



FIRST EDITION

IAF PARTS

Automotive Parts Integrity and Distribution Standard

Quality, traceability and network compliance
Across automotive retail and distribution channels

WORKING DRAFT 0.1 | TECHNICAL REVIEW

Technical validation and formal adoption are required before operational certification.
See Clause 36 and Annex L.

International Automotive Federation

English master text | 13 September 2026

iaf.com

Document control

Control	Entry
Proposed short name	IAF PARTS
Full title	Automotive Parts Integrity and Distribution Standard
Edition designation	First Edition
Development status	Working Draft 0.1 for technical consultation
Draft date	13 September 2026
Prepared for	International Automotive Federation
Language	English
Normative structure	Clauses 1 to 36 and Annexes A to I
Informative material	Foreword and Annexes J to L
Approval status	Not adopted and not authorised for certification claims
Revision principle	Retain clause identifiers and record changes and reasons

The working file is editable. Reviewers should identify a clause, the proposed replacement wording, the technical reason, supporting evidence and the affected business profiles. Examples illustrate application and do not override a requirement. Where a trial cannot meet a proposed requirement, the gap shall be recorded; the trial shall not describe the gap as conformity.

Contents

Select a section to navigate to it.

Document control	2
Foreword	5
1 Scope	6
2 Application and requirement conventions	7
3 Terms and definitions	8
4 Governance and accountability	9
5 Market access and obligations	10
6 Product risk classification	11
7 Supplier and source approval	12
8 Purchasing and product responsibility	12
9 Product technical assurance	13
10 Authenticity and fraud prevention	14
11 Product data and vehicle fitment	15
12 Identification and traceability	16
13 Digital parts passports and data exchange	17
14 Receiving inspection and release	18
15 Storage and inventory integrity	18
16 Packaging and labelling	19
17 Transport and cross border distribution	20
18 Retail sales and customer information	20
19 Online marketplaces and remote fulfilment	21
20 Network and franchise compliance	22
21 Installation and technical support interfaces	23
22 Electrified and high energy products	23
23 Electronic parts and software support	24

Contents continued

Select a section to navigate to it.

24 Used repaired and remanufactured parts	25
25 Additive manufacture and special applications	26
26 Returns warranty and core recovery	27
27 Nonconformity incidents and recalls	27
28 Information security and privacy	29
29 Responsible sourcing and environmental performance	29
30 Continuity resilience and obsolescence	30
31 Competence worker safety and measurement	31
32 Monitoring audit and improvement	31
33 Conformity evaluation and claims	32
34 Change control and future technology	33
35 Implementation and transition	34
36 Proposed scheme governance	34
Annex A Product risk classification	35
Annex B Functional applicability profiles	36
Annex C Minimum product and transaction data	37
Annex D Lifecycle states and events	40
Annex E Product verification planning matrix	41
Annex F Sampling and decision rules	43
Annex G Incident response and recall verification	44
Annex H Assessment and critical gates	46
Annex I Performance indicators	48
Annex J Implementation forms and worked examples	50
Annex K Future development directions	52
Annex L Technical validation and publication agenda	53

Foreword

This working draft proposes IAF PARTS as an integrated standard for the integrity of automotive replacement parts and the networks that identify, procure, store, distribute, sell, recover and support them. Its purpose is to make product quality, vehicle compatibility, provenance and corrective action verifiable throughout the aftermarket, including digital and circular channels.

The proposed standard is prepared for the International Automotive Federation. It is a technical development document for consultation, trials and revision. It has not been presented as an adopted standard, a regulatory approval, an operational certification programme or evidence of international recognition. Adoption, scheme launch and use of any IAF conformity mark require separate decisions by IAF.

The text establishes requirements through the word “shall”. These requirements define the proposed conformity model and may be trialled against this exact draft. Proposed numerical limits, response times and assessment frequencies are design choices for this document, not representations of universal legal requirements or validated industry performance. Annex L identifies the validation work needed before publication. Legal duties apply independently.

The central proposition is that a part should reach a customer only when its identity, application, condition, release status and supporting evidence agree. A convincing label, a complete digital record or a successful warehouse audit alone cannot establish that a product is safe for a particular vehicle.

The standard is designed for independent aftermarket businesses as well as vehicle manufacturer networks. Comparable evidence is assessed without preference for a brand, origin, ownership model, distribution model or technology provider. Small enterprises may use proportionate manual controls if those controls achieve the same safety and traceability outcomes.

1 Scope

1.1 Purpose and outcomes

This standard specifies requirements for organisations controlling automotive parts and related product information across sourcing, import, distribution, wholesale, retail, online sale, fulfilment, returns and recovery. It establishes an auditable chain between the physical product, its technical evidence, its declared vehicle application and the parties responsible for it.

The intended outcomes are prevention of unsafe or misrepresented supply; reliable identification and fitment; timely containment of suspect stock; transparent customer information; recoverable product histories; and responsible continuation of vehicle service. Organisations shall demonstrate these outcomes through operational evidence rather than policy statements alone.

1.2 Products and vehicle coverage

The scope includes mechanical, structural, electrical, electronic, fluid, chemical, energy storage, thermal, sensing, communication, interior, exterior and accessory products intended for vehicle maintenance, repair, replacement, retrofit or upgrade. It includes packaged software, software entitlements and calibration data when supplied as part of a replacement or retrofit function.

Applicable vehicles include passenger cars, commercial vehicles, buses, motorcycles, trailers, specialised road vehicles and supported off road vehicle applications. Combustion, hybrid, battery electric, fuel cell and future propulsion architectures are included when the relevant hazards are assessed. The organisation shall identify vehicle classes actually covered by its capability; a broad product catalogue shall not imply technical coverage of every application.

1.3 Organisations and channels

The standard applies to importers, brand owners, buying groups, wholesalers, retailers, warehouse operators, logistics providers, online marketplaces, brokers, fulfilment businesses, franchise networks, recyclers, remanufacturers and suppliers of digital part data. Manufacturers may apply it to aftermarket release and distribution interfaces. Installers may apply it to parts receipt, configuration, installation records and feedback interfaces.

An organisation shall apply requirements to its activities and to outsourced activities it controls or contracts. Annex B allocates functional profiles. An organisation performing several roles shall apply the combined profiles. A broker, marketplace or drop shipper shall not treat absence of physical custody as absence of product responsibility.

1.4 Boundaries

The standard defines product assurance and distribution controls. It does not itself specify every design dimension, material limit, durability cycle or vehicle approval test for every possible part. For each offered application, the organisation shall establish a controlled product assurance specification under Clause 9 and Annex E, including applicable quantitative acceptance limits and the basis for them.

Conformity to this standard does not establish vehicle roadworthiness, approval of a modification, compliance with every national law, product certification, installation competence or guaranteed accident prevention. Those conclusions require their own evidence and applicable decisions. Repair workshop operations beyond the interfaces stated in Clause 21 are outside the default scope.

2 Application and requirement conventions

2.1 Requirement language

“Shall” identifies a requirement. “Should” identifies a recommendation. “May” identifies permission. “Can” identifies a capability or possibility. Normative annexes form part of the proposed requirements. Informative annexes provide implementation aids and do not add conformity obligations.

The organisation shall maintain an applicability register covering every numbered clause and normative annex. Each entry shall identify the responsible role, implementation evidence and applicable sites, products or channels. A nonapplicable entry shall include an activity based justification approved by the accountable manager and reviewed during assessment.

2.2 Exclusions and proportional implementation

Requirements shall not be excluded solely because a business is small, a service is outsourced, a product is supplied through an intermediary or an activity generates little revenue. Requirements triggered by hazards remain applicable whenever the hazard is present. Functions genuinely absent from the scope may be excluded with supporting evidence.

Manual records, controlled spreadsheets and existing enterprise systems may be used. The organisation shall show that its chosen method preserves required identifiers, access controls, release authority, traceability and response capability. No specific commercial platform, ledger architecture, identifier subscription or central database is required by this standard.

2.3 Evidence and precedence

The organisation shall implement applicable law in each destination market. If a requirement in this standard conflicts with law, the organisation shall document the conflict, apply the law and seek a scope clarification. A conflict shall not be silently treated as fulfilment of the affected requirement. Where requirements are compatible, the more protective applicable control shall be implemented.

Evidence may be internal or supplied by a competent external party. The organisation shall evaluate its authenticity, relevance, completeness and current applicability. A commercial certificate, supplier declaration or legal approval shall support only the claims and products it actually covers. This standard incorporates no external document by normative reference.

2.4 Time and record conventions

Elapsed hours in this standard mean consecutive hours, including nights, weekends and public holidays. A working day means a day in the organisation’s published operating calendar. Event records shall preserve time zone or offset; cross border exchange shall permit conversion to a common time basis. Immediate action means action without avoidable delay and is not permission to wait until a stated maximum time.

3 Terms and definitions

Term	Meaning in this standard
Organisation	The legal entity or defined group of entities responsible for the declared scope
Responsible product operator	The identifiable party accepting technical and market responsibilities for a product
Part	A physical component, material, assembly or controlled digital item supplied for a vehicle function
Part family	Items grouped by documented common design, function, process and failure mechanisms for justified evidence reuse
Fitment	Verified compatibility with a defined vehicle configuration, installation position and operating application
Provenance	Evidence of origin, legitimate source and relevant history of a product
Authenticity	Consistency between a product's actual identity and its represented identity
Counterfeit	An item or representation deliberately misidentifying origin, identity, status or authorisation
Suspect part	A part for which identity, safety, condition, conformity or provenance is reasonably in doubt
Critical characteristic	A characteristic whose failure can cause severe harm, unlawful operation or loss of a safety function
Lot or batch	A defined quantity produced or processed under identified common conditions
Serial identity	An identifier distinguishing one physical unit throughout its controlled history
Release	An authorised decision that specified evidence supports the next permitted activity
Hold or quarantine	An enforced state preventing unauthorised sale, dispatch, installation or other use
Product assurance dossier	The controlled evidence supporting a specific part and its declared application
Digital parts passport	A persistent, access controlled record linking product identity, evidence and lifecycle status
Custody event	A recorded change in physical possession or responsibility for a part
Transformation event	A recorded operation changing composition, condition, configuration or identity relationships
New part	A part not previously installed or used for its intended service, with production and storage history controlled

Term	Meaning in this standard
Used part	A previously installed or operated part supplied with its relevant condition and history disclosed
Repaired part	A used part on which specified faults have been corrected and the repair scope disclosed
Refurbished part	A used part restored to a declared condition through specified processes, without an implied remanufacturing claim
Remanufactured part	A used core restored through a controlled industrial process to a defined and verified performance specification
Core	An item accepted for assessment and possible remanufacture, without an implied fitness for installation
Recall	An organised action to recover, correct or remove a product already supplied because of a safety or compliance concern
Withdrawal	Prevention of further supply of affected stock before or within the distribution chain
Near miss	An event that could have caused harm or unauthorised release but did not
Controlled digital item	Versioned software, entitlement, model, build file or calibration associated with a part or function
Evidence gap	Missing, inconsistent, outdated or inapplicable information preventing a justified decision
Conformity assessment	Evaluation of a stated scope against the applicable requirements of this exact document version

The organisation shall not substitute marketing terms such as premium, genuine quality, equivalent or smart for the condition and evidence categories defined above. “Original” or a vehicle manufacturer association shall be used only when supported by verifiable identity and authorisation evidence.

4 Governance and accountability

4.1 Declared scope and network map

The organisation shall document its legal entities, brands, sites, warehouses, stores, websites, marketplace accounts, contracted fulfilment locations and countries of sale. The scope shall identify activities, product families, condition categories and exclusions. Changes affecting responsibility or product risk shall be assessed before implementation.

The network map shall identify the responsible operator for each product family and the party controlling each critical process. Overlapping responsibilities shall be resolved contractually. A customer shall have an identifiable contact for safety concerns regardless of how many intermediaries participate.

4.2 Leadership and independence

Top management shall approve an integrity policy, provide resources and appoint an accountable product integrity manager with authority to stop sales, block stock and initiate safety escalation. A named alternate shall provide continuity. Sales targets, supplier incentives and stock write off concerns shall not override safety holds.

The person approving release of a critical suspect part shall be independent of the commercial decision to purchase or sell that part. Small organisations may obtain competent independent review externally. Conflicts of interest shall be declared, recorded and controlled.

4.3 Process ownership and escalation

The organisation shall assign owners for sourcing, technical assurance, catalogue data, traceability, warehousing, transport, customer support, returns, cybersecurity and recall. Each owner shall have documented competence, decision authority and escalation routes. Safety escalation shall remain available outside normal opening hours for high consequence products.

Staff and partners shall be able to report concerns without retaliation. The organisation shall retain reports, assessment decisions and actions, including decisions that no further action is needed. Confidential reporting shall be protected without preventing necessary safety investigation.

4.4 Controlled information

Policies, specifications, instructions, supplier approvals and forms shall carry an owner, version, approval and effective date. Obsolete versions shall be removed from use or clearly identified. Records shall identify who performed and approved each critical decision and shall remain retrievable under Clause 28.

5 Market access and obligations

5.1 Destination specific requirements

Before offering a product into a market, the organisation shall determine applicable requirements for product safety, vehicle use, technical approval, marking, language, consumer protection, chemicals, transport, waste, data protection and import. It shall identify any role acquired by importing, relabelling, modifying or selling under its own name.

A market requirements register shall state the product and vehicle scope, destination, responsible reviewer, evidence required, implementation action and review date. A generic worldwide statement shall not replace market specific evaluation. The organisation shall use competent advice when its own capability is insufficient.

5.2 Legal monitoring and evidence

The organisation shall monitor changes affecting its declared markets and product families. It shall assess changes before their applicable implementation deadlines, update product eligibility and communicate actions to affected partners. Mandatory reports and cooperation with competent authorities shall follow applicable legal times and channels.

Where a product requires an approval, authorisation or declaration, the organisation shall verify the issuer, covered variant, validity and limitations. A document for a similar product, different factory, obsolete software or other market shall not be accepted without a documented applicability assessment.

5.3 Restricted products and ethical trading

The organisation shall block products whose intended supply or use is prohibited in the destination market. It shall prevent the sale of devices or software represented as a means of defeating required emissions, safety, odometer or security functions. Legitimate diagnostic and repair functions shall be distinguished from deceptive bypass functions.

The organisation shall prevent bribery, falsified customs descriptions, intentionally incorrect origin statements and concealment of dangerous goods. Commercial restrictions shall be accurately disclosed. Product safety requirements shall not be used as an unsupported reason to misrepresent lawful competing products.

6 Product risk classification

6.1 Assessment method

Each product family and materially different application shall be classified using Annex A before source approval or listing. The assessment shall consider severity of failure, exposure, detectability before harm, vehicle integration, misuse, counterfeiting incentives, storage sensitivity and software dependency. The highest credible consequence shall determine the minimum risk class.

R1 denotes limited consequence, R2 significant functional or economic consequence, R3 serious safety or compliance consequence and R4 potentially catastrophic or systemic consequence. Financial value shall not determine safety class. A low likelihood estimate shall not reduce a product below the severity floor in Annex A.

6.2 Combined and changing risks

Risk assessment shall include interactions: a decorative cover can obstruct a sensor; a fastening change can alter a load path; a software update can change functional behaviour; and packaging can create a battery hazard. The organisation shall reassess a product when its application, supplier, materials, process, software, condition or incident history changes.

An assembly shall be classified at least as high as its highest consequence function. Embedded components shall remain identifiable where needed for a recall. A supplier's risk classification may inform the assessment but shall not remove the receiving organisation's responsibility to review it.

6.3 Controls and unresolved uncertainty

The classification shall determine verification depth, supplier monitoring, identity granularity, release authority, handling controls and escalation. Annexes A, E and F define minimum requirements. Additional hazards shall result in stronger controls even when a table does not explicitly name the product.

Where evidence cannot resolve a safety relevant uncertainty, the organisation shall hold the product or restrict it to a separately justified and lawful application. It shall not downgrade the risk class to permit sale. Risk acceptance shall identify the decision maker, evidence and residual risk, and shall never authorise prohibited supply.

7 Supplier and source approval

7.1 Initial due diligence

Before first purchase, the organisation shall verify the supplier's legal identity, operating address, relevant production or distribution role, contact channels and right to supply the represented product. Verification shall use independently corroborated evidence appropriate to risk, including a check that payment instructions and trading identity are consistent.

The organisation shall establish the actual manufacturing or remanufacturing source for R3 and R4 products. Where confidentiality limits direct disclosure to commercial staff, a competent authorised reviewer may inspect protected evidence. An unsupported claim of confidentiality shall not make an unknown critical source acceptable.

7.2 Capability and approval scope

Approval shall assess technical capability, product controls, traceability, change notification, complaint handling, recall cooperation and continuity. For R3 and R4 sources, the review shall include manufacturing or process evidence and a justified facility assessment. Remote evidence alone shall be justified by what it can reliably demonstrate.

The approved supplier record shall define permitted product families, source sites, conditions, markets, subcontracting limits and review triggers. Approval of one product shall not automatically approve all products offered by that supplier. The organisation shall verify that samples and routine supply come from the same approved source and controlled process.

7.3 Monitoring and suspension

Supplier performance shall be reviewed at least annually and immediately after a significant safety event, credible counterfeit concern or unapproved change. R4 sources shall receive an additional documented performance review at intervals not exceeding six months. Review depth shall reflect defect trends, source stability and evidence quality.

The organisation shall suspend affected supply when approval conditions fail. Reinstatement shall require evidence that the cause has been corrected and affected stock has been controlled. Payment of a fee or replacement of rejected units alone shall not establish restored capability.

7.4 Exceptional sourcing

Emergency or one time purchases shall undergo the same product safety gates as routine purchases. An expedited approval may change administrative sequencing but shall not bypass source identity, technical evidence, recall screening or release. The organisation shall record the emergency, additional verification and limited scope of approval.

8 Purchasing and product responsibility

8.1 Purchase requirements

Purchase information shall identify the exact part and revision, approved source, intended market, condition category, technical specification, packaging, marking, traceability and supporting documents. Where vehicle fitment or software is relevant, the required application and configuration shall be stated or linked to a controlled record.

Contracts shall require prompt notification of safety concerns, source or design changes, process relocation, software changes and identity compromises. They shall provide access to evidence necessary for investigation and recall, define responsibilities for downstream communication and prohibit undisclosed substitution.

8.2 Own brand and rebranding

An organisation placing its own brand on a product shall accept responsibility for the claims and technical assurance associated with that brand. It shall retain the underlying source identity and ensure access to design, validation and production evidence appropriate to risk. A label change shall not erase manufacturing history.

Repackaging and relabelling shall be controlled transformations. The organisation shall reconcile quantities, retain original lot or serial links and ensure that warnings, shelf life, market eligibility and condition category remain correct. Rebranding shall trigger a review of legal responsibilities under Clause 5.

8.3 Brokers and pooled procurement

A broker shall identify the actual supplying party, custody route, evidence owner and responsible product operator before committing supply. Buying groups shall define which technical approvals are shared and how members receive changes and holds. Shared approval shall remain limited to its specified source and product scope.

Consignment stock, drop shipment and supplier managed inventory shall have explicit release and quarantine authority. The party operating the sales channel shall verify that a safety hold prevents further orders and dispatch through each associated fulfilment route.

9 Product technical assurance

9.1 Product assurance specification

Before release, each part or justified family shall have an approved specification defining function, vehicle applications, interfaces, operating environment, condition, intended service and foreseeable misuse. It shall identify critical characteristics, acceptance limits, required tests, inspection methods and production consistency controls.

Numeric limits shall derive from applicable legal requirements, verified design information, vehicle interface requirements or a documented engineering justification. A comparison with another part shall identify what was compared and why the comparator is suitable. Physical similarity, catalogue interchange or a supplier assertion shall not independently establish equivalent performance.

9.2 Validation and dossier content

The dossier shall contain product identification; drawings or interface definitions; material and configuration information needed for assessment; risk analysis; a verification plan; results; traceability to tested samples; legal evidence; installation requirements; and release approval. Annex E provides a minimum test planning matrix.

The verification plan shall address dimensional fit, functional output, relevant durability, environmental exposure, chemical compatibility, electrical behaviour and vehicle integration as applicable. It shall identify tests omitted and the technical reason. An omission shall be rejected where it leaves an unresolved critical characteristic.

9.3 Evidence quality and production consistency

Test reports shall identify methods, equipment, sample condition, sample source, actual results, acceptance criteria, deviations and authorisation. Pass statements without underlying results shall be insufficient for critical characteristics unless controlled access to the underlying evidence is provided. Measurement uncertainty shall be considered where it can affect a conformity decision.

The organisation shall link routine production to validated configurations through source controls, incoming verification, change review and field monitoring. A successful prototype or first sample shall not establish continuing conformity. Reduced routine testing shall require stable evidence and shall never remove critical release gates.

9.4 Family grouping and substitutions

Evidence may be shared across a family only where the organisation demonstrates common failure mechanisms, relevant materials, manufacturing controls and justified worst case coverage. Variants outside those boundaries shall receive additional verification. The family rationale shall identify the products covered and the limitations of extrapolation.

Substitute products shall be independently assessed for fitment, function, legal eligibility and installation consequences. Customer acceptance of a substitute shall not waive technical requirements. Software, calibration and dependent components shall be considered in any claimed interchangeability.

9.5 Release gate

Release shall require approved source status, an applicable dossier, verified identity, suitable condition, correct market eligibility and no unresolved safety hold. The release record shall identify the person, evidence version and product population covered. R3 and R4 release shall include competent technical authorisation distinct from purchasing approval.

10 Authenticity and fraud prevention

10.1 Threat assessment

The organisation shall assess counterfeit, stolen, diverted, substituted, misgraded and maliciously altered products. The assessment shall include forged evidence, copied identifiers, reused packaging, unauthorised factories, manipulated online listings and fraudulent return swaps. Product value, scarcity, brand exposure and safety consequence shall influence verification depth.

Controls shall combine source verification, document checks, physical examination and appropriate technical evidence. A readable code, a valid looking seal or a plausible invoice shall not alone establish authenticity. Personnel shall know how to escalate mismatches without accusing a party before facts are established.

10.2 Verification and intelligence

The organisation shall verify identity features against controlled information from a legitimate source. For R3 and R4 products, it shall establish a method to investigate duplicate serials, inconsistent lot patterns and quantities exceeding plausible source records. An anomaly shall trigger a hold when it could affect safety or authenticity.

Purchasing, customer complaints, public safety alerts and supplier communications shall feed a controlled fraud intelligence process. Reports shall distinguish suspicion from confirmed findings and preserve evidence. Commercial disputes shall not be represented as confirmed counterfeiting without substantiation.

10.3 Suspect material control

Suspect products shall be physically and electronically segregated. The organisation shall preserve packaging, identifiers, documents and relevant digital evidence. It shall assess other stock from the same source, lot, route or account and extend containment when the boundary cannot be justified.

Suspect items shall not be returned to unrestricted trade. Return for investigation, lawful evidence retention or destruction shall preserve custody and prohibit resale. Confirmation of authenticity shall not remove a separate technical, damage or recall concern.

11 Product data and vehicle fitment

11.1 Master record ownership

Every active item shall have one controlled master record or an equivalent reconciled authoritative record. The record shall include the fields in Annex C, a data owner, version and source. Changes shall be approved, propagated to dependent channels and retained as history.

The organisation shall distinguish manufacturer part numbers, seller stock codes, cross references, serials and vehicle identifiers. Leading zeros, character case where significant, units and market variants shall be preserved. Duplicate records shall not allow held stock to remain available under another code.

11.2 Fitment evidence

Fitment shall be established for the exact configuration that affects compatibility. Relevant attributes may include vehicle type, production range, powertrain, transmission, axle, braking system, steering position, body variant, software version, voltage architecture, installed options and installation position. Vehicle age or model name alone shall be insufficient where relevant variants exist.

The fitment record shall identify the evidence source, applicable limits, exclusions, required companion parts and calibration or coding needs. A cross reference shall be treated as a candidate relationship until its technical basis is validated. Replacing one superseded part may require a kit or a revised installation process rather than a one to one substitution.

11.3 Uncertainty and assisted selection

When vehicle information is incomplete or contradictory, the sales process shall request clarification or refer the case to competent technical review. A result shall be described as unconfirmed until the required evidence is available. R3 and R4 products shall not be represented as confirmed fits on the basis of an unresolved match.

Image recognition, automated language translation and artificial intelligence may assist identification. They shall not invent fitment evidence, critical dimensions or approval status. The organisation shall retain the evidence used for safety relevant recommendations and apply the validation and escalation controls in Clause 34.

11.4 Publication and correction

Listings shall clearly disclose condition, quantity, contents, limitations and representative images. Images of another variant shall not obscure a relevant difference. Product titles, filters and search results shall be checked for misleading claims and missing restrictions.

Safety relevant catalogue errors shall be treated as product incidents. The organisation shall identify prior sales made under the erroneous data, issue necessary warnings and propagate corrected data within the limits in Annex G. Listing deletion alone shall not close the incident.

12 Identification and traceability

12.1 Identity granularity

Each part shall be traceable at the granularity specified in Annex A. The organisation shall preserve original identifiers and use supplementary identifiers where necessary without obscuring legally required marks or creating a false manufacturer identity. The physical marking method shall be compatible with the product's safety and functional performance.

R4 products shall have persistent individual identity. If direct marking would damage the part, an engineered method linking the unit to its controlled carrier and custody history shall be used and validated through installation or final handover. Loss of that link shall result in a hold. A supplementary serial shall not be represented as an original factory serial.

12.2 Chain of custody

Records shall connect each receipt to its source and each dispatch to its recipient or retrievable transaction. They shall preserve quantity, lot or serial, location, event time, status and responsible party. Outsourced and cross border custody shall remain traceable. Consignment and ownership changes shall not interrupt the record.

Anonymous retail transactions may use a receipt or transaction token where lawful. The organisation shall retain a way to identify the sold population and publish or transmit safety information without making unrelated marketing consent a condition of purchase. Known customer contact details shall be used for safety communication in accordance with applicable law.

12.3 Split merge and transformation

Splitting lots, building kits, repacking, dismantling, remanufacturing and combining stock shall preserve parent and child links. The organisation shall account for quantities and prevent one unit from acquiring multiple simultaneously active physical identities. Reworked or remanufactured identities shall retain their predecessors and relevant restrictions.

Where lot identity has been lost, the organisation shall define the broadest credible affected population and hold it. It shall not reconstruct unsupported precision. Reconciliation shall identify losses, scrap, samples, returns and adjustments as separate quantities.

12.4 Retrieval and resilience

Traceability shall support backward and forward queries from a part number, lot, serial, order, supplier or affected software version. R3 and R4 systems shall support urgent population retrieval under Annex G. A query result shall state completeness, exclusions and unresolved gaps.

During connectivity failure, authorised offline records shall preserve unique events and prevent duplicate release. Reconciliation shall occur before uncertain stock is made available. Traceability capability shall be tested under Clause 27 and shall not depend on one person's memory or one unbacked device.

13 Digital parts passports and data exchange

13.1 Required record and access

All in scope products shall have the structured identity and evidence record required by Annex C. R3 and R4 products and controlled circular transformations shall support a persistent digital parts passport or a functionally equivalent accessible digital record. A public scan interface is optional unless separately required by law or contract.

The passport shall identify the responsible issuer, product and version, condition, current restrictions and where authorised users can obtain supporting evidence. It shall distinguish asserted, verified, unknown and not applicable data. An attractive interface shall not conceal missing evidence or represent a data record as product certification.

13.2 Data authority and provenance

Each safety relevant field shall have an identifiable source, update time and version. Corrections shall preserve the superseded value, reason and authorisation. A distributor shall not silently overwrite a manufacturer's statement; it shall preserve the original and record its own correction or dispute separately.

Access shall be allocated by role. Public views shall provide essential product identity, condition and safety status without exposing personal records, theft enabling details or protected technical information. Authorised investigators shall be able to obtain the additional information necessary for containment and evidence review.

13.3 Interoperability and continuity

The organisation shall provide export of required records in a documented machine readable form with a field dictionary, units, time conventions and identity relationships. System integrations shall test schema compatibility, invalid values, duplicate events, delayed messages, access denial and recovery after interruption.

Record access shall remain available through product support, organisational restructuring and platform migration. Contracts with data providers shall define export, migration and continued safety access. The organisation shall not make access to recall status conditional on a paid marketing subscription.

13.4 Trust boundaries

Where cryptographic signatures, secure tags or distributed records are used, the organisation shall manage key ownership, revocation and verification failures. Cryptographic integrity demonstrates that data has not been altered under the chosen model; it does not independently demonstrate that the underlying physical claim is true.

Critical status changes shall invalidate stale available to sell states across connected systems. Offline readers shall display the last successful update and avoid implying current safety status when freshness cannot be verified. Annex D defines the minimum lifecycle state behaviour.

14 Receiving inspection and release

14.1 Receipt control

Incoming goods shall enter a controlled pending receipt state. Personnel shall verify supplier, order, source, part identity, quantities, condition, packaging, lot or serial and required documents. Hazardous consignments shall be accepted only into suitable facilities by competent personnel.

The organisation shall check for active holds, recalls, expired life, tampering, damage, moisture exposure and temperature excursions where relevant. A mismatch between a label, digital record and physical item shall prevent routine release. Urgent customer demand shall not authorise receipt bypass.

14.2 Inspection planning

Inspection plans shall identify characteristics, methods, sampling basis, acceptance criteria, tools and release authority. Annex F defines sampling principles. Product identity and hold status shall be checked for every handled unit or validated homogeneous handling unit; critical physical characteristics shall follow the approved product assurance plan.

Sampling shall consider source changes, inconsistent lots and counterfeit threats. Passing samples shall not release a lot when a known critical defect remains unresolved. When measurement is destructive or infeasible on every unit, the organisation shall rely on a justified combination of validated process controls, representative testing and traceability.

14.3 Disposition and verification

Accepted, rejected, held and conditionally restricted products shall be distinguishable in both inventory systems and physical handling. Restricted release may be used only for a documented lawful nonsafety deviation accepted by the appropriate customer. It shall not apply to unknown authenticity, unresolved critical fitment or missing required safety evidence.

Inspection records shall retain actual findings and identify inspected units or lots. Rejected units shall not be blended into later deliveries without documented corrective action and renewed acceptance. Release permissions shall prevent the inspector or supplier from concealing a previous rejection.

15 Storage and inventory integrity

15.1 Storage conditions

Storage specifications shall address temperature, humidity, light, contamination, corrosion, electrostatic discharge, mechanical load, vibration and incompatible materials as relevant. Limits shall be based on validated product information or engineering justification. One general warehouse temperature range shall not replace product specific limits.

Environmental monitoring shall cover locations where excursions could affect suitability. The organisation shall assess excursions against duration, severity and product sensitivity, hold affected stock and obtain competent disposition. Resetting a sensor or returning conditions to normal shall not establish that exposed stock is acceptable.

15.2 Stock rotation and shelf life

The organisation shall control manufacturing age, shelf life, expiry, opening date and service life restrictions where applicable. First expiry first out shall be used for life limited stock. Extension of shelf life shall require authorised technical evidence and shall preserve the original date and extension basis.

Old stock represented as new shall meet the definition of new and have suitable storage history. Rubber, adhesives, lubricants, batteries, seals, electronic components and pyrotechnic devices shall have product appropriate ageing controls. Appearance alone shall not establish remaining life.

15.3 Location and status accuracy

Location records shall preserve identity through picking, replenishment and internal transfers. Similar looking parts, condition categories and voltage variants shall be separated or controlled to prevent selection errors. Available stock shall exclude holds, recalls, expired units and unapproved returns in every connected sales channel.

Risk based cycle counts shall verify both quantity and identity. Differences involving R3 or R4 products shall trigger an immediate traceability review. Inventory adjustments shall retain reasons, authorisation and affected identities rather than simply forcing book quantities to match physical stock.

15.4 Facility protection

Warehouses shall control unauthorised access, fire and flood exposure, pests, spills and handling damage. Storage layouts shall maintain safe access, emergency routes and separation of incompatible or damaged energy products. The organisation shall define who may enter quarantine and record every removal.

16 Packaging and labelling

16.1 Protective packaging

Packaging shall protect the product through the intended transport route, storage period and handling conditions. Validation shall consider movement, shock, compression, moisture, corrosion, contamination, electrostatic effects and dangerous goods requirements as relevant. Reusable packaging shall be inspected for fitness before reuse.

Packaging that maintains an essential controlled environment shall carry clear opening and resealing instructions. Kits shall identify their contents and prevent loss or substitution of critical accessories. Protective caps and covers shall not create an installation hazard through ambiguous removal instructions.

16.2 Label content

Labels shall provide the information needed to identify the product, condition, responsible party, lot or serial, relevant dates, quantity, market limitations and handling hazards. Required languages and legal markings shall be included. Digital information may supplement physical information but shall not replace mandatory physical warnings.

Human readable identity shall remain available if a machine readable carrier is damaged. Codes shall resolve to the correct record and shall be tested after design or printing changes. Labels shall not imply manufacturer endorsement, certification, recycled content or performance beyond the supporting evidence.

16.3 Repacking and label security

Repacking shall occur under instructions preserving cleanliness, identity and quantity. Original essential warnings shall be retained or accurately reproduced with authority. Partial packs shall carry the necessary lot and life information, including any shorter life after opening.

Unused identity labels and conformity marks shall be controlled against theft and unauthorised use. Incorrect labels shall be destroyed or rendered unusable. Relabelling to conceal expiry, prior use, recall, source or nonconforming status is prohibited.

17 Transport and cross border distribution

17.1 Route and carrier qualification

The organisation shall select carriers capable of maintaining product condition, custody and required hazard controls. Routes shall be assessed for climate, delays, transshipment, security and handling infrastructure. Contracts shall address subcontractors, loss, damage, delivery evidence and incident notification.

Dispatch checks shall verify destination eligibility, order identity, packaging, documentation and current release status. Shipment identity shall link each handling unit to its contents. Delivery confirmation shall identify recipient or authorised location and record exceptions rather than treating an attempted delivery as completed custody.

17.2 Dangerous and sensitive goods

Batteries, pressurised items, chemicals, fuels, pyrotechnic components and other dangerous goods shall be classified, packaged, documented and transported under applicable requirements by competent parties. The organisation shall determine requirements for the actual condition of the item, especially damaged, defective, used or recalled goods.

An ordinary return label shall not be issued for a potentially dangerous return until suitability of the transport route has been assessed. Personnel shall not charge, open, vent, discharge or dismantle a hazardous product merely to make it easier to ship unless a competent authorised procedure specifically permits the operation.

17.3 Border and delivery exceptions

Import and export records shall describe products, condition, origin, value and hazardous status accurately. Customs detention, inspection, repacking or broken seals shall be recorded and assessed before release. Cross border transfers shall preserve traceability even when local commercial codes differ.

Lost, stolen or unattended consignments shall be investigated for both stock loss and diversion risk. Recovered products shall undergo suitability assessment before reentry. The organisation shall identify customers potentially affected by misdelivery and initiate containment when another party may have received an unsafe or incorrect item.

18 Retail sales and customer information

18.1 Pre sale controls

The seller shall present the correct product identity, declared condition, quantity, material limitations, essential fitment qualifications, price and relevant terms before purchase. Where professional installation, calibration, activation, subscription or additional components are necessary, these requirements shall be disclosed before the customer commits.

Sales personnel shall verify the information needed for a fitment claim and record material advice. Where the customer selects without sufficient vehicle information, the seller shall state the unresolved compatibility limits and shall not issue a false fitment confirmation. R3 and R4 unresolved fitment shall trigger technical review before a confirmed application sale.

18.2 Transaction and handover

The transaction record shall link the item, quantity, condition and applicable lot or serial to the sale. The customer shall receive installation and safety information in a usable form and required language. Access to essential instructions shall not depend on acceptance of advertising, unnecessary personal data collection or creation of an unrelated account.

Substitutions shall be disclosed and technically justified before fulfilment. A different brand, remanufactured item or different software capability shall not be supplied as if it were the original order. Where an unsafe or ineligible item is discovered at handover, personnel shall be able to stop the transaction.

18.3 Claims and fairness

Performance, lifetime, environmental and compatibility claims shall be supported by applicable evidence. Comparative statements shall disclose the relevant basis and scope. Claims of universal fit, maintenance free operation or unlimited life shall not be made where known conditions contradict them.

Warranty and return information shall be clear and shall not obscure statutory rights. Safety complaint handling shall remain available regardless of proof of marketing registration. Customers shall be informed of relevant support termination, software restrictions and foreseeable costs needed to keep the supplied function usable.

19 Online marketplaces and remote fulfilment

19.1 Seller and listing accountability

A marketplace shall verify seller identity, responsible product operator, contactability and the scope of products permitted for sale. It shall assign responsibility for product data, fulfilment, safety communication and returns. Onboarding approval shall not be treated as approval of every listing.

Listings shall retain evidence linking the offered product to its actual supplier and fulfilment route. High risk categories shall require review before activation. A marketplace shall define how sellers provide technical evidence and how unresolved concerns block listings, offers and related accounts.

19.2 Transaction integrity

The platform shall prevent blending stock with different provenance, risk status or condition merely because the external product code is the same. Fulfilment systems shall preserve the actual seller and lot or serial supplied to each order. The platform shall test whether a hold remains effective through order routing, automated substitution and split shipment.

The system shall disclose the responsible seller and material delivery or installation conditions. Sponsored rankings, reviews and recommendation tools shall not create unsupported safety or conformity claims. Automated listing generation shall use controlled data and shall be reviewed for critical field errors.

19.3 Takedown and reentry prevention

Safety notices shall reach an operational response team with authority to suspend affected offers. The platform shall search for duplicate listings, altered spellings, copied images, alternate identifiers and repeat seller accounts when a removal could otherwise be evaded. Safety restrictions shall be synchronised with fulfilment partners under Annex G.

Removing a listing shall not delete evidence or affected order histories. Reinstatement shall require an authorised documented resolution. The platform shall maintain customer contact and remedy capability for completed transactions even after a seller leaves or is suspended.

19.4 Remote custody assurance

For drop shipments, the seller or platform shall obtain release status, shipment identity and traceability from the fulfilment party before dispatch. It shall verify performance through sample transactions, exception review and periodic testing. Contractual promises unsupported by actual traceability shall be insufficient.

20 Network and franchise compliance

20.1 Common controls

A network claiming conformity shall define a common control system, participating entities and enforceable responsibilities. Central functions shall provide controlled specifications, training, supplier rules, incident channels and current product restrictions. Local entities shall retain responsibility for correct implementation within their scope.

The central function shall maintain a current site and channel register and shall have authority to require corrective action, suspend affected claims and block unsafe supply. A shared brand, membership or purchasing relationship alone shall not establish eligibility for network conformity.

20.2 Local variation and oversight

Local requirements shall be documented for language, law, market eligibility, infrastructure and customer practices. Local variation shall not weaken the standard's critical gates. Centrally approved products shall be reassessed when sold into a market outside the original approval scope.

The network shall monitor complaints, returns, catalogue corrections, traceability failures and release exceptions by site. Significant outliers shall trigger investigation. A central average shall not conceal a failing location or a severe product incident.

20.3 Membership changes and claims

New sites, acquisitions and outsourced operators shall be assessed before inclusion in a conformity claim. A departing or suspended member shall cease affected claims and retain the records and recall cooperation required for products already supplied. Customers shall be able to verify which specific entities and channels are within the declared scope.

Multisite assessment shall follow Annex H. Sites outside common control shall require separate evaluation. A problem at one site shall be assessed for shared causes across the network before its impact is limited to that site.

21 Installation and technical support interfaces

21.1 Installation information

The supplier shall provide or ensure access to controlled information needed for the declared installation, including orientation, interfaces, required tools, tightening requirements, single use items, consumables, coding, calibration and post installation checks. Requirements shall be specific enough for the part and application. Generic instructions shall not obscure configuration dependent steps.

Safety related installation information shall be reviewed by competent personnel and translated where required. A seller unable to provide essential information shall hold the affected application claim. Restrictions on installation shall be based on competence, safety and lawful access requirements rather than unsupported brand preference.

21.2 Configuration and completion

Where the organisation installs, activates or arranges installation, it shall verify the part, vehicle and software configuration before completion. It shall record relevant serials, tools, software versions, calibration results and completion status. A failed or incomplete safety calibration shall prevent representation of the vehicle function as restored.

The handover shall state any outstanding work, limitations and evidence provided. A component test shall not be represented as proof of integrated vehicle function unless the integration was actually verified. Safety systems affected indirectly by removal, mounting or geometry changes shall be included in the installation assessment.

21.3 Technical access and feedback

The organisation shall provide a route for competent repairers to obtain necessary product information and support under fair, lawful terms. Security sensitive access shall authenticate legitimate need and protect credentials without making routine safety information inaccessible. Applicable restrictions shall be disclosed before purchase.

Field failures, repeated fitment problems and installation ambiguities shall be captured and linked to product and data owners. Evidence shall distinguish a product defect from a configuration issue or installation error. Blaming installation without supporting investigation shall not close a safety complaint.

22 Electrified and high energy products

22.1 Scope and technical compatibility

This clause applies to traction and auxiliary batteries, cells, modules, power electronics, chargers, high voltage assemblies, hydrogen related components and other products with significant stored or transferred energy. The organisation shall define product specific hazards, competent roles, emergency controls and restrictions on handling and supply.

Compatibility evidence shall address voltage range, current capability, chemistry, thermal management, mechanical interfaces, electrical isolation, protective devices, communication and control logic as applicable. A matching connector or nominal voltage shall not establish interchangeability. Modifications to pack composition, protection or control software shall trigger renewed engineering assessment.

22.2 Battery condition and identity

Each traction battery pack and individually traded traction module shall carry persistent unit identity and relevant predecessor links. The record shall identify chemistry, rated characteristics, production information, known damage or thermal events, condition, diagnostic evidence and current restrictions. Unknown history shall be explicitly recorded and assessed.

State of health claims shall identify the quantity measured, reference basis, test conditions, method, date and uncertainty or limitations. Capacity, power capability, internal resistance and safety condition shall not be treated as interchangeable measures. A favourable state of health estimate shall not by itself establish freedom from internal damage or suitability for a new application.

22.3 Handling and screening

Competent personnel shall screen for damage, swelling, leakage, unusual heat, corrosion, electrical exposure and relevant fault information without creating additional hazards. Suspect energy products shall enter a controlled area and response process established by qualified specialists. General warehouse staff shall not perform unapproved electrical measurements, opening or disassembly.

Charging, storage state, isolation, packaging and emergency arrangements shall follow product specific validated instructions and applicable requirements. This standard does not prescribe a universal storage charge level, isolation threshold or thermal response procedure. The organisation shall have approved limits and safe procedures for the exact product and activity.

22.4 Reuse and second applications

Reuse, module replacement and repurposing shall establish a new justified application and responsible operator. The assessment shall include compatibility, remaining capability, protective functions, duty cycle and relevant previous history. A new passport or identity relationship shall preserve the original record and identify the transformation.

When evidence cannot support safe reuse, the product shall be restricted to controlled investigation, recovery or disposal. A change from vehicle service to another application shall not be used to conceal a damaged or recalled condition. Clauses 24, 26 and 29 apply to recovery routes.

23 Electronic parts and software support

23.1 Hardware and software configuration

Electronic control units, sensors, connected accessories and programmable components shall have identified hardware, firmware and calibration versions. The dossier shall define supported vehicle configurations, required dependencies, installation constraints and functions affected by a replacement. Blank, preprogrammed and locked states shall be clearly distinguished.

The organisation shall assess whether a replacement affects diagnostics, security credentials, emissions functions, driver assistance, automated functions or remote services. Unsupported configuration combinations shall be blocked or clearly restricted to an approved nonoperational evaluation context.

23.2 Software authenticity and delivery

Software and calibration shall come from an authorised and verified source appropriate to the product. Delivery shall protect integrity, verify the target identity and prevent installation of an unintended version. Privileged access and signing keys shall be controlled; shared uncontrolled credentials shall not be used for product activation.

An update process shall define interruption handling, recovery and prevention of unsafe downgrade. Recovery shall restore a supported safe state and shall not blindly reintroduce a known vulnerable version. Each update shall retain its version, reason, authorisation and affected product population.

23.3 Vulnerabilities and support life

The responsible operator shall declare a support period or support end date and the scope of vulnerability handling, compatibility maintenance and required services. It shall maintain a route to receive vulnerability reports and communicate safety relevant mitigations. The distributor shall transmit these commitments accurately and identify any gaps.

Where cloud services, subscriptions or remote activation are essential, the customer shall receive this information before purchase. The dossier shall assess loss of connectivity, service termination and provider failure. Continued safety shall not depend on an undisclosed indefinite third party service.

23.4 Transfer and decommissioning

Used connected components shall undergo an authorised process to remove prior user data and resolve ownership or activation locks without bypassing legitimate security. Data erasure shall preserve required product safety history while removing unrelated personal information. Components with unresolved lawful ownership or security restrictions shall not be represented as ready for installation.

24 Used repaired and remanufactured parts

24.1 Acceptance of recovered products

The organisation shall document source, lawful ownership, donor identity where available and relevant service or damage history. It shall assess recall status, crash, flood, fire, corrosion, contamination, wear and tampering. The significance of unavailable history shall be evaluated against the part's risk class.

Parts removed from a vehicle shall not be presumed suitable because the vehicle had been operable. Storage, dismantling and inspection shall preserve identity and avoid damage. Safety relevant donor information shall remain linked to the recovered part without unnecessarily disclosing prior owner personal information.

24.2 Condition claims and process controls

Used, repaired, refurbished and remanufactured products shall be described using the definitions in Clause 3. Inspection grades shall identify what was examined, the measurable acceptance criteria, the assessor and limitations. Cosmetic appearance grades shall not be presented as safety or remaining life grades.

A remanufacturing process shall define core acceptance, dismantling, cleaning, inspection, replacement criteria, controlled restoration, assembly, configuration and final verification. It shall specify the intended output performance and warranty terms. A simple cleaning, repainting or fault reset shall not justify a remanufactured claim.

24.3 Critical and restricted reuse

Single use, deployed, life expired or irreversibly damaged safety components shall not be returned to service. R4 pyrotechnic restraint devices shall be excluded from used or refurbished retail supply under this draft. Any future controlled recovery route for those devices requires a separately approved product protocol and a formal revision or authorised supplement; a local concession is insufficient.

For other R3 and R4 recovered products, reuse shall require unit level history sufficient for risk assessment, applicable engineering acceptance criteria and documented functional verification. Unknown damage or life history affecting a critical characteristic shall prevent release. Seller disclaimers shall not substitute for evidence.

24.4 Traceability and residual life

Transformation records shall connect original and released identities, replaced critical components, process version and verification results. The remanufacturer shall be identifiable as the responsible operator for the transformed product. A remanufactured item shall not be represented as unused original production.

Remaining life claims shall state method, assumptions and limitations. Previous service shall not be erased by resetting a counter unless the reset is technically appropriate, authorised and accompanied by retained history. Related passport records shall preserve recall and restriction information.

25 Additive manufacture and special applications

25.1 Design authority and application limits

On demand, additively manufactured, reverse engineered and custom parts shall have an identifiable design authority and a controlled intended application. The organisation shall verify rights to use design information and shall evaluate relevant legal requirements. Availability of a digital model shall not establish permission or suitability to manufacture it.

Legacy vehicle scarcity and discontinued supply shall not reduce technical acceptance criteria. Where original information is unavailable, a competent engineering assessment shall establish interfaces, loads, environment, material behaviour and verification needs. Limitations shall be disclosed before supply.

25.2 Manufacturing evidence

The dossier shall connect the approved design file, version, build preparation, material lot, machine, process parameters, orientation, post processing and inspection to each released population. Reused feedstock, repairs to build files and outsourced finishing shall remain controlled. A file checksum shall verify file integrity without being treated as proof of design adequacy.

The verification plan shall consider anisotropy, internal defects, dimensional variation, surface condition, fatigue and environmental effects where relevant. Simulation and digital twins may support the case but shall be validated for their intended use. Safety relevant release shall include appropriate physical evidence unless a technically justified accepted method establishes equivalent assurance.

25.3 Local manufacture and change

Distributed production sites shall demonstrate capability for the approved process and material. Approval at one site shall not automatically cover another machine, material source or build configuration. Every material change shall trigger a documented review of validation coverage.

Software controlled demand planning shall not autonomously substitute a material, geometry or process for a released safety part. The organisation shall preserve design decision authority and prevent unapproved files from entering production or being marketed as approved replacements.

26 Returns warranty and core recovery

26.1 Return intake

Returned products shall enter a hold state and shall be identified against the original transaction wherever practicable. The organisation shall verify identity, condition, installation or use, packaging, expiry, recall status and evidence of tampering or substitution. A refund decision shall be separate from a decision to restock.

The return channel shall screen for dangerous goods and provide suitable instructions before transport. Customers shall not be told to conceal damage or hazardous status. Safety related returns shall be escalated under Clause 27 even if the customer requests only a commercial remedy.

26.2 Restocking and warranty investigation

Restocking shall require an authorised examination demonstrating that the returned item meets the conditions of its proposed sale category. Opened or installed products shall not be automatically restored to new stock. An R3 or R4 returned unit with uncertain identity, use or exposure shall remain blocked pending competent resolution.

Warranty analysis shall capture symptom, application, lot or serial, use conditions, configuration, investigation and outcome. Repeated claims shall be assessed collectively for product or data defects. Rejection of a warranty claim shall not remove the duty to investigate credible safety evidence.

26.3 Core transactions and disposition

Core charges, eligibility, return condition and credit criteria shall be disclosed before purchase. Core inventory shall remain distinct from ready to install stock. Acceptance for credit shall not imply technical suitability for remanufacture.

The organisation shall track cores through evaluation, transformation, component recovery or disposal. Products sent for destruction shall be rendered unsuitable for deceptive reentry, and records shall identify quantities, identities where required, recipient and disposition evidence. Environmental controls shall apply to residues and recovered materials.

27 Nonconformity incidents and recalls

27.1 Detection and immediate containment

The organisation shall operate a process covering complaints, inspection failures, supplier alerts, catalogue errors, cyber incidents, field failures and external safety reports. It shall record when credible information was first received, affected products, potential harm and the initial decision. Staff shall have authority to place precautionary holds before final cause confirmation.

Potentially severe safety concerns shall trigger immediate containment and the escalation limits in Annex G. The organisation shall block stock, orders, dispatch, listings and relevant software delivery through all controlled channels. It shall not wait for commercial agreement or proof of injury before taking justified protective action.

27.2 Population and risk assessment

A competent team shall establish the affected population using source, lot, serial, production range, software, fitment data and event history. Where uncertainty prevents a narrow boundary, containment shall cover the wider credible population. The organisation shall record assumptions and update the population as evidence develops.

Assessment shall consider severity, exposure, detectability, vulnerable users, installation state and the possibility of common causes in related products. It shall determine necessary authority notifications, customer instructions, withdrawal, repair, replacement, refund or recall. Mandatory legal actions shall not be delayed by internal time limits.

27.3 Communication and remedies

Safety communications shall identify the affected product, risk, identification method, required action, available remedy and contact route in clear language. Messages shall separate immediate protective instructions from background information. They shall avoid minimising a known hazard or requiring customers to prove a defect before receiving urgent safety information.

The organisation shall notify identifiable business recipients and customers, coordinate public communication for uncontactable populations and track delivery failures. Partners shall acknowledge and confirm action. An unanswered message shall trigger escalation and alternative channels rather than being recorded as completed protection.

27.4 Reconciliation and closure

The recall ledger shall distinguish in stock, supplied, contacted, acknowledged, returned, repaired, replaced, disposed and unlocated quantities or units. The organisation shall report both notification coverage and effective remedy coverage. A high email delivery rate shall not be presented as completion of a physical recall.

Closure shall require a documented decision supported by population reconciliation, evidence of effective action, residual risk and any required external acceptance. Unresolved units shall remain visible with ongoing measures. Root cause correction shall address systemic failures and verify that the same route cannot release the product again.

27.5 Exercises and preparedness

The organisation shall run a traceability and recall exercise at least annually and at intervals not exceeding six months where R4 products are supplied. The exercise shall include a realistic historical transaction and at least one outsourced or digital channel when present. Annex G defines scenarios and pass criteria.

Exercises shall test identification, blocking, communication, reconciliation and response during staff absence or system disruption. Simulated customer or authority messages shall be clearly marked and shall not be sent externally without an authorised exercise arrangement. Failed objectives shall result in corrective action and a focused repeat exercise.

28 Information security and privacy

28.1 Protected information and access

The organisation shall inventory systems and data supporting product identity, catalogue publication, release, traceability, customer records and software delivery. It shall assess confidentiality, integrity and availability risks, including supplier access and cloud dependencies. Access rights shall reflect job needs and be reviewed when roles or employment change.

Privileged and remote access shall use strong authentication, including multiple factors where technically feasible. Any exception shall have a documented equivalent control and expiry. Shared administrator accounts shall be prohibited unless an unavoidable technical constraint is controlled through attributable access and review.

28.2 Integrity and recovery

Critical records shall have change logs, access restrictions and protected backups. Restores shall be tested at least annually and after major system changes. The organisation shall verify that restored product status, recall blocks and transaction sequences are complete before normal release resumes.

Interfaces shall validate inputs and reject malformed or unauthorised changes. Cybersecurity incidents affecting fitment, identity, availability to sell or software integrity shall be treated as product integrity incidents. Evidence shall be preserved without allowing an investigation to prolong unsafe availability.

28.3 Privacy and retention

Personal information shall be limited to lawful, necessary purposes, with defined access, retention and deletion. Vehicle identifiers shall be treated as potentially linkable to individuals. Public passports shall not expose owner names, addresses, precise personal travel information or unrestricted transaction histories.

The organisation shall set a retention schedule covering legal duties, declared product life, support, expected claims and recall investigation. For nonpersonal technical and traceability records, the draft minimum is ten years after last supply of an affected lot for R3 and R4, and five years for R1 and R2, extended where risk or law requires. Technical evidence supporting an active product shall remain available throughout its supply period and the applicable subsequent period.

Personal data shall not be retained automatically for those full technical periods where a shorter lawful period applies. The organisation shall preserve product traceability through minimised or pseudonymised transaction links and define alternative safety contact arrangements. Legal holds shall be controlled and released when no longer justified.

29 Responsible sourcing and environmental performance

29.1 Supply chain responsibility

The organisation shall assess material sourcing and business practices for risks of forced labour, child exploitation, unsafe work, illegal extraction, corruption and serious environmental harm. Assessment shall prioritise credible risk and product exposure and shall include an accessible grievance route. Supplier declarations shall be corroborated where risk warrants.

The organisation shall document preventive and corrective action and evaluate its effects on affected people. Suspending a supplier shall include assessment of safe supply continuity and responsible remediation where feasible. Commercial urgency shall not excuse knowingly unlawful sourcing.

29.2 Materials and chemicals

The organisation shall obtain information necessary to control restricted substances, chemical hazards, transport and end of life obligations in its markets. It shall preserve safe handling information for fluids, coatings, adhesives, batteries and relevant materials. Missing essential hazard information shall prevent release.

Material recovery and circular sourcing claims shall distinguish physically traceable content, attributed content and estimates. The organisation shall prevent double counting and disclose the allocation basis. A recycled content claim shall not be used as evidence that a critical material meets its mechanical or electrical specification.

29.3 Measured environmental claims

Environmental comparisons shall state product function, boundary, period, data quality and significant assumptions. Energy, emissions, waste and water indicators shall identify measurement or calculation methods. The organisation shall avoid claiming a universal environmental advantage when results depend on transport, service life, energy source or allocation choices.

Priority actions shall consider prevention of wrong part returns, avoidable damage, excessive packaging, obsolete inventory and unnecessary disposal. Remanufacture and reuse shall preserve technical safety gates. Emissions or waste improvements shall not be achieved by shifting uncontrolled hazards to recovery workers or downstream communities.

29.4 Waste and recovery controls

Waste, cores and reusable products shall be correctly distinguished under applicable requirements. Transfers shall use competent authorised recipients and retain quantity and disposition evidence. The organisation shall assess risks of illegal export, informal hazardous processing and unsafe reentry into the market.

30 Continuity resilience and obsolescence

30.1 Business impact assessment

The organisation shall identify critical dependencies in supply, warehousing, transport, data, personnel, utilities and product support. It shall assess disruption scenarios including fire, flooding, extreme heat, cyberattack, border interruption, supplier failure and service provider withdrawal. Recovery priorities shall protect people and preserve product integrity.

Continuity plans shall identify decision makers, communications, alternate sites or sources, recovery objectives and the evidence required before restart. Alternative supply shall pass normal technical and source gates. Emergency demand shall not permit unverified safety substitutions.

30.2 Product and digital obsolescence

The organisation shall monitor source discontinuation, component scarcity, material changes and software support end dates. It shall notify affected business customers of material support limitations and maintain a documented plan for stock, substitutes, tooling or controlled redesign where justified.

Long term stock shall be assessed for ageing and continued legal or configuration suitability. Purchasing a lifetime quantity shall not create a lifetime fitness claim. Essential digital records, keys and activation dependencies shall have continuity arrangements proportionate to the supplied function.

30.3 Recovery verification

Restart after disruption shall verify stock condition, current product restrictions, system reconciliation and competence availability. Backlogged orders shall be checked against updated hold status before dispatch. Tests of continuity arrangements shall identify what was actually exercised and what remains unproven.

31 Competence worker safety and measurement

31.1 Role competence

The organisation shall define competence for purchasing, data publication, inspection, release, handling, sales advice, installation support and incident response. Competence shall include relevant products, hazards, methods, legal responsibilities and escalation. Training attendance alone shall not demonstrate the ability to perform a critical task.

Authorisation for R3 and R4 decisions shall require demonstrated technical capability. Practical observation, supervised work and assessment of representative cases shall be used as appropriate. Temporary workers and contractors shall receive controls equivalent to those required for the tasks they perform.

31.2 Safe work and facilities

The organisation shall assess occupational risks including lifting, racking, vehicles, machinery, chemicals, stored energy, electrical work and fire. Competent persons shall define safe procedures, equipment and emergency arrangements. Staff shall be permitted to stop unsafe work without commercial penalty.

High voltage, pyrotechnic, pressurised and damaged energy products shall be handled only by specifically authorised personnel within suitable facilities. This document shall not be used as a practical dismantling or emergency response instruction. The organisation shall maintain product and site specific procedures developed by qualified persons.

31.3 Equipment and measurement validity

Inspection and test equipment shall be suitable for the range, resolution and uncertainty needed for the decision. Calibration or verification shall have a documented metrological basis, interval and status. Reference items and software based measuring tools shall be controlled against deterioration and unauthorised changes.

When equipment is found unsuitable, the organisation shall assess previous decisions made with it, identify potentially affected product and take containment action. Adjusting the device alone shall not close the issue. Records shall identify equipment, result, reference, date and authorisation.

32 Monitoring audit and improvement

32.1 Performance monitoring

The organisation shall monitor the indicators in Annex I where applicable and establish justified objectives for additional risks. Metrics shall use defined populations, periods and denominators. Results shall be segmented where necessary by risk class, site, supplier, product family and sales channel.

Uncertainty, missing data and small samples shall be visible. A zero incident count shall not be treated as proof of safety without considering exposure and reporting capability. Incentives shall not discourage recording complaints, returns, holds or near misses.

32.2 Internal audit

An internal audit programme shall cover all applicable requirements, profiles, sites and outsourced critical interfaces within each twelve month period. Sampling within processes may be risk based. Auditors shall be competent and sufficiently independent of the work assessed; small organisations may use competent external auditors.

Audits shall follow actual products and transactions through source approval, evidence, listing, custody, sale and response. They shall include negative tests, such as an attempted purchase of held stock, and shall protect live operations from unintended release or customer contact. Document review alone shall not establish operational effectiveness.

32.3 Corrective action and management review

Nonconformities shall identify the requirement, objective evidence, affected scope and significance. The organisation shall contain the issue, determine cause, correct the system and verify effectiveness. Training shall not be accepted as the sole corrective action when system permissions, unclear specifications or incentives caused the failure.

Top management shall review performance, incidents, audits, supplier issues, changing risks, resource adequacy and improvement at least annually. Additional review shall follow a major integrity failure. Decisions shall identify owners, due dates and evidence of completion.

33 Conformity evaluation and claims

33.1 Object of evaluation

Evaluation shall identify the legal entity, sites, channels, activities, product families, condition categories, markets, risk classes and document version assessed. A process or network evaluation shall not be represented as product certification. Where only part of an organisation is assessed, claims shall make that boundary clear.

This draft permits internal gap assessments and controlled pilot evaluations only. Public certification, registration or conformity marks shall require IAF to adopt the relevant standard and authorise an operational scheme. A trial report shall state that it evaluates Working Draft 0.1 and shall not imply an approved certification outcome.

33.2 Evidence and decision

Assessment shall combine document review, observation, interviews, transaction tracing, data verification and operational challenge tests. The assessor shall apply Annex H, including profile coverage and critical gates. Remote methods shall be used only where they provide reliable evidence of the matter assessed.

Each finding shall be classified as critical, major or minor under Annex H. A positive conformity conclusion shall require fulfilment of all applicable requirements and verified closure of nonconformities within the claimed scope. No numerical average, membership status or commercial relationship shall compensate for a failed requirement.

33.3 Claims after scheme adoption

If an operational scheme is adopted, a claim shall state its object, scope, applicable edition and verifiable current status. Product labels shall not carry a network conformity statement in a form that suggests individual product approval. Statements such as globally approved, legally accepted everywhere or safe in every vehicle shall be prohibited unless independently established for the exact claim.

Suspension, restriction and withdrawal shall be communicated to affected parties and reflected in any public status record. The claim holder shall remove misleading claims promptly and maintain responsibilities for previously supplied products. Clause 36 defines the proposed scheme governance requirements.

34 Change control and future technology

34.1 Change assessment

Changes to product design, material, manufacturing site, source, software, packaging, fitment data, identifiers, systems or distribution routes shall be reviewed before implementation. The review shall identify affected evidence, risk classification, legal obligations, inventory, customer information and necessary revalidation.

The organisation shall distinguish administrative corrections from changes affecting product safety or application. An unchanged commercial part number shall not prevent revision control. Old and new configurations shall remain identifiable where interchangeability or recall boundaries differ.

34.2 Artificial intelligence and automation

Automation used for sourcing, fitment, authenticity assessment, release advice or customer instructions shall have a defined intended use, accountable owner and validation plan. The plan shall address false acceptance, missed restrictions, incomplete inputs, out of distribution cases and model or data changes. Performance shall be evaluated on representative configurations, including known difficult negative cases.

Safety relevant outputs shall be linked to verifiable controlled evidence and shall support abstention and human escalation. A probabilistic confidence score shall not replace mandatory identity, fitment or release evidence. Unvalidated model changes shall not enter production decision paths.

34.3 Connected monitoring and autonomous distribution

Condition sensors and predictive alerts shall have defined accuracy, limitations, maintenance and missing data behaviour. A sensor reading shall be evaluated against product specific acceptance criteria. Loss of a signal shall not silently be treated as acceptable condition.

Autonomous warehouses, delivery systems and agent initiated purchasing shall preserve authorised decisions, custody, hold enforcement and human intervention. The organisation shall test misrouting, duplicate orders, stale data and emergency stop behaviour. Automated speed shall not reduce the evidence required to release a product.

34.4 Emerging architectures

For novel battery chemistries, new energy carriers, software defined components and future vehicle interfaces, the organisation shall use the same hazard and evidence principles before supply. A technology readiness label shall not be treated as proof of suitability. Annex K sets out proposed development directions without asserting dates of universal adoption or guaranteed performance.

35 Implementation and transition

35.1 Implementation baseline

An organisation starting implementation shall map its products, roles, sites and critical hazards, establish the applicability register and perform a documented gap assessment. It shall prioritise immediate control of unknown sources, unsafe stock, unresolved recalls and missing critical fitment evidence. A phased programme shall state responsibilities, resources and milestones.

Incomplete implementation shall be described as such. A project plan, training completion or installed software shall not justify a conformity claim. Critical safety controls shall operate before the affected product is supplied under any declared pilot scope.

35.2 Legacy inventory and records

Legacy stock shall be assessed for identity, source, condition, technical evidence and market eligibility. Missing information may be recovered through verified records or competent examination. It shall not be invented or inferred solely to populate a mandatory field.

Legacy R3 and R4 products lacking evidence needed to support safety or identity shall remain on hold or move to an authorised nonservice disposition. Lower risk stock shall still meet its applicable gates. Transition periods shall not authorise sale of known unsafe or prohibited products.

35.3 Evidence of readiness

Readiness shall include approved suppliers, completed technical files, validated data, effective stock controls, trained personnel, a completed traceability exercise, tested incident communication and corrective action closure. The organisation shall conduct an internal review before inviting external evaluation.

Once IAF adopts an edition, any transition arrangements shall identify the previous and new requirements, effective dates and treatment of existing claims. Those arrangements shall be issued by IAF rather than invented by individual claim holders. Urgent safety changes may require immediate action independent of an administrative transition period.

36 Proposed scheme governance

36.1 Technical stewardship

Before operating an IAF PARTS conformity scheme, IAF shall approve its rules, competence criteria, decision process, complaints route and public claim conditions. Standard development shall include technically diverse participation from manufacturers, independent distributors, repairers, digital channels, recovery businesses and users without allowing one commercial interest to control decisions.

The technical process shall record proposed changes, evidence, conflicts of interest, consultation outcomes and reasons for acceptance or rejection. Product specific supplements shall identify their scope and relationship to this standard. A supplement shall not quietly remove a core critical gate.

36.2 Assessment impartiality and appeals

Assessment personnel shall demonstrate relevant product and process competence and disclose conflicts. Commercial staff shall not make conformity decisions on their own clients. The decision function shall be independent of the evaluation activity and shall have access to sufficient evidence to challenge findings and scope.

Applicants shall have a documented route to appeal decisions and complain about conduct. Appeals shall be reviewed by competent persons not responsible for the original contested decision. An appeal shall not automatically lift a justified safety suspension or prevent required protective action.

36.3 Surveillance and transparency

The adopted scheme shall publish how status is granted, maintained, restricted, suspended and withdrawn. It shall establish surveillance based on product risk, changes, complaints and performance. Annex H proposes assessment intervals for validation before launch; no certificate duration is established by this working draft.

The scheme shall maintain a verifiable status record containing only necessary scope and status information. It shall distinguish organisation conformity, individual product evaluation and membership. Fees shall be transparent and shall not determine technical outcomes.

36.4 Review and urgent revision

IAF shall establish review triggers for emerging failure patterns, new vehicle architectures, regulatory changes, new evidence and stakeholder feedback. Urgent changes shall include rationale, affected scopes, effective dates and implementation guidance. Claims of global suitability shall be supported by representative validation across regions, business sizes and technology profiles.

Before adoption, the validation agenda in Annex L shall be completed or each unresolved matter shall be explicitly resolved by an authorised technical decision with supporting evidence. Publication shall identify residual limitations and a process for ongoing correction.

Annex A Product risk classification

Normative

A.1 Severity floors and minimum controls

The following classes are minimum severity based categories. Examples illustrate possible classification in ordinary applications; the actual application and foreseeable failure shall determine the final class. A product shall be escalated when integration creates a more severe consequence.

Class	Credible consequence and examples	Minimum assurance and identity
R1	Limited loss of appearance or convenience without a credible safety effect; some decorative items	Approved source, defined acceptance criteria, receipt and transaction traceability; lot or equivalent source population where available
R2	Material functional failure, vehicle downtime, substantial loss or environmental release without the R3 or R4 severity; some noncritical accessories	Applicable dossier, source and batch traceability, functional verification plan, controlled condition and fitment
R3	Serious injury potential, road safety degradation or significant compliance failure; many lighting, tyre, steering, braking and driver assistance applications	Technical release, batch traceability at minimum and unit identity where needed to isolate harm; validated critical characteristics and urgent recall capability

Class	Credible consequence and examples	Minimum assurance and identity
R4	Credible fatal or catastrophic failure, uncontrolled high energy event or systemic compromise of a critical function; pyrotechnic restraints, traction batteries and selected critical control or pressure applications	Persistent individual identity, independent technical release review, strong source and process evidence, enhanced security and twice yearly recall exercises

“Independent technical release review” means a competent reviewer separate from the commercial purchase approval and from the unsupported claim being accepted. It need not be an external certification service. Product classification shall not depend solely on the category examples above.

A.2 Mandatory risk record

The risk record shall contain: product and application; intended function; failure or misuse scenario; severity basis; exposure and uncertainty; safety related interfaces; counterfeiting and source risks; storage and transport hazards; software dependencies; selected class; required controls; assessor; approver; and review triggers.

Where a numerical scoring tool is used, the organisation shall retain the severity floor. Multiplication of low probability or high detectability scores shall not reduce an R4 credible consequence to a lower class. Risk controls shall be evaluated individually for effectiveness and shall not be assumed independent when they share a common data source.

A.3 Additional identity rules

Individual identity shall be required regardless of the general class for individually traded traction packs and modules, programmable safety units where version history is necessary, and recovered R3 or R4 products whose unit history determines acceptance. Bulk consumables shall retain batch identity through repacking and dispensing. The receiving transaction shall identify the dispensing batch or bounded batch population.

For an R1 item without an original batch, the organisation shall create a receipt population identifier linked to source, date and quantity and shall disclose the limitation. This allowance shall not apply when safety, law or the product’s assurance plan requires finer traceability.

Annex B Functional applicability profiles

Normative

B.1 Core and triggered requirements

All organisations shall apply Clauses 1 to 6, 10 to 13, 27 to 35 and relevant normative annexes to their declared activities. Clause 36 applies to an operator of the proposed conformity scheme. The table identifies additional direct responsibilities; it does not create exclusions from requirements triggered by actual activities or hazards.

Profile	Typical role	Additional responsibilities
P1	Manufacturer supplying the aftermarket or own brand operator	Clauses 7 to 9 and 14 to 18; product dossier, production link, claims and source change control

Profile	Typical role	Additional responsibilities
P2	Importer broker or buying group	Clauses 7 to 9 and 17 to 18; destination eligibility, evidence access and actual source verification
P3	Wholesaler distributor or warehouse	Clauses 7 to 9 and 14 to 18; receipt, preservation, release and downstream traceability
P4	Retailer or direct online seller	Clauses 7 to 9, 14 to 19 and 26; product information, fitment, transaction and remedy
P5	Marketplace or remote fulfilment coordinator	Clauses 7 to 9 and 18 to 19; seller controls, release assurance, transaction identity and safety takedown
P6	Carrier or logistics provider	Clauses 14 to 17; receipt at custody boundary, preservation, dangerous goods and exception evidence
P7	Franchise or network controller	Clause 20 plus every activity under central control; scope accuracy, common rules and network containment
P8	Dismantler recycler repairer or remanufacturer	Clauses 7 to 9, 14 to 18 and 24 to 26; donor or core history, transformation and verified condition
P9	Parts data or digital service provider	Clauses 11 to 13 and 19 where relevant; source evidence, data validation, version control and propagation
P10	Installation or activation interface provider	Clauses 14, 21, 23 and 26 as applicable; receipt, configuration, completion evidence and feedback

Clauses 22 to 25 apply to any profile handling the relevant high energy, electronic, recovered or specially manufactured product, whether or not the organisation performs the underlying manufacturing operation. A retailer can obtain technical evidence from a competent supplier; it shall verify applicability rather than reproduce all manufacturing tests itself.

B.2 Outsourcing responsibility

For each outsourced critical activity, the applicability register shall identify who performs the task, who approves it, who retains evidence and who acts on an incident. The organisation shall demonstrate access to records within the required response time. A contract without verified operational access shall not fulfil this requirement.

Annex C Minimum product and transaction data

Normative

C.1 Data rules

“All” below means required for every product record within scope. “Triggered” means mandatory when the stated condition exists. Empty fields shall not be used to imply that a check was completed. A not applicable value shall have an approved reason; an unknown value shall have a gap owner and shall prevent release when the missing value is safety critical.

Field group	Applicability	Minimum content
Record identity	All	Persistent record identifier, schema version, revision, owner and update time
Product identity	All	Manufacturer or responsible operator number, seller code, revision and readable description
Responsible operator	All	Legal identity, product responsibility role and contact route
Actual source	All	Supplier identity, approved scope and source evidence; factory or remanufacturing site for R3 and R4
Condition	All	New, used, repaired, refurbished, remanufactured or core; assessment basis
Risk	All	R1 to R4, assessment reference, reviewer and critical attributes
Origin claims	All where made	Declared origin and supporting evidence, with origin distinguished from shipping location
Lot and serial	Annex A	Original and supplementary identifiers, relationship and issuer
Market eligibility	All	Permitted destinations, vehicle or use restrictions and applicable evidence
Vehicle fitment	Application specific products	Configuration qualifiers, installation position, evidence and exclusions
Dimensions and ratings	Where needed for selection or safety	Values, tolerances, units and controlling specification
Supersession	Replacement relationship	Predecessor, successor, direction, conditions and kit or software dependencies
Technical evidence	All	Dossier or approved acceptance specification, version and retrieval route
Legal evidence	Where required	Applicable approval or declaration, scope, limitations and validity assessment
Installation	Where required	Instruction version, tools, coding, calibration, consumables and competent installation needs
Life information	Life sensitive items	Manufacture date, expiry, opening date, extension basis and limitations
Storage and transport	All	Required conditions, hazards, packaging and excursion assessment rules
Chemical information	Chemical or material hazard	Substance restrictions and accessible safe handling information

Field group	Applicability	Minimum content
Hardware and software	Programmable or connected items	Versions, dependencies, activation state, supported combinations and update history
Digital support	Dependent functionality	Support period or end date, essential service and entitlement restrictions
Energy product data	Clause 22	Chemistry or energy medium, ratings, identity, condition, diagnostic method and relevant history
Recovered history	Clause 24	Donor or core link, known use and damage, inspection, process and replaced critical items
Custom manufacturing	Clause 25	Design authority, file revision, material, process, build identity and verification
Environmental claims	Where made	Functional basis, boundary, data quality, allocation and verification evidence
Current status	All	Release, restriction, hold, recall or final disposition and authorising record
Custody event	Every custody transfer	Event identity, time, source, destination, item population, quantity and responsible party
Transformation event	Every transformation	Input and output identities, quantities, process version, operator and disposition
Sale link	Every sale	Order or receipt token, actual product supplied, date, recipient record where lawful and fulfilment route
Evidence provenance	Safety relevant fields	Source, assertion or verification state, version, approver and correction history

C.2 Controlled values and validation

Condition, lifecycle status, risk class and verification state shall use controlled values. Numeric fields shall distinguish zero from unknown, include units and reject impossible ranges. Date fields shall distinguish production, receipt, release, expiry and update dates. Mandatory fields shall be validated before publication or release.

An export shall preserve data relationships and restrictions. Commercial cross references may remain proprietary, but records required to establish safety, legal eligibility and incident populations shall be accessible to authorised reviewers under suitable confidentiality controls.

C.3 Data quality challenge cases

The organisation shall test at least: a leading zero in a part number; conflicting voltage variants; opposite installation positions; a superseded part requiring a kit; expired stock; a reused serial; an unknown software version; a recalled lot offered under a second seller code; and a safety field changed while an order is open. Each case shall produce the expected restriction or escalation.

Annex D Lifecycle states and events

Normative

D.1 State model

Product condition and lifecycle status shall be separate fields. A new part may be recalled, and a remanufactured part may be released. Systems shall not infer release solely from condition, location, ownership or payment.

State	Permitted purpose	Required control before next state
Pending receipt	Record delivery and initial screening	Match source, order, identity and required documents
Under review	Inspection or technical assessment	Complete evidence and authorised disposition
Released	Permitted supply within stated scope	Live hold check at allocation and dispatch
Restricted	Specifically approved limited lawful use	Visible restriction, authorised recipient and evidence; no unresolved safety concession
Quarantined	Secure hold pending investigation	Competent documented resolution before any release
Recall blocked	Stop supply and perform corrective action	Verified remedy and authorised decision; no automatic expiry
Dispatched	Controlled transfer underway	Recipient or delivery exception record
Supplied	Product handed to customer or business recipient	Retain traceability and safety communication capability
Return pending review	Returned product awaiting assessment	Identity and condition verification before restocking
Transformation in progress	Controlled repair remanufacture or repacking	Parent and child reconciliation plus new release evidence
Retired or destroyed	No further installation or supply permitted	Final disposition evidence and prevention of identity reuse

D.2 Event validity

Each status change shall carry event identity, time, actor, reason, evidence and affected population. Only authorised roles shall change release or hold status. A purchase, refund, stock transfer, label reprint or database synchronisation shall not remove a hold.

The system shall reject impossible transitions or route them to authorised review. It shall test concurrent orders against a new hold, duplicate messages, late arrival of a previous released status and attempted reuse of a retired serial. A newer safety hold shall take precedence over a delayed older release message.

D.3 Physical and digital reconciliation

Digital state shall correspond to physical access and handling. The organisation shall test whether staff can pick or dispatch quarantined stock despite the displayed status. Physical products without a reliable digital match, and digital records without the expected physical stock, shall be investigated rather than silently corrected.

Where a supplied product is later recalled, the supplied event shall remain in history while recall status becomes current. A remedy shall identify the action performed and any new configuration or identity. Historical events shall not be deleted to make the record appear continuously conforming.

Annex E Product verification planning matrix

Normative

E.1 Use of the matrix

The matrix defines subjects to consider, not a universal laboratory test programme. For every applicable row, the product assurance plan shall define the failure mechanism, sample configuration, conditioning, method, quantitative acceptance limit, uncertainty treatment and evidence owner. Where a subject is not applicable, the technical reason shall be recorded. More specific hazards shall be added.

Product group	Verification subjects	Release evidence to identify
Braking and hydraulic parts	Pressure integrity, leakage, output consistency, thermal duty, wear, fluid compatibility and installation interfaces	Applicable ratings, tested configurations, critical dimensions and life restrictions
Steering suspension and load carrying parts	Geometry, strength, fatigue, joint integrity, corrosion, articulation and fastening interfaces	Load case basis, material and process evidence, installation requirements
Tyres wheels and wheel attachments	Size and load suitability, speed and use restrictions, structural integrity, mounting and ageing	Exact application, ratings, production identity and condition assessment
Restraints and pyrotechnic products	Identity, system compatibility, deployment related evidence, environment and controlled handling	Verified source, individual identity, applicable system evidence and restrictions
Body glazing and closures	Fit, load paths, visibility, latching, attachment, impact related interfaces and sensor effects	Dimensions, materials, relevant integration evidence and installation details
Lighting and signalling	Light output, colour, distribution, aiming, thermal behaviour, sealing and electrical interaction	Market eligibility, variant identity, measured performance and aiming needs
Filters and fluid system parts	Filtration or flow, pressure drop, leakage, burst resistance, cleanliness and chemical compatibility	Medium, operating envelope, performance results and change intervals where claimed

Product group	Verification subjects	Release evidence to identify
Belts chains bearings and rotating parts	Geometry, load and speed capability, wear, lubrication, noise and durability	Material and dimensional evidence, installation conditions and service limitations
Fluids lubricants adhesives and sealants	Composition related claims, functional performance, compatibility, contamination, ageing and handling hazards	Batch evidence, shelf life, application restrictions and safe use information
Exhaust and emissions related parts	Flow, thermal endurance, leak tightness, sensor interactions and continued required function	Market and application evidence, operating limits and installation requirements
Electrical wiring connectors and fuses	Conductor capacity, insulation, temperature rise, contact performance, protection and environmental sealing	Ratings, termination requirements, electrical evidence and variant distinction
Sensors control units and connected devices	Accuracy, calibration, latency where relevant, electrical immunity and emissions, software and integration	Hardware and software versions, acceptance results and dependency map
Traction batteries and power conversion	Electrical and thermal compatibility, protective behaviour, isolation, condition, interfaces and fault response	Unit history, applicable safe test evidence, support and handling restrictions
Hydrogen and pressure components	Material compatibility, pressure containment, leakage, fatigue, connection integrity and life restrictions	Rated conditions, production identity, inspection and replacement limits
Interior accessories and retrofit equipment	Retention, visibility, distraction, flammability where relevant, electrical load and interference with safety functions	Application, attachment method, required checks and limitations
Recovered and remanufactured products	Incoming history, damage and wear, controlled restoration, critical replacements and final function	Unit or core links, process record, measured acceptance and disclosed condition
Additive and custom products	Design basis, material condition, process capability, internal defects, anisotropy, dimensions and durability	Approved file, build and material identity, post processing and validated scope

E.2 Minimum verification plan record

The plan shall state the part family and variants; intended applications and markets; drawings or interfaces; hazards and critical characteristics; limits with their technical basis; test method and edition or internal revision; sampling unit; population and selection method; conditioning; equipment and competence; pass and fail rules; treatment of uncertainty; report format; and release authority.

The plan shall identify which characteristics require every unit verification, which are assured by validated production controls and which require periodic or change triggered tests. A claim that testing is unnecessary shall identify the alternative evidence and demonstrate why it addresses the same failure mechanism.

E.3 Technical report acceptance

The receiving reviewer shall verify that the tested item represents the supplied item, including site, material, geometry, software and condition. Report authenticity shall be checked where risk warrants. Evidence shall be rejected when the sample cannot be identified, acceptance limits are missing, results contradict the conclusion or important deviations are unexplained.

An approval shall identify the exact scope and any outstanding nonsafety limitations. A product failing a critical characteristic shall remain on hold. Repeated testing shall not be used to select only favourable results; failed and repeated results shall remain in the dossier with their investigation.

Annex F Sampling and decision rules

Normative

F.1 Separate purposes

The organisation shall distinguish supplier qualification, product validation, incoming lot acceptance, process monitoring and audit sampling. A sample size suitable for one purpose shall not be transferred to another without justification. This annex does not establish a universal acceptable defect rate for automotive parts.

Every plan shall define its population, sampling unit, selection method, characteristics, acceptance and rejection rules, escalation and treatment of detected defects. The lot shall be sufficiently homogeneous for the proposed inference. Different sources, revisions, conditions or unknown identities shall not be combined merely to reduce sample size.

F.2 Mandatory gates

Identity, current safety status and required release evidence shall be checked for every transaction and applicable handling unit. Known critical defects have zero acceptance for release: finding one requires containment of the affected population and technical investigation. Zero acceptance of detected critical defects does not imply that a finite sample proves zero defects in the population.

For critical characteristics requiring every unit verification by the approved technical plan, sampling shall not replace that verification. Where every unit testing is destructive or technically inappropriate, the plan shall justify the process controls, representative tests and evidence needed to manage residual risk.

F.3 Illustrative detection planning values

The following values support planning only. They assume independent random sampling from a large stable population, consistent defect probability and perfect detection of the chosen defect in a sampled unit. The actual organisation shall justify whether those assumptions apply and select a plan appropriate to the hazard.

Hypothetical defect prevalence	Random samples needed for at least 95 percent chance of finding one or more	Interpretation
10 percent	29	Detection planning for a common defect; not evidence of low residual defect risk
5 percent	59	Detection planning for the stated prevalence and assumptions

Hypothetical defect prevalence	Random samples needed for at least 95 percent chance of finding one or more	Interpretation
1 percent	299	Detection planning requiring much larger coverage for rarer defects

The probability of missing all defects equals the probability of selecting a nondefective unit raised to the number of independent samples. For a finite lot sampled without replacement, the organisation shall use an appropriate finite population calculation. Clustering, deliberate fraud, imperfect tests or biased selection can invalidate the values above.

F.4 Selection and escalation

Samples shall be selected by a method preventing supplier or operator selection of only favourable items. Selection shall span relevant cartons, production periods, shifts or source subgroups. The organisation shall retain sample identities and results, including rejected and damaged samples.

Evidence of instability, source change, repeated defects or false documents shall increase verification and may require supplier suspension. Reduced inspection shall require documented stable performance and shall be reversed when its conditions cease. Rejected lots shall not be relabelled or repeatedly resampled into acceptance without an approved corrective process.

F.5 Decision near a limit

The decision rule shall state how measurement uncertainty and borderline results are treated. Results for a critical characteristic whose uncertainty prevents a justified pass shall not be released as unconditionally conforming. The organisation shall obtain better evidence, apply a conservative documented rule or hold the affected product.

Annex G Incident response and recall verification

Normative

G.1 Proposed response limits

These limits are proposed maximum internal control times for pilot validation. They apply from first receipt of credible information that a product may cause serious harm or has a critical integrity failure, unless a row states a different start event. They do not establish legal deadlines. Immediate protection and earlier applicable legal duties take precedence.

Action	Maximum proposed elapsed time	Completion evidence
Escalate to the accountable safety role	1 hour	Named recipient, timestamp, affected product and initial concern
Enforce precautionary sales and dispatch block	1 hour	All controlled channels blocked; manual shutdown where electronic control fails

Action	Maximum proposed elapsed time	Completion evidence
Alert responsible upstream and downstream business partners	4 hours	Affected known partners contacted with hold instructions and acknowledgement request
Retrieve initial affected R3 or R4 population	4 hours	Available stock, transactions, recipients and known gaps; broader hold where uncertain
Complete initial competent risk review	24 hours	Written action decision, notifications, population assumptions and owner
Reconcile a complete operational traceability extract	24 hours	Known quantities and unit links reconciled, unresolved gaps separately identified
Begin direct safety notification to identifiable affected customers	24 hours after a decision that notification is required	First notifications issued and remaining population scheduled; sooner for imminent harm
Propagate a confirmed critical catalogue correction	4 hours after approval of the correction	Controlled channels updated or affected offers remain blocked
Reassess unacknowledged critical partner alerts	4 hours after dispatch of the alert	Alternative contact or escalation and continued supply restriction

The organisation shall act on credible preliminary information and shall not postpone the starting time by delaying internal registration. When a deadline is missed, it shall record the actual time, cause, additional protection and corrective action. If a complete population cannot be established, the report shall say so and maintain conservative containment.

G.2 Exercise design

The exercise controller shall select a real historical part population and add a simulated safety concern. Selection shall rotate through product classes, sites, channels and suppliers. R4 exercises shall include unit identity. At least one exercise in each twelve month period shall include a deliberately incomplete record or unavailable responsible person.

The exercise shall test source identification, available and supplied stock, all sales channels, a partner response route, customer contact logic, quantity reconciliation and hold effectiveness. Live external messages shall only occur under a previously authorised exercise arrangement. Test data shall not contaminate actual product status after the exercise ends.

G.3 Pass criteria and quantities

An exercise passes only when all affected simulated stock and offers are blocked within the defined time; every sampled unit or lot can be traced to its source and actual transaction; required recipients or lawful contact alternatives are identified; quantities reconcile; and every data gap is explicitly reported and contained. An identified gap is good reporting but is not itself a passing traceability result.

For quantity reconciliation, the total received or created quantity shall equal the sum of quantities currently held, supplied and not returned, consumed in documented transformations, destroyed, sampled or otherwise disposed, adjusted for verified returns and linked transformations without double counting. Each quantity shall carry its unit of measure and evidence. Unexplained variance is a failed exercise objective.

G.4 Scenario library

The organisation shall select relevant cases from: a critical supplier lot alert; a recalled unit returned and relisted; a wrong vehicle fitment rule; a duplicate serial; a compromised software package; a marketplace seller leaving during a recall; a battery incident with uncertain history; a source plant change; and a cyber outage during urgent withdrawal. Scenarios shall become more demanding when repeated exercises show stable basic capability.

G.5 Notice and closure content

A safety notice shall include case identifier, issue date, responsible operator, affected identifiers and images where useful, risk, immediate customer action, remedy, contact method and update route. A closure record shall identify the affected population, actual remedies, unresolved exposure, ongoing restrictions, cause, verified corrective action and approval. Confidential investigation detail may be protected without withholding essential customer safety information.

Annex H Assessment and critical gates

Normative

H.1 Assessment stages

The assessment process shall establish scope and applicability, review documented readiness, evaluate operations, trace transactions, perform controlled challenge tests, record findings, review corrective evidence and make an independent decision. Each stage shall retain its evidence and limitations. A desktop review may establish readiness but shall not alone establish operating conformity.

H.2 Critical gates

Gate	Required outcome	Example of a critical failure
G1 Source and authenticity	Critical products have verified source and identity	Known counterfeit or unresolved critical source identity released
G2 Technical assurance	Critical application and characteristics have applicable evidence	Safety product released with missing or contradicted essential technical evidence
G3 Fitment and configuration	Safety relevant selection and dependencies are verified	Known incompatible safety part represented as suitable
G4 Hold enforcement	A hold prevents supply through all controlled channels	A known dangerous or recalled product remains purchasable or dispatchable
G5 Traceability	Affected critical populations can be bounded and retrieved	Lost R4 identity makes effective containment impossible
G6 Condition and handling	Hazards and product deterioration are controlled	Known dangerously damaged energy product returned to ordinary sale
G7 Digital integrity	Safety relevant data and software are controlled	Unauthorised safety software or falsified release data supplied
G8 Honest claims and escalation	Claims match evidence and credible hazards are acted upon	Concealed severe defect or deliberately false conformity evidence

The examples are not exhaustive. Critical classification shall depend on evidence of severe risk, deliberate deception or inability to prevent serious unsafe supply. The assessor shall record the technical rationale and affected scope.

H.3 Finding classes and decisions

A critical nonconformity is a failure causing or credibly enabling severe unsafe supply, defeating essential containment, or deliberately falsifying material evidence. It requires immediate protective action and prevents a positive decision for the affected scope. Where the failure is systemic, the affected scope shall include all dependent activities.

A major nonconformity is a missing or ineffective required process, a significant repeated failure or an evidence gap that prevents confidence in fulfilment but is not classified as critical. A minor nonconformity is an isolated lapse with limited effect where the required process remains demonstrably effective. An observation is an improvement opportunity where no requirement has been shown to fail.

A positive conclusion shall require verified closure of all nonconformities within the claimed scope. The decision record shall identify residual limitations and approved nonapplicability. A numerical maturity score may support improvement planning but shall be reported separately and shall never override conformity findings.

H.4 Scope sampling and multisite evaluation

Initial evaluation shall include every distinct activity and hazard profile, the central controlling function and every R4 handling or release site. For additional R1 to R3 sites under demonstrably common control, the assessor shall select a documented representative sample covering region, size, process differences, product risk, performance and recent changes. A fixed square root formula alone shall not justify coverage.

The sample shall expand where common control is weak, a significant failure is found or material variation is discovered. Sites outside common control shall require separate assessment. The assessment report shall distinguish visited sites from sites covered through a justified sampling model.

H.5 Proposed ongoing assessment intervals

For validation of a future scheme, the maximum interval between external operational evaluations is proposed as twelve months, reduced to six months for scopes containing R4 supply or significant instability. These are surveillance proposals, not certificate validity periods. The adopted scheme shall validate resources, sampling, effectiveness and affordability before establishing final intervals.

Significant changes, serious complaints, suspected deception or critical incidents shall trigger additional evaluation without waiting for a scheduled visit. Relevant product restrictions shall remain in force until evidence supports lifting them. A commercial renewal payment shall not restore status.

Annex I Performance indicators

Normative

I.1 Measurement principles

The organisation shall calculate applicable indicators at least monthly and review trends and exceptions. For low volumes, a rolling period may supplement monthly values but shall not hide a critical event. Each report shall identify the period, population, data source, exclusions and responsible reviewer.

Indicator	Calculation or measure	Interpretation and control
Source approval coverage	Active supplied product lines from approved sources divided by all active supplied lines	Required release gate is 100 percent; report exceptions individually
Mandatory data completeness	Released records meeting all applicable required fields divided by released records checked	100 percent for checked release population; unknown safety critical fields fail
Critical dossier coverage	Released R3 and R4 records with applicable approved dossiers divided by released R3 and R4 records	100 percent required; report every uncovered record and containment
Traceability success	Challenged populations fully traced within the required time divided by challenged populations	100 percent of exercises required to pass; sample size disclosed
Hold escape count	Units or transactions supplied after an applicable hold should have taken effect	Zero target and immediate investigation of every escape

Indicator	Calculation or measure	Interpretation and control
Fitment error rate	Confirmed organisation caused wrong fitment order lines divided by fulfilled application specific lines	Separate safety severity and root cause; do not mix with unrelated customer returns
Provenance exception count	Unresolved source or identity concerns by product class	No released unresolved safety critical exception; track detection and closure
Receipt discrepancy rate	Receipt lines with identity condition quantity or document discrepancies divided by receipt lines	Separate discrepancy types and supplier causes
Damage rate	Units damaged in controlled storage or transport divided by handled units	Report route and product class and avoid counting one unit repeatedly
Expired stock release count	Units supplied after applicable expiry or unsupported life extension	Zero target and assess every release for safety and customer action
Recall notification coverage	Identifiable affected recipients successfully notified divided by identifiable affected recipients	Distinguish sent, delivered and acknowledged; disclose unknown recipient population
Recall remedy coverage	Affected supplied units with verified remedy divided by affected supplied units requiring remedy	Report unlocated and unresolved units; do not substitute notification rate
Corrective action timeliness	Actions completed by their risk justified due date divided by actions due	Report critical and major overdue actions separately
Critical data propagation time	Elapsed time from approval of a critical correction to effective channel update or block	Compare with Annex G; report slowest channel and failures
Support coverage	Supported software dependent products divided by active supplied software dependent products	Disclose ended support and customer impact; no false continuing support claim
Core recovery yield	Accepted output units from a defined core cohort divided by assessed core units	Separate reuse, remanufacture, component recovery and disposal outcomes
Packaging intensity	Packaging mass divided by shipped product mass or another declared functional unit	State boundary and compare like products and routes

I.2 Interpretation safeguards

For required 100 percent coverage indicators, a sampled audit result shall be described as sample coverage and shall not be claimed as proof of the entire population. The organisation shall use system controls and reconciliation to support population level claims. A zero denominator shall be reported as not applicable for the period, not as zero performance or 100 percent success.

Commercial performance indicators such as delivery speed or return cost shall be reviewed alongside safety and integrity measures. A reduction in complaints achieved by restricting reporting access is not

improvement. Targets without universal limits in this table shall be risk justified locally and shall not be advertised as requirements of IAF PARTS.

Annex J Implementation forms and worked examples

Informative

J.1 Applicability and responsibility worksheet

An implementation team can use the following record for each requirement. Repeating the record as a form is preferable to compressing long evidence descriptions into a wide spreadsheet printed at an unreadable size.

Requirement identifier: [enter clause or annex]. Activity and product profile: [enter]. Applicable sites and channels: [enter]. Risk class or trigger: [enter]. Accountable owner: [enter]. Performing party: [enter]. Evidence location and version: [enter]. Current status: [implemented, gap or not applicable]. Justification for any nonapplicability: [enter]. Action and due date: [enter]. Reviewer and review date: [enter].

J.2 Supplier approval worksheet

Supplier legal identity and address: [enter]. Trading and payment verification: [enter]. Actual product source and facility: [enter]. Product families and markets requested: [enter]. Risk classes: [enter]. Technical evidence reviewed: [enter]. Facility or process assessment: [enter]. Traceability and recall capability: [enter]. Change notification arrangement: [enter]. Open concerns: [enter]. Approved scope and restrictions: [enter]. Decision, approver and review date: [enter].

Suggested review questions are: Can the supplier connect routine deliveries to the approved source? Can it retrieve affected populations? Does it report changes before shipment? Can it provide actual critical results rather than only a logo or declaration? What happens when the ordinary contact is absent?

J.3 Product assurance and release worksheet

Product and revision: [enter]. Actual source: [enter]. Condition category: [enter]. Intended vehicle configurations and markets: [enter]. Risk class and rationale: [enter]. Critical characteristics: [enter]. Acceptance limits and basis: [enter]. Test plan and results: [enter]. Fitment evidence: [enter]. Software and installation dependencies: [enter]. Lot or serial population: [enter]. Storage and life restrictions: [enter]. Active hold check: [enter]. Unresolved gaps: [enter]. Technical release decision and authorisation: [enter].

This worksheet summarises a dossier; it does not replace drawings, underlying reports or controlled instructions. A reviewer should be able to follow each critical claim to its evidence and determine exactly which supplied variants are covered.

J.4 Incident and recall worksheet

Case identifier and first credible receipt time: [enter]. Reporter and contact: [enter]. Product identifiers and suspected population: [enter]. Potential harm: [enter]. Immediate controls and actual times: [enter]. Upstream and downstream contacts: [enter]. Risk assessment owner: [enter]. Customer and authority actions: [enter]. Quantity reconciliation: [enter]. Unlocated or unresolved units: [enter]. Remedy evidence: [enter]. Cause and corrective action: [enter]. Closure basis and approver: [enter].

J.5 Worked example of a critical fitment error

A distributor discovers that a catalogue rule maps a braking component to two vehicle variants, although only one variant is supported by the technical file. The error is credible before any customer reports an accident. The distributor identifies the affected part codes, blocks the unsupported application and related open orders, and checks whether the same rule has propagated to retail and marketplace channels.

The population review includes previous transactions completed while the incorrect rule was active. Technical personnel assess the actual risk and determine necessary customer and authority actions. The corrected catalogue record identifies the valid vehicle configuration and evidence. A test verifies that the invalid configuration is rejected and that a second seller code cannot evade the restriction.

The corrective action investigates why the unsupported relationship entered the catalogue and why publication checks accepted it. Closure depends on controlling prior supply and verifying the corrected process, not only editing the displayed description.

J.6 Worked example of a returned traction module

A retailer receives a traction module returned as unused. Its identifier matches a sale, but the connector condition and diagnostic record indicate possible installation. The retailer places the item on hold, uses the approved energy product handling route and asks competent personnel to assess the conflicting history. A commercial refund may proceed independently of the technical decision.

The module is not placed back into new stock merely because its packaging is intact or a reported state of health appears high. The disposition considers identity, use, exposure, diagnostic limitations, compatibility and the applicable acceptance specification. If the history cannot support safe supply, the item moves to controlled investigation or recovery.

J.7 Worked example of marketplace containment

A marketplace receives a credible recall notice for a lot sold by several sellers. It identifies the actual fulfilment lots, blocks every affected offer and stops open shipments. It searches for duplicate listings and checks whether shared inventory mixed the lot with other sources. Where the physical boundary is uncertain, the hold covers the wider credible population.

Seller suspension does not erase order records. Customer notifications and remedies continue through the marketplace's assigned responsibility model. The completion report distinguishes notices delivered from units actually remedied and preserves unresolved cases.

J.8 Suggested implementation sequence

Phase 1 establishes accountable owners, the scope map, critical stock holds and a usable incident contact route. Phase 2 establishes product risk classification, supplier approval and mandatory data. Phase 3 completes assurance dossiers, fitment control and custody records. Phase 4 tests systems, trains authorised roles and performs realistic recalls and negative transaction tests. Phase 5 closes gaps and submits the defined scope for evaluation when the relevant scheme is available.

The phases are a practical sequence without a fixed completion promise. A small retailer and a multinational network will need different resources. Critical safety controls take effect before affected supply; administrative phasing does not relax them.

Annex K Future development directions

Informative

K.1 Intended contribution

IAF PARTS proposes a continuous evidence chain across physical goods, product data and corrective action. Its distinguishing design choices are application aware release, traceability across condition changes, enforceable marketplace holds, disclosure of software support and inclusion of recovered and newly manufactured alternatives under the same evidence principles.

The following directions are proposals for development and testing. They do not assert that an IAF infrastructure already exists, that a technology will become universal by a particular date, or that any automated system can eliminate defects.

Proposed capability	Automotive benefit to test	Conditions before operational use
Cross network safety status exchange	Faster transmission of recalls and restrictions between otherwise separate systems	Common semantics, authenticated issuers, privacy, failure handling and tested propagation
Portable digital parts passports	Evidence remains accessible after resale, remanufacture or platform migration	Persistent identity, export, protected history and sustainable record ownership
Verified automated fitment	Fewer unsupported vehicle matches and clearer uncertainty handling	Validated configuration data, negative tests, abstention and accountable review
Machine readable release evidence	Faster evidence checks without replacing technical responsibility	Defined evidence scope, revocation, provenance and controls against copied claims
Condition aware distribution	Earlier identification of harmful storage or transport exposure	Product specific limits, reliable sensors and justified disposition methods
Controlled circular identity	Safer recovery and transparent history after repair or remanufacture	Parent and child records, history preservation and verified output specification
Distributed manufacturing assurance	Responsible local production for scarce or legacy parts	Design authority, process equivalence, material control and applicable physical validation
Software support transparency	Clearer purchasing decisions and fewer unsupported replacement functions	Published dependencies, support commitments, transition and secure recovery
Privacy preserving safety contact	Better recall reach with less unnecessary personal data	Lawful purpose, minimal records and tested contact alternatives
Resilient cryptographic identity	Continued verification as security threats and algorithms change	Key lifecycle planning, migration tests and maintained physical evidence links

K.2 Development discipline

Technology trials should compare the proposed method with the current process using defined safety, quality, cost and accessibility measures. Results should include failure cases, false acceptance, false rejection and operational burden. Promising demonstrations should not be advertised as proven global capability before representative validation.

Future versions may add specialised protocols for new energy products, automated vehicle modules, advanced materials and interoperable recall networks. Such additions should preserve the core rule that physical suitability, truthful representation and effective containment require evidence independent of the attractiveness of the technology.

Annex L Technical validation and publication agenda

Informative

L.1 Matters requiring decision before adoption

This working draft is deliberately comprehensive but does not claim that every product specific method or global implementation question has been resolved. The proposed requirements require technical review, legal applicability checks and operational trials. The following agenda defines concrete remaining development work.

Work item	Validation question	Required output before adoption
Risk classes	Do severity floors and examples produce consistent decisions across products and reviewers?	Tested classification cases, resolved disagreements and revised guidance
Product protocols	Are acceptance methods sufficient for the critical product families in the launch scope?	Approved product specific test and evidence protocols with quantitative limits
Response times	Can the proposed one, four and twenty four hour controls work across business sizes and regions?	Timed pilot evidence, justified final limits and realistic staffing assumptions
Record retention	Are five and ten year technical minima proportionate to service life, law and cost?	Documented retention basis and privacy compatible implementation
Unit identity	Can required individual identity survive packaging changes, installation and recovery?	Physical and digital lifecycle trials including identity loss scenarios
Circular parts	Are reuse restrictions and condition definitions clear and technically sufficient?	Product specific acceptance and prohibited reuse decisions
Battery evidence	Can health and history records support the stated release decisions consistently?	Validated methods, uncertainty treatment and safe handling interfaces
Software support	Are support disclosures and secure transfer requirements enforceable in actual supply chains?	Supplier commitments, customer disclosure examples and failure scenarios

Work item	Validation question	Required output before adoption
Data exchange	Can different systems exchange status and history without losing restrictions or privacy?	Interoperability tests, data dictionary refinements and migration results
Sampling	Do plans match actual heterogeneity, detection capability and defect consequences?	Qualified statistical and engineering review of practical plans
Assessment model	Are site coverage, competence and proposed surveillance intervals effective and affordable?	Witnessed pilot assessments, assessor criteria and adopted scheme rules
Market application	Are claims and responsibilities accurate in intended launch jurisdictions?	Market applicability reviews and lawful claim wording
Accessibility	Can smaller firms and limited connectivity sites meet outcomes without excessive dependence on vendors?	Tested manual and digital implementation routes and support materials

L.2 Pilot populations

A useful pilot programme would include independent and manufacturer associated channels; small retailers and large networks; physical and online sales; multiple languages and climates; new and recovered products; high energy and software dependent items; and at least one outsourced fulfilment chain. Participation should be selected to test variation rather than only showcase highly mature organisations.

Pilot evidence should record starting capability, resources, implementation gaps, time to retrieve a population, actual hold effectiveness, data quality, staff usability and adverse effects. No numerical target should be adopted solely because it is easy for one pilot participant to meet.

L.3 Review log and acceptance

Each proposal for revision should identify the clause, issue, evidence, proposed text, affected profiles and safety consequences. Technical decisions should record review participants, conflicts of interest, rationale and dissent requiring follow up. Unresolved critical design issues should remain visible rather than being hidden by a clean publication layout.

Before publication, reviewers should confirm that every requirement has an accountable actor, an observable action or outcome and identifiable evidence; every exception has a bounded justification; all cross references are correct; claims are supportable; and translation preserves technical meaning. The adopted version should retain traceability to this draft through a controlled change record.

L.4 Draft revision history

Version	Date	Development record
Working Draft 0.1	13 September 2026	Initial integrated proposal containing 36 clauses and 12 annexes for consultation and validation

End of working draft