



FIRST EDITION

IAF PSR SUPPLIER RECOGNITION

Programme Standard

A corporate quality and trust framework for automotive product and system suppliers across the supply network.

PREPARED FOR IAF ADOPTION

Version 1.0 | 16 September 2026
English master text

International Automotive Federation

iaf.com

Document control

Item	Controlled value
Programme	IAF Product & System Supplier Recognition Programme (IAF PSR)
Document	Standard and Internal Directives
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

A corporate quality and trust framework for automotive product and system suppliers across the supply network.

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
Programme purpose and trust model	5
Scope and eligibility	5
IAF quality adoption and applicability	6
Supplier profile map	6
01 Legal identity, scope and accountability	7
02 Leadership, policy and governance	8
03 IAF quality adoption and claim substantiation	8
04 Obligations and responsible commercial conduct	9
05 Risk management and product safety	10
06 People, competence and working conditions	10
07 Design, development and engineering change	11
08 Supply network and purchased assurance	12
09 Industrialisation and production readiness	12
10 Manufacturing and assembly control	13
11 Measurement, testing and release evidence	14
12 Identity, configuration and traceability	14
13 Preservation, logistics and delivery	15
14 Software, cybersecurity and information integrity	16
15 Aftersales, warranty and lifecycle support	16
16 Complaints, field action and emergency response	17
17 Environmental responsibility and circularity	18
18 Resilience and continuing ability to deliver	18
19 Contract manufacture, intellectual property and interfaces	19
20 Customer confidence and service fulfilment	20
21 Performance, indicators and evidence quality	20
22 Internal audit and management review	21
23 Corrective action and verified effectiveness	22
24 Recognition obligations and continuing truth	22
25 Customer product and system acceptance	23
26 Long-term supply, obsolescence and ecosystem integrity	24
Supplier profiles - selection and use	24
SYS Integrated systems and module suppliers	24
CMP Mechanical components and subassemblies	25
ELE Electrical, electronic and semiconductor suppliers	26
MAT Materials, chemicals and consumables	26
SWD Software, data and digital product suppliers	27
PROC Special-process and contract production suppliers	27
TLS Tooling, equipment and production technology suppliers	28
ENE Energy storage, propulsion and charging-system suppliers	29
REM Remanufactured, repaired and circular-product suppliers	29
DST Controlled product supply and distribution	30

Technology and future-capability domain map	31
T01 Electric propulsion, batteries and energy storage	31
T02 Charging and energy interfaces	32
T03 Connected and software-defined products	32
T04 Automated driving and machine intelligence	33
T05 Digital twins, virtual evidence and automated inspection	34
T06 Advanced materials and automated manufacturing	34
T07 Circular products, remanufacture and product information	35
T08 Low-carbon production and resilient resources	36
T09 Human-centred and accessible mobility	36
T10 Heavy, special-purpose and emerging mobility	37
IR01 Programme authority, eligibility and adoption	38
IR02 Scope, multiple sites and technical families	38
IR03 Audit evidence, duration and sampling	39
IR04 Findings, decisions and recognition term	40
IR05 Public status, recognition record and mark	40
IR06 Fair process, confidentiality and protected reporting	41
IR07 Records, digital trust and oversight	42
IR08 Implementation, global use and future development	42
Annex A - Definitions and interpretation	43
Annex B - Decision and status matrix	44
Annex C - Minimum scope and decision data	45
Annex D - Audit coverage and duration rules	45
Annex E - Deadlines, clocks and records	46
Annex F - Performance and interpretation	47
Annex G - Recognition statement and claim boundary	48
Annex H - Launch, acceptance and future development	48
Annex I - Controlled document set	48
Annex J - Supplier sites, case units and responsibility	49
Annex K - Product approval and corporate recognition interface	50

Programme purpose and trust model

IAF PSR establishes a practical route from a corporate quality claim to verified implementation, independent recognition and continuing accountability. It connects legal responsibility, operational control, authentic evidence, customer outcomes and transparent scope/status. The intended benefit is justified confidence in the organization activities, products and related services within a defined boundary.

The programme is technology-neutral and available to eligible organizations worldwide where competent assessment, safe access and lawful operation can be established. Geography, size, membership, sponsorship or commercial importance shall not lower essential requirements. Acceptance by an individual customer or authority remains a specific fact to establish, not an automatic consequence of this document.

Layer	Normative coverage
Common corporate baseline	104 requirements in 26 sections, addressing the organization and its controlled industrial activities.
Supplier profiles	10 profiles, each adding 4 requirements; select all relevant profiles.
Technology domains	10 modules, each adding 4 requirements when its technology or risk trigger exists.
Internal directives	8 directives with 32 requirements, governing IAF operation and reciprocal applicant obligations.
Assessment total	216 separately identified requirements, plus complete evaluation of any additional IAF requirement text claimed as implemented.

Recognition is a controlled conclusion

The organization adopts the quality basis, implements it, submits original evidence and permits audit. IAF tests the evidence, verifies closure and makes an independent decision. Active status is supported by annual surveillance, physical site visits, change reporting and enforceable claim limits. A claim without a bounded scope or current evidence is insufficient.

Scope and eligibility

Eligible scope comprises integrated systems, mechanical components, electronics, materials, digital products, special processes, tooling/equipment, energy systems, circular products and controlled distribution. Apply the ten supplier profiles according to actual responsibility. Include related services where the applicant accepts direct responsibility and demonstrates actual control.

Passenger and commercial vehicles, buses, motorcycles, trailers, micromobility and declared special-purpose or off-road vehicles may be covered. State the exact products, application limits and market responsibilities. A legal entity may use multiple profiles. Pure membership, awards, training, unrestricted brokerage and independent testing/assessment are not eligible supplier activities by title alone. Controlled distribution requires the DST profile and actual product accountability; it does not imply that the source manufacturer is recognised.

Boundary of assurance

Corporate recognition assesses implemented corporate controls and demonstrated operation. It does not certify every product, create vehicle homologation, authorize a conformity-assessment body, replace market permissions or guarantee contractual success. Other IAF product, quality or identity programmes retain their own criteria and decisions. No external-standard equivalence or universal legal acceptance shall be implied.

IAF quality adoption and applicability

This Standard provides a self-contained IAF corporate quality baseline. The executive shall adopt it and identify any additional IAF quality texts claimed as implemented. Complete the adoption schedule and requirement-level evidence map for each such text. A working draft or pilot remains a development basis until formally approved. PSR recognition alone does not certify the complete IAF standards portfolio.

Determine applicability at the lowest practical requirement. Core controls apply according to actual responsibility; profile and technology modules supplement them. Outsourced operations remain controlled responsibilities. Non-applicability requires evidence of an absent activity or responsibility and independent acceptance. IAF-only operator duties are assessed through separate operator-assurance records, not by applicant declarations.

Essential decision gates

Gate	Minimum conclusion needed
Eligibility and identity	Accountable entities, sites and scope are clear; lawful access and operation are supported.
Implemented history	At least six months, one internal audit and one management review.
Actual cases	At least three complete production/release/delivery cases per included family/site.
Technical evidence	Applicable controls, profiles, modules and additional claimed criteria are supported.
Physical audit	All initial operational sites and critical outsourced operations necessary to verify claims assessed; mandatory site/shift/process coverage achieved.
Closure and decision	All applicable requirements Met; no open initial findings; independent three-person decision.
Public trust	Validated status verification, exact scope schedule and authorized claim/mark controls.

Supplier profile map

Profile	Application
SYS Integrated systems and module suppliers	Suppliers accountable for the integration of multiple components, functions or supplied subsystems.
CMP Mechanical components and subassemblies	Producers of mechanical parts, fasteners, structures, assemblies and replacement components.
ELE Electrical, electronic and semiconductor suppliers	Suppliers of sensors, controllers, harnesses, connectors, electronic assemblies and semiconductor devices.
MAT Materials, chemicals and consumables	Suppliers of metals, polymers, fluids, coatings, adhesives, chemicals and automotive production consumables.
SWD Software, data and digital product suppliers	Suppliers of embedded software, automotive platforms, models, datasets and directly related digital services.
PROC Special-process and contract production suppliers	Suppliers performing machining, joining, heat treatment, coating, finishing, assembly or other contracted transformation.
TLS Tooling, equipment and production technology suppliers	Suppliers of tools, fixtures, machinery, automation, test equipment and associated production engineering.

Profile	Application
ENE Energy storage, propulsion and charging-system suppliers	Suppliers of cells, battery packs, power conversion, electric propulsion and charging-related systems.
REM Remanufactured, repaired and circular-product suppliers	Suppliers restoring or requalifying automotive components and systems for defined continued or alternative use.
DST Controlled product supply and distribution	Suppliers accountable for sourced products, configuration, authenticity, technical handover and supply continuity.

01 Legal identity, scope and accountability

PSR-01.01 Accountable legal entity

The organization shall identify the legal entity accountable for its products, services and recognition claim, with registration, ownership, operating permissions and authorized representatives. A brand, group name or distributor agreement shall not substitute for an accountable entity. Every included subsidiary shall be separately named and accept its responsibilities.

Essential gate. Evidence: Registration, ownership chart and signed entity undertakings.

PSR-01.02 Defined supplier responsibility boundary

Define every included site, product/system family, customer application, related service and technology. State whether the supplier designs, integrates, manufactures, processes, configures, distributes or supports the output. Identify the actual source of manufacture and the party controlling final acceptance. Capability claims shall distinguish demonstrated work from planned investment and prototype activity.

Essential gate. Evidence: Entity/site/family schedule with role and source-of-manufacture fields.

PSR-01.03 Customer, supplier and sub-tier interfaces

Map responsibility across the direct customer, system integrator, design owner, source manufacturer, sub-tier processors and service operator. Assign control of specification, change, acceptance, release and field remedy at each handover. Recognition shall not automatically extend to customers, subsidiaries, upstream sources, downstream distributors or a complete vehicle.

Essential gate. Evidence: Signed responsibility map and bounded scope rows.

PSR-01.04 Local operation and language

Provide competent access to the languages, locations, shifts and source records needed for assessment. Translation shall preserve technical meaning and original records shall remain available. If access, safety or lawful evidence transfer prevents a necessary audit, the affected scope shall remain unrecognised until equivalent direct evidence is obtained.

Evidence: Access plan, interpreters, originals and restrictions register.

02 Leadership, policy and governance

PSR-02.01 Executive ownership

Assign an executive accountable for quality, product safety, customer outcomes and truthful corporate claims. Approve measurable objectives, resources and escalation routes. Review serious failures directly; commercial targets shall not override release criteria, containment or required notification. Delegation shall identify decisions that remain reserved to accountable management.

Essential gate. Evidence: Board mandate, objectives and escalation decisions.

PSR-02.02 Independent challenge

Give competent quality and safety personnel authority to stop release or production when acceptance criteria are not met. Protect this authority from retaliation and sales pressure. A person responsible for creating a material nonconformity shall not alone authorize its closure or release a concession affecting safety.

Essential gate. Evidence: Stop-work records and independent release authorizations.

PSR-02.03 Management structure

Define process owners, deputy arrangements and interfaces across development, purchasing, operations, digital services and field support. Combined roles are permitted where competence, workload and independent checks remain effective. Outsourcing or centralization shall not remove responsibility for customer commitments or product integrity.

Evidence: Organization chart, role descriptions and interface reviews.

PSR-02.04 Ethical direction

Operate an accessible reporting channel for employees, contractors and affected parties. Protect good-faith reports, restrict identities and investigate objectively. Prohibit bribery, falsified test results, concealed defects and retaliation. Record remedial action and review whether incentives encourage unsafe release, understated failures or misleading sales claims.

Essential gate. Evidence: Protected reports, investigation controls and incentive review.

03 IAF quality adoption and claim substantiation

PSR-03.01 Adopted quality basis

Adopt this programme quality baseline and identify every additional IAF requirement text claimed as implemented. Record exact title, edition, approval status, scope and responsible owner. A draft, membership record or implementation plan shall not be represented as an approved standard certificate or completed conformity assessment.

Essential gate. Evidence: Authorized adoption schedule and controlled requirement texts.

PSR-03.02 Requirement-level implementation map

Map every applicable PSR requirement and each additional claimed IAF requirement to its process, owner, original evidence and evaluation result. Assess exclusions at the lowest practical requirement. Missing evidence, outsourcing, cost or a low historical failure rate shall not justify non-applicability. Resolve disputed applicability before a recognition decision.

Essential gate. Evidence: Clause-level matrix with approved exclusions and evidence IDs.

PSR-03.03 Demonstrated supplier operating history

For initial recognition, demonstrate at least six months of implemented operation, one completed internal audit and one management review. Each included responsibility-family/site shall have at least three distinct completed production, release or delivery cases with acceptance and traceability evidence. Repeated copies of one record do not create independent cases. Low-volume and newly established suppliers shall wait for sufficient actual evidence.

Essential gate. Evidence: Dated operation and case population; three complete cases per family/site.

PSR-03.04 Truthful conformity statements

Distinguish the PSR corporate recognition conclusion from any separate IAF product rating, identity record, test report or standard certification. Additional conformity claims shall identify their separately verified basis. Future adoption, partial implementation and unresolved evidence shall be disclosed as such; recognition shall not convert them into full conformity.

Essential gate. Evidence: Public claims register and claim-to-decision mapping.

04 Obligations and responsible commercial conduct

PSR-04.01 Obligation register

Identify applicable product, workplace, environmental, trade, privacy and consumer obligations for each operating location and destination market. Assign owners, current evidence and change monitoring. Where requirements conflict, obtain competent resolution and stop the affected release until a lawful, technically acceptable route is established.

Essential gate. Evidence: Market obligation register, permissions and compliance reviews.

PSR-04.02 Truthful capability and commercial representations

Substantiate specifications, origin, authorized-source status, capacity, lead time, software entitlements, warranty and environmental statements. Distinguish owned capability from contracted capability and disclose technically material limits before commitment. A nomination, quotation, customer audit, prototype success or corporate recognition shall not be presented as product acceptance or unrestricted vehicle compatibility.

Essential gate. Evidence: Claim register, quotation review, capability evidence and approvals.

PSR-04.03 Integrity of transactions

Control contracting authority, conflicts, gifts, agents and payment changes. Verify parties and delivery instructions proportionately to fraud risk. Protect customer property and confidential information. Record complaints about invoicing, substitution, counterfeit supply or diverted payments and investigate links to wider operational weakness.

Evidence: Contract approvals, agent checks and fraud response records.

PSR-04.04 Remedy and transparency

Provide clear terms for delivery, rejection, repair, replacement, refunds where due and dispute escalation. Communicate material inability to fulfil obligations promptly and accurately. Preserve contractual and customer rights; recognition shall not be used to dismiss a legitimate complaint or imply that IAF assumes the organization liabilities.

Evidence: Customer terms, remedy decisions and communication records.

05 Risk management and product safety

PSR-05.01 Lifecycle risk ownership

Maintain a live risk register spanning design, procurement, production, transport, use, service and end-of-life responsibilities. Evaluate foreseeable misuse, vulnerable users, combinations of failures and supplier dependency. Define owners, prevention, detection and response, then update assessments after changes, incidents and new field evidence.

Essential gate. Evidence: Lifecycle risk assessments linked to controls and changes.

PSR-05.02 Safety allocation and critical characteristics

Identify how supplied output can affect vehicle, worker or user safety, including component combinations and foreseeable misuse. Translate allocated safety duties into controlled critical characteristics and verifiable interface assumptions. Trace these through requirements, engineering, sub-tier controls, release and field monitoring. Obtain competent resolution of missing safety information before affected supply; a customer commercial waiver shall not establish safety.

Essential gate. Evidence: Safety responsibility matrix, assumptions and characteristic-to-control trace.

PSR-05.03 Safe release and escalation

Prevent release where safety, legal conformity or essential integrity is unproven. Quarantine affected products and configurations, preserve evidence and evaluate previously delivered populations. Make decisions on containment and notification without waiting for a complete root-cause analysis. Provide clear stop, escalation and authorized restart criteria.

Essential gate. Evidence: Release holds, containment populations and restart approvals.

PSR-05.04 Risk verification

Test whether controls actually prevent or detect the defined failure under credible operating conditions. Include abnormal operation, degraded resources and human error. A numerical risk score shall not conceal an unacceptable consequence or replace technical judgment; failed assumptions shall trigger new evidence and re-evaluation.

Essential gate. Evidence: Challenge tests, adverse results and risk review decisions.

06 People, competence and working conditions

PSR-06.01 Task competence

Define competence for design approval, critical production, inspection, software release and field remedy roles. Demonstrate ability through observed work and assessment, then authorize bounded tasks. Training attendance alone is insufficient. Reassess after long absence, major technology change, repeated error or withdrawal of an underlying qualification.

Essential gate. Evidence: Role competence criteria, observations and authorization matrix.

PSR-06.02 Human performance

Control fatigue, workload, communication, ergonomic barriers and error-prone interfaces where they affect quality or safety. Provide understandable work instructions and safe escalation. Temporary and contracted workers shall receive equivalent task preparation and supervision; production pressure shall not bypass competent staffing or required independent verification.

Evidence: Shift plans, task design reviews and supervision evidence.

PSR-06.03 Respect and protection

Prohibit forced labour, abusive recruitment, unlawful child labour, discrimination and retaliation in controlled operations. Identify high-risk labour arrangements and pursue remedy for credible harm. Provide safe reporting and worker interviews without management coaching or intimidation. Age and identity checks shall respect privacy and lawful retention.

Essential gate. Evidence: Workforce due diligence, grievance access and remedy records.

PSR-06.04 Knowledge continuity

Preserve critical process knowledge, lessons learned and deputy capability. Protect technical information while enabling authorized access at the point of use. Record competence risks from turnover, site moves and automation. Validate that new staff and digital assistance can execute the actual controlled process reliably.

Evidence: Knowledge records, deputy coverage and change readiness reviews.

07 Design, development and engineering change

PSR-07.01 Customer requirements and interface baseline

Review the complete requirement package, including drawings, data models, interfaces, software behaviour, environmental conditions, lifetime, appearance, cleanliness, packaging and service obligations where applicable. Reconcile conflicting revisions and identify who may interpret or change requirements. Manufacturing-only suppliers shall assess feasibility and escalate unsafe or ambiguous design inputs without claiming design authority.

Essential gate. Evidence: Versioned customer requirement register and resolved feasibility questions.

PSR-07.02 Product and system validation

Plan verification and intended-application validation for the released hardware, software, materials and system interfaces. Use representative production routes, tolerances, operating environments and adverse cases. Record test failures, repeat tests, deviations and any unresolved integration assumptions. A passing component test shall not establish complete-system safety or suitability for an untested customer application.

Essential gate. Evidence: Requirement-to-test matrix, original results and bounded validation decision.

PSR-07.03 Supplier engineering and configuration change

Assess changes to source, material, formulation, design, software, process, equipment, tool, location or acceptance method before implementation. Identify affected customers, contractual notification rules, necessary approval, revalidation and implementation boundary. Emergency substitution shall remain traceable and shall not bypass essential safety or required customer authorization. Verify old and new configuration segregation and field compatibility.

Essential gate. Evidence: Change dossier, customer disposition, qualification and cut-in genealogy.

PSR-07.04 Development learning

Capture field failures, manufacturing variation, service difficulties and customer feedback in future designs. Review maintainability, disassembly, secure updating and accessibility where relevant. Control experimental work and prototypes separately from released products, with explicit restrictions on sale, use and recognition claims.

Evidence: Lessons learned, design updates and prototype controls.

08 Supply network and purchased assurance

PSR-08.01 Risk-based sub-tier qualification

Identify the actual manufacturing and processing chain for critical purchased output, including customer-nominated sources. Evaluate competence, controls, capacity, authenticity, change discipline and source continuity. Nomination does not remove supplier responsibility to escalate unresolved risk. Tier number, a certificate or a purchasing score alone shall not establish product-specific assurance.

Essential gate. Evidence: Sub-tier risk map, actual-site evaluations and approval boundaries.

PSR-08.02 Sub-tier flow-down and verification rights

Flow relevant technical, safety, authenticity, traceability, change, retention and support duties to sub-tiers. Define approval and concession authority, escalation contacts and access to original evidence. Verify that critical requirements reach the operation that controls the characteristic. Where disclosure is restricted, establish a lawful controlled review route; essential evidence shall remain independently verifiable.

Essential gate. Evidence: Contracted requirements, cascading maps and verified access arrangements.

PSR-08.03 Incoming and purchased-output assurance

Select acceptance checks from product and source risk, observed performance and validated evidence. Confirm identity, configuration, authenticity and applicable characteristics before use. Retain the basis for reduced inspection and restore checks when evidence changes. A favourable delivery record shall not justify accepting counterfeit, substituted, expired or unverified critical output.

Essential gate. Evidence: Receipt evidence, source trends and inspection-change decisions.

PSR-08.04 External laboratory and digital evidence

Establish that external test, inspection, simulation and data providers are competent for the actual method, range, configuration and decision. Link reports to identifiable samples and obtain the technical basis, raw evidence and limitations needed for review. Check authenticity and changes to reports. Outsourcing evidence generation shall not transfer the supplier responsibility for release.

Essential gate. Evidence: Provider assessment, sample chain, report authentication and technical review.

09 Industrialisation and production readiness

PSR-09.01 Product-to-process readiness

Translate released design and customer requirements into the actual process sequence, risks, operating windows, control points, reaction rules and release checks. Link every critical characteristic to its control and owner. Demonstrate readiness of the actual tools, cavities, fixtures, software, materials, people and sub-tiers. Unresolved production assumptions shall remain visible in the readiness decision.

Essential gate. Evidence: Linked process flow, risk/control records and actual-route trial results.

PSR-09.02 Capacity and sustainable delivery commitment

Demonstrate usable capacity at the constraint operation using representative demand mix, changeovers, maintenance, staffing, inspection, rework and supplier availability. Distinguish theoretical speed from accepted output at sustained quality. Evaluate peak, service-part and recovery demand before committing. Additional stock or overtime shall not conceal an unqualified process or an unsustainable staffing plan.

Essential gate. Evidence: Constraint-run evidence, capacity calculation and customer commitment review.

PSR-09.03 Controlled launch and escalation

Define enhanced checks, containment boundaries, evidence review frequency and objective exit criteria for new or changed supply. Include digital deployments and transferred processes where relevant. Review defect escapes and customer observations independently. A planned end date, production target or favourable aggregate score alone shall not authorize exit from enhanced controls.

Essential gate. Evidence: Launch control plan, actual results, defect review and exit authorization.

PSR-09.04 Prototype and low-volume integrity

Identify prototype, pilot, special-build and service-part output and control its permitted use. Explain differences from the intended serial route and prevent unauthorized substitution into serial supply. Low volume may justify alternative evidence methods but shall not remove traceability, acceptance, competence or critical validation. Preserve the specific customer disposition for any bounded development shipment.

Essential gate. Evidence: Build status, route differences, use restrictions and acceptance evidence.

10 Manufacturing and assembly control

PSR-10.01 Controlled execution

Provide current instructions, process parameters, verified materials and competent staff at every relevant workstation. Control line clearance, tool settings, software versions and error-proofing. Prevent unauthorized bypass of inspection or interlocks; monitor bypass events and require safe documented restoration before normal operation resumes.

Essential gate. Evidence: Work instructions, parameter records and bypass log.

PSR-10.02 Special-process and hidden-feature control

Validate processes whose essential characteristics cannot be fully established by later inspection. Control parameter windows, loads, recipes, equipment state, operator competence and periodic challenge evidence. Link records to affected lots and define retrospective containment after a lost parameter or failed check. Destructive sampling, virtual evidence and final testing shall be justified for the actual hidden-feature risk.

Essential gate. Evidence: Qualified windows, challenge results, lot parameters and impact assessment.

PSR-10.03 Tools, equipment and customer property

Identify ownership, permitted use, condition and maintenance of tools, gauges, fixtures, test assets and software licences. Control cavity identity, spare parts, storage and tool-life limits. Verify capability after repair, transfer or long inactivity. Prevent unauthorized use, extra production or disposal of customer-owned assets and preserve agreed recovery or return arrangements.

Essential gate. Evidence: Asset register, condition checks, recovery rights and change qualification.

PSR-10.04 Nonconforming output

Identify, segregate and control nonconforming, suspect, repaired and reworked output. Obtain authorized technical disposition and required customer consent. Verify rework against defined criteria and preserve original failure records. Scrap and rejected identifiers shall be controlled to prevent unauthorized re-entry into the supply chain.

Essential gate. Evidence: Disposition log, rework verification and scrap reconciliation.

11 Measurement, testing and release evidence

PSR-11.01 Measurement suitability

Demonstrate that methods, instruments, software and people can resolve the acceptance decision required. Evaluate calibration, uncertainty or measurement variation as relevant, environmental effects and data processing. A calibration label alone shall not demonstrate suitability for the actual range, tolerance, fixture or production decision.

Essential gate. Evidence: Method validation, calibration and measurement capability studies.

PSR-11.02 Test integrity

Identify the tested item and configuration, conditions, method, equipment, operator, date and original observations. Preserve failed, aborted and repeated runs with reasons. Protect raw data from silent alteration; corrections shall remain traceable. Results shall not be selectively omitted to create a false appearance of conformity.

Essential gate. Evidence: Original test files, audit trails and repeat-run justifications.

PSR-11.03 Acceptance rules and bounded concessions

Define acceptance criteria and decision rules before testing or release, including measurement uncertainty where material. Concessions shall identify exact product, quantity, time, characteristic, risk, customer authority and expiry. They shall not waive law, essential safety or integrity. Repeat deviations require cause correction, not indefinite renewal. A concession is not general approval of a product family.

Essential gate. Evidence: Acceptance basis, technical decision and controlled concession register.

PSR-11.04 Release authority and shipment integrity

Authorize release only after required internal checks and applicable customer dispositions are complete. Verify exact configuration, quantity, destination and supporting records. Separate technical release from commercial pressure and physical shipment. Mark incomplete development output with explicit permitted use; corporate recognition shall never be used to override a missing product or customer approval.

Essential gate. Evidence: Release record, customer disposition, shipment lock and approver authority.

12 Identity, configuration and traceability

PSR-12.01 Part, system and digital configuration identity

Maintain controlled identity for products, materials, batches, systems, firmware, software and applicable service configurations. Record revision, variant, source and status; prevent reuse of an identifier for incompatible output. Preserve correspondence between customer identifiers and supplier identifiers. A label or digital token shall resolve to trustworthy underlying records rather than act as proof by itself.

Essential gate. Evidence: Identifier rules, revision histories, cross-reference and delivery manifest.

PSR-12.02 Genealogy across supply tiers

Link released output backward to critical materials, sub-tier lots, processing, tests, tools and software, then forward to recipients and applicable integration records. Address splitting, merging, rework, substitutions and returns without erasing lineage. Reconcile quantities and time boundaries sufficiently to identify a defensible affected population after an upstream defect or compromised software component.

Essential gate. Evidence: Bidirectional genealogy, quantity balance and exception resolution.

PSR-12.03 Traceability challenge

At least annually, conduct a timed backward-and-forward traceability exercise using actual output selected independently of the process owner. Establish a justified retrieval target beforehand and reconcile affected quantities and destinations. Treat unexplained gaps as nonconformities, contain the potential population and verify correction.

Essential gate. Evidence: Exercise scope, elapsed times, reconciliation and closure evidence.

PSR-12.04 Records and authenticity

Retain quality and release evidence for at least ten years after last supply or end of promised support, whichever is later, subject to longer duties and holds. Apply proportionate retention to personal data. Ensure records remain interpretable and authentic after system migration; a hash alone does not prove truthful collection.

Evidence: Retention schedule, migration checks, access controls and holds.

13 Preservation, logistics and delivery

PSR-13.01 Preservation controls

Protect product identity, cleanliness, moisture condition, shelf life and physical integrity during storage and transport. Define handling of hazardous energy and sensitive components. Verify packaging and route assumptions against realistic risks; damaged or uncontrolled consignments shall receive technical disposition before delivery or use.

Evidence: Packaging validation, condition records and damage disposition.

PSR-13.02 Inventory integrity

Control incoming, released, quarantined, obsolete and returned stock using distinguishable states. Reconcile inventory movements and prevent unauthorized substitution. Verify storage-life extensions by competent evidence, not relabelling alone. Confirm that electronic inventory status matches physical location and identification.

Essential gate. Evidence: Stock-state controls, reconciliation and shelf-life decisions.

PSR-13.03 Delivery, configuration and receipt

Verify the released identity, revision, quantity, packaging, destination and required evidence before dispatch or digital delivery. Protect transit and installation conditions, then resolve receipt discrepancies. Keep on-time, complete, correct-configuration and accepted-delivery results distinguishable. Customer receipt or payment alone shall not be treated as technical acceptance of unverified output.

Essential gate. Evidence: Release-to-delivery trace, receipt discrepancies and configuration checks.

PSR-13.04 External logistics

Define and monitor responsibilities for carriers, warehouses, distributors and export handling. Preserve critical environmental and custody data across transfers. Changes in route or provider shall be reviewed when they affect product integrity, traceability, legal obligations or customer commitments.

Evidence: Logistics agreements, route reviews and transfer records.

14 Software, cybersecurity and information integrity

PSR-14.01 Secure supplier software lifecycle

Control requirements, source, dependencies, toolchain, build, test, release and deployment. Maintain a delivered software component inventory with versions, licences, integrity identifiers and support ownership. Assess vulnerability relevance to the actual configuration, protect signing secrets and verify provenance. Generated code and outsourced development require competent review and do not transfer safety or security responsibility.

Essential gate. Evidence: Versioned component inventory, build provenance and release assurance.

PSR-14.02 Updates, compatibility and recovery

Validate each update against supported hardware, software, calibration and interface combinations. Authorize distribution, protect integrity and confirm completion; a downloaded package is not an installed remedy. Provide safe failure handling and a validated recovery route, recognizing that rollback may itself be unsafe. Preserve version, recipient, deployment and adverse-result history through service and ownership changes.

Essential gate. Evidence: Update compatibility matrix, deployment evidence and recovery tests.

PSR-14.03 Data protection and access

Limit collection and access to necessary information with a defined lawful purpose. Protect personal, customer and proprietary data through role controls, secure transfer, retention and deletion. Assess digital suppliers and report material compromises through required channels. Audit evidence shall not require unnecessary public disclosure of sensitive data.

Essential gate. Evidence: Data map, permissions, transfer controls and incident records.

PSR-14.04 Automated decisions

Validate automated inspection, scheduling and release logic against defined performance and failure conditions. Monitor drift, overrides and false acceptance. Assign accountable human decision owners and maintain a safe fallback. An algorithm or generative assistant shall not alone decide corporate recognition or conceal the original basis for a quality decision.

Essential gate. Evidence: Automation validation, drift monitoring and human review records.

15 Aftersales, warranty and lifecycle support

PSR-15.01 Product and system support commitments

Define warranted performance, service life, response duties, repair data, spares, security support and end-of-support dates appropriate to each contract and application. Confirm resources and access rights for promised support. Control differences among customer programmes using the same product. A subscription, business transfer or sub-tier exit shall not silently remove an accepted support obligation.

Essential gate. Evidence: Contractual support matrix, resource plan and service-performance evidence.

PSR-15.02 Service competence and control

Provide current service instructions, competent personnel, suitable tools and controlled replacement parts across authorized service networks. Validate repairs and safety-related calibrations. Capture actual performed work, installed configurations and unresolved conditions; outsourced service remains subject to effective manufacturer oversight.

Evidence: Service authorization, repair records and network review.

PSR-15.03 Field information and accessibility

Collect complaints, warranty claims, incidents and repair difficulties using consistent definitions and exposure denominators. Provide usable reporting and accessible safety communication for affected users. Investigate low-frequency severe events promptly; a low overall complaint rate shall not dismiss a credible critical failure.

Essential gate. Evidence: Field data, trend reviews and user communication tests.

PSR-15.04 End-of-support and transfer

Plan safe withdrawal of products, services and digital functions. Preserve necessary safety records, vulnerability routes and remedy capability after commercial discontinuation. Assess data, keys, software, parts and liability when support transfers to another provider; notify affected users of material limitations and actions.

Evidence: Withdrawal plan, transfer agreement and residual-risk review.

16 Complaints, field action and emergency response

PSR-16.01 Complaint handling

Provide accessible complaint channels, acknowledge receipt and assign impartial handling appropriate to the concern. Preserve evidence, involve technical owners and communicate decisions with reasons. Distinguish ordinary service disputes from product safety, deception or systemic quality failures; escalation shall not depend on customer purchasing power.

Evidence: Complaint register, investigation and response trail.

PSR-16.02 Coordinated field action and remedy

Maintain contacts and authority to notify customers, trace affected output, stop further supply and coordinate field remedies. Demonstrate the ability to establish a defensible population across sub-tiers and customer integrations without waiting for complete root cause. Distinguish notified, reached, repaired, updated and verified-effective cases. Preserve necessary customer and authority reporting duties.

Essential gate. Evidence: Field-action exercise, recipient trace, remedy completion and residual exposure.

PSR-16.03 Urgent incident reporting

Notify IAF within 48 hours of awareness of a credible serious safety incident, systemic falsification, material recognition-scope failure or major compromise of relevant evidence. Take immediate protective action and comply with any earlier binding notification. Initial notice may be incomplete but shall identify known facts, uncertainties, containment and responsible contacts.

Essential gate. Evidence: Incident notice, awareness time and containment record.

PSR-16.04 Learning and restoration

Verify root cause, affected configurations, remedy feasibility and post-remedy performance before lifting internal holds. Review whether other products, sites or customers share the failure mechanism. Preserve adverse history and communicate corrections to recipients of misleading information; closure shall not erase the original event.

Essential gate. Evidence: Cross-scope impact review and independent effectiveness verification.

17 Environmental responsibility and circularity

PSR-17.01 Material and substance responsibility

Identify supplied material composition, restricted substances, resource impacts and handling hazards relevant to destination and use. Trace declarations to actual materials and sources, with uncertainty and revision controls. Validate recovered or alternative inputs for the required performance. Environmental claims shall not conceal a loss of safety, durability, repairability or responsible sourcing.

Essential gate. Evidence: Material declarations, source evidence, hazard controls and change validation.

PSR-17.02 Credible performance claims

Substantiate environmental statements with defined boundaries, periods, units, methods, data quality and uncertainty. Separate measured results from estimates and future targets. Explain allocation, recycled-content and mass-balance assumptions where used; avoid double counting or presenting purchased claims as physical changes without qualification.

Essential gate. Evidence: Claim dossiers, source data and reconciliation records.

PSR-17.03 Repair, recovery and reuse

Consider durability, repairability, safe disassembly, reuse and recovery within product responsibilities. Validate the condition and limits of recovered parts or materials before use. Preserve identity and performance evidence so circular activity does not conceal prior damage, degraded safety or unsuitable second-life operation.

Evidence: Recovery criteria, condition assessments and reuse validation.

PSR-17.04 Improvement and external harm

Set measurable priorities for material environmental impacts and review progress with accountable owners. Assess adverse effects on neighbouring communities and shared resources. Investigate credible grievances and implement remedy. Achievements in one area shall not offset uncontrolled harm or misleading claims in another.

Evidence: Improvement objectives, monitoring and grievance actions.

18 Resilience and continuing ability to deliver

PSR-18.01 Supply continuity and concentration risk

Identify constraint sub-tiers, scarce components, shared infrastructure, logistics routes, tooling, skilled people, software dependencies and single-source knowledge. Assess common-cause failure and geographic concentration across apparently separate suppliers. Agree recovery priorities and decision owners. Alternative supply shall meet applicable approval and change requirements before serial use.

Essential gate. Evidence: Dependency map, recovery priorities and qualified alternative-source plan.

PSR-18.02 Tested recovery

Exercise critical recovery scenarios at least annually and after material change. Verify safe restart, data restoration, product disposition and customer communication. Alternative materials, sites and suppliers shall satisfy normal technical approval; emergency sourcing shall not create an undocumented exception to safety or traceability.

Essential gate. Evidence: Recovery exercise, restore tests and restart approvals.

PSR-18.03 Resource and financial continuity

Demonstrate sufficient arrangements to sustain quality controls, agreed support and material remedies. Review foreseeable inability to fund commitments, critical insurance or contractual protection where relevant. Disclose material continuity threats to IAF. Recognition shall not be advertised as a credit rating, investment assurance or guarantee of solvency.

Evidence: Resource review, support funding and continuity disclosures.

PSR-18.04 Orderly cessation

Plan controlled reduction, insolvency-related disruption, site closure and transfer of operations. Protect customer property, safety records, pending complaints and field remedies. Notify IAF before planned cessation of recognised activity and promptly after unplanned loss of capability; stop unsupported recognition claims.

Essential gate. Evidence: Cessation plan, records custody and customer protection steps.

19 Contract manufacture, intellectual property and interfaces

PSR-19.01 Design ownership and build-to-print accountability

Before accepting work, assign design authority, manufacturability review, process validation, test approval, release, change and field-action duties. A build-to-print supplier shall execute the approved specification and report known defects or unsafe ambiguity; a system integrator shall control allocated interfaces. No contractual label shall be used to avoid a responsibility the supplier actually performs.

Essential gate. Evidence: Customer responsibility agreement and design/process authority matrix.

PSR-19.02 Intellectual property and evidence access

Protect customer designs, source code, test data, tooling and controlled know-how. Verify rights to use, modify, supply and support third-party content. Establish restricted evidence-review arrangements that preserve technical substance and original provenance. A non-disclosure agreement shall not become an unexplained refusal of essential assurance or conceal unauthorized copying and counterfeit content.

Essential gate. Evidence: Rights register, protected review plan and customer-property controls.

PSR-19.03 Outsourced critical operation

Retain effective technical access and control over outsourced operations essential to the scope. Require relevant original records and permit necessary IAF witnessing through contracts. If the needed evidence or access is unavailable, exclude the affected activity or defer recognition; contractual assurances alone are insufficient.

Essential gate. Evidence: Access clauses, witnessed operations and outsourced evidence.

PSR-19.04 Interface change control

Coordinate technical and commercial changes between brand owner, contract factory and service operator. Establish who informs customers and regulators, updates identity records and maintains post-sale support. Changes in responsibility shall be approved and traceable before affected products are presented under a recognised scope.

Evidence: Joint change approvals and updated interface matrix.

20 Customer confidence and service fulfilment

PSR-20.01 Quotation, nomination and contract feasibility

Review customer requirements, technical assumptions, capacity, lead time, support, changes, liability allocation and acceptance routes before commercial commitment. Record unresolved matters and obtain competent approvals. Distinguish quotation, nomination, development authorization and serial-supply release. Contract pressure shall not authorize shipment, unsupported capability claims or deletion of adverse evidence.

Essential gate. Evidence: Contract review, assumptions log and role-based acceptance gates.

PSR-20.02 Service outcome control

For engineering, installation, digital or other related services included in scope, define deliverables, acceptance criteria, competence and evidence of completion. Monitor outsourced service interfaces and unintended effects on product configuration. A manufacturer recognition claim shall identify which services were actually assessed.

Evidence: Service plans, acceptance records and bounded scope statements.

PSR-20.03 Honest performance communication

Provide customers with accurate quality, delivery and support information. Distinguish committed dates from forecasts, complete delivery from partial fulfilment and original yield from reworked output. Correct material errors in previously supplied reports and prevent selective reporting that hides recurrent failures.

Evidence: Customer dashboards, correction notices and data reconciliation.

PSR-20.04 Fair access and remedy

Offer practical routes for customers and affected users to obtain essential safety information, raise concerns and pursue agreed remedies. Consider accessibility, language and geographic constraints. Protect complainants from adverse treatment and monitor whether remedy delays or exclusions undermine the commitments used to establish trust.

Evidence: Contact routes, remedy ageing and accessibility review.

21 Performance, indicators and evidence quality

PSR-21.01 Supplier quality and trust indicators

Monitor first-pass quality, defect escapes, customer returns, delivery completeness, configuration accuracy, response time, recurring findings, source risk and support effectiveness. Define denominator, time basis, severity and responsibility. Separate an organization-wide trend from programme or site results. No attractive score shall compensate for unverified release, falsified evidence or an unresolved essential safety condition.

Evidence: Indicator dictionary, source data, adverse trends and management actions.

PSR-21.02 Data reconciliation

Reconcile reported performance to original production, shipment, service and finance records as appropriate. Control duplicates, exclusions, changed definitions and restatements. Report missing data and uncertainty. Preserve both initial failure and final disposition so repair or reclassification cannot artificially improve first-pass or escape measures.

Essential gate. Evidence: Data lineage, reconciliation and restatement log.

PSR-21.03 Comparability and interpretation

Compare like products, configurations, exposure and periods. Distinguish a rate change caused by denominator, product mix or detection from an actual improvement. Explain statistical limitations of small samples and avoid universal capability claims derived from a short, selected or unrepresentative production run.

Evidence: Trend analysis with exposure, mix and limitation notes.

PSR-21.04 Action on deterioration

Define escalation thresholds for adverse indicators and serious single events. Investigate causes, allocate resources and verify actions at relevant sites and products. Leadership shall review overdue actions and recurring misses; targets shall not be retrospectively changed merely to conceal poor performance.

Evidence: Escalation records, management decisions and action verification.

22 Internal audit and management review

PSR-22.01 Risk-based internal audit

Complete an internal audit before initial recognition and at least annually thereafter. Cover all applicable requirements, sites, shifts and controlled activities over a planned cycle, with annual attention to critical risks and prior failures. Auditors shall be competent and independent of the work audited to a degree appropriate to the risk.

Essential gate. Evidence: Audit programme, competence and coverage matrix.

PSR-22.02 Effective audit evidence

Use observation, original records, independent interviews and forward-and-backward traces. Include adverse cases and unannounced process observations where justified and lawful. Record contradictions and sampling limits. A checklist tick without identifiable evidence shall not establish implementation or support closure of a finding.

Evidence: Audit trails, samples, observations and reasoned conclusions.

PSR-22.03 Management review

At least annually, review quality objectives, safety, customer outcomes, supplier performance, resources, changes, audit results and unresolved risks. Decide actions with owners and deadlines. Include whether recognition claims remain accurate and whether continued operation can meet support and remedy commitments.

Essential gate. Evidence: Review inputs, decisions and follow-up evidence.

PSR-22.04 Learning across sites

Share relevant lessons and verify implementation where the same risk exists. Central corrective action shall be tested at affected sites rather than assumed effective throughout the group. Retain local exceptions, cultural or language barriers and process differences in the improvement decision.

Evidence: Cross-site deployment and local effectiveness checks.

23 Corrective action and verified effectiveness

PSR-23.01 Containment and impact

On discovery of nonconformity, contain affected work, identify potentially delivered output and assess wider scope. Preserve original evidence and assign accountable action owners. The first response shall protect users and truthful information; immediate correction alone shall not be recorded as proof that the cause has been removed.

Essential gate. Evidence: Containment record and affected-population assessment.

PSR-23.02 Cause and systematic action

Determine technical, human, management and detection causes using verifiable evidence. Select actions that address recurrence and escape, including similar operations. Avoid unsupported attribution to operator error. Record why alternatives were rejected and how changes will be implemented without creating new safety, quality or support risks.

Evidence: Cause analysis, systemic actions and change risk review.

PSR-23.03 Effectiveness verification

Set measurable closure criteria and a representative observation period before claiming success. Use an independent competent verifier for material findings. Re-perform failed controls, review new production and field data, and check other affected sites. Training records or revised procedures alone shall not establish effective closure.

Essential gate. Evidence: Closure criteria, new evidence and verifier authorization.

PSR-23.04 IAF finding deadlines

For initial recognition, all applicable findings shall be closed and verified before grant. During active recognition, an isolated Minor may remain open for at most 90 calendar days only with protected safety, validity and integrity. A Major requires immediate containment and a 30-calendar-day closure target; unresolved affected scope enters suspension review. Critical findings trigger immediate protective suspension review.

Essential gate. Evidence: Finding log, verified closure and scope/status decisions.

24 Recognition obligations and continuing truth

PSR-24.01 Bounded public status

Use Corporate Recognised wording only for the active legal entity, named sites and approved activities in the current recognition schedule. Display the recognition ID and verification route with material claims. Membership, application, readiness assessment, product tests and supplier status shall not be represented as corporate recognition.

Essential gate. Evidence: Approved wording, current schedule and public-use samples.

PSR-24.02 Material changes

Notify IAF before implementing planned changes that alter scope, control, site, ownership, technology or capability; unplanned material changes shall be notified within five calendar days of awareness. Apply the 48-hour rule for serious incidents. Expanded activities remain outside recognition until independently reviewed and approved.

Essential gate. Evidence: Change register, notices and revised scope decisions.

PSR-24.03 Audit and monitoring cooperation

Provide safe physical access, original evidence and independent interviews for scheduled and justified special audits. Maintain annual monitoring and supply requested performance information. Refusal, falsification or inability to verify an essential claim shall trigger restriction, deferral or protective status action appropriate to the affected scope.

Essential gate. Evidence: Access records, annual reports and monitoring responses.

PSR-24.04 Expiry, suspension and withdrawal

Stop new recognition claims for expired, suspended or withdrawn scope and correct misleading public material. Preserve truthful historical records and support outstanding remedies. Renewal is not automatic; a pending application or appeal shall not extend the term or restore recognition unless an authorized decision explicitly does so within programme rules.

Essential gate. Evidence: Claim withdrawal, historical records and remedy continuity.

25 Customer product and system acceptance

PSR-25.01 Approval boundary and ownership

For every included product/system family, define whether customer approval is required, what evidence is required and who may approve supply. Maintain an approval dossier tied to exact customer, product revision, manufacturing or delivery route, site and intended application. Where no customer approval is required, document the contract basis and independent internal release. IAF corporate recognition shall not supply a missing customer decision.

Essential gate. Evidence: Approval register, contract basis, exact scope and signatory authority.

PSR-25.02 Complete qualification dossier

Compile requirements, responsibility allocation, risk controls, process readiness, measurement suitability, validation results, material and software identity, capacity evidence, traceability and unresolved limitations as applicable. Retain original adverse results and the rationale for representative or worst-case selections. A summary warrant or signed cover shall not replace the underlying technical evidence.

Essential gate. Evidence: Controlled dossier manifest with original evidence and limitation links.

PSR-25.03 Disposition and change effect

Record acceptance, rejection, pending review or a permitted bounded deviation with its authority, conditions and validity. Determine what design, source, process, tool, location, software or support changes trigger resubmission. Verify written approval where required before affected shipment. Apply stricter customer notification duties when agreed; no universal notification period shall be inferred from this programme.

Essential gate. Evidence: Customer disposition history, change triggers and reapproval evidence.

PSR-25.04 Transfer and ongoing assurance

Carry approved requirements into production, purchase controls, release checks, service information and delivered configuration. Reconfirm evidence after material change or adverse performance and at justified intervals. Preserve approval status during plant transfer, supplier takeover and system integration. An approved sample shall not establish continuing conformity of uncontrolled production.

Essential gate. Evidence: Approval-to-operation map, requalification results and transfer checks.

26 Long-term supply, obsolescence and ecosystem integrity

PSR-26.01 Obsolescence intelligence

Monitor discontinuation, unsupported software, exhausted tool life, unavailable material and loss of critical expertise before they impair supply or support. Identify affected customer programmes and committed service periods. Notify through agreed routes, explain uncertainty and develop qualified alternatives. A last-time purchase shall include preservation, authenticity, quantity and lifetime risk review.

Evidence: Lifecycle watchlist, programme impact map and last-time-buy rationale.

PSR-26.02 Counterfeit and diversion prevention

Control authorized sourcing, provenance, distribution rights and suspect stock. Assess brokers, excess stock, returned products and recycled electronic components according to authenticity risk. Quarantine disputed identity and preserve chain of custody. Prevent unauthorized remarking, product diversion and re-entry of rejected output. Escalate credible counterfeit evidence through appropriate customer and protective channels.

Essential gate. Evidence: Provenance chain, suspect-product investigations and disposition records.

PSR-26.03 Data portability and sustainable exit

Plan lawful continuity of customer-critical records, configuration knowledge, service keys, repair information and agreed tooling access after insolvency, acquisition, contract exit or provider closure. Protect security and intellectual property while preserving necessary support. Test recoverability and define who may authorize transfer; a theoretical escrow or undocumented backup is not demonstrated continuity.

Essential gate. Evidence: Exit plan, access rights, recovery test and authenticated transfer controls.

PSR-26.04 Multi-customer impact and systemic learning

Evaluate whether a failure, vulnerability, material defect or common-source change affects other customers and product families. Share timely, technically useful warnings within lawful confidentiality limits and preserve responsibility for each decision. Track recipient action and unresolved exposure. Competitive sensitivity shall not justify withholding information necessary to prevent credible serious harm.

Essential gate. Evidence: Cross-programme impact assessment, protected notices and action tracking.

Supplier profiles - selection and use

Apply every profile that describes actual responsibility. A system integrator with internal component manufacture applies SYS and CMP; embedded software adds SWD where relevant. Controlled distributors performing transformation also apply the applicable production or digital profile. Selection does not waive any relevant common requirement. Supplier assessment as evidence does not itself recognise that supplier.

SYS Integrated systems and module suppliers

Suppliers accountable for the integration of multiple components, functions or supplied subsystems.

SYS-01 Allocated system responsibility

Define system boundaries, interfaces, allocated functions and acceptance responsibility with the customer and participating suppliers. Maintain a traceable architecture and record assumptions about vehicle integration. A supplier may claim only the functions and conditions it has verified; unresolved responsibility gaps shall prevent affected release.

Essential gate. Evidence: System architecture, interface agreement and acceptance ownership.

SYS-02 Combination and variant validation

Validate relevant hardware, software, calibration and environmental combinations, including worst-case tolerances and fault propagation. Explain which variants share evidence and which need additional verification. Component conformity shall not by itself establish system performance, compatibility or safe degraded behaviour.

Essential gate. Evidence: Variant matrix, integration tests and failure-propagation evidence.

SYS-03 Coordinated configuration release

Control the exact integrated bill of materials, versions, approved sources, test state and release package. Verify consistency between assembled, tested and delivered configurations. Identify any integration performed by the customer and provide clear instructions, constraints and acceptance evidence for that handover.

Essential gate. Evidence: Released system manifest and configuration-to-test trace.

SYS-04 System-level field responsibility

Maintain ability to investigate interacting failures and coordinate component suppliers, customers and service operators. Preserve synchronized evidence and assess common effects across variants. Distinguish a defective component from an integration failure without delaying necessary protection while commercial responsibility is disputed.

Essential gate. Evidence: Joint investigation records, field population and coordinated remedy.

CMP Mechanical components and subassemblies

Producers of mechanical parts, fasteners, structures, assemblies and replacement components.

CMP-01 Critical geometry and properties

Translate function and loading into controlled dimensional, material, surface, cleanliness and mechanical-property requirements. Verify measurement capability and production representativeness. Record any supplied-design uncertainty that affects interchangeability, durability or safety and obtain resolution before affected supply.

Essential gate. Evidence: Characteristic matrix, dimensional evidence and property validation.

CMP-02 Tool, cavity and process identity

Retain the link from output to tooling, cavity, machine, settings, material and process route where needed to contain variation. Validate repairs, transfers and alternative production routes. Do not pool incompatible cavities or machines to hide an unstable or unqualified source.

Essential gate. Evidence: Cavity-level process records and post-change validation.

CMP-03 Load and life evidence

Justify fatigue, wear, corrosion, joint, sealing or other lifetime verification for the actual application. State acceleration models, sample limitations and boundary conditions. Production changes that affect a failure mechanism shall trigger review of the previously accepted performance evidence.

Essential gate. Evidence: Lifetime test rationale, original failures and configuration limits.

CMP-04 Replacement compatibility

Establish fit, function and application boundaries for original and replacement parts. Control catalogue mapping, marking and installation instructions. A visually similar part or matching nominal dimension is insufficient evidence of equivalent performance; prohibit misleading interchangeability claims and unsafe substitutions.

Essential gate. Evidence: Compatibility evidence, catalogue approval and installation information.

ELE Electrical, electronic and semiconductor suppliers

Suppliers of sensors, controllers, harnesses, connectors, electronic assemblies and semiconductor devices.

ELE-01 Electronic design and source control

Identify electrical, thermal, timing, environmental and endurance requirements and component derating assumptions. Trace semiconductor and electronic component provenance, revision and approved sources. Assess process-node, fabrication, packaging and die changes where they could affect reliability or intended use.

Essential gate. Evidence: Design limits, source genealogy and change-impact evidence.

ELE-02 Assembly and latent-defect control

Control sensitive handling, moisture, contamination, joining profiles, cleaning and rework. Validate hidden joints and latent-defect risks with technically appropriate methods. Keep recipe, lot and board identity linked so that a process excursion can be traced to affected assemblies and customers.

Essential gate. Evidence: Assembly qualification, excursion records and latent-defect checks.

ELE-03 Hardware and software compatibility

Verify electrical interfaces, startup, timing, diagnostics, power loss, disturbance and recovery behaviour with the released software or calibration. Record supported variants and installation constraints. A bench pass with a different firmware or load shall not establish conformity of the delivered configuration.

Essential gate. Evidence: Hardware/software matrix, disturbance and recovery evidence.

ELE-04 Lifecycle authenticity and support

Manage ageing, counterfeit risk, discontinuation and substitute component qualification over the committed support period. Maintain accessible technical change notices and approved equivalent-source decisions. Explain the limits of screening; it shall not convert unidentified provenance into a fully traceable original-source claim.

Essential gate. Evidence: Authenticity plan, obsolescence register and substitution approvals.

MAT Materials, chemicals and consumables

Suppliers of metals, polymers, fluids, coatings, adhesives, chemicals and automotive production consumables.

MAT-01 Composition and batch definition

Define controlled composition, formulation, grade, physical properties and batch boundaries. Link declarations to actual source and production evidence and control blending, recycled input and reprocessing. Protect proprietary recipes through competent restricted review while keeping conformity verifiable.

Essential gate. Evidence: Batch composition, source records and controlled formulation.

MAT-02 Representative sampling and stability

Justify how samples represent tanks, coils, melts, containers or blended lots. Evaluate variability, homogeneity, contamination and stability under intended storage and use. Preserve sampling locations and handling conditions; a favourable isolated sample shall not conceal an uncharacterized batch.

Essential gate. Evidence: Sampling plan, variability evidence and stability results.

MAT-03 Handling and application conditions

Provide accurate safety, storage, mixing, curing, shelf-life and compatibility information relevant to the customer process. Verify material behaviour within the declared application window. Control transport excursions and expiry; relabelling or retesting alone shall not extend life without a justified technical basis.

Essential gate. Evidence: Application window, transport checks and expiry-extension review.

MAT-04 Composition changes and declarations

Assess formulation, source, substance and process changes against customer approval, destination obligations and long-term performance. Update declarations and identify the first affected batch. Environmental or recycled-content claims shall preserve traceability and disclose the calculation boundary and uncertainty.

Essential gate. Evidence: Change-to-batch map, declarations and claim substantiation.

SWD Software, data and digital product suppliers

Suppliers of embedded software, automotive platforms, models, datasets and directly related digital services.

SWD-01 Digital deliverable and rights boundary

Define the released artifact, functions, interfaces, data rights, dependencies and support obligation. Distinguish development assistance from responsibility for an operational function. Identify rights to use and redistribute code, models and data; disclose restrictions that affect customer deployment, repair or continued support.

Essential gate. Evidence: Digital product definition, rights register and responsibility map.

SWD-02 Reproducible and authentic release

Preserve source and dependency versions, toolchain, build parameters, review results and artifact integrity. Demonstrate a reproducible or otherwise defensibly verifiable release and protect signing credentials. Link generated artifacts to the approved baseline; a repository tag alone shall not prove what was delivered.

Essential gate. Evidence: Build provenance, artifact hashes and authorized release evidence.

SWD-03 Operational reliability and isolation

Validate interface contracts, performance limits, data quality, tenant separation, failure behaviour and recovery for the actual deployment. Monitor meaningful service outcomes and dependency failures. Prevent one customer configuration, update or data set from compromising another without detection and containment.

Essential gate. Evidence: Deployment validation, isolation tests and service-recovery results.

SWD-04 Vulnerability and support continuity

Maintain a vulnerability intake, relevance assessment, coordinated remedy and customer notification process. Define support windows and secure access to necessary release knowledge after staff or supplier exit. Escalate unsupported dependencies and residual exposure; a severity score alone shall not determine whether a safety-relevant action is needed.

Essential gate. Evidence: Vulnerability decisions, notifications, update evidence and exit plan.

PROC Special-process and contract production suppliers

Suppliers performing machining, joining, heat treatment, coating, finishing, assembly or other contracted transformation.

PROC-01 Customer process responsibility

Agree the supplied inputs, operation boundary, acceptance criteria, special characteristics and permitted process changes. Verify incoming state and report unsuitable or ambiguous inputs. A customer-owned design does not authorize uncontrolled processing or remove the duty to report known unsafe results.

Essential gate. Evidence: Process agreement, incoming review and resolved technical queries.

PROC-02 Qualified operating window

Establish validated process windows, equipment condition, load patterns, consumables and competent personnel. Demonstrate controls for hidden properties and process interruptions. Changes outside the window require technical review and qualification before affected release; nominal machine settings alone are insufficient evidence.

Essential gate. Evidence: Qualification trials, operating envelopes and interruption controls.

PROC-03 Lot integrity through transformation

Preserve identity across split loads, mixed customer work, rework, subcontract processing and scrap. Reconcile quantities and prevent cross-contamination or return of unprocessed items as completed. Link reported results to actual load and process records rather than generic conformance statements.

Essential gate. Evidence: Load genealogy, quantity reconciliation and original process data.

PROC-04 Independent completion and return

Verify completion against the agreed process and product requirements, including destructive or indirect evidence where justified. Identify deviations, concessions and unresolved limits in the delivery record. Customer urgency shall not override a hold on unverified work or authorize a false processing certificate.

Essential gate. Evidence: Completion checks, release authority and accurate return documentation.

TLS Tooling, equipment and production technology suppliers

Suppliers of tools, fixtures, machinery, automation, test equipment and associated production engineering.

TLS-01 Intended production capability

Define product characteristics, capacity, operating conditions, interfaces, safety functions and acceptance criteria for the delivered asset. Distinguish machine performance from capability of a complete customer process. Resolve site utilities, installation assumptions and customer-supplied elements before final commitment.

Essential gate. Evidence: Equipment requirement baseline and site-interface agreement.

TLS-02 Acceptance at real use conditions

Demonstrate relevant repeatability, output quality, cycle performance, protective functions and recovery at agreed representative conditions. Record differences between factory trials and installed operation. A demonstration using selected parts or disabled protections shall not establish unrestricted production capability.

Essential gate. Evidence: Trial plan, original results, installed checks and limitations.

TLS-03 Controlled lifecycle changes

Identify hardware, control logic, tooling revisions, safety settings and remote-access configuration. Validate modifications and repairs for their effect on output conformity and worker protection. Preserve backups and recovery instructions, and prevent service access from silently altering a qualified customer process.

Essential gate. Evidence: Asset configuration, service changes and recovery validation.

TLS-04 Support and measurement integrity

Provide competent training, maintenance, spare parts, calibration or verification instructions and end-of-life support information. Where the asset measures or accepts product, establish decision capability and ongoing check requirements. Equipment supply under PSR does not authorize independent laboratory or inspection-body claims.

Essential gate. Evidence: Support package, measurement validation and bounded claims.

ENE Energy storage, propulsion and charging-system suppliers

Suppliers of cells, battery packs, power conversion, electric propulsion and charging-related systems.

ENE-01 Energy responsibility and interfaces

Define responsibility for stored energy, electrical isolation, thermal control, mechanical containment and protective communication across supplied modules. Validate interface assumptions with the system customer. Product transport, service and damaged-state handling shall be considered alongside normal operation.

Essential gate. Evidence: Energy architecture, interface allocation and hazard controls.

ENE-02 Production genealogy and consistency

Link released output to critical cell, material, joining, power-device, firmware and calibration identities. Demonstrate production consistency for parameters affecting energy safety and lifetime. Bound the affected population after a source or process excursion, including mixed lots and repaired modules.

Essential gate. Evidence: Energy-system genealogy and critical-process records.

ENE-03 Abnormal and degraded conditions

Verify relevant fault, abuse, ageing, isolation loss, communication loss and protection behaviour under justified safe test conditions. State untested combinations and dependence on vehicle-level controls. A declared rating or single nominal-performance test shall not establish the complete safety envelope.

Essential gate. Evidence: Fault evidence, degraded-state limits and residual assumptions.

ENE-04 Service, reuse and end-of-life

Define safe diagnosis, isolation, replacement, storage, transport and recovery for the delivered configuration. Reuse and second-life claims require condition assessment and validation for the new duty. Preserve ownership of support and field actions after system disassembly or a change of business model.

Essential gate. Evidence: Service controls, second-life decision and lifecycle responsibility.

REM Remanufactured, repaired and circular-product suppliers

Suppliers restoring or requalifying automotive components and systems for defined continued or alternative use.

REM-01 Input acceptance and provenance

Define acceptable core identity, history, damage, contamination and remaining-life information. Segregate unknown or unsuitable input and preserve original identifiers. The absence of a visible defect shall not establish fitness for remanufacture or authorize removal of prior failure history.

Essential gate. Evidence: Core acceptance criteria, source history and rejection records.

REM-02 Restoration process and changed capability

Control disassembly, inspection, replacement, processing, software and reassembly against the declared target capability. Validate changes from the original specification or application. Identify what is restored, upgraded or left unverified and prevent a claim of equivalent performance without supporting evidence.

Essential gate. Evidence: Restoration specification, process route and validation limits.

REM-03 Individual release and traceability

Link each unit or justified lot to inspected condition, replaced parts, process records and final acceptance. Control reuse of life-limited elements and hidden damage. Preserve the connection to original identity and any new configuration without misrepresenting the item as newly manufactured.

Essential gate. Evidence: Restoration genealogy, acceptance results and truthful marking.

REM-04 Warranty and safe reuse information

Provide accurate application, installation, service and warranty information reflecting restored capability and residual limits. Monitor returns and repeat failures by core source and restoration route. Support field containment and safe disposal where continued use cannot be justified.

Essential gate. Evidence: Warranty scope, customer information and restored-product field data.

DST Controlled product supply and distribution

Suppliers accountable for sourced products, configuration, authenticity, technical handover and supply continuity.

DST-01 Authorized source and accountable supply

Identify actual source manufacturers, permitted distribution rights and customer technical requirements. Demonstrate authority and competence for every claimed supply activity. Corporate recognition of the distributor shall not imply recognition of the source manufacturer, product certification or permission to obscure country, source or configuration.

Essential gate. Evidence: Source authorization, manufacturer identity and scope boundaries.

DST-02 Authenticity and configuration acceptance

Verify identity, revision, condition, provenance and required original acceptance evidence before supply. Apply additional controls to brokers, aged inventory, returned products and scarce electronic parts. Quarantine uncertain authenticity; invoice continuity alone shall not establish technical conformity.

Essential gate. Evidence: Receipt and authenticity checks with original release evidence.

DST-03 Preservation and transformation limits

Control storage, shelf life, handling, packaging, firmware loading, kitting and installation instructions. Treat any actual modification or transformation through its relevant additional profile and approval route. Repackaging or remarking shall preserve traceability and shall not conceal an unapproved substitute or altered product.

Essential gate. Evidence: Storage evidence, configuration history and transformation approval.

DST-04 Customer remedy and upstream coordination

Maintain ability to reach affected customers, retrieve traceability and obtain competent source support for defects, obsolescence and field actions. Define replacement, repair and continuity responsibilities. Escalate unresolved upstream evidence and prevent sales commitments that exceed actual technical support or lawful supply rights.

Essential gate. Evidence: Customer/source contacts, remedy cases and continuity evidence.

Technology and future-capability domain map

Domain	Trigger
T01 Electric propulsion, batteries and energy storage	Cells, modules, packs, battery management, power electronics and related manufacturing or support.
T02 Charging and energy interfaces	Vehicle charging, supply interfaces, bidirectional energy functions and related connectivity.
T03 Connected and software-defined products	Connected functions, remote diagnostics, over-the-air updates and continuing digital features.
T04 Automated driving and machine intelligence	Automated functions, learning systems and safety-relevant machine intelligence used in products or operations.
T05 Digital twins, virtual evidence and automated inspection	Simulation, digital representations and data-driven inspection used to support technical decisions.
T06 Advanced materials and automated manufacturing	Novel joining, additive manufacture, robotics, flexible production and advanced material systems.
T07 Circular products, remanufacture and product information	Repairability, reused materials, second life and controlled lifecycle information.
T08 Low-carbon production and resilient resources	Credible energy, emissions, water and resource claims and the resilience of related operations.
T09 Human-centred and accessible mobility	Ergonomics, usability, occupant wellbeing and the needs of diverse users.
T10 Heavy, special-purpose and emerging mobility	Heavy vehicles, trailers, off-road and special-purpose configurations, new energy and unfamiliar use cases.

T01 Electric propulsion, batteries and energy storage

Cells, modules, packs, battery management, power electronics and related manufacturing or support.

T01-01 Energy safety

Identify electrical, thermal, mechanical and chemical hazards across manufacture, transport, charging, use, repair and damaged-product handling. Verify protective controls and competent emergency response. The selected test programme shall address the actual chemistry, packaging, configuration and use limits.

Essential gate. Evidence: Energy safety dossier and configuration-specific tests.

T01-02 Battery genealogy

Link safety-relevant material and cell batches to modules, packs, control software and delivered products. Preserve repair, replacement and state-of-health information where relied upon. Validate traceability through pack reconfiguration or second-life transfer rather than assuming the original identity remains sufficient.

Essential gate. Evidence: Cell-to-pack genealogy and modification history.

T01-03 Abnormal condition control

Define containment for damaged, suspect, overheated or deeply degraded energy systems. Verify safe storage, isolation, transport and competent disposition. Monitor failures after release and identify the potentially affected population; a passed routine functional test alone shall not justify release of a damaged system.

Essential gate. Evidence: Quarantine, abnormal-event response and disposition evidence.

T01-04 Performance and second-life claims

Substantiate capacity, range contribution, durability and second-life suitability with stated conditions, ageing assumptions and uncertainty. Distinguish measured performance from projections. Reassess safety and support obligations for changed use; remaining capacity alone shall not prove suitability for repurposing.

Evidence: Performance dossier and repurposing risk evaluation.

T02 Charging and energy interfaces

Vehicle charging, supply interfaces, bidirectional energy functions and related connectivity.

T02-01 Interface compatibility

Define supported electrical, mechanical, communication and user interfaces. Test representative combinations and known adverse interoperability cases. Record unsupported combinations and fail-safe responses; compatibility with one test partner shall not imply universal interoperability.

Essential gate. Evidence: Interface matrix and interoperability evidence.

T02-02 Safe operation

Verify protection against electrical, thermal, environmental and misuse hazards in the actual installation and operating context. Address interruptions, isolation, emergency stopping and degraded communications. Allocate responsibilities between vehicle, charger, installer and service operator.

Essential gate. Evidence: Safety tests and interface responsibility record.

T02-03 Metering and customer information

Verify measurement and billing-related data where provided, including timestamps, losses, tariffs and interrupted sessions. Present limitations and dispute routes clearly. Changes to measurement software or energy-management algorithms shall be controlled and re-evaluated where they affect customer outcomes.

Evidence: Measurement validation and transaction reconciliation.

T02-04 Bidirectional and grid interaction

For bidirectional or managed charging, validate operating limits, authentication, conflicting commands and safe loss of external control. Establish ownership of battery degradation and support claims. Treat new energy-service functionality as a controlled scope and configuration change.

Essential gate. Evidence: Energy-control validation and agreed operating limits.

T03 Connected and software-defined products

Connected functions, remote diagnostics, over-the-air updates and continuing digital features.

T03-01 Connected-service boundary

Identify connectivity dependencies, back-end providers, data flows and the functions affected by loss or compromise. Define supported regions and service lifetime. Demonstrate safe degradation and understandable user communication when external connectivity is unavailable.

Essential gate. Evidence: Connectivity architecture and degraded-mode tests.

T03-02 Update campaign control

Bound each update campaign by exact compatible configurations, approved evidence and rollout criteria. Monitor installation and functional outcomes, contain adverse results and support safe recovery. Preserve status for offline or unreachable products and do not count download completion as successful remedy.

Essential gate. Evidence: Campaign manifest, deployment results and rollback evidence.

T03-03 Identity and credential lifecycle

Control device and service identities, privileged access, signing keys and credential transfer. Revoke compromised access and prevent unauthorized reuse after ownership change, dismantling or remanufacture. Verify that secure maintenance remains possible throughout the promised support period.

Essential gate. Evidence: Credential controls, revocation and ownership-transfer tests.

T03-04 Feature and subscription integrity

Align advertised features, paid entitlements and actual availability. Explain connectivity, geographic, user and time limits. Material withdrawal or impairment shall receive technical and customer-impact review with lawful, agreed remedy; recognition shall not endorse an unvalidated future feature.

Evidence: Entitlement tests, disclosures and withdrawal review.

T04 Automated driving and machine intelligence

Automated functions, learning systems and safety-relevant machine intelligence used in products or operations.

T04-01 Intended operating envelope

Define the task, operating conditions, users, performance limits and foreseeable misuse of each automated function. Identify fallback and accountable decision owners. Validate transitions outside the supported envelope and avoid marketing that encourages operation beyond demonstrated capability.

Essential gate. Evidence: Operating-envelope definition and transition validation.

T04-02 Data and model control

Control data provenance, selection, labels, permission, bias and representativeness. Version models and training or adaptation settings; evaluate rare but consequential cases. A larger dataset or higher average accuracy shall not substitute for evidence covering relevant failure modes and affected user groups.

Essential gate. Evidence: Dataset records, model versions and disaggregated evaluation.

T04-03 Independent challenge and monitoring

Use competent challenge tests, independent review and field monitoring appropriate to consequences. Set limits for drift and unexpected behaviour, then define containment or reversion. Learning after release shall remain within authorized change controls and shall not silently alter the safety basis.

Essential gate. Evidence: Challenge results, drift limits and intervention records.

T04-04 Human responsibility

Provide understandable limitations, alerts, oversight and safe intervention where human participation is required. Validate workload and response assumptions in representative conditions. An automated score shall not alone determine safety acceptance, customer remedy or IAF corporate recognition.

Essential gate. Evidence: Human-factors evidence and accountable approval records.

T05 Digital twins, virtual evidence and automated inspection

Simulation, digital representations and data-driven inspection used to support technical decisions.

T05-01 Context of use

Define the decision that virtual evidence supports, required credibility and relevant physical conditions. Bound each model to validated assumptions and configurations. Do not use a convenient simulation as a replacement for necessary physical evidence outside its demonstrated context.

Essential gate. Evidence: Model-use statement and validation boundary.

T05-02 Correlation and uncertainty

Compare predictions with independent physical or operational observations and explain discrepancies. Evaluate sensitivity, numerical uncertainty and data limitations. Maintain traceable model, solver, parameter and dataset versions so results can be reproduced or critically reviewed.

Essential gate. Evidence: Correlation studies and reproducibility package.

T05-03 Inspection performance

Validate automated inspection for relevant defect classes, line conditions and misleading inputs. Measure false acceptance and false rejection separately, with sample limitations. Provide a controlled human review route and monitor drift after changes to lighting, material, equipment or software.

Essential gate. Evidence: Inspection validation and false-acceptance monitoring.

T05-04 Evidence authenticity

Preserve raw input, transformation history and review decisions for synthetic or digitally generated evidence. Mark synthetic content clearly and prevent it from being presented as an observed physical event. Demonstrate original data integrity independently of any hash, signature or persuasive visualization.

Essential gate. Evidence: Evidence lineage and synthetic/physical distinction.

T06 Advanced materials and automated manufacturing

Novel joining, additive manufacture, robotics, flexible production and advanced material systems.

T06-01 Process qualification window

Define and validate material, machine, software, build and post-processing conditions that govern performance. Establish when changes invalidate the process window. Results from laboratory coupons or another machine shall be transferred only with a justified and verified technical basis.

Essential gate. Evidence: Qualified process envelope and transfer validation.

T06-02 Hidden-feature assurance

Identify internal, anisotropic or otherwise difficult-to-inspect characteristics. Combine validated process controls and appropriate verification to establish their reliability. Preserve critical process data and reject unsupported extrapolation from external appearance or limited surface inspection.

Essential gate. Evidence: Hidden-feature controls and representative verification.

T06-03 Human and robot integration

Verify safe, quality-controlled interaction between workers, robots, flexible fixtures and digital work instructions. Test interruption, restart, manual override and mixed production. Assess whether changed tasks or automation obscure defects that operators previously detected.

Essential gate. Evidence: Integration tests, restart checks and competence evidence.

T06-04 Technology change management

Plan controlled introduction, competence development and fallback for emerging technology. Distinguish experimental lines from recognised production. Retain legacy support and configuration evidence when new manufacturing methods replace earlier processes or materials.

Evidence: Technology introduction gates and fallback readiness.

T07 Circular products, remanufacture and product information

Repairability, reused materials, second life and controlled lifecycle information.

T07-01 Lifecycle data identity

Define the identity, provenance, ownership and update responsibility of product lifecycle information. Separate public, customer and restricted data. Verify that an accessible digital record refers to the actual product and revision; a scannable code alone shall not establish conformity.

Essential gate. Evidence: Lifecycle data schema and identity verification.

T07-02 Recovered-content assurance

Verify source, quality and chain of custody for recovered inputs. Explain allocation and mixing assumptions and prevent double counting. Confirm technical suitability for the intended safety and performance demands; environmental benefit shall not justify an unvalidated material substitution.

Essential gate. Evidence: Recovered-input dossier and claim reconciliation.

T07-03 Repair and disassembly

Provide technically sound repair and disassembly instructions for authorized lifecycle activities. Address hazardous energy, structural integrity, data removal and reused components. Test relevant procedures and clarify which changes require new validation or alter the recognised scope.

Evidence: Validated repair/disassembly instructions and scope effects.

T07-04 Second-life responsibility

Assign responsibility for changed use, condition assessment, new limits, support and field remedies. Maintain links to original and modified identities. Distinguish remanufactured performance claims from a new-product claim and provide evidence appropriate to the changed operating conditions.

Essential gate. Evidence: Second-life dossier and responsibility transfer.

T08 Low-carbon production and resilient resources

Credible energy, emissions, water and resource claims and the resilience of related operations.

T08-01 Measurement boundaries

Define facilities, products, periods, units and material lifecycle stages included in a resource or emission claim. Identify primary data, estimates and exclusions. Preserve calculation versions and explain whether a result describes a physical reduction, a contractual instrument or a future objective.

Essential gate. Evidence: Boundary statement, data lineage and claim explanation.

T08-02 Comparable product claims

Use consistent functional performance, service life and allocation assumptions when comparing products or options. Assess material sensitivity and uncertainty. Do not advertise a minor operational saving as a verified whole-lifecycle advantage without evidence covering the claimed boundary.

Essential gate. Evidence: Comparison assumptions, sensitivity and review.

T08-03 Resource continuity

Assess energy and water constraints, extreme events and dependency on critical materials. Test continuity options without bypassing approved process or safety limits. Verify the impact of alternative energy, cooling, recycled water or substituted material on actual manufacturing quality.

Evidence: Resource scenarios and alternative-process validation.

T08-04 Transition accountability

Assign owners, milestones, funding and performance measures for transition commitments. Review whether actions shift harm to suppliers, communities or end users. Distinguish achieved outcomes from unverified expectations and correct claims when assumptions or delivery schedules materially change.

Evidence: Transition plan, progress evidence and revised disclosures.

T09 Human-centred and accessible mobility

Ergonomics, usability, occupant wellbeing and the needs of diverse users.

T09-01 User and task diversity

Define intended users, tasks, abilities, environments and foreseeable barriers. Include relevant variation in size, age, language and ability in evaluation. Explain limitations in the tested population and avoid universal accessibility or comfort claims from a narrow sample.

Evidence: User requirements and representative evaluation plan.

T09-02 Safety-related interaction

Validate controls, displays, warnings and handover interactions under distraction, fatigue and degraded conditions. Assess whether foreseeable confusion can cause harm. Marketing or user training alone shall not compensate for an unsafe interface where a feasible design control is required.

Essential gate. Evidence: Human interaction tests and safety disposition.

T09-03 Service accessibility

Provide understandable instructions, safety notices and remedy access through usable channels. Evaluate barriers created by digital-only service, subscription dependence or unavailable local support. Establish effective alternatives where necessary to fulfil actual safety and customer commitments.

Evidence: Accessibility review and alternative support routes.

T09-04 Wellbeing claims

Substantiate comfort, air quality, noise and wellbeing claims using defined conditions, methods and evidence. Distinguish engineering performance from medical assertions. Investigate adverse user feedback and avoid presenting corporate recognition as validation of unassessed health benefits.

Evidence: Claim evidence and adverse-feedback review.

T10 Heavy, special-purpose and emerging mobility

Heavy vehicles, trailers, off-road and special-purpose configurations, new energy and unfamiliar use cases.

T10-01 Duty and application boundary

Define actual loads, duty cycles, environments, operators and service demands. Assess multi-stage manufacture and body or equipment integration. An approval basis for ordinary road use shall not automatically extend to off-road, severe-duty, emergency or unusual operating conditions.

Essential gate. Evidence: Duty-cycle definition and integration evidence.

T10-02 Novel energy and hazard review

For hydrogen, alternative fuels or other unfamiliar energy systems, identify hazards, containment, detection, emergency response and competent maintenance. Validate the actual installed configuration and credible failures. Do not infer equivalent safety from a conventional energy architecture.

Essential gate. Evidence: Novel-energy risk dossier and emergency validation.

T10-03 Small-series control

Maintain configuration-specific design, build, test and release evidence for small series and unique units. Identify common validated features and independently justify differences. A low production volume shall not excuse missing safety evidence, traceability or support capability.

Essential gate. Evidence: Unique-unit records and difference assessment.

T10-04 Future-use governance

When a new application lacks sufficient evidence or an adopted technical module, restrict it to controlled development until the necessary criteria and validation exist. Use expert review and pilots to develop prospective requirements. Do not grant public recognition to a speculative capability merely to support innovation messaging.

Essential gate. Evidence: Research boundaries, pilot review and adoption decision.

IR01 Programme authority, eligibility and adoption

IR01-01 Adoption and launch

IAF shall formally adopt the edition, effective date, roles, contact channels and implementation notice before issuing recognition. Validate pilots, assessor competence, independent decisions, complaints and status verification. This prepared document set shall not itself confer recognition or prove that an operating registry or acceptance agreement exists.

Essential gate. Evidence: Adoption resolution, pilot outcomes and launch readiness record.

IR01-02 Eligible supplier scope

Accept accountable product and system suppliers in the ten defined profiles, including qualified digital and controlled-distribution activities. Apply every relevant profile and technology module. Membership, a sales introduction, unrestricted brokerage, training or independent assessment alone is not supplier recognition; actual controlled output and evidence are required.

Essential gate. Evidence: Eligibility review and accepted scope/profile selection.

IR01-03 Readiness without public status

A private readiness review may identify gaps, but shall not issue Corporate Recognised status, a public approval badge or a provisional recognition certificate. The initial six-month operation and three-case family/site floor remain mandatory. Inform applicants that eligibility and complete paperwork do not guarantee grant.

Essential gate. Evidence: Readiness boundary and applicant communication.

IR01-04 IAF quality texts and transition

Use a controlled schedule of IAF requirements with exact editions and approval status. PSR is a self-contained corporate quality baseline; it does not automatically certify every other IAF text. Additional claimed conformity needs its own complete mapping and assessment. Adopt new requirements prospectively with published transition and unresolved-scope rules.

Essential gate. Evidence: Controlled criterion schedule and transition decisions.

IR02 Scope, multiple sites and technical families

IR02-01 Recognition unit

Each decision shall identify accountable legal entities, sites, activity profiles, product/service families, technology modules and exclusions. A group schedule shall name every included entity and its undertaking; entities outside the decision shall not inherit status. Retain stable entity, site and scope-row identifiers through revisions.

Essential gate. Evidence: Approved recognition schedule with stable identifiers.

IR02-02 Operational-site coverage

Before initial recognition and renewal, physically audit every included operational site. Audit each such site physically at least annually during the term. Operational sites include manufacturing, processing, warehouse/configuration and accountable software engineering/release centres. Assess central/support controls annually; retain necessary direct evidence of critical outsourced operations. Remote workers are assigned to a controlled operational centre, not automatically separate sites.

Essential gate. Evidence: Site coverage plan and completed physical-audit records.

IR02-03 Family grouping

Group products only where design responsibility, process route, critical characteristics, technology and risk are sufficiently comparable. Record worst-case choices and differences. A family boundary shall not be broadened merely to reduce audits or case counts. Every included family/site shall satisfy the operating-history and completed-case gate.

Essential gate. Evidence: Technical family rationale and representative-case matrix.

IR02-04 Change and partial restriction

Assess material changes before extending scope. A coherent unaffected scope may remain active only when shared causes and interfaces are controlled and the independent decision states the exact boundary. Update public scope promptly; a broad badge shall not conceal a suspended plant, activity or product family.

Essential gate. Evidence: Change assessment, coherent restriction and status update.

IR03 Audit evidence, duration and sampling

IR03-01 Audit team and independence

IAF shall assign at least two competent auditors collectively covering management, industrial processes and relevant technologies. Exclude personnel with employment, consultancy, ownership or material commercial ties to the applicant in the preceding 36 months, and longer where a threat remains. Declare other conflicts and protect independent worker and customer evidence.

Essential gate. Evidence: Competence matrix, conflict clearance and team appointment.

IR03-02 Minimum supplier audit planning

Initially plan at least two auditor-days for central governance plus two per operational site up to 100 effective workers, three for 101-500 and four above 500. Add one day per affected site for each factor: novel safety-critical technology, more than two material shifts, complex critical outsourcing or unresolved systemic risk. Each included operational site requires at least one full operating day physically on site.

Essential gate. Evidence: Duration calculation, additions and approved coverage plan.

IR03-03 Case and process sampling

At each family/site review at least three completed cases, including changed and adverse cases where available; add more to cover actual risks and contradictions. Witness every critical process family and release route and observe at least two shifts where more than one operates. Cover remaining shifts within the annual programme. These floors are not statistical confidence claims.

Essential gate. Evidence: Case population, independent selections and witness/shift coverage.

IR03-04 Evidence sufficiency

Triangulate original records, observation and independent interviews. Give at least half of on-site audit time to process observation, witnessing and interviews. Remote tools may supplement required physical audits but shall not replace them. Increase duration and samples when evidence is conflicting, inaccessible or insufficient; record limitations and unsupported scope.

Essential gate. Evidence: Evidence manifest, actual time log and sufficiency conclusion.

IR04 Findings, decisions and recognition term

IR04-01 Finding classification

Classify findings as Minor, Major or Critical using consequence and systemic extent, not negotiation. Pending is unverified evidence; NA requires an inherent scope reason approved by the auditor. A serious safety or integrity threat is Critical. Disclose affected scope, objective evidence and the failed requirement and allow 15 calendar days for factual response.

Essential gate. Evidence: Finding records, scope impact and factual-response trail.

IR04-02 Independent initial decision

A three-person IAF panel, uninvolved in audit or applicant consultancy, shall review competence, conflicts, evidence, scope and closure. All three participate; at least two affirmative reasoned votes are needed to grant. Every applicable requirement and additional claimed criterion shall be Met. No open initial finding, score average or commercial promise can substitute for this gate.

Essential gate. Evidence: Three-person vote record and verified initial closure package.

IR04-03 Term and surveillance

Recognition lasts at most three years from the grant decision, subject to annual surveillance due by months 12 and 24 and the annual physical-site rule. Renewal shall be independently decided before expiry; apply at least six months beforehand. A pending audit, appeal or renewal shall not silently extend the term.

Essential gate. Evidence: Decision dates, surveillance calendar and renewal record.

IR04-04 Active findings and urgent protection

During an active term apply the 90-day Minor maximum, 30-day Major closure target and immediate Critical protective-suspension review. Record containment and prior-output impact. A decision to continue coherent unaffected scope requires evidence and reasons; missed surveillance or inability to verify essential controls requires suspension review.

Essential gate. Evidence: Active finding controls and protective status decisions.

IR05 Public status, recognition record and mark

IR05-01 Controlled wording

The authorized status is IAF Corporate Recognised, used with the exact named scope and recognition ID. Certificates or statements shall describe corporate implementation assurance and its limits. They shall not imply universal legal acceptance, product-by-product approval, accreditation as a test body or a guarantee against defects or commercial loss.

Essential gate. Evidence: Approved statement, scope annex and claim samples.

IR05-02 Verification before publication

IAF shall validate a public or controlled manual verification service before issuing live status. Show legal entity, sites, scope, dates, conditions and current/historical status without exposing confidential findings or personal data. A code or signature verifies record linkage and authenticity, not the truth of every product claim.

Essential gate. Evidence: Verification tests and published minimum record.

IR05-03 Mark licence and misuse

Use only IAF-approved artwork and a recorded licence for active scope. Do not place the corporate mark on products, product labels, packaging or test reports in a way that implies product certification. Monitor misleading use, require correction and suspend rights where material misuse persists or creates immediate harm.

Essential gate. Evidence: Licence, artwork approval and misuse responses.

IR05-04 Status event integrity

Retain immutable history of grant, extension, restriction, suspension, expiry, withdrawal and restoration. Display the effective time and scope; publish protective changes normally within two business days. Correct stale copies through notice and verification links, preserving historical facts rather than deleting adverse status events.

Essential gate. Evidence: Authorized status events, notices and publication audit trail.

IR06 Fair process, confidentiality and protected reporting

IR06-01 Impartial operation

Separate IAF assessment and decision activity from sales, membership recruitment, sponsorship and applicant consultancy. Review structural conflicts at least annually. No commercial relationship shall buy a technical outcome. Staff incentives and committee composition shall support independent challenge and balanced industry/user interests.

Essential gate. Evidence: Impartiality review and role-separation evidence.

IR06-02 Complaints and protected concerns

Provide accessible confidential channels, acknowledge complaints normally within five business days and assign independent handling. Investigate evidence proportionately and protect good-faith reporters. Notify parties of reasoned outcomes and remaining review routes without disclosing unnecessary confidential material. Do not suppress a credible safety concern because litigation or a commercial dispute exists.

Essential gate. Evidence: Complaint log, protection controls and reasoned outcomes.

IR06-03 Appeals

Permit an appeal within 30 calendar days of decision notification. Use three competent reviewers who did not audit, decide or advise the original case. Record conflicts, evidence and reasons; target a determination within 45 calendar days after a complete submission. Necessary proportionate protection remains in effect during appeal.

Essential gate. Evidence: Appeal record, independent panel and final reasons.

IR06-04 Confidential information

Agree lawful access, restricted review, secure transfer and retention before collecting evidence. Share only what is necessary for competent assessment, required reporting and fair process. Preserve identities and trade secrets in public records. Confidentiality shall not be used to hide falsification or deny essential evidence; unresolved access prevents a supported conclusion.

Essential gate. Evidence: Data-access agreement, permissions and disclosure record.

IR07 Records, digital trust and oversight

IR07-01 Decision record retention

IAF shall retain application, evidence manifest, audit, finding, decision, appeal and status records for at least ten years after expiry or withdrawal, subject to longer holds. Limit unnecessary personal data. The organization retains product evidence under PSR-12.04; the two clocks shall not be confused.

Essential gate. Evidence: Role-specific retention and deletion/hold records.

IR07-02 Registry integrity

Control creation and modification of recognition identities, scope versions and status through authorized roles, separation of duties and recoverable audit trails. Test backup restoration and protect signing credentials. During an outage, return unavailable or unresolved with retrieval time and provide a controlled manual verification route.

Essential gate. Evidence: Registry access, recovery and outage verification tests.

IR07-03 Assessor consistency

Calibrate auditors and decision panels using common cases, witnessed performance and review of disagreement. Monitor bias, conflicts, overturned decisions and weak evidence. Authorize by actual competence and technology scope; generic audit experience alone shall not authorize unfamiliar high-risk industrial assessment.

Essential gate. Evidence: Calibration cases, observed audits and authorization limits.

IR07-04 Independent programme review

Audit programme operation annually and commission an independent effectiveness review at least every three years. Review false or overstated claims, surveillance timeliness, complaint outcomes and serious events. Publish aggregate performance without exposing confidential cases and adopt corrective improvements through controlled change.

Evidence: Programme review, performance report and corrective actions.

IR08 Implementation, global use and future development

IR08-01 Validated supplier pilots

Before launch, pilot at least an integrated system supplier with critical sub-tiers, a component or special-process producer, a software/digital supplier and a controlled-distribution or circular-product supplier. Include a failed case and a contested decision. Validate actual case definitions, physical operational-site coverage, forms, audit effort, decisions and status verification; resolve weaknesses before issuing recognition.

Essential gate. Evidence: Pilot coverage, results and launch gate decision.

IR08-02 Acceptance development

Build confidence through transparent criteria, competent auditing and documented acceptance arrangements with actual users. State the geography, purpose and limits of each arrangement. Neither this programme design nor a recognition record shall be described as accepted by every country, customer or authority without specific evidence.

Essential gate. Evidence: Acceptance register and bounded public statements.

IR08-03 Proportionate access

Permit organizations of different sizes and regions to use existing records and integrated systems where they satisfy requirements. Support competent translation and lawful protected access. Proportionality may change evidence format and audit additions, but shall not waive essential safety, integrity, physical audit or initial operating-history gates.

Evidence: Access arrangements and reasoned proportionality decisions.

IR08-04 Future modules and transition

Monitor new products, materials, energy systems and digital practices. Develop requirements through technical review, balanced consultation and pilots, then publish a prospective adoption and transition notice. Unvalidated future capability stays outside active recognition; preserve earlier decisions and explain the effect of changes on each scope.

Evidence: Research register, consultation, pilot and transition record.

Annex A - Definitions and interpretation

Term	Controlled meaning
Corporate recognition	Independent IAF conclusion that the named organization implements applicable corporate quality and trust controls within its exact scope.
Recognised unit	Named accountable legal entity or expressly named group entities, sites and activities covered by one decision and scope schedule.
Product family	Technically justified grouping with comparable responsibility, process route, critical characteristics, technology and risk.
Operational site	An actual controlled production, process, warehouse/configuration or accountable digital engineering/release centre. A mailing address alone is not a site; remote workers are assigned to an evidenced controlled centre.
Support function	Engineering, purchasing, digital operation or other work materially supporting included scope.
Completed case	An actual production, software-release or service/delivery case with requirements, execution, acceptance, release and traceability records.
Operating history	Dated evidence that the applicable controls were implemented in actual operation, not merely written or planned.
Critical process family	Process group whose failure can materially affect safety, conformity, hidden characteristics or essential integrity.
Original evidence	Records and observations with identifiable provenance, configuration, date and correction history sufficient for independent review.
Adoption schedule	Controlled list of exact IAF criterion texts, editions, approval status, claims and implementation responsibilities.
Met	Sufficient verifiable evidence of fulfilment of the applicable requirement.
Minor	Isolated lapse with no demonstrated loss of essential safety, validity or integrity; still requires correction and verified closure.
Major	Systemic or consequential failure, missing essential control or material threat to reliable performance.

Term	Controlled meaning
Critical	Serious actual or imminent harm, systemic falsification or severe integrity failure requiring immediate protective review.
Pending	Unverified, incomplete or inaccessible evidence; never equivalent to Met.
NA	Inherent non-applicability accepted with a recorded scope reason; never lack of implementation or resources.
Concession	Authorized bounded deviation where lawful and technically acceptable; cannot waive an essential safety requirement.
Auditor-day	Eight hours of substantive assessment work; travel and breaks excluded. Two auditors for eight hours equal two auditor-days.
Effective workers	Relevant permanent, temporary and contracted workforce across included operations and shifts; explain part-time equivalents and shared roles.
Private readiness	Non-public gap review with no Corporate Recognised status, provisional certificate or public mark rights.
Scope extension	Independently approved addition to a recognition schedule; planned expansion is not active coverage.
Recognition record	Authorized decision statement and scope schedule linked to current and historical status verification.

Annex B - Decision and status matrix

Situation / status	Required treatment
Applicant / Under assessment	Administrative only; no recognition rights.
Initial open finding or Pending	Defer/refuse affected scope or independently exclude a coherent unsupported activity; no conditional initial grant.
All applicable Met	Eligible for independent decision; checklist completion does not automatically grant recognition.
Corporate Recognised	Active only for named scope and dates, subject to continuing obligations.
Restricted	Only explicitly retained coherent scope active; limitations displayed.
Active isolated Minor	May remain open at most 90 calendar days with protected safety, validity and integrity.
Active Major / Critical	Immediate containment; Major 30-day target then suspension review if unresolved; Critical immediate protective review.
Suspended	No active claims for affected scope; protection and remedy obligations continue.
Expired / Withdrawn	Stop active claims, preserve truthful history and outstanding remedy capability.
Restored	Independent reasoned decision after verified control; no backdating or automatic extension.

Interim protective authority

For a credible serious safety or integrity threat, the programme manager together with an independent competent technical lead may issue an immediate interim suspension, with recorded reasons, exact scope and prompt notice. A three-person independent panel shall review it within five business days and confirm, narrow or revoke the measure with reasons. Escalate a threatened review delay to the governing authority; retain only protection that remains necessary and proportionate. Interim action does not decide the final merits or waive appeal rights.

Annex C - Minimum scope and decision data

Record	Mandatory fields
Entity	Stable ID; legal name; registration/jurisdiction; ownership; accountable representative; undertaking.
Site	Stable ID; address; actual processes; support functions; shifts; workforce; responsible technical management.
Scope row	Stable row ID; entity/site; activity profiles; family; technology modules; design responsibility; related services; markets; exclusions; version/dates/status.
Adoption	Exact IAF title/edition; approval status; claim boundary; applicability map; evidence; responsible owner and decision reference.
Audit	Plan and actual time; team competence/conflicts; sites/shifts; process witnesses; case populations/selections; originals; findings and limitations.
Decision	Three members, individual votes/reasons, verified closure, final scope version, dates, monitoring and appeal notice.
Public record	Recognition ID; named scope; criterion edition; active/historical states; restrictions; dates; verification route/time.
Status event	Affected IDs; former/new state; effective/publication times; reasons suitable for disclosure; authorizer; notices and history.

Annex D - Audit coverage and duration rules

The following are normative planning floors, not fixed-price durations or statistical guarantees. Increase time and samples until sufficient evidence exists. Do not reduce a mandatory floor by counting travel, report writing, parallel tasks twice or unperformed observation.

Element	Rule
Initial central governance	At least 2 auditor-days.
Initial each site	At least 2 auditor-days up to 100 effective workers; 3 for 101-500; 4 above 500.
Initial site additions	Add 1 day for each applicable factor: novel safety-critical technology; more than two material shifts; complex critical outsourcing; unresolved systemic risk.
Physical presence	At least one full operating day at each included operational site. At least half on-site time for observation, witnessing and interviews.
Team	At least two competent auditors in the assigned team; the visit allocation must still cover all necessary expertise. Both need not attend every low-risk task together.

Element	Rule
Surveillance floor	At least 1 central auditor-day plus 1 auditor-day per included operational site; retain two-auditor team, full-day physical visit, annual every-site coverage and sufficient expertise.
Renewal	Full initial planning rules and physical coverage of every included operational site before expiry.
Cases	At least 3 complete cases per family/site; add for differences, changes, adverse evidence and contradictions.
Witness and shifts	Every critical process family and release route; observe at least two shifts where multiple shifts operate; cover remaining shifts in the annual programme.

Illustrative calculation

One 70-worker assembly site with no additions and one 300-worker battery plant with novel safety-critical technology and three material shifts: 2 central + 2 assembly + 3 battery + 1 technology + 1 shifts = 9 auditor-days. Actual evidence may require more. Two plants with two families each require at least 12 completed cases (2 x 2 x 3), independently selected and justified.

Annex E - Deadlines, clocks and records

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 operational 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.

Calendar days include weekends and holidays. Business days follow the notified IAF operating calendar. Record notification and receipt times. Service targets permit reasoned delay with communication; maximum terms and mandatory gates do not silently extend. Longer legal or contractual retention and evidence holds prevail. Minimize personal data that are not needed to retain the technical decision basis.

Annex F - Performance and interpretation

Measure	Definition and required caution
First-pass yield	Initially conforming units / total units entering the defined process. Keep rework recovery separate.
Delivered unit defects	Confirmed nonconforming delivered units / delivered units in the bounded population. State period, severity and unit-versus-defect basis.
On-time complete delivery	Orders completed within the agreed window / orders due. Disclose partial delivery treatment.
Complaint and field outcomes	Define confirmed case, product exposure, configuration, severity and response/remedy ageing; low rates do not dismiss serious events.
Recall/field remedy	Verified completed remedies / affected population. Notifications and downloads are not completed protection.
Traceability retrieval	Elapsed retrieval time, completeness and quantity reconciliation against a pre-set justified target.
Action effectiveness	Verified sustained correction, recurrence and escape, including other affected sites.
Resource and support	Continuity test results, support capability and fulfilled commitments; no implication of financial guarantee.

No universal performance score is established by PSR. Define technically justified targets and binding acceptance criteria, assess real outcomes and do not compensate for an essential failure with a good aggregate result. Worked calculations in the Implementation Manual are illustrative.

Annex G - Recognition statement and claim boundary

An issued record shall use: [Legal entity] is IAF Corporate Recognised for [bounded activities] at [named sites], under recognition ID [ID] and scope schedule [version], from [effective date] to [expiry], subject to current status verification. It shall state the assessed criterion edition and the method to verify current and historical scope.

The statement shall explain that corporate recognition concerns implemented organizational controls and demonstrated operation within the schedule. It is not product-by-product certification, a market authorization, a conformity-assessment-body accreditation or a guarantee against defects or commercial loss. Additional IAF programme claims require their own valid evidence and decision.

Annex H - Launch, acceptance and future development

Before operational use, IAF shall adopt the programme, assign competent independent roles, validate representative pilots and adverse decisions, test records and status verification, publish contact and appeal routes, and record a launch authorization. Assess audit floors through pilots and increase them where the evidence requires. These prepared documents do not assert that those actions are already complete.

Maintain an acceptance register with actual parties, geography, purpose and limits. Seek confidence through demonstrable performance and user review. Develop future modules through technical review, consultation and pilots; publish transition rules prospectively and preserve the scope and status history of earlier decisions.

Annex I - Controlled document set

Document	Role
Standard and Internal Directives	Normative corporate baseline, profiles, technology modules, operator rules and annexes.
Applicant Guide	Practical preparation, submission, audit and continuing duties.
Implementation and Evidence Manual	Technical interpretation, examples and defensible evidence.
Audit and Recognition Manual	20 operating procedures, authority separation and decisions.
Status and Mark Usage Rules	Public wording, verification, licensing, misuse and history.
Corporate Recognition Application	Legal, executive, scope and evidence declarations.
Scope, Sites and Adoption Schedule	Bounded scope rows and IAF requirement adoption map.
Self-Assessment and Evidence Dossier	Implemented practice, original evidence, performance and gaps.
Assessment Checklist	216 mapped requirements, findings and decision records.
Product/System Approval and Change Dossier	Customer requirement, qualification, acceptance, change and handover evidence.
Governance and Monitoring Toolkit	Controlled forms for the complete recognition lifecycle.

Controlled change

The Standard prevails over supporting guidance and forms. A missing field is not a waiver. Identify the editions used in every completed record. Correct administrative defects without changing technical obligations; adopt substantive rule changes with prospective transition. Keep examples distinct from mandatory requirements and preserve previous authorized versions.

Annex J - Supplier sites, case units and responsibility

An operational site is an accountable location at which included output is engineered, produced, processed, configured, warehoused or released. Every included operational site receives the physical initial, annual and renewal coverage required by IR02 and Annex D. Central/support functions receive annual assessment by justified physical and remote evidence. The same assessed work shall not be counted twice as central and site time.

Distributed personnel shall be assigned to an actual controlled engineering/release centre with accountable supervision, secure work and retrievable original evidence. Every private home or generic cloud data centre is not automatically a separate applicant site. Critical outsourced activity nevertheless requires sufficient direct evidence, including physical witnessing where necessary to establish the process claim; an access restriction cannot create a waiver.

Supplier responsibility	Meaning of a completed actual case
System/component/electronic/energy	An actual completed build, batch, release or delivery with configuration, execution, acceptance and recipient linkage.
Material/special process	A completed material batch or customer processing load with sampling/process evidence, acceptance and quantity reconciliation.
Software/data/digital	A distinct controlled release, customer delivery or deployment with requirements, artifact identity, verification, authorization and operational acceptance evidence. Duplicate copies or download counts are not distinct cases.
Equipment/tooling	A completed asset delivery or contracted acceptance stage with verified configuration, capability, applicable site handover and support records.
Circular/remanufactured	A completed restored unit or justified lot with original condition, controlled restoration, release and customer trace.
Controlled distribution	A completed supplied lot with authentic source, actual receipt/configuration, preservation, acceptance and recipient records.

Each included responsibility-family/site requires at least three distinct complete cases and six months of implemented operation. Independent auditors select from the actual population; they add changed, adverse or uncertain cases as needed. Shared records may support several requirements but shall not artificially multiply the case population. A wholly new family or site remains outside an existing scope until its required evidence and extension decision are complete.

Annex K - Product approval and corporate recognition interface

The supplier shall maintain a controlled product/system qualification dossier for each included family and required customer/application boundary. The dossier shall identify the exact configuration, responsibility, source route, requirements, risks, qualification evidence, limitations, acceptance authority and release conditions. Apply the supporting approval/change records with justified non-applicability for genuinely absent activities; a blank field is not an accepted exclusion.

Where customer approval is required, record its actual authorized disposition before affected supply. Where it is not required, retain the contractual basis and competent internal release. Development permission, receipt, payment, nomination and a corporate recognition record shall not be substituted for a required technical acceptance. A lawful bounded concession shall state its exact quantity, time, use and conditions and shall never waive essential safety or integrity.

Changes shall be evaluated for technical validation, customer notice/approval, stock segregation, implementation identity and IAF recognition-scope effects. PSR does not prescribe a universal customer notification period; meet the applicable agreed duty, including any earlier obligation. Separate customer disposition, supplier release and IAF recognition decisions shall remain identifiable throughout the evidence trail.

The public statement shall identify the Product & System Supplier Recognition Programme and PSR edition, in addition to Corporate Recognised, exact scope and recognition ID. Similar wording under another IAF programme does not extend or transfer scope automatically. Reuse existing original evidence where valid, while retaining the additional requirement review and separately authorized programme decision.