records	Cannot declare vehicle conformity
Market Profile Owner	Dated rules, sources, categories and monitoring	Requires independent approval
Assessor	Evidence examination and findings	Does not decide their own case
Independent Reviewer	Completeness, evidence and closure checks	Separate from assessment
Decision Maker	Reasoned scoped decision	Separate from assessment and review
Publication Officer	Public projection, claims and verification tests	Cannot expand approved scope
Security and Privacy Leads	Access, incidents, lawful data processing and recovery	Do not alter technical outcomes
Duty Officer	Urgent triage and protective restriction	Requires prompt independent review
Appeals Committee panel	Independent challenge determination	Three unconflicted case members

Staffing rule

One person may hold more than one organizational role only where case independence is preserved. For each technical case the assessor, independent reviewer and decision maker are distinct. The publication checker is independent of public-data preparation. Duty coverage and substitutes are recorded before launch.

Time rules and service targets

Calendar days include weekends and holidays. Working days follow the published calendar of the legal operator; that calendar must not be used to delay urgent safety action. All incident timestamps use UTC. A longer local service target cannot extend a statutory deadline.

Activity	Period	Basis
Complaint acknowledgement	7 calendar days	Constitution Article 24
Complaint initial response	30 calendar days	Constitution Article 24
Complaint normal determination	60 calendar days	Reasoned extension permitted
Appeal filing	30 calendar days after notice	Constitution Article 24
Appeal normal determination	60 calendar days	Reasoned extension and revised date
Serious event participant notification	Without undue delay and within 24 hours	Shorter legal duty prevails
Duty triage	Within 4 hours of receipt	Continuous duty coverage required
Critical public status propagation	Within 15 minutes after authorization	Service restricted if integrity uncertain
Independent urgent-action review	Within 2 working days	Published operator working-day calendar
Active profile review	At least quarterly and on material notice	Owner monitors official sources
Case maintenance review	At least annually and on relevant events	Not an official approval expiry
Recovery exercise	At least quarterly	Verify restrictions and freshness
Standard maintenance	At least annually	Normally 60-day material consultation

P01 Establish and authorize the programme

Accountable function: Presidential Council and Secretariat

Entry condition: A proposal to operate AUTOID or materially expand its functions has been accepted for development.

1 Establish the legal operator

Record legal entity, address for notices, contractual responsibility, insurance or liability arrangements and the entity that controls personal data. Identify any separate assessment provider. Do not use the federation name to obscure the party responsible for the service.

2 Approve governance

Assign programme manager, registrar, technical lead, market-profile owners, assessors, independent reviewers, decision makers, privacy lead, security lead, duty officer and Appeals Committee interface. Record delegation limits and substitutes. No individual may perform assessment, independent review and final decision for the same case.

3 Approve participation and provider instruments

Confirm the applicable membership conditions separately from technical eligibility. Prepare service terms covering evidence rights, accuracy, notification duties, access, confidentiality, liability, remedies and exit. Execute provider memoranda and scope schedules before an external body claims IAF authorization.

4 Prepare the release baseline

Approve this standard, the manual, checklist, technical schema, country profiles, fee principles, retention schedule and public claim templates as one controlled release. Publish the available categories and exclusions. Record the consultation and independent review results.

5 Make the launch decision

Use F08 and the operator checklist to assemble readiness evidence. Obtain independent readiness review, then Council authorization with effective scope and date. Release only functions that pass their gates; keep all others disabled. Secretariat updates the master list and service catalogue.

Retained outputs: Approved charter, delegation register, participant terms, provider instruments, effective release manifest and F08.

Stop and escalation rule: If corporate authority, independent decision capacity, lawful data processing or continuity funding is missing, the programme remains in development. A launch date cannot waive a failed gate.

Standard section mapping: 01, 02, 18, 19, 23, 24.

P02 Develop and maintain a jurisdiction profile

Accountable function: Market Profile Owner and Technical Lead

Entry condition: A territory and vehicle category are proposed for an operational assessment route.

1 Define the route

Specify territory, road-vehicle category, new or used vehicle status, production stage and intended action: new-type approval, production, market placement, import, registration or modification. Select authority approval, manufacturer self-certification, individual approval or exemption as applicable.

2 Build the obligations matrix

Use official current sources and record instrument, amendment, requirement, category, trigger date and transition rule. Address vehicle safety, environmental obligations, software and cybersecurity, production conformity, labelling, import and registration prerequisites. Do not combine them into one unqualified conformity field.

3 Define evidence acceptance

For each row state required evidence, acceptable issuer and designation, method, decision rule, configuration applicability, source authentication and freshness. Identify tests that may be shared and those that require market-specific evidence. Record any recognition basis explicitly.

4 Validate independently

A competent legal reviewer checks route and dated obligations; a separate technical reviewer checks category, evidence feasibility and completeness. Resolve comments and log exclusions. Approve a profile identifier and immutable version only when no essential issue remains unresolved.

5 Maintain and notify

Monitor official sources, review at least quarterly and open an immediate impact review after a material notice. Identify all dependent assertions, transition dates and required reassessments. Pause new claims where reliable applicability cannot be established.

Retained outputs: Controlled profile and row-level applicability template F02; source register; independent approval and monitoring plan.

Stop and escalation rule: The initial research note is an orientation aid, not an activated market profile. Missing legal interpretation remains unresolved and blocks the affected scope.

Standard section mapping: 03, 09, 10, 16.

P03 Receive an application and verify the applicant

Accountable function: Registrar

Entry condition: An organization submits F01 or its authenticated digital equivalent.

1 Register intake

Assign a case reference, record receipt time and retain the original submission. Acknowledge within seven calendar days as a programme service target. Check the requested output: identity record, scoped conformity statement, unit binding or change. Explain the applicable process and record version.

2 Verify the organization

Confirm legal identity and registration with independent sources. Verify the representative through a trusted business channel and inspect their mandate. Identify manufacturer, importer, brand owner and data steward independently; do not assume these roles coincide.

3 Check administrative eligibility

Apply published participation rules and any required membership condition. Record lawful or scheme-authorized non-member access separately. Identify language support and reasonable accessibility needs. Administrative eligibility must not change technical acceptance criteria.

4 Define requested scope

List model boundaries, variants, configurations, categories, territories, intended dates, production stage and available evidence. Classify prototypes and exceptional routes explicitly. Confirm evidence-use rights and privacy classification before collecting detailed files.

5 Accept or return for completion

Issue a written scope and missing-information list. Assign a case manager only when enough information exists to plan assessment. Do not label a received or accepted application as approved. Store commercially sensitive material in the restricted case area.

Retained outputs: F01, verified organization and representative record, case scope, missing-information log and assigned case manager.

Stop and escalation rule: If authority to submit is doubtful, quarantine the case without reserving a public identity. Suspected impersonation goes to P13.

Standard section mapping: 02, 03, 04, 18.

P04 Resolve identity and allocate the object hierarchy

Accountable function: Registrar and Identity Reviewer

Entry condition: The organization and case scope have passed intake checks.

1 Build the hierarchy

Create or locate the legal organization and model. Document why the engineering family is one model and identify aliases. Define variant selection rules and frozen configurations. Link vehicles, components, software and facilities only when those object classes are supported by the release.

2 Search for duplicates

Compare engineering codes, manufacturers, aliases and external identifiers. Review similarity candidates manually. For a VIN conflict, preserve both submissions and independently establish the physical and source identity; do not merge to make the conflict disappear.

3 Confirm identity relationships

Check model-to-regulatory-type mappings by market. Record rebranding, shared platform, predecessor, successor and multi-stage relationships without implying automatic evidence transfer. Obtain the identity reviewer approval.

4 Reserve transactionally

Generate the class-coded UUID identifier using the controlled allocator. Enforce uniqueness, the issuer-scoped idempotency key and the exact request digest. Preserve the reservation even if later abandoned; it may become a non-public tombstone but shall not be reassigned.

5 Release an identity record where appropriate

An identity-only record may be published after the identity and public-data checks pass even while conformity assessment remains not_assessed. Its display must say that technical conformity has not been assessed. The registrar cannot promote it to a conformity result.

Retained outputs: Object hierarchy, duplicate-resolution record, allocation log and identity state decision.

Stop and escalation rule: A new UUID does not resolve an unresolved physical identity. Disputed identity blocks positive verification and unit binding.

Standard section mapping: 03, 04, 05, 06, 08, 12.

P05 Capture and authenticate the evidence dossier

Accountable function: Assessor and Evidence Custodian

Entry condition: A case has an agreed configuration and market scope.

1 Receive securely

Scan uploads, preserve original bytes and assign evidence references. Record issuer, edition, date, covered subject, original digest, classification and usage rights. Extracted fields must retain links to the original pages or data records.

2 Authenticate the source

Use the official register, issuer signature or independently verified contact. Confirm issuer competence and territorial scope at the relevant date. Record exactly what the check established: authenticity, source status, configuration applicability or all of these. An email from an unverified address is not sufficient.

3 Review the technical content

Check complete reports, test methods and editions, acceptance limits, units, conditions, specimen identification, deviations, uncertainty where required and result statements. Identify limitations, exclusions and any missing annexes.

4 Link evidence to requirements

Complete F02 for each applicable row. A single document may support multiple rows only with an explicit mapping. Shared evidence requires a documented equivalence or carry-forward rationale. Preserve differences among manufacturer declarations, test reports and authority approvals.

5 Resolve conflicts

Record contradictions in F03 and the findings log. Request clarification from competent sources. Keep the affected scope on hold until the independent reviewer accepts the resolution. Do not delete unfavourable evidence or use an AI-generated summary as the source document.

Retained outputs: Evidence ledger, authenticated originals, F02 matrix, F03 verification records and unresolved-evidence log.

Stop and escalation rule: If authenticity or essential applicability cannot be established, report insufficient evidence. The applicant may pursue independent source confirmation; the assessment shall not assume authenticity.

Standard section mapping: 09, 10, 11.

P06 Assess the configuration and applicable requirements

Accountable function: Lead Assessor

Entry condition: Identity has been verified and the evidence dossier is ready for planned assessment.

1 Plan the examination

Name qualified assessors, the independent reviewer and proposed decision maker. Record risks, all configurations, profiles, witnesses, site work and sampling of recurring records. Check conflicts before giving access to the case.

2 Assess every applicable row

For each requirement examine authenticity, technical sufficiency, exact scope and temporal applicability. Record conforming, nonconforming, not applicable with approved rationale, or pending. Pending is not a pass. Review all critical identity, approval, exemption and baseline fields without sampling.

3 Assess product and production links

Check worst-case variant rationale, software baseline, hardware dependencies and production conformity evidence. When a configuration range is claimed, verify the boundary conditions and exclusions. Match vehicle-level claims to actual build records and affected population definitions.

4 Record and discuss findings

State the requirement, observed evidence, affected population, classification and action. Give the applicant an opportunity to correct factual mistakes and submit corrective evidence. Record disagreements; do not negotiate away required criteria.

5 Verify correction effectiveness

Evaluate the cause, extent, correction and prevention. A new report or revised procedure is not enough if the failed control remains ineffective. Reopen related cases if the issue is systemic. Submit a complete assessment package to independent review.

Retained outputs: Assessment plan, completed checklist, findings and closure log, technical report and recommendation.

Stop and escalation rule: Critical findings trigger P13 immediately. An identity-only record may remain visible with appropriate restrictions, but a failed technical scope shall not receive a positive statement.

Standard section mapping: 07, 08, 09, 10, 11, 14.

P07 Review decide and notify

Accountable function: Independent Reviewer and Decision Maker

Entry condition: The assessor has submitted the complete case record.

1 Review the file independently

Confirm competence, conflicts, scope, applicable profile edition, evidence chain, configuration coverage and closure of every relevant requirement. Recalculate any derived result used in the decision. Return gaps to assessment with a written reason.

2 Apply the decision threshold

Require all applicable checklist answers to be conforming or justified not applicable for the claimed scope. No unresolved critical, major or minor failure may be hidden by a score. Where a smaller scope can stand independently, define a new explicit restricted scope and recheck all interfaces before deciding it.

3 Make the reasoned decision

The decision maker selects identity-only, verified scoped statement, refusal, restriction, suspension, withdrawal or supersession as appropriate. Record the requirement basis, configurations, market profiles, evidence checked, limitations, maintenance requirements and authorized public wording.

4 Set independent states

Record identity state, each assessment state, external source status, evidence currency and safety-alert status separately. An external legal-status field must be based on the named source, not inferred from IAF opinion. If no reliable source check exists, leave it not_checked.

5 Notify and control release

Complete F04, send the decision and reasons, explain the 30-calendar-day appeal filing period and designate the publication checker. Release occurs only after P08. Record notification time so the appeal period can be established.

Retained outputs: Independent review, reasoned decision F04, exact statement text, status events and notification record.

Stop and escalation rule: When independent personnel are unavailable, obtain authorized external capacity. Do not let the assessor sign their own decision because the case is urgent.

Standard section mapping: 01, 02, 11, 12, 22.

P08 Publish and verify the issued record

Accountable function: Publication Officer independent of data preparation

Entry condition: An authorized identity or scoped conformity decision is ready for publication.

1 Build the approved projection

Select only allowlisted public fields. Display manufacturer, model, exact configuration or range, separately named markets and routes, identity and assessment meaning, currency, restrictions, safety alerts and issuer. Keep evidence files, personal data and private VIN information outside the projection.

2 Verify the meaning

Compare the page and extract to the decision. Avoid a universal approved badge. An authority approval should be described as a source record verified for the specified scope; a manufacturer declaration must retain that source description.

3 Check links and access

Scan the actual QR, confirm the operator-controlled domain and exact record identity, and test anonymous and restricted access. Test nonexistent IDs, retired IDs, stale statements and suspended states. Confirm that identifiers and tokens do not reveal private data.

4 Release atomically

Commit the signed decision, revision and authorized public projection together or through a controlled outbox that prevents premature positive display. Record the released revision and checker. When an asynchronous projection is behind, display its timestamp and suppress current claims beyond its freshness limit.

5 Confirm recipients and preserve history

Send the issued extract to the applicant, record permitted mark use and retain the historical display. Register authorized downstream subscriptions for changes. The public correction channel shall remain available without a paid account.

Retained outputs: Released public record, signed extract if enabled, verification test and mark permission.

Stop and escalation rule: If public and decision records disagree, stop publication and treat any already exposed misleading statement as a controlled incident.

Standard section mapping: 12, 13, 18, 19, 20.

P09 Bind individual production vehicles

Accountable function: Manufacturer Data Steward and Registrar

Entry condition: A verified configuration is available and a manufacturer requests vehicle-level records.

1 Define the population

State facility, production period, categories, configuration selection and explicit inclusions and exclusions. Use protected lists when VIN ranges would include unrelated vehicles. Verify source authority and the right to process unit-level data.

2 Validate each vehicle

Check VIN or lawful alternative under the profile, production data, as-built configuration and source completion record. Flag duplicate or inconsistent bindings. A VIN decoder may assist interpretation but shall not replace authenticated manufacturer or inspection evidence.

3 Check build and conformity linkage

Confirm each vehicle belongs to the configuration and scope covered by evidence. Preserve incomplete and completed stages and separate final-stage obligations. If the claimed scope depends on production conformity, confirm that the production period and facility are covered.

4 Issue controlled unit identifiers

Allocate AID-U identifiers transactionally. Store full VINs in a protected identifier vault and use a restricted lookup mechanism. Public model statistics shall not enable enumeration of unit identifiers or owner information.

5 Maintain as-built and current states

Keep the original configuration relationship immutable. Add dated relationships for later modifications, software updates or battery replacement. Show unknown current configuration where no reliable update exists; do not assume every vehicle received an update because it was released.

Retained outputs: Validated vehicle population, unit identities, protected VIN bindings, as-built and current relationships.

Stop and escalation rule: Unresolved clone or VIN conflict is quarantined. A unit outside the configuration boundary cannot inherit the model assessment.

Standard section mapping: 05, 07, 08, 14, 18.

P10 Control product changes and software updates

Accountable function: Manufacturer Data Steward and Lead Assessor

Entry condition: A participant reports a change or surveillance detects a changed product.

1 Register the change

Use F05 to record source, awareness date, effective date, affected objects, reasons and whether vehicles already exist in the field. Identify interim restrictions and any urgent authority reporting duty.

2 Classify the change

A pure clerical correction changes a record revision. A material technical change creates a new configuration ID. A new engineering family or different legal manufacturer may require a new model ID. Record rationale and obtain review; uncertain materiality is treated as material until resolved.

3 Build the delta matrix

List changed hardware, software, calibration, battery, suppliers, facilities and interfaces. Mark affected legal requirements, test worst cases, production controls and prior evidence. Require new tests or authority action where the old scope does not cover the change.

4 Review and decide the new scope

Apply P05 to P07. Keep the original assessment available for its original configuration unless contrary evidence justifies restriction. Link the new assessment to its predecessor and explain any remaining valid older scopes.

5 Update and monitor deployment

Publish only the authorized scope. Record the actual population receiving software or physical modifications and the source confirming completion. Do not mark a unit updated from a campaign announcement alone. Monitor rollout issues and return safety concerns to P13.

Retained outputs: F05, delta matrix, new configurations, revised evidence mappings and unit-level deployment events.

Stop and escalation rule: A commercial software release date cannot override a pending safety or regulatory review.

Standard section mapping: 07, 12, 14, 15, 17.

P11 Monitor sources and maintain current statements

Accountable function: Surveillance Coordinator

Entry condition: An issued record requires continuing evidence currency and lifecycle monitoring.

1 Set the maintenance plan

For each market and source specify automated or manual channel, check interval, maximum age, responsible officer, outage behaviour and annual case review. Establish a shorter interval for high-risk or unstable evidence.

2 Collect and reconcile updates

Monitor active connected high-risk approval and recall sources at least daily where lawfully available. Record source time and retrieval time. Reconcile changes using authoritative IDs rather than text similarity alone. A failed source call must not reset the last-successful-check clock.

3 Propagate currency changes

When a review date or source maximum age is exceeded, set review_due or stale and suppress an unqualified current result. A still-valid cryptographic signature does not make stale source information current.

4 Investigate triggered risk

Review complaints, changed laws, supplier incidents, production deviations and provider restrictions. Bound affected configurations and units. Use P10 for technical change and P13 for immediate safety or integrity issues.

5 Close the review

Record verified sources, findings, decisions and next due dates. Explain any sampling and residual source gaps. Quarterly management reporting shall include overdue cases, source outages and misleading display incidents, not just the number of issued IDs.

Retained outputs: Monitoring logs, maintenance decisions, updated source timestamps and quarterly metrics.

Stop and escalation rule: If reliable source access is unavailable, display the limitation and suspend new positive claims that depend on it. Do not describe the feed as real-time.

Standard section mapping: 09, 14, 16, 17.

P12 Handle production deviations and supplier issues

Accountable function: Lead Assessor and Manufacturer Quality Contact

Entry condition: A production discrepancy, supplier change or provider restriction may affect issued records.

1 Contain the population

Obtain batch, facility, date, part and configuration data. Distinguish confirmed affected units from potentially affected units. Apply precautionary restrictions to the uncertain range where the risk warrants it.

2 Evaluate cause and extent

Review manufacturing deviation, supplier evidence, test results and original worst-case rationale. Check whether the issue existed when earlier decisions were made. Do not assume a later provider suspension invalidates all historical evidence.

3 Set corrective evidence

Require an action plan addressing process cause, product correction, reinspection and any authority obligations. Define sample expansion or full-population verification proportionate to the defect and ability to bound the population.

4 Review release independently

Verify effectiveness and obtain a new decision for any restored scope. A new management-system certificate is not sufficient evidence that affected vehicles were repaired or conforming.

5 Update dependent records

Record which models, configurations, lots and units are restricted or cleared. Notify relying parties and maintain links to unresolved cases and safety campaigns.

Retained outputs: Bounded affected population, corrective-action record and independent restriction or restoration decision.

Stop and escalation rule: An unbounded critical defect routes to P13. Commercial pressure shall not shorten required verification.

Standard section mapping: 10, 14, 15, 16, 17.

P13 Respond to a safety or integrity incident

Accountable function: Duty Officer with Security or Technical Lead

Entry condition: A credible severe hazard, false approval, identity cloning or key compromise is reported.

1 Log and triage

Record awareness, receipt, source, confidence and affected scope in F06. Participants notify without undue delay and within 24 hours; the duty function triages within four hours of receipt. Identify any shorter legal obligation and the responsible legal notifier.

2 Protect users and preserve evidence

Apply a scoped restriction to potentially misleading positive results. Freeze destructive administrative actions, preserve relevant originals and logs, and segregate compromised credentials or sources. If status integrity is uncertain, affected verification returns restricted or unavailable.

3 Notify competent parties

Inform the responsible manufacturer and relevant IAF functions. The designated legal duty holder makes statutory notifications. Public notices shall use verified facts and necessary risk information; confidential investigations shall not suppress an essential safety warning.

4 Review and propagate

An independent officer reviews the interim measure within two working days. Commit authorized critical changes immediately and ensure public propagation within 15 minutes. Record delivery failures and use a controlled alternate communication route for high-risk recipients.

5 Remedy and close

Distinguish authority recall status, model campaign status and unit remedy completion. Require authenticated unit-specific evidence for a remedied flag. Close only after scope, containment, source status and corrective effectiveness are established, then review systemic lessons.

Retained outputs: F06, incident timeline, public restriction, source notifications, unit remedies and closure review.

Stop and escalation rule: The operator does not remotely disable vehicles. Any operational vehicle action remains with legally authorized parties and their validated safety procedures.

Standard section mapping: 15, 17, 19.

P14 Handle privacy requests and controlled disclosure

Accountable function: Privacy Lead

Entry condition: A data request, proposed sharing arrangement or personal-data incident is received.

1 Identify the purpose and authority

Determine the dataset, requester, purpose, controller role and relevant jurisdiction. Verify identity proportionately. Do not collect a full identity document when a less intrusive confirmation is sufficient.

2 Check the permissible response

Apply the processing inventory, lawful basis, contract and legal deadlines. Separate personal data from manufacturer trade secrets and public technical data. Consult legal review for conflicts involving authority requests, litigation or cross-border transfers.

3 Prepare minimal disclosure or correction

Use a controlled extract, redact unrelated data and preserve context. Corrections shall update derived public projections and indexes. If deletion is required, schedule replica and backup expiry and preserve only a lawful minimal audit record.

4 Approve and transmit securely

Use a second reviewer for sensitive bulk disclosure. Record recipient, legal basis, fields, security method and time. Public verification shall never become a substitute for a controlled data-subject response.

5 Close and verify

Check completion of correction, deletion or access provision, record the response and remaining restrictions, and update the data inventory when the case exposes a design gap.

Retained outputs: Rights or disclosure case, legal basis, approved extract and verified completion record.

Stop and escalation rule: Do not put personal data on an immutable public ledger. A record-retention interest does not automatically defeat a lawful deletion request.

Standard section mapping: 18, 19, 21.

P15 Handle complaints and appeals

Accountable function: Secretariat and independent Appeals Committee panel

Entry condition: A concern or challenge to an IAF decision is received.

1 Classify and preserve

A complaint concerns conduct, procedure or inaccurate data; an appeal challenges a decision. Record both routes if needed and preserve the original file. A complaint is acknowledged within seven calendar days, receives an initial response within 30 and normally a determination within 60.

2 Check appeal timing

An appeal may be filed within 30 calendar days of notified decision. Record notification evidence, filing time and any legally required accommodation. Do not invent an undisclosed retroactive filing bar.

3 Appoint independently

Use the Appeals Committee competence roster and rotation to appoint three unconflicted members. Exclude anyone involved in the original case, selection influence or material commercial interest. Where necessary, use independent external professionals.

4 Review and determine

Provide a fair opportunity to submit evidence and respond. Consider interim measures without automatically removing justified safety restrictions. Normally determine within 60 calendar days, with written reasons for extensions. The panel may affirm, set aside or remit within its remit.

5 Implement and learn

Assign corrective actions, update records, notify affected recipients and confirm implementation. Protect good-faith reporters and preserve lawful external remedies. Use appeal trends to improve rules and training without targeting appellants.

Retained outputs: F07, independent panel record, reasoned determination and completed implementation.

Stop and escalation rule: The older quality procedure uses different service periods and Board terminology. AUTOID follows the Constitution precedence and requires formal alignment of subordinate procedures before release.

Standard section mapping: 01, 02, 22.

P16 Operate secure interfaces and recover the service

Accountable function: Security Lead and Registry Operations Lead

Entry condition: The service is ready for operational deployment or has suffered an outage.

1 Enforce trust boundaries

Separate public read models, authenticated case services, restricted evidence storage and signing infrastructure. Apply object-level and tenant-level authorization to every operation, including exports and search. Treat imported files and URLs as untrusted input.

2 Control releases

Use reviewed code, schema migration plans, dependency scanning and independent security testing. Test negative cases for stale status, revoked keys, data leakage, forged approvals and replayed requests. Record release and rollback approval.

3 Monitor and back up

Measure availability, response time, failed writes, event lag and source freshness. Back up encrypted records and key recovery materials under separate controls. Target four-hour recovery time and 15-minute recovery point; measure actual performance rather than assuming the design target was achieved.

4 Restore consistently

Restore into an isolated environment, reconcile event positions and missed restrictions, verify authorization and key state, and mark uncertain records unavailable. Do not reopen public positive verification until current restrictions are applied.

5 Exercise and improve

Run a restoration exercise at least quarterly and a full independent readiness check before initial release. Record measured times, missing data, key recovery, status correctness and follow-up actions.

Retained outputs: Release record, security evidence, monitoring dashboard and tested recovery report.

Stop and escalation rule: A healthy web server is not proof of a current registry. Recovery fails if it restores an obsolete positive status over a newer suspension.

Standard section mapping: 05, 12, 19, 20, 21.

P17 Manage external acceptance and ecosystem adoption

Accountable function: Programme Manager and authorized IAF signatory

Entry condition: A manufacturer, authority, laboratory, fleet, insurer or platform proposes reliance on AUTOID.

1 Define the useful transaction

Choose a concrete use case such as evidence reuse for homologation preparation, supplier identity checks, recall matching or verified model lookup. Identify the recipient decision that AUTOID supports and the information still needed from official sources.

2 Evaluate fit and limits

Compare the recipient requirements with AUTOID fields, assurance process, maintenance and liability model. Identify missing legal basis, data rights, category coverage and technical gaps. Do not promise universal recognition.

3 Run a bounded trial

Agree datasets, permitted use, acceptance criteria, confidentiality and exit. Measure duplicate reduction, retrieval time, error discovery, status freshness and implementation effort. Include negative cases and independently review results.

4 Execute a scoped arrangement

Document parties, exact outputs, territory, use, monitoring, data exchange, liability, suspension, termination and public wording. Statutory recognition requires its own lawful instrument; a memorandum or commercial agreement does not create it.

5 Publish accurately and maintain

Describe the relationship as trial participation, contractual reliance or statutory recognition according to evidence. Maintain a current acceptance register and remove outdated claims when conditions lapse. Preserve existing user access and lawful export on exit.

Retained outputs: Trial protocol, measured results, acceptance agreement, public wording and maintenance owner.

Stop and escalation rule: A participant may find AUTOID useful without accepting it as legal proof. Record this honestly and improve the agreed use case.

Standard section mapping: 02, 09, 20, 24.

P18 Audit improve and expand the programme

Accountable function: Quality Lead and Presidential Council

Entry condition: A planned review, significant failure or new-scope proposal is due.

1 Audit requirements

Use the operator checklist to review all 120 controls for relevance and implementation. Sample cases across routes and categories while fully checking decision-critical elements. Auditors shall be independent of the activity audited.

2 Review performance and risk

Quarterly management review examines adverse outcomes, overdue cases, source outages, duplicate conflicts, appeals, privacy incidents, staffing and continuity. Investigate metrics that reward volume over evidence quality.

3 Control corrective action

Define cause, extent, containment, owner, due date and effectiveness check. Restrict the service if failure undermines trustworthy decisions. Document the rationale for reopening related cases.

4 Consult and revise

Conduct annual standard maintenance and normally 60-day consultation for material changes. Preserve comments and dissent, obtain independent quality review and Council publication authorization. Issue controlled transitions and update linked forms and schemas together.

5 Expand through gates

For each new market, category or automated function, repeat profile, competence, privacy, security, pilot and release checks. Publish a clear available-scope catalogue rather than a roadmap presented as current coverage.

Retained outputs: Audit and management review, corrective actions, revised release manifest and controlled expansion decision.

Stop and escalation rule: A successful narrow pilot does not authorize global rollout. No market profile becomes operational merely because it appears in the roadmap.

Standard section mapping: 01, 09, 16, 21, 23, 24.

Worked implementation cases

All examples below are illustrative. They create no actual vehicle approvals or manufacturer records.

One model two markets

A fictional battery-electric passenger-car model has one AID-M, two variants and three configurations. The EU route holds an authenticated approval record for configuration C1; the US route holds an attributable manufacturer self-certification dossier for C2. Each market has its own profile, evidence, state and timestamp. The shared model does not transfer one market outcome to the other. A third country remains not_assessed until its profile and evidence are complete.

Battery and braking calibration change

The manufacturer replaces a battery with a heavier pack and changes braking calibration. The model identity remains stable but a new AID-C is created. Mass, electrical safety, braking, range and software-related evidence are reviewed. Existing C1 vehicles retain their C1 history; only authenticated updated units gain a dated link to C2. A general software campaign announcement does not update every vehicle record.

An uploaded approval is forged

A convincing approval PDF contains an identifier that does not match the authority record. The assessor records the discrepancy and contacts the issuer through an independently verified channel. The affected assertion remains in_review or refused; if already published it is suspended with a proportionate notice. Other evidence from the same source is reviewed for extent. The case is not rescued by a valid PDF hash.

Recall after valid issuance

An authority publishes a recall for a defined production population. AUTOID keeps model identity verified, opens a safety alert and records the source action separately. The effective display becomes qualified or restricted depending on the actual impact. Unit remedies require authenticated completion evidence. Closing one unit does not close the entire campaign.

Historic vehicle with a short chassis number

A lawful historic-vehicle pathway uses a non-17-character chassis number. The profile records the applicable identifier scheme and inspection evidence. The registry preserves that value and labels its scope. It does not force an invented modern VIN or infer a current-production approval.

Source outage during verification

The official source connector has failed beyond its maximum age. The last record and check time remain visible, but the result is marked stale and is not returned as current positive conformity. A restored connection must reconcile missed suspensions before the service restores a current result.

Badge engineered vehicle

Two brands share a platform but have different legal manufacturers and restraint calibrations. AUTOID records linked platform relationships and separate model responsibilities. Technical evidence is reused only where permission and an explicit applicability rationale exist; restraint and other changed evidence must be reviewed independently.

Adoption and rollout roadmap

The following sequence is a planning proposal. Time ranges start after the project is authorized and depend on staff, agreements and evidence. Passing a date is not passing a gate.

Gate	Work	Indicative timing	Exit evidence
Gate 0	Charter and legal design	Weeks 1 to 4	Operator, authority, liability, privacy, independence and budget approved
Gate 1	Core specification and consultation	Weeks 5 to 12	Data model, profiles, 60-day consultation and comment disposition
Gate 2	Sandbox and issuer onboarding	Weeks 13 to 20	Schema, trust registry, restricted evidence store, trained assessors
Gate 3	Bounded pilot and independent testing	Weeks 21 to 32	Two regulatory routes, five organizations, 20 cases and 1,000 test units
Gate 4	Controlled operational release	Weeks 33 to 40	No unresolved launch blockers, tested recovery, Council scope release
Gate 5	Acceptance agreements and expansion	Months 11 to 18	Measured reliance trials, executed scoped agreements, new-profile gates

Pilot acceptance protocol

Select at least two distinct regulatory routes and five independent organizations. Assess at least 20 model or configuration cases and 1,000 synthetic or lawfully authorized vehicle records. Include a shared-platform case, multi-stage vehicle, material software update, changed battery, duplicate identity, forged evidence, stale source, open recall, unit remedy and independent appeal. These minimums test operational coverage; they do not statistically establish global reliability.

Release measurements

Measure evidence retrieval time, duplicate and scope errors detected, outstanding findings, case handling effort, unauthorized-data exposure, source freshness, critical status propagation, restoration time and correct recovery of restrictions. Record every failed test and its correction. An independent reviewer verifies outcomes; the Council authorizes only the exact passing scope.

Commercial and institutional adoption

Start with benefits recipients can measure: one stable model reference, reusable authenticated dossiers, fewer mismatched configurations and reliable recall linkage. Offer open public model verification and portable technical exports. Use transparent participation and pricing principles and protect SMEs from unnecessary administration. Claims of public-authority acceptance require verified legal instruments; private contracts shall describe their narrower reliance.

Form and register index

Form	Purpose	Primary procedure
F01	Application and object scope	P03
F02	Jurisdiction applicability and evidence row	P02 P05 P06
F03	Evidence authentication record	P05
F04	Assessment and independent decision	P07 P08
F05	Material change and carry forward	P10
F06	Safety incident and recall action	P13
F07	Appeal and independent determination	P15
F08	Launch authorization and accepted scope	P01 P18

The fillable companion provides reusable blank forms. Completed forms become classified case records. More than one F02 row or F03 record will normally be needed; duplicate the relevant blank form as a separate controlled record or use its digital schema. A typed name in a text field is not a cryptographic signature.

Operating registers

Maintain controlled registers for organizations and mandates; identifiers and aliases; profiles and obligations; issuers and provider scope; cases and evidence; decisions and public claims; findings and corrective actions; source checks and recalls; complaints and appeals; access and incidents; retention and legal holds; and external acceptance agreements. These may be database views rather than separate spreadsheets, provided their control and audit functions remain intact.