



FIRST EDITION / WORKING DRAFT 0.11

IAF AQMS

Automotive Quality Management System

Requirements for organizations, products,
services, processes and personnel

DRAFT FOR TECHNICAL REVIEW

All fourteen clauses and Annexes A to P are included. Technical review and independent validation remain pending. This is not an approved standard or a basis for issuing an IAF AQMS certificate.

Document control

Field	Entry
Document identifier	IAF AQMS
Intended edition	First Edition
Revision	Working Draft 0.11
Development stage	Stage 11 of a cumulative single-document development process
Language	English
Requirements drafted	Clauses 1 to 14 and Annexes A, F, G, H, I, K and P
Next development work	Conduct sector reviews and pilots; validate scheme operations
Approval status	Technical approval and publication authorization pending

How to use this working document

Read Clause 1 before selecting applicable requirements. Identify the legal entity, sites, products, services and responsibilities being assessed. Use the applicability register in Annex A to record decisions at the lowest relevant subclause. A heading alone does not establish that every requirement beneath it applies.

Clauses 1 to 14 and Annexes A, F, G, H, I, K and P contain proposed requirements. Annexes B to E, J and L to O, front matter, notes and examples are informative. Draft status and pending approval apply throughout.

Required records may be integrated into existing systems. Separate procedures, departments or software are not prescribed for every requirement. Existing controls may be used when they meet the requirements and provide accessible evidence.

Revision history

Revision	Change	Review status
WD 0.1 to 0.6	Drafted main clauses and Annexes A to I	Technical review pending
WD 0.7 to 0.10	Added Annexes J to O; clarified I4 and G8	Independent validation pending
WD 0.11	Added maintenance and transition controls in Annex P	Operational validation pending

Development principle

IAF AQMS contains independent proposed requirements. Technical approval and operational validation remain pending. External endorsement or recognition is not established.

Contents and development map

Clause	Subject	Status in WD 0.11
1	Purpose scope and application	Drafted
2	Terms and definitions	Drafted
3	Management and responsibilities	Drafted
4	Planning and risk management	Drafted
5	Personnel resources and information	Drafted
6	Design and development	Drafted
7	Purchasing and suppliers	Drafted
8	Production and operations	Drafted
9	Product and technology requirements	Drafted
10	Services and aftersales	Drafted
11	Measurement testing and conformity control	Drafted
12	Performance and improvement	Drafted
13	Audits and assessment	Drafted
14	Certification and decision rules	Drafted
Annex A	Applicability register	Drafted
B to E	Sector guide, source review, pilot protocol and readiness	Informative
Annex F	Assessment personnel qualification	Drafted
Annex G	Certification body authorization and oversight	Drafted
Annex H	Audit and certification records	Drafted
Annex I	Certificate information and status control	Drafted
Annex J	Pilot cases and expected reasoning	Informative
Annex K	Audit duration validation and approval	Drafted
L to O	Review, pilot records and implementation guidance	Informative
Annex P	Standard maintenance and transition control	Drafted
Notes	Continuation and review record	Informative

1 Purpose scope and application

1.1 Intended outcomes

The organization shall establish and operate a quality management system that enables consistent delivery of conforming automotive products and services, control of risks affecting their safety and intended performance, reliable evidence of conformity, and improvement based on operating and field experience.

The system shall connect management decisions with the activities through which customer requirements are received, translated, fulfilled and verified. It shall address the consequences of failure throughout the life cycle for which the organization has responsibility.

1.2 Sector coverage

IAF AQMS is intended for vehicle manufacturers; manufacturers and suppliers of parts, materials and production equipment; developers of automotive software and electronic systems; engineering and technical service providers; laboratories; logistics and distribution organizations; sales and aftersales organizations; remanufacturers; and organizations performing assessment or certification within the automotive value chain.

Vehicle activities may include passenger vehicles, commercial vehicles, buses, motorcycles, trailers, bodies, conversions and special-purpose vehicles. A scope involving other mobility products or off-road machinery shall identify those products explicitly and establish which automotive requirements and additional technical controls are relevant. Eligibility under IAF AQMS does not establish eligibility under another certification scheme.

1.3 System boundaries

The organization shall define a scope identifying its legal identity, sites, remote support locations, products, services, technologies, customer groups and activities. The scope shall identify responsibilities for design, manufacture, installation, software operation, service and field support where these are undertaken.

The scope shall describe material interfaces between sites and with external providers. It shall distinguish activities directly performed from activities controlled through contracts or other arrangements. A sales description shall not be used as a substitute for a verified statement of actual operations.

The organization shall retain the approved scope and make an accurate version available to customers and assessors. A change in ownership, operating location, product technology or responsibility shall trigger review where it could alter the scope or the applicable requirements.

1.4 Common requirements and activity requirements

Clauses 1, 3 and 4 provide common requirements. Clause 2 provides the definitions used throughout the standard. Clause 5 applies to resources and activities that affect conformity; conditional requirements within it apply only when their stated conditions exist.

Clauses 6 to 8 establish activity-specific requirements for development, purchasing and operations. Clauses 9 to 11 establish product and technology requirements, services and detailed conformity controls. Clauses 12 and 13 establish common performance and internal assessment requirements, with additional provisions for relevant assessment roles. Clause 14 distinguishes obligations of certification bodies from obligations of

applicants and certified organizations. Until the standard and operational scheme are approved, this working document supports development review only.

A business category shall not determine applicability on its own. For example, a service provider that develops diagnostic software has development and software responsibilities even if it does not manufacture hardware. A component manufacturer that commissions testing remains responsible for controlling the purchased testing service.

1.5 Applicability decisions

The organization shall evaluate applicability at the lowest practical numbered requirement. It shall use three statuses: Applicable, Partially applicable and Not applicable. Partially applicable shall be used only at an aggregate level and shall identify the applicable and non-applicable subordinate requirements separately.

A Not applicable decision shall identify the absent activity or responsibility, the evidence supporting that absence, any related outsourced activity, and any relevant customer or legal obligation. Lack of resources, lack of implementation, commercial inconvenience and a low historical failure rate shall not constitute justification for non-applicability.

The person preparing the register shall understand the organization's activities and the relevant requirements. The responsible manager shall approve the register. An independent assessor shall evaluate the justification when performing an assessment; the assessor shall not silently remove a requirement from the assessment criteria.

Disagreement about applicability shall be recorded with the disputed requirement and the supporting evidence. It shall be resolved before a conformity conclusion is issued for the affected scope. The assessment report shall distinguish disputed applicability from a demonstrated failure to satisfy an applicable requirement.

1.6 Outsourced activities

The organization shall retain accountability for conformity of the products and services it supplies when work is outsourced. It shall define the required outcomes, responsibilities, acceptance criteria, communication arrangements and evidence to be obtained from external providers.

An outsourced operational requirement may be fulfilled through effective provider controls and verified evidence where the wording allows this. The organization shall not classify the control of that activity as Not applicable solely because another party performs the work. Access restrictions shall be resolved through suitable assurance arrangements and shall not justify an unsupported conformity claim.

1.7 Mandatory obligations and conflicts

The organization shall identify applicable legal, regulatory and contractual requirements for its activities and intended markets. It shall assign responsibility for keeping this information current and for translating it into operating controls.

When requirements conflict, the organization shall seek an authorized resolution before the affected commitment, operation or release. It shall not accept a customer concession as permission to breach a mandatory legal requirement. Where a more demanding compatible customer requirement applies, the organization shall include it in the acceptance criteria.

Conformity with IAF AQMS shall not be represented as vehicle type approval, market authorization, product certification or conformity with another management system standard unless those separate claims have their own valid basis.

1.8 Interpretation of provisions

Shall indicates a requirement. Should indicates a recommendation. May indicates permission. Can indicates possibility or capability. Notes and examples explain requirements without adding obligations.

Unless expressly stated otherwise, the organization is the subject responsible for a requirement. Role-specific requirements shall identify the responsible role. Statements in the front matter, development map and informative development notes are not requirements for an assessed organization.

Evidence requirements specify information that shall be available; they do not require duplicate records or a prescribed format. A single controlled record may demonstrate several requirements where each relevant connection can be established.

1.9 Proportional implementation

The organization shall select controls proportionate to the severity of potential failure, product and process complexity, operating scale and degree of external dependence. It shall retain the basis for controls whose extent or frequency is determined by risk.

A small organization may combine roles when competence and necessary independence are maintained. It shall not combine roles where doing so would permit a person to make an unsupported independent assessment or certification decision on their own work.

1.10 Required evidence

The organization shall retain an approved scope, an applicability register, assigned process responsibilities, relevant obligation records and the decisions resolving requirement conflicts. These records shall identify their current revision or date and the person responsible for approval.

2 Terms and definitions

2.1 Organization

A person or group operating under an identified legal and management structure with defined responsibilities for the scope being assessed. A corporate group and an individual operating site are not interchangeable scope descriptions.

2.2 Automotive product

A vehicle, part, material, equipment item, software item or integrated system supplied for a defined automotive application. Inclusion within this definition does not make every technical requirement applicable to that product.

2.3 Automotive service

An activity supplied to support the development, manufacture, distribution, operation, maintenance, assessment or recovery of automotive products. A service may include both a performed activity and a delivered output such as a report or software update.

2.4 Process

A set of related activities that transforms defined inputs into intended outputs under specified controls. A process may cross departments, sites or organizational boundaries.

2.5 Conformity and nonconformity

Conformity is fulfilment of an applicable requirement. Nonconformity is failure to fulfil an applicable requirement. A nonconformity statement identifies both the requirement and the objective evidence of failure.

2.6 Objective evidence

Information that can be verified and that supports a conclusion about an activity, condition or result. Examples include observations, measurements, traceable records and reproducible analyses. An unsupported assertion is not objective evidence.

2.7 Applicability

The relationship between a requirement and the activities, responsibilities or obligations within an organization's scope. Applicability concerns whether a requirement is relevant, not whether it has already been implemented.

2.8 Risk

The possibility of an event or condition affecting an intended result, considered with its consequences and uncertainty. Under this standard, risks include effects on conformity, safety, delivery, evidence integrity and continuity of support.

2.9 Product safety

The condition in which risks of harm arising from a product within its intended use and reasonably foreseeable misuse have been evaluated and controlled against applicable requirements and acceptance criteria.

2.10 Special characteristic

A product characteristic or process parameter requiring specific identification and control because of its effect on safety, regulatory conformity, fit, function, durability or a customer-defined critical outcome.

2.11 Verification

Confirmation through objective evidence that specified requirements have been fulfilled. Verification may involve review, analysis, inspection or testing against defined criteria.

2.12 Validation

Confirmation through objective evidence that a product, service, process or system is suitable for its specified intended use under representative conditions. Validation criteria and the intended use are defined before the conclusion is reached.

2.13 Competence

Demonstrated ability to apply relevant knowledge and skills to achieve the required result. Attendance at training is an input to competence development and does not by itself demonstrate competence.

2.14 Qualification and authorization

Qualification is documented confirmation that a person meets defined prerequisites and assessment criteria. Authorization is the organization's permission for that person to perform identified tasks within stated limits. An external qualification does not automatically grant unrestricted internal authorization.

2.15 Process owner

The person assigned authority and accountability for the performance, controls, interfaces and improvement of a defined process. A process owner may coordinate work carried out by several functions.

2.16 External provider

A party outside the assessed organizational boundary supplying a product, service or process that can affect the organization's fulfilment of requirements. A group company may be an external provider relative to a particular assessed scope.

2.17 Traceability

The ability to establish relevant identity, history, application, configuration or location through linked records. The required depth of traceability depends on the product, activity, risk and applicable obligations.

2.18 Configuration

An identified combination of product, hardware, software, data and documentation versions that defines a controlled state. A released configuration includes the information needed to distinguish it from other states.

2.19 Correction

Action addressing a detected nonconformity or its immediate effect. A correction may restore an individual output without eliminating the cause of recurrence.

2.20 Containment

Temporary controls that prevent further exposure to suspected or confirmed nonconforming outputs while the extent and causes are being determined. Containment has defined boundaries, responsibilities and conditions for removal.

2.21 Corrective action

Action that eliminates a verified cause of a nonconformity to prevent recurrence. Its effectiveness is evaluated against criteria related to the original failure and comparable exposure.

2.22 Concession

Documented authorization to accept or use a specified nonconforming output within stated limits when legally permissible. A concession identifies the affected scope, approving authority and expiry or quantity limit.

2.23 Release

Authorization to proceed to a subsequent stage, supply an output or place a controlled configuration into use after the relevant acceptance criteria have been satisfied or an allowable exception has been authorized.

2.24 Audit

A planned, evidence-based evaluation of activities and results against defined requirements, performed with the independence appropriate to its purpose. System, process, product and service audits address different assessment objects.

2.25 Auditor and lead auditor

An auditor is a person competent and authorized to perform a defined audit. A lead auditor additionally directs the audit team and is responsible for coordinating the audit plan, evidence evaluation and reporting.

2.26 Technical expert and technical reviewer

A technical expert supplies specialist knowledge to an assessment without automatically holding auditor authority. A technical reviewer evaluates the adequacy of assessment information for a defined decision; the role and necessary independence are specified for that decision.

2.27 Impartiality

The ability to reach and maintain objective judgments without improper influence from personal, financial, organizational or commercial interests. Identifying a conflict does not itself demonstrate that it has been adequately controlled.

2.28 Special process

A process for which conformity of the resulting output cannot be fully established by subsequent inspection or testing without disproportionate or destructive verification. Such a process requires control of qualified operating conditions and, where relevant, personnel and equipment.

2.29 Field event

An observed failure, complaint, incident or performance condition occurring after supply or during use. A field event may require immediate safety action before its cause is confirmed.

2.30 Evidence integrity

Preservation of the completeness, accuracy, identity and change history of information used to support decisions. It includes preventing the concealment, fabrication or misleading selection of results.

2.31 Quality critical task

A task whose incorrect execution can materially affect product or service conformity, safety, traceability or the validity of a conformity decision. The organization identifies such tasks from its activities and risk evaluation.

2.32 AI supported decision

A decision in which a machine learning or other artificial intelligence system provides a classification, prediction, recommendation or action affecting quality. The organization remains accountable for controls over its use.

3 Management and responsibilities

3.1 Applicability

This clause applies to every organization adopting the standard. Responsibilities may be distributed across sites, but an accountable management authority shall be identified for the complete assessed scope.

3.2 Understanding the operating context

The organization shall identify internal and external conditions that can affect its ability to deliver conforming products and services. It shall consider changes in customers, technology, workforce capability, supply availability, operating environments, infrastructure and intended markets.

The organization shall determine whether climate-related conditions or transition requirements affect quality, continuity, materials, storage, transport or customer commitments. It shall address identified effects within the relevant controls rather than relying on an unsupported environmental claim.

The context assessment shall be reviewed at least annually and when a material change or event occurs. The review shall identify actions, responsible persons and affected processes.

3.3 Interested parties and obligations

The organization shall determine the interested parties whose requirements affect the assessed scope and identify the relevant obligations. These may include customers, end users, employees, external providers, regulators and parties relying on technical reports or assessments.

Customer requirements shall be reviewed for technical feasibility and clarity before acceptance. Requirements received through drawings, portals, contracts, software interfaces or subsequent changes shall be linked to the affected product, service or process.

The organization shall identify an owner for monitoring each significant source of changing requirements. Changes shall be evaluated, communicated and implemented before their effective date or an agreed permissible implementation date.

3.4 Quality policy

Top management shall establish a quality policy appropriate to the activities and risks within the scope. The policy shall commit the organization to meeting applicable requirements, protecting evidence integrity, addressing safety risks and improving process performance.

Top management shall ensure that the policy is translated into measurable objectives and operational responsibilities. Relevant personnel shall understand how the policy affects their own decisions. The policy shall be reviewed when the scope or strategic direction materially changes.

3.5 Management accountability

Top management shall provide resources and authority for effective operation of the quality management system. It shall review significant quality risks, recurring failures, overdue actions and conflicts between delivery commitments and conformity requirements.

Management shall not permit delivery targets or financial incentives to override required controls. When resource constraints prevent compliance, it shall reduce or suspend the affected activity, obtain an allowable revised commitment or provide the resources necessary to restore control.

Decisions accepting residual risk shall be made by persons with the authority and technical competence appropriate to its consequences. A general management approval shall not replace technical evidence required for product safety or regulatory conformity.

3.6 Process ownership and interfaces

The organization shall identify its processes and their interactions. For each process it shall define a responsible owner, intended outputs, acceptance criteria, required resources, principal risks and performance measures appropriate to the process.

Handoffs between departments, shifts, sites and external providers shall identify the information, product status and authorizations to be transferred. Unresolved responsibilities shall be escalated before they cause an uncontrolled handoff.

The process owner shall investigate adverse trends and verify that changes made to improve one process do not compromise another. Performance measures shall support decisions and shall not be selected solely because they are easy to collect.

3.7 Safety and conformity authority

The organization shall identify persons authorized to stop work, prevent shipment, quarantine suspect output, suspend a service or inhibit an unsafe software release. This authority shall be available during each operating shift or service period where the relevant risk exists.

A person raising a credible safety or conformity concern shall be able to escalate it without retaliation. Management shall ensure that concerns are recorded, assessed and resolved by competent personnel. Immediate protective action shall not wait for completion of a root cause investigation when delay would create unacceptable exposure.

Restart or renewed release after a stop shall require evidence that the initiating condition has been controlled, affected outputs have been addressed and the specified restart criteria have been met. The authorization and its basis shall be recorded.

3.8 Ethics and conflicts of interest

The organization shall establish rules prohibiting falsification of results, bribery, concealment of material defects and improper influence over conformity decisions. The rules shall apply to employees and relevant contracted personnel.

Personnel shall disclose interests that can affect the objectivity of inspection, test, audit, supplier selection or certification decisions. The organization shall assess disclosed and identified conflicts and assign controls such as reassignment, independent review or restriction of authority.

The organization shall provide a route for reporting concerns and shall control access to reports to protect legitimate confidentiality. Allegations shall be assessed fairly, and findings and actions shall be recorded. Confidentiality shall not be used to prevent a required safety or regulatory notification.

3.9 Customer communication and commitments

The organization shall define communication channels and responsible persons for technical clarification, order changes, quality concerns, delivery disruption and urgent field matters. Critical communication shall reach a person authorized to act within a risk-appropriate time.

Commitments concerning capability, capacity, test coverage and product performance shall be supported by evidence. Statements made in quotations, certificates, reports or marketing material shall be consistent with the actual scope and limitations of the supplied output.

Where a customer requirement cannot be met, the organization shall communicate the limitation before commitment or as soon as it becomes known. An agreed change shall be recorded and communicated to all affected activities.

3.10 Control of organizational change

Changes to organization structure, ownership, operating sites, key responsibilities or outsourcing arrangements shall be evaluated for their effect on quality controls and obligations. Continuity of competence, records, authorization and customer support shall be addressed before the changed arrangement becomes effective.

The organization shall assign responsibility for confirming completion of the transition. Temporary arrangements shall have defined owners, limits and review dates. Unfinished transition actions shall remain visible to management until resolved.

3.11 Required evidence

The organization shall retain its context reviews, obligations register, quality policy, process responsibilities, relevant management decisions, stop and restart authorizations, conflict controls and significant customer communications. Records shall show decisions and their implementation rather than attendance alone.

4 Planning and risk management

4.1 Applicability

This clause applies to every organization. The depth and methods of planning shall reflect the nature of its products, services, technologies and responsibilities. The organization shall not omit risk evaluation solely because it has not experienced a relevant failure.

4.2 Quality objectives

The organization shall establish objectives for relevant functions and processes, including outcomes affecting customers and end users. Each objective shall identify a measure, a defined calculation or assessment method, a baseline where available, a target, an owner and a review frequency.

Plans to achieve objectives shall identify actions, resources and completion dates. Where an objective is not achieved or an adverse trend emerges, the responsible owner shall evaluate the causes and initiate an appropriate response. Targets shall not encourage suppression of complaints or manipulation of reported results.

4.3 Identification of risks

The organization shall identify risks across the activities within its scope, including foreseeable failure of products, processes, services, suppliers, equipment, information systems and human controls. It shall use relevant customer feedback, field events, previous development experience, audit findings and operating data.

Risk evaluation shall consider failure consequences, likelihood, uncertainty and the ability to detect or contain failure before exposure. The organization shall identify safety-related and regulatory risks separately so that an aggregated score cannot conceal a severe consequence.

The method, assumptions, participants and significant conclusions shall be recorded. Where quantitative information is unreliable, uncertainty shall be stated and controls selected accordingly. An apparent numerical precision shall not substitute for technical judgment.

4.4 Risk treatment and residual risk

For significant risks, the organization shall define preventive controls, detection or containment controls where needed, action owners and implementation dates. Preference shall be given to eliminating the cause of failure where reasonably achievable within the applicable requirements.

Before accepting residual risk, the organization shall verify implementation of the specified controls and evaluate their effectiveness. Acceptance shall identify the authorizing role, the evidence used, any conditions and the circumstances requiring reconsideration.

Customer approval or internal acceptance shall not authorize a breach of applicable legal requirements. A risk that remains outside the established acceptance criteria shall prevent the affected commitment or release until adequately resolved.

4.5 Opportunities and planned improvement

The organization shall identify opportunities to improve conformity, reliability, delivery, error prevention and resource effectiveness. Proposed improvements shall be assessed for unintended consequences before introduction.

The organization shall determine how the benefit will be measured and when it will be reviewed. Where a change fails to deliver the expected benefit or introduces unacceptable risk, the organization shall revise, reverse or otherwise control the change.

4.6 Operational planning

The organization shall plan the sequence, resources and acceptance points needed to fulfil a product or service commitment. The plan shall identify required inputs, competent personnel, equipment, external dependencies, verification activities and release authority.

Capacity planning shall consider bottlenecks, maintenance, calibration, staff availability, rework and foreseeable interruptions. The organization shall verify capability before accepting a commitment that exceeds previously demonstrated operating conditions.

Where several projects share resources, conflicting priorities shall be resolved through a controlled decision. A schedule change shall not bypass required validation, inspection or authorization.

4.7 Planned changes

The organization shall evaluate changes affecting product, service, process, supplier, equipment, software, data or location before implementation. The evaluation shall identify affected configurations, risks, approvals, verification or validation needs and communication requirements.

A change shall have an identified owner and defined implementation and acceptance criteria. Personnel shall use the authorized instructions and configuration from the effective point of change. The organization shall preserve traceability between output produced before and after the change where necessary for risk control.

Emergency changes shall receive an expedited review by authorized personnel, with compensating controls and subsequent verification. Emergency status shall not waive mandatory acceptance criteria. Temporary changes shall specify expiry, monitoring and restoration conditions.

4.8 Business continuity

The organization shall identify interruptions that could prevent fulfilment of customer or safety obligations. It shall consider loss of utilities, equipment, key people, materials, transport, facilities, digital systems and critical external services, as relevant to its scope.

Continuity plans shall define activation criteria, decision authority, communication contacts, alternative arrangements, recovery priorities and the records needed to manage affected output. Recovery objectives shall be based on obligations and the consequences of interruption.

Alternative facilities, suppliers, tools or methods shall meet required qualification and approval conditions before being used. A continuity plan shall not authorize an uncontrolled substitution merely to maintain delivery.

4.9 Testing continuity arrangements

The organization shall test significant continuity arrangements at least annually using scenarios appropriate to its risks. Tests may include simulations, contact checks, controlled failover or restoration exercises. The exercise shall not expose customers or workers to uncontrolled hazards.

Test records shall identify the scenario, assumptions, participants, observed results and gaps. Actions arising from a test or actual interruption shall be assigned, tracked and verified. A documented rationale shall explain any test element that cannot safely be performed and the alternative evidence used.

4.10 Recovery and restart

Before restarting an interrupted activity, the organization shall assess equipment condition, materials, environment, personnel readiness, software configuration and data validity as relevant. It shall determine whether additional inspection, first-output verification or revalidation is needed.

Products and records created during an uncertain operating period shall be identified and evaluated before release. Recovery of an information system shall include checks that the restored data are complete and suitable for current operations.

The responsible authority shall record the restart decision and any temporary restrictions. Normal operating status shall be restored only after the specified criteria are met.

4.11 Escalation and incident communication

The organization shall establish thresholds and response times for escalation of safety events, conformity failures, evidence compromise and material disruption. Response times shall meet applicable obligations and be proportionate to the consequences of delay.

The organization shall maintain current contacts and identify who can notify customers, authorities and other affected parties. Notifications shall distinguish confirmed facts from unresolved questions and shall be updated as reliable information becomes available.

4.12 Required evidence

The organization shall retain objectives and plans, significant risk assessments, treatment and acceptance decisions, capability and capacity evaluations, change approvals, continuity plans, exercise results, incident communications and restart records. Risk assessments shall be revisited when their assumptions are invalidated by new evidence.

5 Personnel resources and information

5.1 Applicability

This clause applies to resources affecting the quality management system and the conformity of supplied products or services. Requirements for a particular resource or technology apply when that resource or technology is used or controlled within the scope.

5.2 Resource planning

The organization shall determine the personnel, facilities, equipment, digital services, information and financial resources needed for its commitments. It shall assess resource adequacy before significant new commitments or changes in operating volume or technology.

Resource shortages that can compromise conformity shall be escalated to management. Temporary arrangements shall be evaluated for competence, supervision, reliability and continuity before use.

5.3 Role profiles and competence criteria

The organization shall define competence criteria for roles affecting quality and safety. Criteria shall address relevant technical knowledge, practical skills, experience, understanding of applicable instructions and the ability to recognize abnormal conditions.

For quality critical tasks, the criteria shall identify prerequisites, assessment methods, pass criteria, supervision needs and authorization limits. A generic job title or an unverified claim of experience shall not be sufficient evidence of competence.

Where an external authority or customer prescribes a qualification, the organization shall verify its relevance, validity and scope. A qualification covering one technology or method shall not be assumed to cover another.

5.4 Competence assessment

The organization shall assess competence before assigning a person to work independently on a quality critical task. Assessment shall include a practical demonstration where correct execution depends on applied skill. Knowledge tests may supplement practical evidence but shall not replace it without a justified basis.

Assessors shall have the competence necessary to judge the task and shall use defined criteria. For tasks involving significant safety consequences, result acceptance or independent evaluation, the organization shall provide an assessment or review independent of the candidate's self-assessment.

Assessment records shall identify the task, criteria, method, assessor, evidence, result and any limitations. Unsuccessful candidates shall receive appropriate development and shall be reassessed before independent authorization.

5.5 Authorization and supervision

The organization shall maintain a current record of personnel authorized for quality critical tasks. Each authorization shall identify the person, task or method, relevant equipment or technology limits, effective date and any expiry or review conditions.

Trainees and persons with restricted authorization shall work under defined supervision. Supervisors shall be able to intervene and shall be responsible for confirming the acceptability of outputs before release where required.

The organization shall prevent unauthorized assignment, including through shift scheduling and access controls where appropriate. Absence of the usual authorized person shall not justify informal transfer of their authority to an unqualified substitute.

5.6 Continued competence

The organization shall define reassessment intervals based on task risk, frequency of practice, technical change and demonstrated performance. Competence shall also be reviewed following significant method changes, extended absence, relevant errors or evidence that previous assessment results are no longer reliable.

The review shall consider observed work, quality results, technical updates and relevant feedback. Authorization shall be restricted or suspended where competence is no longer demonstrated. Restoration shall require evidence that the identified gap has been addressed.

5.7 Training and awareness

The organization shall identify training needs from role requirements, risk assessments, changes, performance and future commitments. Training shall have defined learning outcomes and a means of evaluating whether those outcomes have been achieved.

Personnel shall understand the consequences of incorrect work, the relevant special characteristics, stop and escalation rules, evidence integrity requirements and the limits of their own authority. Instructions and training shall be presented in a language and form the personnel can understand.

Training effectiveness shall be evaluated through subsequent application where the learning outcome concerns work performance. Attendance records alone shall not be treated as proof of effectiveness.

5.8 Contracted and temporary personnel

The organization shall apply relevant competence, awareness, authorization and supervision controls to agency workers, contractors and temporary personnel. Contract status shall not reduce the controls required for the assigned task.

Before assignment, the organization shall verify evidence supplied by an agency or contractor and determine whether additional assessment is needed. Access rights and authorizations shall be updated promptly when an assignment changes or ends.

5.9 Work conditions and human factors

The organization shall identify working conditions that can affect reliable performance, including fatigue, workload, visibility, noise, temperature, ergonomics, task complexity and interruption. It shall provide controls suitable for the activity and applicable occupational requirements.

For quality critical tasks, the organization shall consider the risk of misunderstood instructions, similar-looking items, incorrect data entry and missed handoffs. Controls may include clear identification, independent checks, error prevention and task design. Repeated human error shall trigger examination of system conditions as well as individual competence.

5.10 Facilities and utilities

Facilities, layouts and utilities shall support the intended activities and protect product, material and evidence integrity. The organization shall control access, segregation, contamination, environmental conditions and safe movement where these affect conformity.

Required operating conditions shall be defined and monitored at a frequency appropriate to their effect. A condition outside an established limit shall trigger assessment of affected outputs and action before release. Changes to layout or utilities shall be evaluated under the change controls in Clause 4.

5.11 Equipment suitability and maintenance

The organization shall determine whether equipment, tools, fixtures and software are suitable for their intended tasks before use. Acceptance shall consider operating range, accuracy where relevant, capacity, interfaces, protective functions and required documentation.

Equipment affecting conformity shall be identified and maintained under a plan based on failure consequences, use, condition and manufacturer information. Maintenance completion and material findings shall be recorded. Overdue maintenance shall be evaluated before continued use is authorized.

Following maintenance, repair or modification that can affect output, the organization shall verify restoration of the required condition before normal operation. Defective or unverified equipment shall be identified and prevented from unintended use.

5.12 Monitoring and measuring resources

The organization shall identify resources used to establish acceptance of products, processes and services. It shall ensure that their range, resolution, uncertainty where relevant and operating conditions are suitable for the decision being made.

Calibration or verification shall be performed at defined intervals or before use where necessary. The basis for traceability shall be documented. Where recognized reference standards are unavailable, the organization shall establish and validate an alternative reference or comparison method suitable for the intended decision.

When a measuring resource is found unsuitable, the organization shall assess the validity of earlier results and the status of affected outputs. It shall record the impact assessment, notifications and any repeat measurements or other actions. Detailed testing and calibration provisions are established in Clause 11.

5.13 Organizational knowledge

The organization shall identify knowledge necessary to sustain its activities, including technical decisions, known failure mechanisms, process settings and lessons from previous work. It shall make this knowledge accessible to relevant personnel while protecting confidential information.

The organization shall address dependence on individual knowledge through suitable documentation, mentoring or other transfer arrangements. Before the loss of a key person or external service, it shall evaluate the effect on ongoing conformity and support obligations.

5.14 Document creation and approval

Documents used to direct or demonstrate work shall identify their purpose, owner and current revision or effective date. Technical content shall be reviewed for adequacy and approved by authorized personnel before use.

Instructions shall state the information needed to perform the task correctly, including relevant acceptance criteria and actions for abnormal conditions. Approval shall verify technical suitability, not merely formatting. Documents of external origin shall be controlled when necessary for fulfilling requirements.

5.15 Access and revision control

The organization shall ensure that current instructions and specifications are available at the point of use. It shall prevent unintended use of obsolete versions and preserve earlier versions when necessary to interpret historical outputs or decisions.

Changes shall identify the affected content, approval and effective implementation point. Where a change affects competence or operating practice, relevant personnel shall be informed or trained before using the revised method. Emergency verbal instructions shall be confirmed in a controlled record before affected output is released.

5.16 Record integrity and retention

Records shall identify the activity or output, relevant date, responsible person or validated automated source, results and applicable criteria. The organization shall protect records against loss, unauthorized alteration and misleading omission.

Corrections shall preserve the original information or a recoverable audit trail and identify the person, date and reason for the change. The organization shall not delete failed results to create the appearance of an uninterrupted sequence of acceptable results.

Retention periods shall reflect legal, contractual, product life cycle, safety and evidence needs. The organization shall define who can authorize disposal and shall suspend routine disposal when records are relevant to an active investigation, claim or required preservation instruction.

5.17 Information security for quality activities

The organization shall identify information and digital systems whose compromise could affect conformity, continuity or safety. It shall define access rights, protect credentials, manage security updates and control remote access in proportion to the identified risks.

Changes to systems supporting quality decisions shall be tested before deployment. The organization shall maintain recoverable backups of essential records and verify restoration at risk-based intervals. Detection of unauthorized change or suspected compromise shall trigger containment and evaluation of affected decisions and outputs.

Security controls shall include externally hosted systems where the organization relies on them. Contracts and operating arrangements shall address availability, access to records, incident notification and recovery or export of essential information.

5.18 Automated and AI supported quality decisions

The organization shall identify automated tools that influence inspection, classification, acceptance or other quality decisions. For each significant use, it shall define the intended application, approved operating range, required input quality, acceptance criteria and responsible decision owner.

Before operational use, the organization shall validate the tool against representative conditions and relevant failure cases. Evaluation shall address the consequences of false acceptance and false rejection. For AI systems, the organization shall control model and data versions and assess whether the validation evidence represents the actual operating population.

Changes to models, decision thresholds, input data pipelines or operating conditions shall be evaluated before continued reliance. The organization shall monitor performance and define triggers for human review, restricted use or withdrawal. Where failure could cause severe harm or an invalid release, protective controls shall prevent the automated output from being accepted without the required assurance.

The organization shall retain sufficient information to reconstruct significant decisions, including the applicable configuration and input identification, subject to lawful privacy constraints. Use of an external AI service shall not transfer accountability for the quality decision to the service provider.

5.19 Communication and handover

The organization shall define the information needed for reliable handover between personnel, shifts, sites and external parties. Handover shall communicate unresolved abnormalities, temporary controls, equipment status, affected output and outstanding approvals.

Urgent messages shall use a channel appropriate to the consequence of delay and shall require confirmation of receipt where necessary. The organization shall identify a fallback when the normal communication system is unavailable.

5.20 Required evidence

The organization shall retain role criteria, competence assessments, authorizations, training effectiveness results, relevant work-condition evaluations, equipment acceptance and maintenance records, measuring-resource status, controlled documents, retention rules and digital-system assurance records.

Records shall permit a reviewer to connect a quality critical task with the authorized person or controlled automated system that performed it. The organization may use integrated systems provided that access, traceability and integrity requirements are maintained.

6 Design and development

6.1 Applicability

This clause applies when the organization determines or changes requirements, characteristics, architecture or methods needed to realize a product, service or operating process. It applies to development performed internally or controlled through external providers. Requirements for a specific development activity apply only when that activity or responsibility exists.

An organization manufacturing to customer drawings may determine that product design is not applicable when it has no product design responsibility. It shall nevertheless apply relevant development requirements to manufacturing processes, tooling, inspection methods and changes under its control. Responsibility for making a design change shall be established before the change is made.

A service organization shall apply this clause when it develops or materially changes a service method, diagnostic application, testing approach or service delivery process. Routine execution of an established approved method does not, by itself, constitute a new development project.

6.2 Development responsibilities and interfaces

The organization shall identify the development authority, approval authority and responsibilities for each product, service and process being developed. Where authority is shared, it shall define the boundaries between parties and identify who resolves interface requirements and conflicting decisions.

The development plan shall identify required participation from relevant engineering disciplines, production or service delivery, quality, purchasing and field support. Personnel responsible for safety, regulatory conformity and cybersecurity shall participate where the subject can affect their responsibilities.

External development arrangements shall specify required deliverables, access to evidence, ownership or permitted use of necessary information, change notification and support obligations. Restrictions on access shall be resolved before they prevent verification, approval or continued support.

6.3 Feasibility and acceptance of development commitments

Before accepting a development commitment, the organization shall evaluate whether the required performance, timing, resources, skills, capacity and supply arrangements can be achieved. The evaluation shall address new technology, uncertain requirements, intended operating conditions and dependencies on external parties.

Unresolved feasibility issues shall have an owner, planned resolution and decision deadline. The organization shall communicate limitations that affect its commitment to the relevant customer or commissioning authority. A commercial commitment shall not be treated as evidence of technical feasibility.

Feasibility shall be reconsidered when requirements, volumes, delivery dates, technology or supply assumptions materially change. Decisions shall identify the evidence reviewed and any conditions attached to proceeding.

6.4 Development planning and decision points

The organization shall maintain a development plan defining stages, deliverables, interfaces, resources, review points and approval criteria. Planning shall connect product or service development with the development of the processes used to realize and verify it.

Each decision point shall identify the required evidence, decision authority and conditions for proceeding. A conditional approval shall identify outstanding work, permitted activities, restrictions and a closure date. No conditional approval shall authorize release that violates an applicable mandatory requirement.

Plans may use sequential, iterative or incremental methods. In every case, the organization shall maintain control of requirements, configuration, verification and release. A short iteration shall not justify omitting evidence needed for the consequence of failure.

6.5 Development inputs and acceptance criteria

The organization shall establish inputs covering intended use, reasonably foreseeable misuse, functional and performance needs, interfaces, intended markets, customer commitments and applicable mandatory requirements. Inputs shall address life, reliability, maintainability, operating environments and support needs where relevant.

For a service, inputs shall define the service outcome, customer interaction, required response, completion criteria and handling of interrupted or unsuccessful delivery. For a process, inputs shall include output requirements, expected variation, capacity, materials, equipment and verification needs.

Inputs shall be sufficiently clear to support objective acceptance decisions. Conflicting, incomplete or untestable requirements shall be resolved with the authorized source. Assumptions shall be identified, assigned for confirmation and reviewed before decisions that depend on them.

6.6 Requirements traceability

The organization shall identify development requirements and maintain their connection to design outputs, risk controls, verification and validation evidence, and release decisions. Traceability shall support identification of affected items when a requirement changes or evidence becomes invalid.

The depth of traceability shall reflect complexity and failure consequences. Safety and regulatory requirements shall remain individually traceable to their implemented controls and supporting evidence. A document reference alone is insufficient where it does not identify the relevant requirement or result.

Derived requirements shall identify their basis and approval. Requirements allocated to external providers shall remain connected to the acceptance evidence obtained from those providers.

6.7 Design risk analysis

The organization shall analyze how the proposed design can fail to fulfil its intended functions and the consequences for users, other persons, connected systems and subsequent operations. The analysis shall consider foreseeable conditions, interfaces, dependent failures and lessons from similar applications.

The organization shall select a documented analysis method suitable for the subject. The method shall identify functions, failure conditions, causes, consequences, existing controls and required actions. A failure mode and effects analysis or another justified method may be used; a risk score shall not replace review of severe consequences.

Actions shall favor elimination of hazards or prevention of failure where practicable. Reliance on detection, warnings or operating instructions shall be justified against the actual use conditions. Residual risks shall be evaluated and accepted by an authorized competent person before the relevant release.

6.8 Special characteristics

The organization shall identify characteristics requiring special control through customer requirements, mandatory obligations and its own risk analysis. It shall maintain consistent identification from development outputs through supplier instructions, process controls, inspection records and change decisions.

For each special characteristic, the organization shall specify the acceptance limit, responsible process, control method and reaction to loss of control. Where different customer symbols are used, a controlled mapping shall prevent ambiguity.

Designation of a special characteristic shall trigger evaluation of the adequacy of measurement, process capability and failure prevention. Removal or downgrading of that designation shall require documented technical justification and any required customer approval.

6.9 Architecture and interface control

For products or services containing interacting elements, the organization shall define the architecture and interfaces necessary for correct integration. Interfaces shall address physical fit, energy, signals, data, timing, environmental conditions and responsibilities as relevant.

The organization shall evaluate failures caused by incompatible versions, incorrect assumptions, unavailable dependencies or unexpected interactions. Interface changes shall be communicated to affected parties and verified at the integrated level before release.

For connected or electronically controlled functions, the development record shall connect relevant safety and security assumptions to implementation and verification evidence. Additional technology requirements are established in Clause 9 and apply according to the supplied function and responsibility.

6.10 Design outputs

Design outputs shall define the product, service or process sufficiently for controlled realization, verification and support. Outputs shall include applicable specifications, acceptance criteria, special characteristics, configuration identifiers and instructions necessary for safe and conforming use.

Product outputs shall include material and component requirements, drawings or equivalent digital definitions, interface information and relevant installation and maintenance requirements. Software outputs shall include controlled executable or deployable items, configuration information and the evidence needed to reproduce or identify the released version.

Service outputs shall define methods, competence requirements, customer information, completion evidence and escalation conditions. Process outputs shall define the operating sequence, resources, parameters, verification controls and reactions to abnormal conditions.

Outputs shall be reviewed for completeness, consistency with inputs and usability by the receiving activity before approval. Development assumptions that remain relevant to operation shall be communicated explicitly.

6.11 Technical reviews

The organization shall conduct technical reviews at planned points and when significant uncertainty or change requires reconsideration. Reviews shall evaluate progress against inputs, unresolved risks, interface compatibility and readiness for the next activity.

Review participation shall include competence relevant to the decision and sufficient independence to challenge significant assumptions. The organization shall prevent schedule or commercial authority from substituting for technical acceptance.

Records shall identify the configuration reviewed, evidence considered, participants, findings, decisions and actions. Actions shall be tracked to verified closure; recurring unresolved actions shall be escalated before they undermine the decision criteria.

6.12 Verification

The organization shall plan and perform verification to determine whether outputs meet specified inputs. Verification shall use defined methods, acceptance criteria, responsible personnel and an identified configuration.

Verification may include calculation, simulation, inspection, testing or other technically justified means. Where models or simulations support acceptance, the organization shall establish their suitability, assumptions, limitations and correlation with relevant physical or operating evidence.

Failed, inconclusive and interrupted activities shall be recorded and evaluated. Repeating an activity shall not erase earlier failure evidence. After correction, the organization shall determine the need for regression verification of affected and interacting requirements.

6.13 Validation

The organization shall validate that the developed product, service or process can achieve intended outcomes under representative use conditions. Validation planning shall address relevant users, operating environments, duty cycles, foreseeable misuse and limits of the claimed application.

Validation shall use configurations and conditions representative of the intended release. Where a prototype, surrogate or accelerated method is used, the organization shall justify its relevance and address differences that could affect the conclusion.

For services, validation shall evaluate the complete delivery sequence, including customer inputs, human decisions, handovers and unsuccessful or interrupted cases. For software, validation shall address the intended operating environment and relevant interactions with hardware, data and external services.

Unresolved validation failures shall prevent unrestricted release of the affected application. A restricted trial shall have explicit authorization, defined boundaries, monitoring, containment and termination criteria, together with any required external approvals.

6.14 Manufacturing and service process development

The organization shall develop the realization process in conjunction with the product or service it supports. It shall define the process sequence, interfaces, resource needs, expected output and points where errors can be introduced or escape detection.

Process risk analysis shall address material variation, setup errors, equipment and tool deterioration, human factors, measurement limitations, rework and external operations. It shall connect identified risks to prevention controls, inspection and reaction plans.

The organization shall confirm that process instructions, control plans, equipment, measurement resources and personnel competence are consistent with the approved design. Process development responsibility remains applicable when the product design belongs to another party.

6.15 Prototypes and development samples

The organization shall identify prototypes and development samples by configuration, purpose and release restrictions. It shall control materials, manufacture, inspection and disposition sufficiently to interpret the resulting evidence.

Differences from intended production or normal service delivery shall be recorded and considered when using sample results. Samples built using exceptional selection, adjustment or supervision shall not be treated as representative without justification.

Unapproved development items shall be prevented from entering unrestricted supply. Where a customer receives such an item, its status and permitted use shall be communicated through an authorized arrangement.

6.16 Readiness and initial approval

Before routine supply begins, the organization shall demonstrate that the approved output can be realized under the intended operating conditions. The readiness review shall cover design status, process validation, capacity, personnel, supplier readiness, measurement, traceability and reaction arrangements.

Production evidence shall represent relevant equipment, tooling, materials, operating rates and shifts. Service evidence shall represent the intended staffing, systems, volume and delivery conditions. Gaps in representativeness shall be identified and resolved or subject to an authorized restriction with additional assurance.

The organization shall assemble an approval record proportionate to the supplied item and risk. It shall include the approved configuration, relevant verification and validation results, process controls, outstanding restrictions and release authority. Customer-specific approval submissions shall be completed when required by contract.

Approval of samples or an initial submission shall not be treated as permanent approval of subsequent changes. The organization shall define the changes that require renewed evidence or external approval.

6.17 Development changes and configuration

The organization shall identify the proposed change, reason, affected configuration and implementation point. Impact analysis shall address requirements, interfaces, risks, verification, suppliers, work in progress, delivered items and support information.

The change shall be reviewed and approved by the relevant authority before implementation. Verification and validation shall be repeated to the extent necessary to establish the changed configuration and its interactions. Required customer or regulatory authorization shall be obtained before the affected release.

The organization shall preserve the ability to identify earlier configurations and the units, lots or services to which each configuration applies. For digital delivery, configuration control shall include dependencies and deployment records needed to determine what was actually supplied.

6.18 Transfer and support readiness

The organization shall transfer approved outputs to the activities responsible for realization and support. Receiving personnel shall confirm that the information, resources, competence and unresolved restrictions are understood and sufficient for their tasks.

Transfer shall include relevant risk controls, special characteristics, maintenance information, service limitations and feedback arrangements. Where development and realization occur at different organizations or sites, interface responsibilities shall be confirmed before routine supply.

The organization shall establish how field failures, service findings and production experience return to the development authority. Findings that invalidate a design assumption shall trigger impact review and appropriate change or containment.

6.19 Development closure and retained evidence

The organization shall close a development stage only when required evidence is available and outstanding actions have an authorized disposition. Closure records shall distinguish fulfilled requirements from deferred work, accepted restrictions and unresolved issues.

Retained evidence shall include the development plan, inputs, traceability, risk analyses, reviews, approved outputs, verification and validation results, initial approval and change history. It shall be sufficient to reconstruct the basis of a release decision for the relevant configuration.

7 Purchasing and suppliers

7.1 Applicability

This clause applies to externally provided products, materials, processes and services that can affect conformity, safety, delivery or the reliability of evidence. It includes outsourced manufacturing, development, testing, logistics, calibration, software services and externally provided personnel where relevant.

The organization shall apply controls to providers under common ownership when their outputs cross a defined responsibility boundary. Customer nomination or approval of a supplier shall not remove the organization's receiving, communication or escalation responsibilities.

7.2 Provider classification and control planning

The organization shall identify its relevant external providers and classify the control needed according to the consequence of failure, complexity, detectability, performance and dependence on the provider. Classification shall consider single sources, long replacement lead times and limited access to evidence.

The control plan shall define qualification, purchasing information, acceptance checks, monitoring and re-evaluation. It shall state the rationale for reduced controls and the conditions requiring increased controls.

Changes in supplied technology, location, ownership, performance or subcontracting shall trigger review where they could change the assurance needed. The organization shall maintain an approved source record identifying the scope and any restrictions of approval.

7.3 Supplier selection and qualification

Before initial approval, the organization shall evaluate the provider's ability to meet the specified technical, capacity, competence and delivery requirements. Evaluation shall consider relevant experience, facilities, process controls, traceability, evidence integrity and continuity arrangements.

Qualification methods may include review of records, sample evaluation, technical trials, remote assessment and on-site assessment. The selected combination shall be justified by risk and by the reliability of the available evidence. Where documentary review cannot establish control of a critical process, further direct or independently verified evidence shall be obtained.

Approval shall identify the supplied scope, approved site or delivery arrangement, relevant processes and restrictions. Approval of one site, process or technology shall not automatically extend to another.

7.4 Use of certificates and external assessments

Where supplier qualification relies on a certificate, approval or external assessment, the organization shall verify its validity, scope, issuing body and relevance to the supplied activity. It shall consider any limitation, suspension or unresolved finding affecting reliance.

A management system certificate shall not be accepted as proof that a specific item or batch conforms. A test report shall not establish ongoing process control beyond the evidence and scope it supports.

If an expected credential is unavailable, the organization shall determine whether alternative assurance is permitted and sufficient. It shall not waive a mandatory contractual or legal qualification requirement without an authorized change to that requirement.

7.5 Purchasing specifications and requirement transfer

Purchasing information shall define the output to be supplied, applicable revision, acceptance criteria, quantity or service scope and delivery requirements. It shall include special characteristics, required competence, verification evidence, identification and preservation requirements where relevant.

The organization shall communicate change notification duties, nonconformity notification, permitted subcontracting and necessary access to records or activities. The provider shall confirm understanding of requirements whose ambiguity could affect conformity before work proceeds.

Technical requirements shall reach the relevant execution point at the provider. Transmission of a general quality manual shall not replace clear identification of the requirements applicable to the purchase.

7.6 Subtier and outsourced process control

The organization shall require providers to control their own external providers where those activities affect the purchased output. Requirements necessary for safety, conformity, traceability and evidence integrity shall be transferred to the relevant supply level.

The organization shall determine which subtier sources or processes require visibility, advance notification or approval. The extent shall reflect risk and contractual access; commercial confidentiality shall be addressed through appropriate assurance arrangements.

For outsourced special processes, the organization shall obtain evidence of process qualification, operating control and acceptance relevant to its output. A provider's purchase order to a subcontractor shall not, by itself, demonstrate that the process was controlled.

7.7 Supplier development and conditional approval

Where a provider has a capability gap that can be controlled without breaching a mandatory requirement, the organization may grant conditional approval. The approval shall define the gap, permitted supply, additional verification, accountable owner, completion date and withdrawal criteria.

The organization shall verify closure of development actions through evidence of effective implementation. A repeatedly extended action date shall trigger reconsideration of the supply decision and escalation to the responsible management.

Supplier development shall focus on the causes of poor performance and the ability to sustain conforming supply. Additional sorting may provide temporary protection but shall not be accepted as evidence that the underlying process has improved.

7.8 Initial and changed supply approval

Before routine acceptance of a new or materially changed supply, the organization shall determine the evidence needed to confirm conformity and process readiness. Requirements shall reflect the purchased output and may include samples, test results, process information, capacity evidence and an approved configuration record.

The approval decision shall identify the supplier, location, supplied item or service, revision, evidence and any limitation. Items received before approval shall remain controlled against unintended use.

Changes requiring reapproval shall be defined in advance, including relevant changes in material, process, tooling, software, location or subtier source. The extent of renewed verification shall follow the impact of the change.

7.9 Incoming acceptance and release to use

The organization shall establish acceptance controls before purchased outputs are used or supplied onward. Controls shall verify identity, revision, condition and required evidence, together with the technical checks needed for the risk and provider performance.

Sampling or reliance on provider data shall have a documented basis. The organization shall periodically evaluate whether the selected controls remain effective, including the possibility of false or unrepresentative evidence.

Acceptance status shall be identifiable. Missing evidence, damage, incorrect identity or failed checks shall trigger hold and disposition. Emergency use before completion of normal verification shall require an authorized, traceable and recoverable arrangement and shall not bypass a mandatory release condition.

7.10 Authenticity and material provenance

The organization shall identify purchased outputs for which substitution, counterfeit supply or uncertain origin can affect conformity or safety. Controls shall address approved sourcing, identity checks, batch linkage and authenticity of supporting records.

For brokered, obsolete or scarce components, the organization shall evaluate additional risks before purchase and define enhanced verification where needed. A commercial description of equivalence shall not substitute for technical approval of a replacement.

Suspected counterfeit or substituted items shall be segregated, investigated and prevented from re-entering legitimate supply without a documented acceptable disposition. Affected customers or authorities shall be notified where required.

7.11 Externally supplied technical and digital services

For testing, calibration, engineering and assessment services, purchasing controls shall define the method or required outcome, acceptance evidence, competence, independence where relevant and limitations of the reported conclusion.

For hosted systems, software tools and data services affecting quality decisions, the organization shall define availability, change notification, information protection, data recovery and exit arrangements. It shall validate suitability for its intended use before operational reliance.

The organization shall evaluate changes in service conditions or provider technology that can invalidate prior acceptance. Access to the evidence needed to support past quality decisions shall be maintained for the required retention period.

7.12 Supplier performance monitoring

The organization shall monitor supplier conformity, delivery, responsiveness and the effectiveness of corrective action. Monitoring shall include disruptions, repeat failures, unauthorized changes and evidence reliability where relevant.

Performance evaluation shall use defined measures, periods and escalation thresholds appropriate to the supplied activity. Significant safety or regulatory failures shall be escalated on their own merits and shall not be offset by favorable average scores.

Results shall inform acceptance controls, supplier development, re-evaluation and sourcing decisions. Relevant performance findings shall be communicated to the provider with clear expectations for response.

7.13 Supplier nonconformity and containment

When supplied output is nonconforming or suspected of being nonconforming, the organization shall identify the potentially affected population and protect its own operations and customers. Containment shall extend to stock, work in progress, goods in transit and delivered output where relevant.

The organization shall require the provider to investigate causes and implement corrective action proportionate to the consequence and recurrence risk. It shall verify the effectiveness of actions before reducing temporary controls.

Concessions shall identify the exact deviation, affected quantity or period, authorized use and expiry. Supplier agreement alone shall not authorize the organization to depart from its customer's acceptance requirements.

7.14 Supplier changes and continuity

The organization shall define supplier changes requiring advance notification and approval. It shall evaluate the effect on configuration, capability, validation, traceability and customer commitments before the changed supply is accepted.

For critical dependencies, the organization shall establish continuity arrangements covering disruption, loss of capability and source exit. Alternative supply shall be technically qualified to the necessary extent before release to use; urgency shall not establish equivalence.

Transfers shall address tooling, technical data, retained records, work in progress and last approved supply. The organization shall preserve traceability through the transition and monitor the new arrangement for emerging failures.

7.15 Re-evaluation and withdrawal

The organization shall re-evaluate supplier approval at planned intervals and after significant adverse events. Review shall consider current performance, changed scope, credential status, corrective action and continuity risks.

Suspension or withdrawal shall specify the affected scope, purchasing restrictions, treatment of open orders and conditions for reinstatement. Relevant purchasing and receiving personnel shall receive the updated decision before further acceptance.

Reinstatement shall require evidence that the cause of withdrawal has been addressed and that the provider can again meet the approved scope. Commercial need alone shall not justify reinstatement.

7.16 Required evidence

The organization shall retain provider classifications, qualification and approval records, purchasing requirements, acceptance evidence, performance reviews, change decisions and corrective action verification. Conditional approvals and concessions shall remain linked to the affected supply.

Records shall allow a reviewer to connect a purchased output with its approved source, applicable specification, acceptance result and any subsequent restriction. Duplicate supplier records are not required where a controlled shared system provides this connection.

8 Production and operations

8.1 Applicability

This clause applies to controlled realization of products and the operational processes used to deliver services. Physical manufacturing requirements apply where the corresponding activity exists; general operational controls apply to service delivery where relevant.

Organizations shall evaluate applicability by activity rather than by company name or industry label. A laboratory may have no assembly operation but shall control its operating instructions, acceptance status, externally provided work and nonconforming outputs. Detailed service and laboratory provisions are established in Clauses 10 and 11.

8.2 Operational planning and work authorization

The organization shall translate approved requirements into an authorized production order, service instruction or equivalent controlled work package. The package shall identify the required output, applicable configuration, resources, sequence and acceptance conditions.

Before work begins, the organization shall confirm availability of approved inputs, competent personnel, suitable equipment, current instructions and required approvals. Unresolved constraints shall be assessed and controlled before affected work is authorized.

Scheduling shall account for real capacity, maintenance, verification and permitted operating limits. Expedite instructions shall not override defined technical controls without an authorized change and an evaluated basis.

8.3 Process sequence and control plan

The organization shall define the operating sequence and its interfaces, including external operations, inspections, transfers and permitted rework. The defined sequence shall agree with the approved process design and actual execution.

A control plan or equivalent integrated record shall identify the output or parameter to be controlled, requirement, method, frequency or trigger, responsible role, record and reaction to failure. It shall incorporate special characteristics and the controls established through process risk analysis.

The control plan shall be reviewed after significant process changes, failures or evidence that a control is ineffective. A change to a control shall be evaluated for its effect on downstream verification and release.

8.4 Work instructions and execution records

Instructions shall be available at the point of use in a form the performing personnel can understand. They shall identify the work sequence, critical settings, acceptance criteria, relevant precautions and actions when an abnormal condition occurs.

The organization shall ensure that electronic instructions display the applicable approved revision and that loss of system access has a defined response. Local edits, handwritten changes and temporary instructions shall be subject to authorization and revision control.

Execution records shall identify the work performed, relevant item or service, operator or validated automated source, date and required result. Completion marks shall reflect actual work and shall not be entered in advance of the activity.

8.5 Setup and changeover verification

The organization shall verify setup before initial operation and after a change that can affect output. Verification shall address relevant material, tool, fixture, program, settings, measurement resources and line clearance.

First-output checks or another justified method shall confirm that the setup produces acceptable output before unrestricted continuation. The approved setup condition and verification result shall be recorded.

Changeover shall prevent mixing of products, labels, materials, software versions and acceptance records. Where last-output comparison supports setup assurance, its use and acceptance criteria shall be defined and the reference item protected from deterioration or confusion.

8.6 Process capability and stability

The organization shall determine whether process performance can consistently meet requirements under intended conditions. Evaluation shall consider relevant variation over time, machines, cavities, shifts, material sources and other influential conditions.

Where statistical capability measures are used, the organization shall justify the data selection, measurement suitability, distribution assumptions and stability of the process. An index calculated from unrepresentative or unstable data shall not be used as sufficient evidence of sustained capability.

Acceptance criteria for capability shall reflect customer requirements and the consequence of failure. Where quantitative capability analysis is unsuitable, the organization shall define another evidence-based means of demonstrating consistent performance.

An incapable or unstable process shall have containment, improvement action and increased verification sufficient to protect conformity. The organization shall verify improvement before removing additional controls. Inspection alone shall not be described as restoration of process capability.

8.7 In-process control and reaction

The organization shall perform the checks specified in the control plan at the defined intervals or events. Results shall be available soon enough to prevent avoidable continuation of uncontrolled work or release.

The reaction plan shall define who can stop work, how affected output is identified, the containment boundary, escalation and restart authority. Loss of control shall trigger evaluation back to the last adequately supported acceptable condition, with expansion where uncertainty warrants it.

Personnel shall record abnormal results and actions without alteration to make the process appear conforming. Repeated adjustment to remain within acceptance limits shall trigger evaluation of underlying process stability.

8.8 Error prevention and detection devices

The organization shall identify operations where foreseeable errors require engineered prevention or detection. It shall verify that the selected device or control addresses the intended failure and that its failure is detectable or otherwise controlled.

Challenge checks shall use defined methods and representative fault conditions at a frequency based on risk, use and device reliability. Challenge items shall be identified, protected and prevented from entering normal supply.

Failure or bypass of a device shall trigger a defined response. Temporary bypass shall require documented authorization, an effective alternative control, a defined duration and verification before normal operation resumes.

8.9 Special process qualification

Where the result of a process cannot be adequately verified by subsequent inspection or testing, the organization shall establish and maintain process qualification before routine use. Qualification shall demonstrate that the defined process, resources and operating window can achieve the required output.

The qualification basis shall identify materials, equipment, tooling, personnel competence, critical parameters, loading or application conditions and acceptance evidence. Examples may include joining, heat treatment, coating, bonding and certain additive manufacturing operations; classification shall depend on the actual verification limitations.

The organization shall monitor and retain the parameters necessary to demonstrate execution within the qualified conditions. Missing or out-of-limit critical parameter evidence shall trigger hold and technical disposition of affected output.

Requalification triggers shall include changes or deterioration that could invalidate the qualified basis. The extent of requalification shall be justified and approved by personnel competent in the process. An unverified final appearance shall not substitute for process qualification.

8.10 Tooling fixtures and reference items

The organization shall identify tooling, fixtures, gauges and reference items affecting conformity and control their approved use, condition and configuration. It shall define inspection, maintenance, storage and replacement criteria appropriate to wear and failure consequences.

Repairs or modifications that can affect output shall be evaluated and verified before return to use. Interchangeable tooling shall be managed so that the actual tool or cavity can be traced where needed to investigate or contain defects.

Customer-owned tooling and reference items shall be identified and protected. Loss, damage or unsuitability shall be recorded and communicated to the owner with its effect on current and planned supply.

8.11 Equipment maintenance and restart

The organization shall maintain equipment to sustain the approved process conditions. Maintenance planning shall use equipment criticality, operating history, manufacturer information and observed deterioration.

Unplanned failure shall trigger assessment of output produced before detection, not only repair of the equipment. Replacement parts and maintenance changes shall be evaluated for compatibility with the approved process.

After maintenance, prolonged shutdown, utility failure or other significant interruption, the organization shall verify readiness before routine operation resumes. Verification shall address relevant settings, safety and quality controls, calibration status, environmental conditions and first acceptable output.

8.12 Identification and traceability

The organization shall identify materials, work in progress, completed products and service outputs sufficiently to prevent confusion and establish status. Identification shall remain usable through handling, storage, external processing and delivery.

Traceability requirements shall be based on mandatory and customer obligations and the need to investigate, contain or recall affected output. The defined granularity shall address serial numbers, batches, time periods, process equipment, software configurations and supplied inputs where relevant.

The organization shall preserve links when lots are split, combined, reworked or transferred. For software-enabled products, records shall identify the installed or deployed configuration where it affects conformity.

Traceability shall be tested at planned intervals by following representative outputs to inputs and inputs to affected outputs. The organization shall evaluate completeness and retrieval time against its incident response needs and correct gaps.

8.13 Customer and external property

The organization shall identify and protect property provided by customers or other parties for use in its operations. Property may include materials, tooling, vehicles, samples, technical information, software and personal or commercially sensitive data.

Receipt checks shall identify missing, damaged or unsuitable property before reliance. Storage, access and permitted use shall follow the agreed conditions and relevant obligations.

Loss, damage, unauthorized use or loss of integrity shall be recorded and reported to the owner. The organization shall agree disposition and evaluate effects on affected output and evidence.

8.14 Material handling storage and preservation

The organization shall control handling, storage, packaging and internal transport to prevent deterioration, contamination, damage and mix-up. Conditions shall reflect the material or product, including relevant moisture, temperature, electrostatic, cleanliness and shelf-life limits.

Stock rotation shall account for expiry and deterioration risk. Expired or suspect items shall be held until an authorized technical decision establishes acceptable use or disposition; changing a label shall not extend a material's technical life.

Preservation controls shall cover intermediate states, returns and externally stored goods for which the organization retains responsibility. Packaging and transport arrangements shall be verified as suitable for the intended route and handling conditions.

8.15 Cleanliness and contamination control

Where contamination can affect conformity, the organization shall define the required cleanliness condition and controls for the product, process and environment. The basis shall identify relevant contaminants, limits and verification methods.

Controls shall address sources such as particles, fluids, residues, incompatible materials, packaging and maintenance activities. Cleaning operations shall be validated or otherwise demonstrated effective for the intended condition.

Changes in cleaning agents, equipment or preservation shall be evaluated before use. Failed cleanliness results shall trigger assessment of affected output and the effectiveness of the contamination controls.

8.16 Operational software and automated equipment

The organization shall control programs, recipes, parameters and software versions used to realize or accept output. Access to change them shall be authorized, and the effective version shall be identifiable at the operating point.

Changes shall be evaluated, verified and approved before deployment. The organization shall define recovery arrangements for failed deployment, loss of connectivity and corrupted configuration, including a safe and controlled response where automated operation cannot continue reliably.

Automated records and decisions shall remain linked to the relevant configuration and output. Controls for AI-supported quality decisions in Clause 5.18 apply when such tools are used within operations.

8.17 Temporary changes and alternative controls

The organization shall control temporary departures from the normal process or inspection arrangement. Authorization shall identify the reason, affected requirements, risk evaluation, alternative controls, responsible person, permitted scope and expiry or review point.

Personnel performing the affected work shall be informed before implementation. Required customer approval shall be obtained, and affected output shall be identifiable for follow-up.

The organization shall monitor the temporary arrangement and verify restoration of normal controls. A temporary instruction shall not remain indefinitely through repeated extensions without formal review of the process and its approval basis.

8.18 Rework and repair

The organization shall distinguish rework intended to restore full conformity from repair that makes an item acceptable for an authorized use without necessarily restoring every original requirement. It shall define who can approve each disposition.

Rework and repair instructions shall address the actual defect, approved method, risks introduced by the operation, permitted repetitions and required verification. A repaired item shall require any customer or other authorization necessary for acceptance of the resulting condition.

The organization shall maintain the original identity and record the operations performed and their results. Reworked or repaired output shall not be released until required reinspection or testing has confirmed the authorized acceptance criteria.

8.19 Nonconforming and suspect outputs

The organization shall identify and control nonconforming or suspect output to prevent unintended use or delivery. Controls shall include physical segregation or an equally effective system that remains reliable during transfers and system interruptions.

Disposition shall be made by an authorized competent person and shall identify the affected output, requirement, evidence and permitted action. Unresolved status shall remain on hold. Scrap shall be controlled to prevent its return to acceptable supply.

When nonconformity is discovered after delivery, the organization shall promptly evaluate risk and notify affected parties as required by the consequence and applicable obligations. It shall determine the population affected and initiate containment, correction or field action without waiting for completion of root-cause analysis where delay would increase harm.

8.20 Final verification and release

Before release, the organization shall confirm that planned realization and acceptance activities have been completed for the identified configuration. Required records, approvals and any concession conditions shall be available and consistent with the output being released.

Release shall identify the authorized person or validated automated release arrangement and the evidence supporting the decision. The organization shall prevent release where required checks have failed, evidence is missing or a hold remains unresolved.

Delegated release authority shall have defined competence and limits. Release by a supplier or automated system shall remain subject to the organization's responsibility for the output it supplies.

8.21 Delivery and operational handover

The organization shall verify that delivery documentation, identity, quantity, packaging and required operating or service information agree with the released output. Special handling or use restrictions shall be communicated to the receiving party.

For service delivery, the organization shall retain evidence of the work completed, relevant results, limitations and customer handover where required. An incomplete or interrupted service shall have an explicit status and an agreed next action.

Delivery damage, loss, incorrect configuration or missing information shall trigger investigation and corrective action appropriate to the event. Delivery completion shall not terminate responsibilities that continue under contract, law or the approved support arrangement.

8.22 Operational feedback and required evidence

The organization shall collect operational failures, downtime affecting conformity, scrap, rework, repeated adjustments and release escapes for review. Significant findings shall be returned to the responsible process owner, development authority and supplier management activity as relevant.

Retained evidence shall include authorized work, control plans, setup checks, capability or alternative performance evidence, special process qualifications, operating results, maintenance and restart verification, traceability, temporary controls and release decisions.

Records shall permit reconstruction of the relevant operating conditions and disposition of affected output. Broader performance and improvement provisions will be developed in Clause 12; the operational response requirements in this clause apply within this draft.

9 Product and technology requirements

9.1 Applicability and category selection

This clause establishes additional requirements according to the products, technologies and technical responsibilities within the assessed scope. The organization shall select every relevant category, including categories present within a combined product. Selection of one category shall not exclude another that also applies.

The organization shall distinguish responsibilities for development, integration, manufacture, supply, installation and support. It shall apply each requirement to the activity it performs or controls and record justified non-applicability under Clause 1. A distributor need not perform the original design validation, but shall obtain the assurance needed to establish the suitability of the product it supplies.

Category requirements supplement the common controls in Clauses 1 to 8. Where a new technology is not named, the organization shall identify its relevant failure mechanisms, technical interfaces and acceptance evidence through Clauses 4 and 6 and apply the closest relevant requirements without concealing additional risks.

9.2 Technical requirement and market specification

For each product family, the organization shall establish the intended application, operating limits, target markets and applicable technical requirements. The specification shall distinguish requirements for the supplied item from requirements that must be fulfilled by the vehicle or system integrator.

The organization shall identify the applicable editions and effective dates of external requirements that it has adopted or is obliged to meet. It shall resolve differing market or customer requirements before release and maintain evidence supporting the configuration supplied to each market.

This standard does not establish universal numerical limits for every automotive technology. The organization shall use applicable mandatory and contractual limits and establish technically justified acceptance criteria for remaining risks. An internal limit shall not reduce an applicable mandatory requirement.

9.3 Vehicle and system integration

An organization responsible for integration shall define the vehicle or system configuration, interfaces and permitted combinations of components and software. Integration verification shall address compatibility, installation, operating loads, environmental conditions and interactions affecting safety and performance.

The organization shall evaluate whether component evidence remains valid in the assembled application. It shall identify additional system-level evidence needed where installation, shared resources, control interactions or operating conditions differ from the component qualification basis.

Release evidence shall identify the integrated configuration and its approved application. A component approval shall not be presented as approval of the complete vehicle or integrated system. Changes affecting integration assumptions shall trigger renewed evaluation before release.

9.4 Structural and mechanical products

For structural and mechanical products, the organization shall establish the relevant load cases, interfaces, material properties, dimensional requirements and service conditions. Verification shall address failure

mechanisms relevant to the application, including fatigue, wear, corrosion, deformation and loss of retention where applicable.

Manufacturing controls shall preserve the properties on which design acceptance depends. Material substitution, heat history, forming, joining, surface treatment and repair shall be evaluated where they can alter those properties.

The organization shall define assembly conditions such as fastening, alignment, lubrication and adjustment where they influence conformity. Technical acceptance shall consider the assembled condition and relevant life-cycle exposure, rather than dimensional compliance alone.

9.5 Braking steering restraint and other safety functions

For functions whose failure can cause loss of vehicle control or protection, the organization shall identify safety-related requirements and maintain traceability to design, production and acceptance evidence. The analysis shall cover relevant normal, degraded and foreseeable fault conditions.

The responsible design or integration authority shall establish the required failure response, monitoring, warning and recovery behavior. Verification shall demonstrate that the defined response remains effective within the intended application and operating limits.

Substitutions, adjustments and repairs affecting these functions shall require authorized technical instructions and verification. Release shall be prevented where a safety-related requirement is unresolved or evidence does not support the claimed configuration.

9.6 Materials chemicals and restricted substances

The organization shall specify material identity, composition or relevant properties, compatibility and conditions necessary to preserve conformity. Purchased and processed material shall remain linked to the required specification and supporting batch evidence.

Where substance restrictions, material declarations or customer disclosure requirements apply, the organization shall obtain and maintain reliable information for the supplied configuration. It shall evaluate the completeness and relevance of supplier declarations and use additional verification when risk or evidence quality warrants it.

Changes in formulation, recycled content, supplier or processing conditions shall be assessed for effects on performance, durability, processing and applicable obligations. A material shall not be accepted solely because its commercial name or nominal grade matches an earlier supply.

9.7 Combustion powertrains fuels and fluid systems

For combustion powertrains and associated fuel, lubrication, cooling and exhaust systems, the organization shall define relevant operating conditions, material compatibility, thermal behavior, pressure limits and control functions. It shall evaluate leakage, loss of lubrication or cooling, incorrect fluid use and other relevant failure conditions.

Where emissions or energy performance requirements apply, the responsible organization shall maintain traceable evidence for the actual hardware and software configuration and the specified test conditions. Calibration changes shall be evaluated for their effect on all affected requirements, not only the intended performance objective.

Production and service controls shall preserve approved settings, fluid cleanliness and interface integrity. The organization shall prevent unauthorized changes that invalidate the approved performance or market conformity basis.

9.8 Electrical and electronic products

For electrical and electronic products, the organization shall define the relevant supply conditions, loads, protection, signal interfaces and environmental exposure. Verification shall address relevant electrical, thermal, mechanical and electromagnetic conditions and their effect on the intended function.

The organization shall control components, assembly processes, configuration and handling conditions needed to preserve reliability. Changes in components or manufacturing processes shall be assessed for compatibility, availability of supporting evidence and the effect on previously qualified performance.

Test coverage shall address foreseeable incorrect connection, abnormal supply and interface conditions where these can affect safety or conformity. A successful functional test under nominal conditions shall not be treated as sufficient evidence for the full specified operating range.

9.9 Electric drive and high voltage systems

For electric drive and high voltage systems, the organization shall identify relevant electrical isolation, energy control, protection and thermal management requirements. Responsibilities for the component, installation and complete system shall be explicit.

The organization shall verify the required behavior during startup, operation, shutdown, charging, faults and service conditions as relevant to its responsibility. Interfaces among the energy source, conversion equipment, drive system and vehicle controls shall be included in the verification basis.

Manufacturing, handling and service activities involving hazardous stored or supplied energy shall be restricted to authorized competent personnel using approved controls. Identification and isolation status shall remain clear during transport, storage, testing, repair and return to service.

9.10 Cells battery modules and battery packs

For cells, modules and packs, the organization shall specify the intended chemistry or technology, operating window, performance, durability and safety requirements relevant to the supplied level. It shall maintain traceability of critical materials, cells, assembly configuration and control software to the extent needed for investigation and containment.

Qualification shall address relevant electrical, mechanical, thermal and environmental exposure, including foreseeable abuse and failure propagation where applicable to the design responsibility. The organization shall define technically justified acceptance criteria and retain the basis for selecting representative test items and conditions.

Manufacturing controls shall address relevant contamination, moisture, joining, sealing, electrical connection and inspection risks. Evidence of acceptance at cell level shall not replace module or pack verification where assembly and integration introduce additional risks.

The organization shall establish procedures for identifying, segregating and managing damaged, defective or otherwise suspect batteries. Handling and transport decisions shall use applicable requirements and a competent assessment of condition. An item with uncertain history shall not be assumed suitable for unrestricted use.

9.11 Battery control diagnostics and condition information

Where battery management or diagnostic functions are supplied, the organization shall define the measurements, estimation methods, protective actions and information needed for the intended application. Verification shall address relevant sensor faults, communication failures, estimation uncertainty and changes with age or operating history.

Claims concerning capacity, remaining life or state of health shall identify the method, conditions and limitations supporting the result. The organization shall prevent estimates from being presented as directly measured facts where that distinction affects a service or safety decision.

Changes to control limits, diagnostic algorithms or configuration shall be evaluated against the battery and vehicle application. The organization shall preserve enough version and service history to determine which units are affected by a correction or revised operating limitation.

9.12 Charging and energy transfer equipment

For charging and energy transfer equipment, the organization shall define electrical, mechanical, communication and environmental interfaces and the permitted operating configurations. Verification shall cover relevant compatibility, protective functions, abnormal conditions and interruption of energy transfer.

Where equipment reports delivered energy or supports payment, the organization shall control the accuracy, integrity and traceability of information used for the transaction and fulfil applicable measurement obligations. Communication compatibility shall not be treated as proof of electrical or installation safety.

Installation and commissioning requirements shall identify checks necessary at the actual site.

Responsibilities for equipment, connection, infrastructure, software services, maintenance and incident response shall be defined before operation begins.

9.13 Hydrogen and other stored fuel systems

For hydrogen and other stored fuel technologies, the organization shall define the intended fuel, pressure and temperature conditions, material compatibility, containment and protective functions. Evaluation shall address leakage, degradation, incorrect connection and relevant storage, transfer and service conditions.

The design and integration authority shall define verification evidence for the supplied configuration and the installation assumptions on which it relies. Components with a defined life, inspection interval or restricted service history shall remain identifiable throughout supply and support.

Work affecting fuel containment or protective functions shall use authorized methods and competent personnel. Return to use shall require the relevant integrity and functional checks and confirmation that required replacement or inspection conditions have been met.

9.14 Software products and embedded software

For software affecting an automotive product or service, the organization shall control requirements, architecture, implementation, dependencies, verification and release. It shall maintain the connection between source or controlled development inputs, build environment and released executable or deployable items to the extent necessary for reproducibility and investigation.

Verification shall address the intended functions, interfaces, failure handling and relevant regression risks. The organization shall define review and test coverage according to criticality and shall record known defects, limitations and their disposition before release.

External software and reusable components shall be evaluated for suitability, version, support and known limitations. The organization shall maintain an inventory of relevant components and dependencies sufficient to identify exposure when a defect, vulnerability or support change is discovered.

Software obsolescence and end of support shall be considered during development and contractual commitment. Loss of access to a development tool or external service shall be addressed where it prevents correction, recovery or required evidence retention.

9.15 Functional safety assurance

Where malfunction of an electrical, electronic or programmable function can create a safety risk, the organization shall establish a documented safety assurance approach proportionate to that risk. It shall identify hazards, required risk reduction, allocated safety requirements and the responsibilities for their implementation and verification.

The safety analysis shall address relevant faults, dependencies and assumptions across the system boundary. Development and verification activities shall provide the independence and competence needed to challenge safety-critical decisions. Any selected safety classification scheme shall be identified with its applicable criteria.

Before release, the responsible authority shall review a coherent body of evidence connecting safety requirements with implemented controls, verification results, residual limitations and operational assumptions. A classification label or process completion checklist alone shall not establish that the required safety outcome has been achieved.

Changes and field findings that invalidate a safety assumption shall trigger reassessment, containment where necessary and communication to affected integrators or users.

9.16 Cybersecurity of connected products and services

For connected products or services, the organization shall identify assets, interfaces and foreseeable threats that can affect safety, conformity, service availability or the integrity of quality information. It shall define security requirements and responsibilities across development, deployment, operation and support.

Controls shall address relevant identity and access, communication, update authenticity, key or credential management, logging and recovery. Verification shall evaluate the effectiveness of controls under representative misuse and attack conditions within an authorized test scope.

The organization shall establish a route for receiving vulnerability information and a process for assessing exposure, prioritizing action and informing affected parties. Decisions to defer a correction shall identify the risk, compensating controls, authority and reconsideration point.

Support commitments shall define how security updates and end-of-support conditions are managed. The organization shall not treat a one-time security test as proof that a connected product remains secure throughout its operating life.

9.17 Driver assistance and automated driving functions

For driver assistance or automated driving functions, the responsible organization shall define the intended function, the permitted operating conditions, user responsibilities and limits of system performance. The defined operating domain shall identify the conditions within which the evidence supports use.

Validation shall address representative and challenging scenarios, relevant interactions with road users, environmental limitations and foreseeable misuse. It shall evaluate performance limitations even when the implemented components operate without an internal fault.

The organization shall define behavior when operating limits are approached or exceeded, including relevant warnings, transition of control and fallback. Human interaction assumptions shall be evaluated through suitable evidence rather than reliance on an instruction alone.

Claims of automation capability shall remain consistent with the validated function and its restrictions. Changes to sensors, algorithms, maps or operating domain shall trigger impact assessment and the necessary renewed validation.

9.18 Artificial intelligence in supplied products and services

Where AI influences a supplied function or decision, the organization shall define the intended use, decision consequences, performance criteria, operating limits and responsible authority. It shall establish the assurance needed for both normal and consequential failure cases.

Data used for development and evaluation shall be controlled for provenance, permitted use, relevance, quality and separation where necessary to avoid misleading evaluation. Performance evaluation shall include relevant populations and conditions, uncertainty, out-of-scope inputs and unequal failure patterns that could affect conformity or safety.

The organization shall control model versions, training or tuning changes and deployment configuration. Learning or adaptation during operation shall be bounded by approved controls; changes outside the validated envelope shall require renewed assessment before continued unrestricted use.

Monitoring shall detect deterioration relevant to the intended outcome and trigger review, restriction or withdrawal. Human oversight shall be specified where needed, including the competence, information and time required for effective intervention. Internal AI-supported quality decisions also remain subject to Clause 5.18.

9.19 Software updates and remote changes

The organization shall control updates affecting product behavior, security, conformity or user information. Before deployment, it shall identify the affected configurations, prerequisites, compatibility, verification evidence and required customer or other authorization.

Deployment shall protect update authenticity and integrity and provide evidence of the configuration actually installed. The organization shall define a controlled response to interruption, failed installation or unsuccessful activation, including recovery or rollback where technically appropriate and safe.

Users and service personnel shall receive information necessary to understand material changes and operating restrictions. Campaign records shall distinguish eligible, attempted, successful, failed and pending updates and support action for units that remain exposed.

9.20 Remanufactured reused and replacement products

The organization shall distinguish new, reused, repaired and remanufactured products in specifications, records and supply information. It shall define eligibility, incoming condition assessment, required restoration, verification and permitted application for each category it supplies.

Replacement compatibility shall be established for the relevant vehicle, system and configuration. Dimensional interchangeability alone shall not justify equivalence where materials, performance, durability, software or protective functions differ.

For reused or remanufactured items, the organization shall evaluate history, deterioration and residual life where relevant to the application. Unknown history shall be treated as uncertainty requiring additional assurance or restriction. Original identification and new processing history shall remain connected where necessary for traceability.

Claims of restored performance or service life shall be supported by acceptance evidence and communicated limitations. Original approval or branding shall not be used to imply authorization of a changed product without a valid basis.

9.21 Production equipment tooling and industrial automation

Organizations supplying production equipment, tooling or automation shall define the intended process, output requirements, capacity, interfaces and conditions of installation and use. Verification shall address the ability to maintain the required process conditions and to detect relevant loss of control.

Acceptance shall distinguish checks completed before shipment from checks required after installation and integration. The supplier shall provide the instructions, configuration information, maintenance requirements and competence needs necessary for controlled operation.

Changes to equipment software, fixtures or measurement functions shall identify their effect on the customer's process qualification and output acceptance. The organization shall communicate relevant restrictions and verification needs with the change.

9.22 Durability circularity and end of life information

The organization shall define service-life assumptions and relevant inspection, maintenance and replacement conditions for its supplied product. Claims concerning durability, repairability, recycled content or recovery shall be supported by an identified method and applicable evidence.

Where dismantling, reuse or recovery is within the scope or an applicable obligation, the organization shall provide the information needed to identify materials, hazardous energy and relevant handling restrictions. Recovery processes shall prevent nonconforming items from returning to unrestricted supply without appropriate qualification.

A change made for resource efficiency shall be evaluated for its effect on safety, performance, durability and traceability. An environmental benefit claim shall not substitute for technical conformity evidence.

9.23 Required evidence

The organization shall retain its category selection, application and market specifications, qualification evidence, configuration records, technical risk decisions and support limitations. Evidence shall distinguish component, subsystem and integrated-system conclusions and show resolution of interface risks and conflicting assumptions. Information needed to fulfil remaining integration or support responsibilities shall be provided to the receiving party.

10 Services and aftersales

10.1 Applicability

This clause applies to automotive services and responsibilities continuing after delivery, including sales support, distribution, installation, maintenance, repair, diagnostics, software operation, fleet support, logistics and recovery where within scope. It also applies to the service delivery aspects of technical testing and assessment; detailed measurement requirements are in Clause 11.

The organization shall identify the service activities it performs or controls and the products, users and locations affected. A manufacturer retaining warranty or field-support responsibility shall apply the relevant aftersales requirements even when service execution is outsourced.

10.2 Service definition and acceptance of work

Before accepting work, the organization shall define the requested outcome, scope, applicable requirements, customer inputs, completion criteria and limitations. It shall evaluate competence, equipment, information access, capacity and any required authorization.

The service agreement or work authorization shall identify responsibility for diagnosis, additional work, third-party involvement, price or time changes where relevant, and communication of unresolved conditions. Material changes to the agreed scope shall be authorized and recorded before implementation, except immediate protective action needed under established emergency arrangements.

The organization shall not promise a result that its methods or available evidence cannot support. Where a customer requests work that would invalidate a mandatory condition or create an unacceptable safety risk, the conflict shall be resolved before affected work proceeds.

10.3 Customer intake and identification

The organization shall confirm the identity of the customer or authorized representative and the vehicle, product, sample or service account concerned. Relevant configuration, condition, complaint and prior work shall be recorded to the extent needed for correct execution and traceability.

Customer-supplied information shall be checked for ambiguity or inconsistency that can affect the work. Known limitations or missing history shall be communicated and accounted for in the service plan.

Items received shall have an identified acceptance status. Existing damage, missing parts and restrictions on testing or use shall be documented and agreed where necessary before the organization assumes control.

10.4 Diagnosis and technical evaluation

Diagnostic work shall use suitable methods, current technical information and competent personnel. The organization shall distinguish observed symptoms, measured findings, probable causes and confirmed causes in its records and communication.

The organization shall evaluate whether the selected diagnostic method covers the reported condition and relevant safety consequences. Replacement of a component shall not be treated as proof that the cause has been established or that related conditions have been resolved.

Where no fault is found, the report shall identify the checks performed, conditions, limitations and any remaining concern. Repeat complaints and intermittent failures shall trigger review of the diagnostic approach and escalation where the evidence remains inconclusive.

10.5 Service competence and authorization

The organization shall define task-specific competence and authorization for service activities, including work affecting vehicle control, stored energy, safety systems, software or technical acceptance. Personnel shall demonstrate the required practical competence before independent assignment.

Authorization shall identify permitted tasks, technologies, methods and restrictions. Changes in product technology, technical instructions or evidence of unsuccessful work shall trigger review of competence under Clause 5.

External personnel shall be subject to equivalent controls for the assigned task. A training attendance record or general trade qualification shall not, by itself, authorize every specialized operation.

10.6 Service information tools and parts

The organization shall provide current authorized technical instructions and verify that tools, diagnostic equipment and software are suitable for the specific application. Access restrictions shall be resolved through legitimate arrangements and shall not justify use of unverified instructions.

Parts, materials and consumables shall be accepted and traceable to the extent required by risk and applicable obligations. Substitution shall require a documented compatibility decision and any necessary customer or technical authority approval.

The organization shall control the versions and settings of service software that can change product configuration. Tools that produce acceptance evidence shall be subject to the relevant measurement and software controls in Clause 11.

10.7 Maintenance repair and installation execution

The organization shall execute work against the authorized scope and retain evidence of significant operations, findings, parts and configuration changes. Work affecting a safety function shall include the verification needed to establish correct restoration or installation.

Instructions shall identify precautions for hazardous energy, lifting, containment and other conditions relevant to the task. Interrupted work shall have a clearly recorded state and controls preventing an incomplete item from being returned to use.

Where an unexpected condition changes the technical basis, the organization shall stop the affected activity, assess the implications and obtain the required authorization. Completion of the original work instruction shall not justify ignoring a discovered safety concern.

10.8 Calibration coding and software service operations

The organization shall identify the conditions requiring calibration, initialization, coding or software configuration after replacement, repair or installation. It shall use the approved method and confirm the required prerequisites and equipment suitability.

Records shall identify the prior and resulting configuration where relevant, the operation performed, acceptance result and responsible person. The organization shall evaluate the effect of a failed or interrupted operation and restore a controlled state before release.

Where a service change affects approval, security, functionality or compatibility, the relevant design or integration authority shall be involved. Access to a coding function shall not be treated as authority to make any available change.

10.9 Service verification and return to use

Before completion, the organization shall verify that the authorized work has achieved the specified outcome and that introduced or affected conditions have been addressed. Verification shall use defined criteria and suitable functional, diagnostic, inspection or test evidence.

The release record shall identify the item or service, work completed, acceptance results, limitations and release authority. Unresolved safety or mandatory conformity conditions shall prevent unrestricted return to use and shall be communicated through an appropriate controlled arrangement.

Where a road or operational test is necessary, it shall be planned with competent personnel, appropriate authorization and controls for the test conditions. An uncontrolled customer trial shall not substitute for required verification.

10.10 Customer handover and service records

The organization shall explain the work completed, relevant configuration changes, remaining restrictions and required follow-up in a form the customer can understand. Information shall distinguish recommendations from conditions necessary for safe or conforming use.

The service record shall provide traceability to significant parts, methods, results and responsible personnel where relevant. The organization shall preserve this information for the period required by its obligations and risk-based retention rules.

Where the customer declines recommended or necessary work, the organization shall record the decision and communicate its implications. Customer refusal shall not authorize a false statement that the item meets requirements or remove a mandatory protective obligation.

10.11 Warranty complaints and field feedback

The organization shall provide accessible means to receive complaints, warranty claims and field observations. It shall record the affected product or service, configuration, reported condition, consequence and available evidence without requiring confirmation of the cause before intake.

Triage shall distinguish urgent safety or regulatory concerns from routine service matters. The organization shall establish response times, escalation routes and ownership proportionate to the consequences and applicable obligations.

Analysis shall consider repeat events, patterns across configurations and failures reported through external service networks. Administrative rejection of a warranty claim shall not remove the need to evaluate a credible technical or safety issue.

10.12 Returned items and failure investigation

Returned items shall be identified, preserved and handled to protect personnel and retain evidence needed for investigation. The organization shall record relevant transport or handling conditions that may have altered the item.

Investigation shall distinguish the received condition from changes introduced during examination. Destructive work shall be authorized and documented, with preservation of necessary observations, samples or records before evidence is consumed.

The organization shall connect findings to design, process, supplier and service history as relevant. Inconclusive results shall remain identified as such and shall not be converted into a finding of no defect without supporting evidence.

10.13 Field actions recalls and service campaigns

The organization shall maintain a process for assessing and initiating corrective field actions within its responsibility. The process shall define decision authority, technical assessment, affected population, notification, remedy, execution and effectiveness monitoring.

When delay could increase exposure to serious harm or breach a mandatory obligation, protective action shall proceed on the available evidence without waiting for complete root-cause confirmation. Decisions and evolving uncertainty shall be documented and reassessed as information improves.

Campaign control shall identify affected units or users and distinguish notified, reached, corrected, unsuccessful and outstanding cases. The organization shall verify that the remedy addresses the technical issue and does not introduce unacceptable new risks.

Closure shall consider residual exposure, incomplete coverage and the effectiveness of communication and remedy. A high completion percentage alone shall not justify ignoring known uncorrected high-risk cases. Required authority reporting and external coordination shall be completed.

10.14 Distribution warehousing and logistics services

Organizations handling or distributing automotive products shall define controls for identity, acceptance status, preservation, stock rotation, configuration and delivery accuracy. Controls shall cover relevant contractors, transfer points and temporary storage.

Transport planning shall account for product condition, packaging, route, environmental exposure and applicable handling requirements. Damage, missing identification, broken seals or breached storage limits shall trigger assessment before onward supply.

The organization shall retain proof of custody and delivery where needed for traceability, acceptance or incident investigation. Logistics completion shall not be recorded solely from an unverified system event where physical receipt or condition must be established.

10.15 Fleet mobility and remotely operated services

For fleet, mobility or remotely operated services, the organization shall define service availability, vehicle or equipment readiness, operating restrictions and responsibilities between the operator, user and external providers. Readiness checks shall address relevant maintenance, open campaigns and configuration status.

The organization shall control access, booking, dispatch and suspension decisions that affect safe or conforming use. Fault reports and interrupted service shall have a response appropriate to the location, users affected and consequence of delay.

Where remote operation or assistance is supplied, communication loss, unclear situational information and limits of human intervention shall be addressed in the approved operating method. Personnel shall have defined authority and competence, and significant decisions shall be traceable.

10.16 Digital service continuity and customer information

For ongoing digital services, the organization shall define availability commitments, dependencies, incident response, recovery and customer communication. It shall verify restoration of essential functions and information after interruption.

Service changes shall be evaluated for compatibility, accessibility of necessary customer information and the effect on existing commitments. Planned withdrawal or end of support shall include timely notice, data access or transfer arrangements where required, and treatment of safety or conformity dependencies.

Customer and vehicle information shall be controlled for authorized access, appropriate use, retention and integrity. Personal or commercially sensitive information shall not be disclosed merely because it is available within a technical support system.

10.17 Service network control

Where service is delivered through dealers, franchisees, agents or subcontractors, the organization shall define the requirements and evidence necessary for consistent delivery. Approval and monitoring shall address competence, instructions, tools, parts, reporting and escalation.

The organization shall verify that critical technical updates and campaign instructions reach the execution point and are implemented. Recurring network failures shall trigger targeted evaluation and corrective action.

Responsibility for customer resolution and technical containment shall remain explicit when several parties are involved. Referral to another organization shall not close a case while an assigned obligation remains unfulfilled.

10.18 Required evidence

The organization shall retain service scope and authorization, intake condition, significant diagnostic and execution records, parts and configuration changes, verification, release and customer handover. It shall maintain complaint, warranty, investigation and campaign records where those responsibilities exist.

Evidence shall connect an individual service outcome with the relevant product or account, method, competent personnel and acceptance decision. Network and digital service records shall support investigation across organizational and system boundaries without requiring duplicate documentation.

11 Measurement testing and conformity control

11.1 Applicability

This clause applies to measurement, inspection, testing, calibration, sampling and technical decisions used to determine conformity of products, processes or services. It applies to internal facilities, mobile or on-site work and controlled external services to the extent of the organization's responsibility.

A laboratory shall apply the requirements relevant to its activities even when it performs no manufacturing. A manufacturer using an external laboratory shall control the purchased service under Clause 7 and verify that the evidence is suitable for its acceptance decision.

These provisions establish requirements within IAF AQMS. They do not, by themselves, confer laboratory accreditation or establish conformity with another laboratory or inspection standard.

11.2 Technical scope and authority

The organization shall define the measurements, methods, ranges, item types, locations and decision activities within its technical scope. It shall identify limitations and distinguish established capability from work requiring development, external support or restricted authorization.

Personnel approving methods, interpreting results or authorizing reports shall have documented competence and authority for the relevant scope. Supervised or developmental work shall be clearly identified and subject to appropriate review before its results support release.

Commercial or production pressure shall not determine technical results. The organization shall control conflicts affecting sampling, execution, interpretation and reporting and provide a route for escalation of interference.

11.3 Review of measurement and test requests

Before work begins, the organization shall confirm the question to be answered, item identification, method, specification, acceptance criteria, reporting needs and intended use of the result. It shall verify that resources and method capability are sufficient for the requested decision.

Where conformity statements are requested, the applicable decision rule shall be established before evaluation and agreed with the customer unless prescribed by a mandatory requirement. Sampling responsibility, customer-supplied information and deviations from normal conditions shall be identified.

An unclear request shall be resolved before a result is used for acceptance. Changes to the agreed work shall be recorded and communicated to affected personnel and the customer where necessary.

11.4 Selection and control of methods

The organization shall select methods suitable for the characteristic, range, material, environment and intended decision. The controlled method shall identify preparation, equipment, conditions, execution, calculations, acceptance of the run and reporting requirements.

The relevant edition or revision shall be identifiable at the point of use. Changes to an external method shall be reviewed for impact before implementation. Obsolete methods shall be used only with a justified authorized basis consistent with applicable obligations.

Where several methods can produce different outcomes, the organization shall establish which method governs acceptance. Results from another method shall not be treated as interchangeable without supporting evidence.

11.5 Method verification and validation

Before introducing an established method, the organization shall verify that it can achieve the performance required under its actual operating conditions. The verification shall address relevant equipment, personnel, environment, range and item characteristics.

Methods developed internally, modified methods and established methods used outside their demonstrated scope shall be validated to the extent necessary for their intended use. Validation shall examine relevant performance characteristics and limitations, including precision, bias, range, selectivity, detection capability and robustness where applicable.

The organization shall define acceptance criteria before evaluating validation results. It shall retain the plan, data, analysis, limitations and approval. A method change or new application shall trigger review of whether existing evidence remains adequate.

11.6 Sampling design and execution

Where the organization samples to support a conclusion about a population, it shall establish a sampling plan appropriate to the population, variation, risk and intended inference. The plan shall define selection, sample size, locations or time points, preparation and treatment of exceptions.

Sampling shall avoid selection bias that could invalidate the conclusion. Deviations from the plan and constraints on access shall be recorded and considered when interpreting the results.

Sampling records shall identify the population or source, method, date, location, responsible person and conditions relevant to the result. A conclusion based on a sample shall not be extended beyond the supported population or conditions.

11.7 Item receipt handling and chain of custody

The organization shall identify each item or sample and record its condition on receipt. Damage, insufficient quantity, uncertain identity, unsuitable preservation or other departures affecting validity shall be resolved or explicitly controlled before work proceeds.

Identification shall remain linked to preparation, subsampling, storage, testing and disposition. Where chain of custody is required, transfers shall identify the responsible parties, dates and conditions necessary to demonstrate control.

The organization shall prevent deterioration, contamination and mix-up through defined handling and storage arrangements. Consumption, return or disposal shall follow the agreed requirements and any need to preserve evidence for review or dispute.

11.8 Facilities environment and site conditions

The organization shall define and monitor environmental conditions that can affect the method or result. It shall control access, interference, cleanliness and separation of incompatible activities where relevant.

Work shall be suspended or restricted when required conditions are not met. The organization shall evaluate results obtained during an uncontrolled period and determine whether repeat work, correction or notification is necessary.

For mobile or customer-site work, suitability shall be confirmed at the actual location. The record shall identify conditions and limitations that affect the validity or interpretation of the result.

11.9 Equipment calibration and metrological traceability

Equipment shall be suitable for the method, range, resolution and required accuracy or uncertainty. The organization shall identify equipment affecting validity and maintain its calibration, verification, maintenance and authorized-use status.

Where metrological traceability is required, the organization shall establish a documented chain to an appropriate reference, with each relevant contribution to uncertainty addressed. Calibration service selection shall consider demonstrated technical competence and scope, not only the presence of a calibration label.

Where traceability to a recognized measurement reference is not technically available, the organization shall establish and justify another suitable reference or comparison basis. The limitation shall be considered in the use and reporting of the result.

Calibration intervals shall be reviewed using stability, use, environment and consequence of failure. Out-of-tolerance equipment shall trigger evaluation of earlier results and affected conformity decisions under a documented technical assessment.

11.10 Reference materials and intermediate checks

Reference materials, standards and check items shall be suitable for their intended use and identified by relevant assigned values, uncertainty, validity and storage conditions. The organization shall control preparation, dilution, handling and expiry where these can affect performance.

Intermediate checks shall be planned to detect deterioration or change between calibrations. The plan shall define the item or standard used, method, frequency, acceptance limits and response to failure.

A failed intermediate check shall not be dismissed solely because the formal calibration date has not expired. The organization shall assess the affected period and determine the validity of intervening results.

11.11 Measurement system analysis

For measurement systems used in production or service acceptance, the organization shall evaluate whether the combined equipment, method, personnel, fixturing, environment and item variation permit reliable decisions. The evaluation shall represent actual operating conditions and relevant users or automated configurations.

Analysis shall address repeatability, reproducibility, bias, stability and resolution as relevant. Attribute or visual decisions shall be evaluated for consistency and the risk of incorrect acceptance or rejection using suitable reference decisions or another justified basis.

Acceptance criteria shall reflect the tolerance, intended use and consequences of error. An unacceptable measurement system shall be improved, restricted or replaced, and affected acceptance decisions shall be evaluated.

11.12 Measurement uncertainty

The organization shall identify and evaluate significant sources of uncertainty where they affect the validity, interpretation or conformity use of a measurement. The evaluation shall address relevant sampling, preparation, equipment, reference values, environmental conditions, method and personnel contributions.

The approach shall be suitable for the method and intended decision and shall use technically justified information. Where a detailed numerical evaluation is not feasible, the organization shall document the limitations and adopt controls that make the result fit for the intended use.

Uncertainty estimates shall be reviewed after changes or new evidence affecting their basis. Reporting shall include uncertainty where required by the customer, method, applicable obligation or interpretation of the result.

11.13 Decision rules and conformity statements

A conformity decision shall identify the specification, applicable limit, result and rule used to account for uncertainty or decision risk. The organization shall define how results close to a limit, insufficient evidence and indeterminate outcomes are treated.

Where a guard band or other acceptance rule is used, its basis shall be documented. The organization shall not select a more favorable rule after observing the result in order to convert a failure into a pass.

Reports shall make clear which results and requirements the conformity statement covers. A limited test shall not support a claim of complete product conformity unless the applicable conformity procedure provides a valid basis for that conclusion.

11.14 Execution and technical records

The organization shall record original observations, relevant conditions, equipment identity, method revision, personnel, calculations and item configuration sufficiently to permit technical review and, where practicable, repetition. Data shall be recorded when the activity occurs or by a controlled automatic capture system.

Changes to technical records shall preserve the original entry or an accessible audit trail and identify the reason and person making the change. The organization shall prevent selective retention of favorable runs or deletion of inconvenient results.

Departures from the method shall be authorized, technically justified and evaluated for their effect on validity. A departure that removes a mandatory acceptance condition shall prevent an unqualified conformity statement.

11.15 Validity monitoring and comparison activities

The organization shall plan monitoring to detect errors, drift and inconsistency in its measurement and testing activities. Suitable approaches may include check samples, replicate work, reference materials, control charts, blind samples and comparisons between personnel or equipment.

Where relevant comparison or proficiency activities are available, the organization shall determine participation according to risk and the need for external assurance. If suitable activities are unavailable, it shall document and implement an alternative means of evaluating performance.

Unsatisfactory or suspicious results shall be investigated and their effect on customer work assessed. Successful participation in one comparison shall not be treated as proof of competence for unrelated methods, ranges or materials.

11.16 Test software automated analysis and data systems

Software used to acquire, transform, calculate, interpret or report results shall be verified or validated for its intended use before reliance and after changes affecting validity. The organization shall control formulas, units, rounding, interfaces, permissions and configuration.

Verification shall include representative inputs, boundary cases and foreseeable invalid data. Transfer between instruments, spreadsheets and reporting systems shall preserve identity, completeness and numerical meaning.

The organization shall maintain recovery and audit-trail arrangements for essential data. AI-supported interpretation shall also meet Clause 5.18, including evidence that model performance is appropriate for the actual measurement application.

11.17 Technical review and reporting

Before issue, an authorized competent person shall review the report for item identity, method, results, calculations, limitations and consistency of conclusions with the evidence. The extent of review shall reflect the consequence of an incorrect report and the effectiveness of validated automated controls.

The report shall identify the issuing organization, unique report reference, relevant customer and item, method, dates, results, units and authorization. It shall identify material deviations, uncertainty where required, sampling limitations and any statement of conformity with its governing rule.

Customer-supplied information and externally obtained results shall be distinguishable where they affect interpretation or responsibility. Opinions or interpretations shall be clearly identified and have a documented technical basis within the competence of the person authorizing them.

The organization shall prevent a report from implying accreditation, approval or scope that it does not hold. Amendments shall identify the original report, changed information, reason and authorization, and affected recipients shall be informed where needed.

11.18 Nonconforming technical work

When an activity or result does not meet the applicable technical controls, the organization shall assess the significance, stop or restrict affected work and prevent unsupported release. It shall identify the period, items, methods and decisions potentially affected.

Disposition shall address repeat work, revised interpretation, withdrawal or amendment of reports and customer notification as appropriate. The organization shall consider the validity of earlier results even when the immediate defect has been corrected.

Work shall resume only after an authorized technical review confirms that the initiating condition is controlled and the required assurance has been restored. Corrective action shall address recurrence where the event indicates a systemic weakness.

11.19 External laboratory and inspection evidence

When using external technical evidence, the organization shall verify the provider's relevant competence, method, scope, item identity and limitations. Required accreditation or customer approval shall be verified for the activity actually performed.

The organization shall assess whether the external result answers its acceptance question and whether sampling, conditions and configuration are representative. It shall resolve ambiguous, inconsistent or incomplete evidence before relying on it for release.

Reproduction of an external result shall preserve its meaning and source. The organization shall not present work performed elsewhere as its own execution or remove a limitation that is material to the conclusion.

11.20 Ongoing verification of product and process conformity

The organization shall determine when conformity must be reconfirmed after initial approval, using changes, operating history, deterioration risk and applicable obligations. The plan shall identify the characteristics, methods, frequency or triggers and acceptance authority.

Periodic or event-based testing shall use items representative of current production or service delivery. Failure shall trigger evaluation of intervening output and the continued validity of the approved process or configuration.

The organization shall connect this evidence with production controls and field findings. A historical qualification report shall not justify continued release where current evidence indicates that the qualification basis is no longer valid.

11.21 Required evidence

The organization shall retain technical scope and authorizations, request reviews, methods, verification and validation, sampling and item records, equipment and reference status, measurement system evaluations, uncertainty and decision rules, original data and authorized reports.

Records shall include validity monitoring, technical nonconformity dispositions and the review of external evidence where relevant. They shall permit reconstruction of how a reported result or acceptance decision was reached, including the limitations of the underlying evidence.

12 Performance and improvement

12.1 Applicability

This clause applies to every organization within the scope of this standard. Performance evaluation shall cover the activities and responsibilities established under Clause 1, including externally provided activities whose results affect the organization's commitments.

An organization performing assessment or certification shall evaluate the quality, impartiality and reliability of those services. It shall not substitute manufacturing indicators for measures relevant to its actual services.

12.2 Performance evaluation plan

The organization shall define what will be monitored, the purpose of each measure, the source of data, the calculation method, the responsible owner and the review frequency. The plan shall identify acceptance limits or objectives and the response required when performance departs from them.

Measures shall address conformity, customer experience, delivery, process effectiveness, significant risks and the effectiveness of improvement actions. Measures shall cover relevant operational levels so that aggregation does not conceal a failing site, shift, product family or service activity.

12.3 Indicator definitions and data integrity

Each significant indicator shall have a controlled definition specifying the population, numerator and denominator where relevant, time basis, exclusions and treatment of missing or corrected data. Changes in definitions shall be identified in trend reports and shall not create a misleading appearance of improvement.

The organization shall verify data completeness and accuracy at intervals appropriate to the consequence of an incorrect decision. Data drawn from automated systems shall remain traceable to a controlled source. Estimates shall be identified, with their limitations and the planned means of obtaining reliable information.

Personnel shall be able to report adverse results without pressure to suppress or reclassify them. Deliberate concealment or falsification shall trigger investigation of affected decisions and the management conditions that permitted it.

12.4 Customer and field performance

The organization shall evaluate customer feedback, complaints, returns, warranty experience, delivery performance and customer assessments relevant to its scope. Absence of complaints shall not by itself establish customer satisfaction or product reliability.

Field information shall be analyzed by relevant configuration, application, age, exposure and failure mode where those distinctions affect the conclusion. The organization shall identify emerging patterns and communicate significant findings to the functions responsible for design, suppliers, production and service.

Safety signals shall be escalated under the incident controls without waiting for a scheduled performance review or a minimum statistical sample. Uncertainty about frequency shall not justify delay when the potential consequence requires protective action.

12.5 Process and supplier performance

Process owners shall evaluate whether their processes achieve the intended outputs under actual operating conditions. Evaluation shall consider variation, first-pass conformity, rework, scrap, interruption, capacity and service completion quality as relevant.

Supplier evaluation shall consider both delivered results and the effectiveness of controls over significant risks. A favorable aggregate rating shall not override an unresolved safety issue, unreliable evidence or repeated failure of a critical process.

Where a process misses its objective, the owner shall distinguish an isolated event from a persistent control weakness and establish an appropriate response. Targets shall not encourage acceptance of nonconforming output or omission of required verification.

12.6 Analysis and interpretation

The organization shall use analysis methods suitable for the data and the decision. Statistical conclusions shall consider sample size, representativeness, measurement reliability and relevant changes in the operating population.

A capability or performance index shall not be used as the sole basis for acceptance when its assumptions are not satisfied. The organization shall identify the assumptions, investigate significant departures and use alternative evidence where necessary.

Reports shall distinguish observed association from a demonstrated cause. Decisions with significant consequences shall consider plausible alternative explanations and the limitations of the available evidence.

12.7 Quality related losses and improvement priorities

The organization shall determine the losses relevant to its activities, including prevention failures, internal defects, external failures, repeat service, delayed delivery and avoidable verification effort. Financial estimates may support prioritization but shall not replace safety and mandatory obligation considerations.

Improvement priorities shall reflect consequence, recurrence, customer impact and feasibility. Management shall assign resources and owners to selected actions and retain the basis for deferring a significant issue. Deferral shall include interim controls and a review date.

12.8 Management review arrangements

Top management shall review the quality management system at least once in every twelve-month period. Reviews may be conducted through an integrated series of meetings when the required inputs, decisions and overall system evaluation are demonstrably covered within that period.

Additional review shall occur when a serious incident, major organizational change, persistent objective failure or significant new obligation calls the adequacy of the system into question. The review shall include persons with authority to commit the resources and changes required.

12.9 Management review inputs

Review inputs shall include progress against previous actions; changes in scope and obligations; customer and field results; process and supplier performance; audit findings; nonconformities and corrective action

effectiveness; resource and competence adequacy; significant risks; continuity experience; and opportunities for improvement.

Inputs shall identify unresolved matters, adverse trends and limitations in the evidence. For assessment and certification services, inputs shall also include impartiality risks, complaints and appeals, consistency of findings and decisions, and personnel monitoring results.

The review shall consider whether the applicability register remains justified and whether changes in technology, outsourcing or business activity require additional controls. It shall examine the effectiveness of arrangements that cross organizational or site boundaries.

12.10 Management review outputs

Top management shall record its conclusion on the continuing suitability, adequacy and effectiveness of the system. Outputs shall identify required changes, resource commitments, revised objectives and actions to address weaknesses or opportunities.

Each action shall have an accountable owner, completion date and means of verifying the intended result. Unresolved resource conflicts and overdue significant actions shall be escalated. Closure shall require evidence appropriate to the decision, rather than confirmation that a meeting occurred.

12.11 Response to nonconformity

On identifying a nonconformity, the organization shall control the affected activity or output, evaluate consequences and determine the extent of potentially affected products, services and decisions. Correction and containment shall be distinguished from action addressing the cause.

The response shall consider output already delivered, work in progress, similar processes, other sites and external providers. Required notifications and protective actions shall follow applicable obligations and the incident arrangements in Clause 4.

The organization shall document the requirement not fulfilled, the evidence, the immediate action and the person responsible for investigation. A disputed commercial claim shall not prevent evaluation of objective conformity or safety evidence.

12.12 Cause and extent analysis

The organization shall determine causes at a depth proportionate to the consequences and recurrence risk. Analysis shall examine why the failure occurred, why existing controls did not prevent or detect it, and whether management or system conditions contributed.

Methods shall be selected for the problem rather than for completion of a prescribed form. Human error, lack of attention and supplier fault shall not be accepted as complete explanations without evaluation of instructions, competence, workload, interfaces, controls and oversight as relevant.

The investigation shall test the proposed explanation against available evidence and evaluate similar conditions elsewhere. Where a cause remains uncertain, the organization shall record the uncertainty, apply protective controls and define further investigation rather than claiming an unsupported root cause.

12.13 Corrective action implementation

Corrective actions shall address the verified causes and the identified extent of the problem. Plans shall identify responsibilities, resources, completion criteria, affected documents and required communication or training.

Changes resulting from corrective action shall be assessed for unintended effects and validated where they can alter product, service or process performance. Temporary containment shall remain effective until permanent controls are demonstrated or an authorized alternative is established.

An overdue action shall trigger review of risk and escalation appropriate to the consequences. Changing a due date shall require a recorded reason and shall not erase the original commitment or the period of exposure.

12.14 Effectiveness verification

The organization shall define effectiveness criteria before closing corrective action. Criteria shall address recurrence prevention, restoration of control and the effectiveness of detection where relevant. Verification shall cover sufficient operating opportunity to support the conclusion.

The person accepting closure shall have the competence and authority to judge the evidence and shall not rely solely on the implementer's assertion. Significant safety or recurring system failures shall receive an independent review of closure evidence.

An action shall be reopened or replaced when subsequent evidence shows that it was ineffective. Repeated failure shall trigger reassessment of the original analysis, the extent evaluation and the adequacy of management oversight.

12.15 Continual improvement and knowledge transfer

The organization shall use performance results, lessons from failures, personnel suggestions and technical developments to improve its system and outputs. Improvement shall include prevention of emerging failures as well as correction of existing problems.

Lessons relevant to other products, sites, suppliers or services shall be communicated and evaluated for application. Relevant risk assessments, development inputs, control plans, instructions and competence requirements shall be updated through controlled changes.

The organization shall verify the result of significant improvements against their intended outcomes and retain unsuccessful learning where it can prevent repetition of an ineffective approach.

12.16 Required evidence

The organization shall retain indicator definitions, reliable performance results, analysis records, management review inputs and outputs, action status, nonconformity investigations, containment decisions, cause and extent evaluations, corrective action evidence and effectiveness conclusions.

Records shall connect a reported issue to the affected scope, responsible decision makers and verified outcome. Integrated action systems may be used when they preserve the distinctions between correction, cause analysis, corrective action and effectiveness verification.

13 Audits and assessment

13.1 Applicability and assessment purpose

Every organization shall operate an internal audit programme covering its quality management system. Additional requirements in this clause apply to organizations and persons performing supplier, independent or certification assessments according to the role undertaken.

Each assessment shall identify whether it is a first-party internal audit, a second-party assessment performed for a customer or purchaser, or an independent third-party assessment. The assessment purpose shall distinguish system, process, product and service evaluation. Certification decisions shall also meet Clause 14.

Product inspection, testing and management review may provide audit evidence but shall not replace an audit that evaluates fulfilment and effectiveness of system requirements. An audit conclusion shall be limited to the criteria and scope actually assessed.

13.2 Internal audit programme

The organization shall establish a programme that covers every applicable system requirement and every process within the defined scope at least once in each twelve-month period. Coverage may be distributed across coordinated audits, provided that interfaces and overall effectiveness are evaluated.

Frequency and depth shall increase in response to significant risk, poor performance, major change, complaints or previous findings. The programme shall identify the sites, activities, shifts and support functions to be assessed and the rationale for sampling repeated activities.

The programme owner shall monitor completion, audit quality and corrective action follow-up. Missed audits shall be escalated and rescheduled promptly with a recorded risk evaluation. A planned omission shall not be represented as completed coverage.

13.3 Audit objectives criteria and scope

The audit plan shall identify objectives, applicable requirements, scope boundaries, sites, activities, dates, methods, team members and responsibilities. Criteria shall include the relevant revision of this standard and the organization's applicable obligations and controlled arrangements.

Before the audit, the team shall review the applicability register, significant risks, process relationships, relevant performance and earlier findings. Unresolved scope or access limitations shall be identified before conclusions are drawn.

A process-based audit shall follow the flow of work and its controls rather than merely check the existence of documents. Evidence shall connect requirements with actual decisions, operating conditions and results.

13.4 Audit duration and resources

The party responsible for the audit programme shall allocate sufficient competent time for preparation, evidence collection, evaluation, reporting and follow-up. The basis shall consider scope complexity, people and shifts, sites, technologies, outsourcing, previous performance, language needs and the extent of remote methods.

Audit time shall not be reduced solely to match a commercial price or an unsupported assertion of low risk. Time spent by an interpreter, trainee or technical expert shall not automatically count as independent auditor time.

If actual conditions prevent completion, the audit leader shall revise the plan and document additional work or the limitation on the conclusion. Unassessed requirements shall not receive a positive conformity conclusion.

13.5 Team selection and independence

The audit team collectively shall have competence for the system, processes and technologies being assessed. The leader shall assign work within each person's demonstrated authorization and provide technical support where necessary.

Auditors shall not audit their own work or approve closure of findings for which they implemented the corrective action. Small organizations may use competent personnel from another function or an external auditor to maintain independence.

Before assignment, team members shall disclose relationships and interests that could affect impartiality. The responsible organization shall evaluate threats, apply controls and decline an assignment when an acceptable level of independence cannot be maintained.

13.6 Audit preparation and opening

The team shall prepare sampling priorities from risk, performance and scope information. Requests for evidence shall be proportionate and shall protect confidential information. The team shall identify any need for special access, safety induction, personal protective equipment or secure technical review.

An opening discussion shall confirm the purpose, criteria, scope, plan, communication contacts, reporting arrangements and handling of findings. It shall explain how immediate safety concerns or evidence integrity issues will be escalated.

Changes to the agreed plan shall be recorded with the reason and any effect on coverage. The organization being audited shall not select all samples or exclude adverse evidence without a documented and legitimate access basis.

13.7 Evidence collection and sampling

Auditors shall collect verifiable evidence through suitable combinations of observation, interview, record review and examination of results. Significant interview statements shall be corroborated where the conclusion depends on their accuracy.

Samples shall represent relevant variation in products, services, shifts, locations, configurations and abnormal conditions. Auditors shall record the sample basis and identifiers sufficient to trace significant findings. Sampling limitations shall be considered in the conclusion.

Unexpected failures shall trigger examination of their extent rather than automatic treatment as isolated events. Auditors shall distinguish evidence of absence from absence of available evidence and shall record access limitations accurately.

13.8 Remote and hybrid methods

Remote methods may be used when the required evidence can be obtained with adequate reliability, confidentiality and interaction. The audit planner shall evaluate technology, identity verification, access, connectivity and the ability to observe the actual activity.

Recorded demonstrations or selected video shall not be treated as equivalent to unrestricted observation without assessing their limitations. Where material handling, special process execution, physical conditions or product safety controls cannot be adequately verified remotely, direct on-site assessment shall be performed.

Failure of a remote method shall lead to alternative evidence collection or additional audit time. It shall not result in an unsupported positive conclusion. Recording of people or confidential operations shall follow agreed and applicable privacy requirements.

13.9 System audit execution

System audits shall evaluate whether responsibilities, planning, resources, operational controls, performance evaluation and improvement operate as a connected system. The team shall examine management decisions and their implementation across relevant functions.

The audit shall test the justification of non-applicability decisions and the effectiveness of controls over outsourced work. It shall evaluate whether the organization recognizes and responds to adverse evidence, including failures outside the immediate sample.

A documented procedure shall not establish conformity when actual practice contradicts it. Conversely, the absence of a separately titled procedure shall not establish nonconformity when the requirement is effectively fulfilled through suitable integrated controls.

13.10 Process audits

Process audits shall evaluate inputs, resources, competence, operating conditions, control methods, acceptance points, handovers and outputs. Sampling shall include normal operation and relevant change, restart, deviation or failure conditions.

For production and special processes, the auditor shall examine the relationship between risk analysis, process parameters, control plans, equipment condition and verification results. For development, purchasing or digital processes, equivalent control relationships shall be evaluated using evidence appropriate to the activity.

The conclusion shall identify the process boundaries and whether the controls achieve their intended result. A process score, where used, shall not conceal a nonconformity or substitute for the classification and action required by this standard.

13.11 Product and service audits

A product audit shall evaluate selected output against defined specifications using suitable inspection, test and record evidence. Samples shall consider significant characteristics, configuration, identification, preservation and the validity of release decisions.

A service audit shall follow selected cases from requirement acceptance through execution, verification, handover and follow-up. It shall consider the customer outcome, technical correctness, authorization and the records needed to reconstruct the service.

Audit sampling shall not replace required routine release controls. A conforming sample shall not be represented as certification of a product family or proof that all delivered output is conforming.

13.12 Findings and classification

Each nonconformity shall identify the applicable requirement, objective evidence and the demonstrated failure. Findings shall be communicated clearly and shall distinguish verified facts from unresolved questions. An observation or improvement suggestion shall not be used to downgrade a demonstrated nonconformity.

A critical nonconformity is a failure that creates a credible immediate threat of severe harm through loss of relevant controls, or deliberate falsification or concealment that materially invalidates the assessment or certification evidence. The auditor shall document the basis for urgency and escalate immediately.

A major nonconformity is a failure that demonstrates absence or systemic breakdown of a required control, or creates substantial doubt about the system's ability to achieve the intended conformity outcome, without meeting the critical definition. Related minor failures shall be evaluated together when they indicate a systemic breakdown.

A minor nonconformity is a demonstrated failure of an applicable requirement that does not meet the critical or major definition. Classification shall consider consequence, extent and control effectiveness rather than the number of written findings alone.

13.13 Immediate escalation and closing discussion

The audit leader shall communicate a critical finding promptly to the responsible management and, for certification assessments, the certification body. The audited organization shall initiate protective action without waiting for the final report.

At closing, the team shall explain the assessed scope, evidence limitations, findings, classifications and conclusion. Disagreement shall be recorded with its basis. The organization shall receive a clear explanation of response and appeal routes where applicable.

Auditors shall not negotiate away a supported finding in exchange for a future commitment. They may correct a finding when new verifiable evidence shows that the original statement or classification was inaccurate, preserving the reason for change.

13.14 Audit report

The report shall identify the audited entity, sites, criteria and revision, dates, team, methods, scope, applicability decisions reviewed, significant samples, limitations, findings and overall conclusion. It shall identify uncompleted work and any departure from the plan that affects confidence in the result.

The report shall distinguish the audit team's recommendation from an independent certification decision. It shall not claim coverage of activities, locations or technologies that were not adequately assessed.

The report shall be issued within an agreed period that supports timely action. Immediate containment information shall be communicated separately when waiting for report completion would create unacceptable delay.

13.15 Follow-up and closure

The audited organization shall respond using the correction, cause, extent, corrective action and effectiveness controls in Clause 12. The audit programme owner shall define response and verification dates proportionate to classification and risk. Certification deadlines shall follow Clause 14.

A competent person independent of action implementation shall evaluate closure evidence. Critical and major findings shall receive verification that implementation and effectiveness are demonstrated; document review alone shall be insufficient where the issue requires observation of actual practice.

The follow-up record shall state the evidence evaluated, verification method, decision and remaining restrictions. Recurrence shall be considered in future audit planning and in reassessing the adequacy of the original closure.

13.16 Common auditor competence

Auditors shall demonstrate understanding of this standard, applicability, process relationships, risk evaluation, evidence sampling, interviewing, finding formulation and reporting. They shall understand the distinction between requirements, guidance, customer preferences and their own preferred methods.

Competence shall include ethical conduct, confidentiality, impartiality, evidence integrity and the ability to recognize when technical support is needed. Auditors shall communicate accurately in the audit language or work through a controlled interpretation arrangement.

Authorization shall be based on assessed knowledge and observed application. Attendance at a course, possession of a job title or length of service alone shall not establish auditor competence.

13.17 Technical and role competence

System auditors shall demonstrate the ability to evaluate connected management and operational controls. Process auditors shall understand the mechanisms, failure modes, process limits and evidence relevant to their assigned processes.

Product and service auditors shall understand applicable specifications, acceptance methods, configuration and relevant safety consequences. Assignments involving software, AI, batteries, cybersecurity or other specialist technologies shall have demonstrable competence for the actual scope.

Audit leaders shall additionally demonstrate planning, team coordination, resolution of evidence conflicts, integration of findings and communication of a defensible conclusion. Technical experts shall work within their assigned expertise and shall not independently issue audit conclusions unless separately authorized as auditors.

13.18 Initial qualification and authorization

The organization employing or engaging auditors shall establish a qualification route comprising relevant education or equivalent demonstrated learning, practical sector experience, audit-method training, assessment of knowledge and witnessed audit performance. Equivalence decisions shall record the evidence and any limitations.

Before independent authorization, a candidate shall demonstrate a complete assigned audit cycle from preparation to reporting under a qualified evaluator. The evaluator shall record performance against defined criteria, including evidence quality, technical judgment and impartial conduct.

An authorization record shall identify approved roles, sectors, processes, technologies, methods and restrictions. Qualification and authorization shall also meet Annex F. A candidate who does not meet a criterion shall complete development and reassessment before receiving the affected authorization.

13.19 Continued competence and performance monitoring

Auditor performance shall be reviewed at least annually using completed work, report quality, feedback, complaint information and relevant technical changes. Authorization shall be formally reassessed at intervals not exceeding three years and following a material competence concern.

Monitoring shall include witnessed performance at least once during each authorization period. The witness shall be competent to evaluate the assigned role and technical scope. A paper review alone shall not establish continued practical auditing competence.

Limited recent practice, extended absence or significant technology change shall trigger evaluation before a new assignment. Authorization shall be restricted or suspended when competence is not demonstrated and restored only after satisfactory reassessment.

13.20 Reviewers assessors and decision personnel

Persons evaluating auditor competence, reviewing certification evidence or making certification decisions shall have competence for their specific judgment and understand the applicable scheme rules. Technical support may supplement, but shall not replace, their ability to evaluate the sufficiency of evidence.

Competence assessors shall use defined criteria and maintain independence from the candidate's self-assessment. Certification reviewers and decision personnel shall meet the separation of duties in Clause 14.

The responsible organization shall monitor consistency between evaluators and address significant differences through calibration of judgment using representative cases. Calibration shall not require uniform conclusions when relevant evidence differs.

13.21 Required evidence

The organization responsible for each audit or assessment shall retain programmes, plans, assignment and conflict checks, competence authorizations, sampling records, findings, reports, follow-up and closure evidence. Records shall establish who performed and reviewed significant judgments.

Personnel records shall include qualification evidence, assessment results, restrictions, witnessed performance, continued development and authorization decisions. Access and retention shall protect personal and commercial information while permitting authorized verification.

14 Certification and decision rules

14.1 Purpose status and role applicability

This clause defines proposed rules for certification of an organization's automotive quality management system against the approved IAF AQMS standard. It does not establish product certification, vehicle approval, accreditation of a certification body or certification of an individual auditor.

The scheme owner shall authorize publication of the standard and operational scheme before certification is offered. No certificate shall be issued against this working draft. References to certification in this clause describe the intended arrangements following approval.

Requirements identifying the scheme owner or certification body apply to those roles. Requirements identifying an applicant or certified organization apply when that status is sought or held. An organization not seeking certification remains subject to applicable system and internal audit requirements but need not create a certification function.

14.2 Scheme ownership and governance

The scheme owner shall identify its legal entity, governing authority, decision responsibilities and the body authorized to approve standard revisions and scheme rules. Public scheme information shall state the identity represented by IAF AQMS so that it is not confused with another organization using the same initials.

The scheme owner shall maintain a documented process for stakeholder input, technical interpretation, complaints, revision and publication. Interpretations shall identify their approval and effective date and shall not be applied retrospectively without a justified transition arrangement. The scheme owner and affected parties shall apply Annex P for maintenance, change approval and transition control.

Before operational launch, the scheme owner shall approve certification-body eligibility, oversight methods, the audit-duration methodology, competence criteria, fees where relevant and transition arrangements. It shall make binding rules available to affected parties and maintain a record of authorized certification bodies.

14.3 Certification body eligibility and accountability

A certification body shall be an identifiable legal entity capable of entering enforceable agreements and accepting responsibility for its decisions. It shall demonstrate the resources, competence, impartiality, confidentiality and record controls needed for the scopes it offers.

Authorization by the scheme owner shall follow evaluation against documented criteria and shall define the permitted scope and oversight conditions. The scheme owner and certification body shall apply Annex G for authorization and oversight. Authorization shall not be described as accreditation unless a separate valid accreditation basis exists.

The certification body shall remain responsible for contracted audit and technical activities. It shall not outsource the final certification decision or permit an intermediary to issue certificates in its name without that decision and its controlled authorization.

14.4 Impartiality and conflicts of interest

The certification body shall identify and control threats arising from ownership, financing, commercial relationships, consultancy, personnel relationships and performance incentives. Its impartiality review shall include input able to challenge commercial interests and shall retain decisions on significant threats.

The certification body shall not design or implement the applicant's management system or provide client-specific corrective solutions and then certify that work. General explanation of requirements and public training may be provided when they do not become client-specific system implementation.

Personnel who provided management system consultancy to a client shall not audit, technically review or decide that client's certification for at least two years after the consultancy ended. The body shall evaluate continuing threats after that period and extend the restriction when necessary.

Sales targets, fees, membership status and promised commercial benefits shall not determine findings or decisions. The body shall refuse or discontinue work when impartiality cannot be maintained.

14.5 Confidentiality and contractual arrangements

The certification body and applicant shall agree the scope, criteria, access, fees, confidentiality, reporting, use of claims, change notifications, complaint handling and consequences of refusal of required access. The agreement shall identify the applicable scheme revision.

The body shall protect confidential information obtained from the client and other sources. Required disclosure shall be limited to the applicable obligation and notified to the affected party where legally permitted. Confidentiality shall not be used to conceal certificate validity or prevent authorized scheme oversight.

The applicant shall provide accurate scope and operating information, allow access to relevant evidence and personnel, and identify restrictions before the audit. Material omission or falsification shall be evaluated under the nonconformity and certification-status rules.

14.6 Application and scope review

Before accepting an application, the certification body shall evaluate the legal entity, sites, activities, products, services, technologies, support functions, outsourcing and proposed non-applicability decisions. It shall verify that the requested scope is within its authorization and available competence.

The scope shall describe actual activities precisely enough to prevent a misleading certificate claim. A broad corporate description shall not conceal unassessed locations or activities. Design responsibility and significant remote support shall be identified where relevant.

Unresolved eligibility, competence, access or applicability questions shall be resolved before the certification audit proceeds. The application review and acceptance decision shall be retained.

14.7 Certification audit programme and duration

The certification body shall establish a programme covering initial readiness assessment, initial implementation audit, surveillance and recertification. The programme shall address all applicable requirements, operational sites, relevant support and technical scope.

Duration shall be calculated using the scheme owner's approved methodology. Before scheme launch, that methodology shall specify a baseline linked to effective personnel and activity complexity, additions for sites,

shifts, technologies and risk, permitted reductions and a justified minimum. It shall be validated through representative pilot assessments under Annex K and applied consistently.

For each client, the body shall retain the baseline, adjustments, justification and resulting allocation. Parallel work shall count only where each auditor performs distinct competent work. Travel and commercial discussions shall not count as evidence-collection time.

14.8 Readiness assessment

The initial readiness assessment shall evaluate scope, applicability, documented arrangements, significant risks, site conditions, internal audit and management review completion, and readiness to demonstrate implementation. It shall identify gaps that could prevent an effective implementation audit.

The body shall communicate readiness concerns and determine whether they are resolved sufficiently to proceed. The readiness assessment shall not be represented as certification or as assurance that the later audit will succeed.

The interval before the implementation audit shall allow correction of readiness concerns while preserving the relevance of evidence. Significant changes during that interval shall trigger additional readiness evaluation.

14.9 Initial implementation audit

The initial implementation audit shall evaluate effective operation of all applicable requirements across the proposed scope. Evidence shall include actual completed work, operating controls, relevant performance and the functioning of internal audit, management review and corrective action.

All operational sites included in the initial certificate shall receive on-site assessment. Remote support may be assessed remotely where Clause 13.8 is satisfied. A proposed site without sufficient operating evidence shall be excluded from the issued scope until adequate assessment is possible.

The audit team shall report findings and recommend a conclusion with its limitations. The body shall complete independent review and decision before any certification claim is authorized.

14.10 Multiple sites and support locations

A certificate covering multiple sites shall identify the legal and management relationships, central control responsibilities and the activities at each location. Central management shall have authority to enforce common controls, obtain performance information and require corrective action at every included site.

Each operational site shall receive assessment during each annual surveillance cycle, with on-site observation of relevant physical activities. Repeated requirement checks may be coordinated across sites, but evidence from one site shall not substitute for verification of another site's actual operations.

Shared support functions shall be evaluated at initial certification and recertification and during surveillance according to risk and change. Findings with possible common causes shall be evaluated across the affected site population before certification decisions are made.

14.11 Nonconformity response periods

For certification assessments, classification shall follow Clause 13.12. The periods below are proposed scheme limits expressed in calendar days. Shorter action periods shall be imposed where consequences or applicable obligations require them.

For a critical finding, the organization shall begin protective action immediately and provide its initial containment evidence to the certification body within twenty-four hours of notification. For a major finding, the organization shall submit containment, cause and corrective action plans within fifteen days and demonstrate verified closure within sixty days. For a minor finding, it shall submit an acceptable response plan within thirty days and implementation evidence within ninety days.

The clock shall start when the finding is formally notified, including an immediate written notification before the final report. The body shall record the notification date and time, agreed reference time zone, due dates and required evidence. Periods stated in hours shall run continuously from notification. For periods stated in days, the notification date is day zero and the deadline is the end of the last calendar day in the recorded time zone. A weekend or holiday shall not extend a period automatically. These periods shall not delay customer or authority notification or protective action required sooner.

14.12 Closure and consequences of overdue findings

Critical and major findings shall be closed through verified correction, cause and extent analysis, implementation and effectiveness evidence before initial certification, scope extension or recertification is granted. A promise or accepted plan shall not constitute closure.

Minor findings may remain open at those decisions only when the response plan is accepted, containment is adequate and the body records why system effectiveness is not in substantial doubt. Implementation shall be verified within ninety days of notification. Final closure shall require effectiveness evidence under Clause 12.14. If insufficient operating exposure prevents that conclusion, the body shall record Implemented with effectiveness pending, the protective controls, required exposure and a follow-up date no later than one hundred eighty days after notification. This status shall not be reported as closed. A critical or major finding shall not use this allowance.

An overdue major finding or failure to maintain effective containment shall result in suspension of the affected certified scope. A missed minor plan or implementation deadline shall trigger evaluation for major classification and a certification-status decision within ten days of the missed deadline; the body shall not allow repeated administrative extensions to replace action. If minor effectiveness remains unsupported at the one-hundred-eighty-day limit, the body shall suspend the affected scope pending verified closure. Lack of production or service opportunity shall not be recorded as evidence of effectiveness.

A confirmed critical finding shall result in immediate suspension of affected certification, subject to restoration under Clause 14.19. For an applicant, certification shall be withheld. These actions shall not replace the organization's duty to control affected output.

14.13 Technical review and decision independence

A competent reviewer who did not perform the audit shall evaluate whether scope, applicability, coverage, evidence, findings and closure support the proposed decision. The reviewer shall identify unresolved gaps and require additional work where necessary.

The certification decision shall be made by authorized personnel who did not perform the audit and have no disqualifying interest. The reviewer may also make the decision when competent and independent. An audit team recommendation shall not bind the decision maker.

Decision records shall identify the evidence, applicable rules, persons involved, conclusion, conditions and dates. A decision shall not be issued when a material evidence or applicability dispute remains unresolved.

14.14 Certificate content and public validity

A certificate shall identify the certification body, certified legal entity, unique certificate number, assessed scope, included sites, approved standard edition, initial certification date, current issue date and expiry date. An attached site schedule shall be controlled as part of the certificate.

The certificate or an accessible controlled scope statement shall identify justified non-applicability decisions that materially limit the scope claim. It shall not imply that excluded design, technology, service or site activities were certified.

The certification body shall provide a means of verifying current certificate validity, scope and status in accordance with Annex I. Public information shall distinguish valid, suspended, withdrawn and expired certificates without disclosing confidential audit evidence.

14.15 Certification cycle and surveillance

The certification cycle shall not exceed three years from the initial certification or recertification decision. The first surveillance shall be completed within twelve months of the initial decision, and subsequent surveillance intervals shall not exceed twelve months.

Every surveillance shall evaluate significant changes, complaints and incidents, previous findings, relevant performance, internal audits, management review, use of certification claims and continued scope validity. Operational sampling shall follow risk and the site rules in Clause 14.10.

The programme shall cover all applicable system requirements during the certification cycle. Surveillance shall provide enough current operational evidence to support continued confidence rather than rely solely on the initial audit record.

14.16 Recertification and expiry

Recertification shall evaluate continued conformity and effectiveness across the full scope, considering the preceding cycle's performance and significant changes. Audit, required closure, technical review and decision shall be completed before certificate expiry.

A certificate shall expire on its stated date if recertification is not decided in time. The body shall not backdate a decision or permit a claim of uninterrupted certification across an expiry gap.

Where recertification is sought after expiry, the body shall evaluate changes and evidence validity and determine the additional assessment needed, including a new readiness assessment where warranted. A new validity period shall begin only from the actual positive decision.

14.17 Changes special audits and interruptions

A certified organization shall notify the certification body within ten days of a material change in legal identity, ownership, scope, site, management control or key technology that could affect certification. A serious safety event, material evidence falsification or loss of essential control shall be notified within twenty-four hours of recognition.

The body shall evaluate the effect on competence, scope and confidence and determine whether a special audit, scope amendment, restriction or suspension is required. A scope extension shall receive assessment and independent approval before the extended claim is used.

Disruption that prevents a scheduled audit shall trigger evaluation of alternative methods under Clause 13.8. Inability to obtain sufficient evidence within the required interval shall lead to suspension; it shall not justify silent extension of validity or an unsupported assurance claim.

14.18 Suspension and scope reduction

The certification body shall suspend certification when required by this clause, when the organization refuses essential assessment or when reliable evidence no longer supports continued certification. It shall define the affected scope, effective date, reasons, restoration conditions and maximum suspension period.

Scope reduction may be used only when the remaining scope can be independently supported and shared causes or interfaces do not undermine its conformity. The body shall not remove a failing activity merely to preserve a misleading broad certification claim.

During suspension the organization shall stop representing the affected certification as valid and shall correct relevant public claims. The body shall update its validity information promptly and notify parties as required by its scheme obligations.

14.19 Restoration withdrawal and termination

Suspension shall not exceed ninety days. Restoration shall require verified fulfilment of the stated conditions and an independent positive decision before that deadline. The original expiry date shall remain unchanged.

The body shall withdraw the affected certification when restoration conditions are not met within the permitted period, when the organization no longer operates the certified scope, or when continued certification cannot be supported. Voluntary termination shall be recorded distinctly from withdrawal for nonconformity.

The organization shall cease use of withdrawn, terminated or expired certification claims and marks. Return to certification after withdrawal shall require a new application and an assessment sufficient to establish current conformity; previous certification shall not create automatic entitlement.

14.20 Transfer between certification bodies

The receiving body shall verify certificate authenticity, status, scope, audit history, open findings, complaints and the reason for transfer. It shall obtain sufficient evidence from the organization and, with appropriate authorization, the previous body.

Suspended, withdrawn or expired certification shall not be transferred as valid. Unavailable history or unresolved significant concerns shall trigger additional assessment or treatment as a new application. Transfer shall not reset finding deadlines or erase adverse evidence.

Acceptance shall require independent review and decision. The receiving body shall preserve the existing cycle and expiry unless it performs a complete recertification assessment and makes a new recertification decision.

14.21 Complaints and appeals

The certification body shall maintain accessible processes for complaints about its services or certified clients and appeals against its decisions. It shall acknowledge receipt, evaluate relevant evidence, protect confidentiality and communicate the outcome and basis to the submitting party.

Persons deciding an appeal shall not have participated in the challenged audit or decision and shall be free of relevant conflicts. Filing a complaint or appeal shall not lead to discriminatory treatment. An appeal shall not automatically suspend protective restrictions supported by credible evidence.

The body shall define and publish handling periods, escalation arrangements and the route for unresolved scheme matters. It shall analyze recurring complaints and overturned decisions to improve competence, consistency and impartiality controls.

14.22 Certification claims and marks

A certified organization shall use certificates and marks only for the valid scope and period authorized. Claims shall identify system certification and shall not imply approval of every product, service result or person, or recognition under a different standard.

The certification body shall establish rules for digital claims, websites, quotations, packaging references and use by subsidiaries or distributors. It shall monitor misuse and require correction, escalating to suspension or withdrawal when misleading claims persist.

Any claim of external accreditation, recognition or equivalence shall be supported by a separate current authorization covering the claimed scope. The IAF AQMS name alone shall not establish such status.

14.23 Certification records and scheme oversight

The certification body shall retain applications, contracts, scope reviews, competence assignments, duration calculations, audit evidence, findings, closure, reviews, decisions, certificates, status changes, complaints and appeals. Retention shall cover at least the current and preceding certification cycles and longer where obligations or unresolved matters require it.

Records shall permit reconstruction of the basis for each certification decision and include the applicable minimum information in Annex H. The body shall control access, revisions, backup and transfer so that a change of personnel or system does not destroy the evidence trail.

The scheme owner shall monitor authorized bodies through risk-based file review, witnessed assessments, performance information and complaint analysis. It shall define corrective action, restriction, suspension and withdrawal of authorization, with independent appeal arrangements. Oversight shall not transfer responsibility for individual certification decisions away from the certification body.

Annex A Applicability register

Normative within the completed standard subject to approval. This annex defines the minimum content of the applicability register. The organization may use another layout that retains the same information.

A1 Required register information

The register shall identify the scope and its revision, the standard revision used, the preparer, approving authority and review date. For each non-applicability or partial-applicability decision it shall identify the exact requirement, the activity or responsibility evaluated, the decision, the evidence and any remaining control obligation.

The register shall be reviewed after a material scope, technology, contractual or outsourcing change and at least annually. An assessment shall sample the underlying facts rather than accepting the register as self-proving evidence.

A2 Blank register structure

Requirement	Decision	Basis and evidence	Approval and review
[Exact clause]	[Applicable or Not applicable]	[Activity and responsibilities; evidence reference; external provider interface]	[Owner; approver; date]
[Exact subclause]	[Applicable or Not applicable]	[Reason; customer and legal obligation check; remaining controls]	[Owner; approver; date]

For an aggregate clause recorded as Partially applicable, attach or reference the individual decisions for its subordinate requirements. A blank entry is an unresolved decision, not a Not applicable decision.

A3 Review questions

- Does the described activity occur anywhere within the scope, including remote support or contracted work?
- Does the organization retain responsibility through its contract, customer commitment or mandatory obligation?
- If direct performance is absent, are selection, specification, monitoring or acceptance controls still required?
- Does the proposed omission weaken the ability to establish conformity, safety or reliable evidence?
- Is the decision supported by current evidence and approved by a responsible person?

A4 Illustrative decisions

The following examples are informative. Decisions shall be based on actual activities and responsibilities and the exact applicable subclauses.

Example	Decision logic
Manufacture to customer drawings	Product design may be non-applicable where responsibility is demonstrably absent. Development of the manufacturing process remains applicable when performed or controlled by the organization.

Example	Decision logic
Independent laboratory	Vehicle assembly requirements would not apply to a testing-only scope. Personnel, methods, equipment, records and supplied testing-service controls remain relevant.
Automotive software developer	Physical component manufacture may be absent. Development, configuration, verification, cybersecurity interfaces and field support remain relevant to the supplied software.
Outsourced heat treatment	The purchaser retains controls over provider selection, requirements, qualification evidence, traceability and acceptance. Outsourcing does not remove responsibility for the supplied part.
Certification body	Production requirements do not apply merely because clients manufacture products. Assessment competence, impartiality, review and decision controls apply to the body's own services.

Annex B Sector application guide

Informative. This guide helps readers select requirements from the single standard. It does not create separate sector standards, grant exclusions or replace the clause-level register in Annex A. A business may use several profiles at the same time.

B1 Selection sequence

Define the legal entity, included locations, supplied outputs and contractual responsibilities. Identify each activity actually performed or controlled, including development, purchasing, production, software operation, testing, repair and assessment. Select the relevant product and technology subjects in Clause 9 by supplied function and risk.

Apply the common system requirements and then evaluate activity requirements at subclause level. Record the evidence for every proposed omission. Where work is outsourced, distinguish the provider's execution from the organization's retained specification, monitoring and acceptance responsibilities.

Treat the rows below as starting points. The suggested clauses are not exhaustive. Clauses 1, 3, 4 and 12 and the internal audit provisions of Clause 13 apply to every organizational profile; Clause 2 defines the language used. Clause 5 follows the resources and tasks used. Clause 14 follows the certification role, not the industrial category.

B2 Activity profiles

Profile	Additional starting points	Applicability boundary to test
Vehicle manufacturer or integrator	6 to 11; especially 9.3 and relevant safety technologies	Integration remains a responsibility even when components, engineering or testing are purchased.
Component manufacturer to customer design	6.14; 7; 8; relevant 9; 11	Absence of product design authority does not remove process development, feasibility or change-control duties.
Materials or chemicals supplier	6 to 8; 9.6; 9.22; 11	Batch formulation, contamination and material conformity need activity-specific evaluation.
Special process provider	7; 8.3 to 8.11; 8.17 to 8.20; 11	End-product inspection does not automatically establish qualification of the process.
Production equipment or tooling supplier	6 to 8; 9.21; relevant 9.8 and 9.14; 10; 11	Commissioning, software interfaces and customer acceptance may remain in scope after delivery.
Software developer or digital service operator	6; 7; 9.14 to 9.19; 10.16; relevant 11	Hardware manufacture may be absent; release, operation, configuration and security interfaces remain.
Battery or energy system supplier	6 to 8; 9.9 to 9.13 as relevant; 10; 11	Cell, pack, charging and stored-fuel responsibilities must be separated by actual scope.
Laboratory or inspection service	7; relevant 10; 11; service and technical audit provisions of 13	Routine test work does not imply product design; method development can trigger Clause 6.
Distributor warehouse or logistics provider	7; applicable 8; 10.14; relevant 11	Product design may be absent; authenticity, preservation, traceability and delivery controls remain.

Profile	Additional starting points	Applicability boundary to test
Dealer repairer or service network	7; relevant 8; 10; relevant 9 and 11	Return-to-use decisions, coding, safety checks and control of replacement parts follow actual work.
Remanufacturer or reuse operator	6 to 8; 9.20; 9.22; 10; 11	Incoming condition, intended life and acceptance need evidence; prior use is not proof of suitability.
Fleet or mobility operator	7; 9.16 to 9.19 where relevant; 10.15 and 10.16; 11	Control depends on responsibility for maintenance, remote functions and customer service.
Audit or certification provider	5; 7; applicable service controls; 13; role-specific 14	Clients' manufacturing duties do not become the body's own operations; competence and impartiality do.

B3 Manufacturing example

Illustrative case: a supplier machines a safety-related bracket to an OEM-controlled design and purchases heat treatment. Its contract permits manufacturing process development but does not permit changes to the product specification. Product architecture development may therefore be non-applicable, subject to evidence of the responsibility boundary.

The supplier still evaluates feasibility, develops the machining process, controls special characteristics, qualifies purchased heat treatment, verifies release and manages changes. A proposed exclusion of all of Clause 6 or all special-process controls would be too broad. The register should identify the exact absent product-design duty and preserve the applicable process and purchasing duties.

B4 Software and laboratory examples

Illustrative software case: a company develops diagnostic software and operates the update service. Physical assembly may be absent, but requirements traceability, validation, approved configurations, customer deployment, security and update recovery remain relevant. A cloud provider is an external provider; responsibility for the supplied service remains with the company.

Illustrative laboratory case: a laboratory performs testing to customer-selected methods and validates a modified test method. Its technical scope drives Clause 11. The method-development activity also needs evaluation under Clause 6. This standard does not itself establish accreditation to ISO/IEC 17025, and an audit of the laboratory's system does not certify each tested product.

B5 Review of disputed boundaries

For each disputed decision, identify the exact requirement, the absent activity claimed, the party actually performing the work and the responsibility retained by the applicant. Compare the contract, workflow and delivered evidence. Record any inconsistency rather than resolving it by choosing a convenient category name.

An assessor verifies the register; management remains responsible for preparing and approving it. If the evidence remains incomplete, record the question as unresolved and limit the assessment conclusion accordingly. A pilot reviewer may propose clearer wording but cannot authorize an exception to another applicable obligation.

Annex C Technical evidence and independent review

Informative guidance. This annex defines how evidence supports the completeness, clarity and practical use of AQMS. It does not add conformity requirements or report completed validation. The numbered AQMS requirements remain the assessment criteria.

C1 Review basis

The review coordinator should identify the exact AQMS revision, intended activities, applicable clauses, reviewers and evidence available. Review should distinguish a weakness in the requirement from a failure to implement an otherwise clear requirement. A familiar subject heading alone does not demonstrate adequate coverage.

Each proposed requirement should be examined for its responsible party, applicability condition, required action, intended outcome and verifiable evidence. Reviewers should identify unclear decisions, missing interfaces and controls that cannot be tested in practice. Actual operational observations and hypothetical exercises should remain separately identified.

C2 Evidence status

Status	Meaning
Available for review	Identified evidence exists and can be examined by an authorized competent reviewer.
Examined with limitations	The evidence supports a defined conclusion, with restrictions on scope, sampling or operating conditions.
Further evidence required	The available evidence cannot support the intended conclusion; additional work is identified.
Independently verified	A competent reviewer has verified the specified conclusion against identified evidence and recorded the result.

No status in this table should be assigned merely because a form exists or an activity is planned. Verification applies to the stated conclusion and scope; it does not establish universal coverage of the automotive sector.

C3 Requirement review record

Use the following fields to connect each review decision to the relevant AQMS provision. Existing records may be used where the same information is retained. Bracketed entries are blank fields, not completed findings.

Record field	Entry to complete
Review identity	[Review ID; AQMS revision; date; activity or sector; reviewer and competence]
Requirement	[Exact AQMS clause; responsible role; applicable activity or condition]
Intended outcome	[Result the requirement is intended to achieve; consequences of failure]
Evidence examined	[Operating record or observation; identifier; date; sample; live evidence or simulation]
Assessment	[Clarity; completeness; practical applicability; evidence sufficiency; limitations]
Proposed action	[No change with reason; revised wording; additional control; additional observation]
Independent disposition	[Decision; reviewer; date; justification; evidence supporting the conclusion]
Follow-up	[Owner; target date; retest criteria; completion evidence; remaining open matters]

The record should preserve original observations and later corrections. An accepted wording change should be linked to its originating issue and checked for effects on related clauses, examples, training and decision rules. Review and amendment controls in Annex P remain applicable.

An unresolved issue affecting safety, reliable evidence or a defensible assessment conclusion should remain visible until resolved. Administrative completion of a review form does not close the technical issue.

C4 Sector coverage and practical verification

The technical review should follow representative activities from customer commitment through execution, acceptance and feedback. It should include the retained responsibilities for outsourced work and the interfaces between products, software, services and supporting functions.

Review area	Question for the reviewer
Scope and responsibility	Does the requirement apply to the actual activity and the responsibility retained by the organization?
Operational control	Can a competent person understand the required action and demonstrate that it operates?
Evidence integrity	Can the result be traced to current criteria, authorized personnel and reliable operating records?
Abnormal conditions	Does the control address a relevant failure, change, interruption or recovery condition?
Proportionality	Can the requirement be implemented at different organizational scales while preserving its intended outcome?
Assessment consistency	Can independent competent assessors reach defensible conclusions using the same criteria and evidence?

C5 Review completion and remaining work

The coordinator should summarize activities examined, evidence limitations, unresolved issues and the actions needed before approval. Missing activity coverage should lead to additional evidence or a clearly limited claim. Planned pilot work must remain identified as planned.

Annexes D and N govern pilot planning and field evidence. Annex K addresses audit-duration validation. Annex L supports technical review and Annex M records open development issues. Publication remains subject to the decisions and gates in Annex E.

AQMS establishes its own proposed requirements. Applicable legal, regulatory and contractual obligations remain controlled under Clause 1.7. This annex does not establish approval, accreditation or recognition by an external organization.

Annex D Pilot assessment protocol

Informative development protocol. The proposed method below is for testing and refining this draft. It is not an operational certification scheme, a certificate entitlement or an approved audit-duration rule. Pilot participation should produce evidence and review comments, not a certification claim.

D1 Pilot objectives and governance

The pilot programme should test whether different competent assessors reach defensible, consistent conclusions using the same requirements; whether applicability decisions preserve responsibilities; and whether the evidence burden is proportionate to the activity and risk. It should also identify gaps and contradictory or untestable wording.

The scheme owner should appoint a pilot coordinator, technical review lead and persons competent to challenge assessment and certification judgments. Participants and reviewers should disclose conflicts. Persons who drafted an organization's implementation should not provide the independent conclusion on that implementation.

Before each pilot, the coordinator should freeze the draft revision, scope, criteria, method and planned duration. A change during the pilot should be recorded and evaluated for comparability. No pilot outcome, attendance or successful simulation should be described as an approved IAF AQMS certificate.

D2 Representative coverage

The initial pilot set should include manufacturing, a special process, materials, production equipment, software, battery or energy technology, laboratory or inspection services, logistics, repair or aftersales, and audit or certification services. One participant may cover several activities, but missing activity coverage should remain visible.

For a practical starting set, the coordinator should seek at least twelve independent organizational scopes, including at least three small organizations and three scopes with multiple sites or shifts. These numbers are proposed development targets, not statistically representative sample sizes. Inaccessible or unavailable categories should remain release limitations until addressed.

Technology risk, organizational size and audit method should be recorded separately. The coordinator should include outsourcing, remote support, customer-owned design and low-frequency work so that the pilot does not test only vertically integrated high-volume production.

D3 Evidence package and preparation

Each participant should provide a scope statement, activity map, applicability register, representative obligation records, process risks, competence assignments, performance information and available audit and management review records. Existing systems and integrated records should be accepted where they provide the required evidence.

The assessors should identify a representative transaction or product history and follow its requirements, execution, acceptance and feedback. Evidence requests should be necessary for the stated assessment purpose. Missing evidence should be classified as unavailable, not presumed conforming.

Commercial and personal information should be minimized in the pilot report. The participant should authorize any use of identifiable case material beyond its assessment. Published findings should use agreed aggregation or anonymization and should not disclose confidential customer requirements.

D4 Candidate duration starting points

The following values are original AQMS hypotheses for pilot planning. They describe initial implementation evidence-collection time for one operational site. Preparation, readiness review, reporting, technical review and decision simulation are planned separately. Operational validation remains required.

Effective personnel at the site	Starting auditor days	Pilot condition
1 to 10	2.0	One day means eight hours of competent evidence-collection work.
11 to 50	3.0	Use the full in-scope population across relevant shifts.
51 to 150	4.0	Include contracted personnel performing in-scope work.
151 to 500	6.0	Record the actual workforce basis and relevant variation.
501 to 1500	8.0	Increase time where complexity or evidence needs require it.
Above 1500	Individual task-based estimate	No extrapolated automatic cap; technical review of the estimate required.

D5 Duration adjustments and worked example

For this pilot method, effective personnel means the number of people performing or supporting in-scope work at the site, including relevant contractors and temporary workers. Count people once at that site and document how part-time, shared and remote roles are allocated. Do not reduce the count for repeated work until the effect has been tested and an adjustment approved.

Add at least half an auditor day for each additional operational shift that requires distinct evidence. Add at least one day for substantial in-scope product development not already adequately covered by the baseline task plan. Add at least one day for each specialist technical domain requiring separate assurance review, such as functional safety or a special process. Combine overlapping additions only when distinct tasks and sufficient coverage are demonstrated.

Estimate additional operational sites individually under the same method. Add time for significant remote support, translation, fragmented records, unresolved prior issues and access constraints from an explicit task estimate. Travel is additional. Do not apply automatic reductions for an existing certificate, low complaint rate, software use or remote assessment.

Example: a 40-person machining site with two shifts and purchased heat treatment starts at three days. A second-shift evidence session adds half a day. One day of review of its heat-treatment specification, provider qualification, traceability and acceptance gives an initial estimate of four and a half auditor days. If the actual task plan needs more time, the estimate increases. This example does not assume the purchaser performs the supplier's process.

Two auditors working distinct competent tasks for one day provide two auditor days, not two calendar days. Observers, interpreters and trainees do not automatically add productive auditor time. Record actual hours and incomplete tasks so that the pilot can test whether the calculation predicts adequate coverage.

D6 Execution and evidence evaluation

Conduct an opening meeting, confirm the frozen criteria and inspect the justification of exclusions. Follow selected work through the relevant functions and evaluate both ordinary controls and abnormal situations. Include at least one change, nonconformity or restart case where the participant has such evidence.

For a dormant or new activity without operating history, use a clearly identified simulation to test wording and preparedness. Do not convert simulated performance into demonstrated operational conformity. Record which conclusions depend on live evidence and which remain developmental.

Use Conforming evidence, Nonconformity, Not applicable verified and Not evaluated as distinct assessment outcomes. The last outcome is an evidence gap and cannot be counted as a pass. A numerical completion measure may show coverage but should not override a critical or major finding.

D7 Independent comparison of judgments

At least two competent reviewers should independently evaluate the same selected evidence packages before discussing conclusions. The coordinator should include supported conformity, missing evidence, a justified omission, outsourcing, a minor lapse, a systemic failure and a credible critical event.

Compare applicability decisions, requirement selection, finding wording, severity and closure judgments. Record the initial conclusions and the reasons for differences. Reconciliation should explain the evidence or wording responsible rather than merely average the reviewers' results.

Any disagreement that could allow unsafe release, conceal a major breakdown or issue an unsupported certificate should be resolved before the affected wording is accepted. Repeat the comparison after a material revision. A high percentage of agreement on easy cases should not offset an unresolved consequential disagreement.

D8 Corrective action and decision simulations

Test the sequence in Clauses 12 to 14 using traceable case dates: notification, initial protection, plan acceptance, implementation verification, effectiveness verification and independent decision. Distinguish calendar deadlines from operating opportunity needed to assess recurrence.

The case set should include a minor finding whose implementation is complete but whose effectiveness cannot yet be demonstrated, an overdue major finding, a critical finding during surveillance, expiry before recertification decision, a transfer with missing history and an appeal against classification.

For each case, record the certificate status that would follow, the responsible decision maker, required evidence and next deadline. Cases are simulations; they do not authorize actual certification. Where the rule permits inconsistent outcomes, revise it and repeat the case.

D9 Evaluation measures and exit criteria

The coordinator should record planned and actual competent hours, coverage achieved, additional evidence requests, unresolved applicability questions, interpretation disagreements, duplicate record requests and

delays caused by the wording. Separate weaknesses of the standard from weaknesses of the participant's implementation.

A pilot series is ready for technical disposition when each selected activity has a completed report; every consequential interpretation disagreement has a recorded resolution or an explicit release block; all proposed duration rules have observed task evidence; and each accepted wording change has been rechecked in an appropriate case.

No missing sector, untested threshold or open technical review should be represented as validated. The review body should approve an explicit limitation or require additional work before publication. Any limitation affecting the advertised sector scope should be resolved by evidence or by narrowing that claim.

D10 Pilot report and change disposition

Each pilot report should identify the participant scope, draft revision, assessors, conflicts, dates, methods, evidence basis, coverage, findings, time data and wording issues. Recommendations should distinguish a necessary requirement change from an implementation suggestion.

The disposition record should connect each accepted revision to its originating issue, justification, affected clauses, approval and retest. Rejected proposals should have a reason. The scheme owner should retain the full development evidence and publish a proportionate account of consultation and validation when the standard is approved.

Annex E Review findings and publication readiness

Informative editorial record for WD 0.5. The review below is an internal drafting review, not an independent technical validation. It identifies completed wording corrections and remaining approval work so that the next revision can proceed from a traceable baseline.

E1 Internal review dispositions

Review item	Disposition in WD 0.5	Remaining verification
Common and role-specific applicability	Clause 1.4 wording updated; Annex B shows profile selection without automatic exclusions.	Pilot mixed activities, outsourcing and small providers.
Minor finding closure versus effectiveness	14.12 now separates accepted implementation from final effectiveness closure and sets a bounded follow-up.	Simulate infrequent production and insufficient evidence at the limit.
Due dates and status decisions	14.11 now specifies time origin and time-zone handling; 14.12 addresses unresolved minor effectiveness.	Test deadlines across locations and certificate expiry.
Certification roles	Audit, technical review and decision separation retained; expert support does not confer decision authority.	Pilot combined reviewer and decision roles in a small body.
Technical evidence	Annex C defines AQMS evidence and technical review records.	Complete independent technical review and pilot validation.
Audit duration	Annex D supplies a pilot hypothesis with personnel bands, additions and recorded actual time.	Validate and approve an operational methodology before launch.
Scope breadth and technical claims	Sector guide preserves conditional technical controls and separate accreditation or product approval claims.	Independent sector specialists to challenge omitted or insufficient controls.
Cross references and continuity	Clause sequence 1 to 14 retained; Annexes B to E added; revision history updated.	Final proof after technical changes and before publication.

E2 Open publication gates

G1 Technical evidence: verify the completeness and testability of AQMS requirements, sector applicability and supporting operational evidence. Resolve material gaps before approval. Internal approval does not establish external endorsement or recognition.

G2 Technical validation: complete sector reviews and representative pilots, assess omissions and proportionality, and resolve findings affecting safety, evidence reliability or consistent assessment. The present draft has no completed real-world pilot results.

G3 Scheme operability: approve the operational audit-duration method, body eligibility and oversight arrangements, personnel qualification administration, certificate register, complaint and appeal routes, fees and enforceable agreements. Written requirements alone do not demonstrate that those functions exist.

G4 Publication authority: confirm the legal scheme owner, authority to publish, name and mark use, consultation disposition and the exact approved text. Record the approval decision, effective date and controlled distribution arrangements.

G5 Transition and monitoring: identify which organizations or bodies must act, what evidence is needed, when requirements take effect and how competence and performance will be monitored. A new edition of an external reference requires impact assessment, not automatic silent incorporation.

E3 Release decision record

The proposed release record should identify the final document revision and checksum, responsible approval authority, independent technical review, source baseline, pilot evidence, unresolved matters and their disposition. It should state the effective date, any transition period and the scopes for which certification may be offered.

If a gate remains open, the decision should retain draft status or define a limited further development release. Editorial completion and page count do not establish readiness for certification. The approving authority should not accept an unresolved safety or evidence-integrity issue merely as a future improvement action.

E4 Working stage identified at WD 0 5

The WD 0.5 review identified the following operational appendices for development: the validated duration method, auditor qualification assessment instruments, certification-body authorization and oversight forms, assessment report and decision records, and the controlled certificate-status data structure. WD 0.6 adds proposed requirements and records in Annexes F to I. Operational duration validation remains open. These additions remain within this single document.

Before those proposed normative appendices are approved, the project should apply the pilot and source-review controls above. Blank review fields and planned cases are development tools; they are not completed assessments or approvals.

Annex F Assessment personnel qualification

Proposed normative annex, subject to approval of the completed standard. This annex supplements Clauses 5 and 13 for organizations that qualify and authorize auditors, audit leaders, technical experts, competence assessors, certification reviewers and decision personnel. It does not establish a separate personal certification scheme.

F1 Qualification responsibility and scope

The organization granting an authorization shall identify the intended role, permitted activities, sector and technology limits, assessment methods and necessary independence. It shall appoint a competent qualification assessor and an authorization authority. The candidate shall not approve their own qualification or authorization.

A qualification assessor may recommend authorization but shall not act as the sole authorization authority for a candidate whom that assessor alone trained. The authorization authority shall independently examine whether the evidence supports the proposed limits. Where internal resources cannot provide the required independence, the organization shall use a competent external reviewer.

The qualification process shall distinguish training completed, competence demonstrated and assignment authorized. An authorization held with another organization may provide evidence but shall not be accepted without verification of its relevance, currency and limits.

F2 Candidate evidence and prerequisites

The candidate shall provide a verified identity, relevant education or equivalent learning, practical experience, training history, prior assessment work where available and declared conflicts. The granting organization shall verify material claims using original evidence, issuer confirmation, work samples or other reliable means.

Experience evidence shall describe the work performed and the responsibility held, rather than only the employer and number of years. A technical scope shall require evidence of understanding its actual failure mechanisms, controls and acceptance decisions. Transferable skills may be recognized where their relevance is demonstrated.

The qualification assessor shall identify any gap before practical assessment. Missing mandatory customer or authority qualifications shall prevent authorization for the affected assignment. This annex does not prescribe a universal university degree or a fixed number of employment years for every sector.

F3 Assessment criteria and evidence methods

Criterion	Required demonstration	Suitable evidence
Requirement interpretation	Separate applicable requirements from guidance and personal preference; identify the responsible party.	Knowledge assessment and reasoned case analysis.
Applicability and scope	Evaluate mixed activities and retained responsibility for outsourced work.	Scope exercise with a justified clause-level decision.
Technical judgment	Recognize significant failure modes, relevant controls and evidence limitations in the assigned domain.	Technical interview, work samples and observed assessment.

Criterion	Required demonstration	Suitable evidence
Evidence collection	Select traceable samples, corroborate material assertions and respond to adverse evidence.	Witnessed audit and review of working records.
Findings and classification	Connect a failure to a requirement and defensibly classify its consequence and extent.	Written findings using conformity, minor, major and critical cases.
Communication and reporting	Explain scope, evidence, limitations and conclusions clearly and accurately.	Observed meetings and completed audit report.
Impartiality and integrity	Disclose conflicts, resist improper influence and protect confidential evidence.	Conflict scenarios and observed professional conduct.
Follow-up and closure	Distinguish correction, implementation and effectiveness; reject unsupported closure.	Corrective action evidence review and decision explanation.

F4 Knowledge and case assessment

The qualification assessor shall use controlled assessment material appropriate to the role. The material shall include requirement interpretation, a disputed omission, outsourced responsibility, insufficient evidence, a systemic failure, an immediate safety concern and a conflict of interest. The candidate shall explain the basis for significant judgments.

Each applicable criterion shall be rated Demonstrated, Not demonstrated or Not evaluated. Independent authorization shall require Demonstrated for every applicable criterion. Strength in one criterion shall not compensate for failure in another. Not evaluated shall not be treated as a pass.

Assessment records shall identify the material revision, candidate response, evaluator conclusion and reason. If a knowledge test includes a numerical score, the score shall supplement these criterion-level decisions and shall not override an essential failure involving safety, evidence integrity or impartiality.

F5 Witnessed performance and role extensions

Before initial independent audit authorization, the candidate shall complete an assigned audit cycle under observation, including preparation, evidence evaluation, reporting and communication of findings. Where no actual nonconformity occurs, controlled cases shall supplement the observation to assess finding and closure judgment. Simulation shall be identified and shall not replace observation of practical audit conduct.

An audit leader candidate shall additionally demonstrate team planning, competence allocation, coordination of evidence, resolution of conflicting conclusions and control of the closing discussion. A technical expert shall demonstrate the ability to explain relevant technical evidence while respecting the limits of their assessment authority.

A certification reviewer or decision candidate shall evaluate a complete case file, identify coverage or closure gaps and record a defensible decision under Clause 14. A competence assessor candidate shall demonstrate criterion-based evaluation and feedback. Authorization for one role shall not automatically authorize another.

An extension to a new technical domain shall require assessment of the additional competence and a witnessed or otherwise directly observed practical evaluation of that domain. The granting organization shall retain the basis for any recognition of existing evidence.

F6 Authorization decision and register

The authorization authority shall review the completed criterion record, witnessed results, unresolved concerns and proposed restrictions. It shall record Grant, Grant with restrictions or Refuse, with reasons. Grant with restrictions shall describe a narrower demonstrated scope or a supervision condition; it shall not conceal a failed essential criterion for independent work.

The authorization register shall identify the person, role, approved scope, restrictions, effective date, reassessment date, granting authority and current status. The assignment process shall check this register before allocating work. Expired, suspended or restricted authorizations shall not be represented as unrestricted.

The person shall receive a clear statement of their authorization and duties to disclose new conflicts, material errors, loss of a required qualification or inability to perform competently. A change in employment or contracting arrangement shall trigger evaluation of the continuing authorization basis.

F7 Monitoring remediation and appeals

Annual performance review and reassessment at intervals not exceeding three years shall follow Clause 13.19. Monitoring shall examine representative work within the authorization, including adverse feedback and any finding or decision later overturned. Witnessing shall be planned across the person's significant technical activities.

When competence is in doubt, the granting organization shall restrict relevant assignments while it investigates. Remediation shall identify the gap, development activity and reassessment evidence. Restoration shall require a recorded competent decision; completion of training alone shall not restore authorization.

The candidate or authorized person shall have access to a review of a refused, restricted or suspended authorization by a competent person not responsible for the contested assessment or decision. Review shall not remove protective restrictions while reliable concerns remain unresolved.

F8 Qualification decision record

Record field	Entry to complete
Person and requested role	[Identity reference; role; sector; process and technology scope]
Prerequisites verified	[Evidence references; verification method; gaps and disposition]
Criteria F3 to F5	[Each applicable criterion; method; result; evaluator; evidence reference]
Witnessed performance	[Audit or case identifier; dates; role observed; scope; limitations]
Independence evaluation	[Conflicts; training relationship; controls; independent reviewer]
Authorization decision	[Grant; Grant with restrictions; Refuse; reason; authority; date]
Validity and monitoring	[Effective date; reassessment date; restrictions; planned monitoring]
Review or appeal	[Request; independent reviewer; evidence; outcome; notification]

Annex G Certification body authorization and oversight

Proposed normative annex for the scheme owner and certification bodies, subject to approval and operational launch under Clause 14. Authorization under this annex is permission to operate within the IAF AQMS scheme. It shall not be presented as external accreditation or recognition by another scheme.

G1 Application and eligibility review

The scheme owner shall require an application identifying the body's legal entity, ownership and governance, proposed sectors and territories, operating locations, contracted resources and responsible management.

The application shall include evidence of legal accountability, financial and operational capacity, impartiality, competence management, confidentiality, complaints and appeals, and certification decision controls.

The scheme owner shall verify the application against Clause 14 and this annex. Existing accreditation or other authorization may support the evaluation when relevant but shall not replace verification of AQMS-specific competence and controls. The owner shall not authorize a scope for which sufficient technical evaluation is unavailable.

The application review shall identify the evaluation team, competence needs, conflicts, methods, evidence requests and proposed duration. The evaluation team shall not include persons whose consultancy or commercial interest prevents an objective conclusion.

G2 Initial evaluation and operational demonstration

The scheme owner shall evaluate the body's central control functions and locations performing significant certification activities. It shall examine sample files from application through review and decision, including personnel authorization, duration calculations, impartiality checks and the management of adverse evidence.

Before an authorized body conducts its first certification in a proposed technical domain, the scheme owner shall witness an assessment or equivalent controlled pre-authorization demonstration covering that domain. The demonstration shall include the independent review and decision process. Mock decisions shall be clearly identified and shall not result in certificates.

For a new body without live certification files, the evaluation shall use complete controlled case files and observed assessment activity. The owner shall record the limitation and require review of the first live file in each authorized domain before its first certificate is released. Documentary readiness alone shall not establish demonstrated operational competence.

G3 Authorization decision and agreement

An authorization decision shall be made by competent personnel independent of the evaluation team and free of relevant conflicts. Critical and major failures shall be verified closed before authorization. A minor failure may remain open only with an accepted plan, adequate control and a defined verification date within ninety calendar days of notification.

The authorization shall identify the legal entity, authorized technical domains, territories or other restrictions, effective date, expiry date and conditions of oversight. Its period shall not exceed three years.

The scheme owner and body shall enter an agreement covering access, reporting, use of marks, fees, records, sanctions, complaints, appeals and continuity if authorization ends.

Authorization shall not be conditional on federation membership or favorable commercial promotion. The scheme owner shall maintain accessible information identifying authorized bodies and the scope and current

status of their authorization. A certificate issued outside the body's authorization shall be treated as an invalid scheme claim.

G4 Routine oversight programme

The scheme owner shall complete an oversight review of each authorized body at intervals not exceeding twelve months. The programme shall examine performance, competence, complaints and appeals, adverse certification decisions, integrity of the public status information and conformity with the approved duration method.

The review shall sample completed certification files and observe live assessment activity according to risk. Each authorized technical domain shall receive witnessed coverage during the authorization period. Significant personnel changes, inconsistent decisions, credible complaints or evidence-integrity concerns shall trigger additional monitoring without waiting for routine review.

The owner shall record planned and completed coverage. If the body has no relevant live work in a domain during the period, continuation of that domain shall require a recorded competence evaluation and witnessing before its next certificate in that domain is released. Absence of work shall not be recorded as satisfactory witnessed performance.

G5 Oversight findings and corrective action

Oversight findings shall identify the requirement, evidence, classification and affected certification activities. Classification shall follow the principles in Clause 13.12, considering consequences for confidence in certification. The body shall evaluate whether the finding affects previously issued certificates and shall identify necessary client-file reviews or reassessments.

A critical finding shall result in immediate restriction or suspension of the affected authorization and protective action to prevent unsupported certification. Major findings shall receive a response plan within fifteen calendar days and verified closure within sixty days. Minor findings shall receive a plan within thirty days and verified implementation within ninety days, with effectiveness evidence appropriate to the affected control.

The scheme owner shall state notification and due dates using the time rules in Clause 14.11. Overdue major findings, ineffective protective controls or unresolved minor findings at the required verification date shall trigger an authorization-status decision. The owner shall not replace verification with repeated unsubstantiated deadline extensions.

G6 Restriction suspension and withdrawal

The scheme owner shall restrict or suspend authorization when the body lacks demonstrated competence, refuses required access, issues unsupported certificates, fails to control material conflicts or does not fulfil significant corrective obligations. The decision shall define the affected scope, reason, effective date, protective conditions and restoration evidence.

A suspended body shall stop new grants, scope extensions and recertification decisions within the affected authorization. Surveillance and protective action for existing clients may continue only under arrangements explicitly approved by the scheme owner and with adequate competence and independence. These arrangements shall not automatically extend client certificate validity.

Suspension shall not exceed ninety calendar days. Restoration shall require verified fulfilment of the conditions and an independent positive decision within that period. Otherwise the owner shall withdraw the

affected authorization. The owner shall update public status information and implement the client-continuity arrangements in G7.

G7 Protection of affected certified organizations

When authorization is restricted, suspended, withdrawn or expired, the scheme owner shall evaluate the effect on each potentially affected certificate. It shall distinguish a body's administrative failure from evidence that a client's certification conclusion is unreliable. It shall not automatically assume either validity or invalidity without evaluating the relevant basis.

The owner shall define who will notify affected clients, maintain certificate-status information, preserve records, perform necessary additional assessment and manage transfer to another authorized body. Transfer shall meet Clause 14.20 and shall not reset unresolved finding deadlines or erase adverse history.

The body shall preserve and make available the records needed for authorized continuity arrangements, subject to applicable confidentiality duties. If reliable evidence cannot be obtained, the owner shall ensure that public certificate information does not continue to imply unsupported validity. Commercial disputes shall not justify destruction or concealment of evidence.

G8 Renewal appeals and scheme learning

Before renewal, the scheme owner shall review the full authorization period, competence coverage, oversight results, corrective action effectiveness and significant changes. Renewal shall require an independent positive decision before expiry. It shall not be backdated. If renewal is not decided by expiry, the authorization shall expire and the body shall stop new grants, scope extensions and recertification decisions in the expired scope. The scheme owner shall update the public authorization status and apply the client-continuity controls in G7; any continuing surveillance or protective work shall require explicit controlled arrangements.

Competent persons independent of the challenged evaluation and decision shall decide the body's appeal. Appeals shall not automatically remove protective restrictions. The owner shall retain the evidence, reasons and outcome notification.

The scheme owner shall analyze oversight trends and inconsistent judgments. Changes shall follow controlled technical review and transition arrangements and preserve each body's independent certification decisions.

G9 Body evaluation and authorization record

Record field	Entry to complete
Applicant and proposed scope	[Legal entity; ownership; locations; domains; territories; responsible management]
Evaluation basis	[Standard and scheme revision; criteria; team competence; conflict checks]
Evidence and observation	[File samples; operating locations; witnessed domains; simulations and limitations]
Findings and affected clients	[Classification; response; verified closure; review of existing certificates]
Independent decision	[Decision; permitted scope; restrictions; effective and expiry dates; authority]
Oversight plan	[Annual review dates; witnessed coverage; triggers; first-live-file conditions]
Continuity and appeals	[Record custodian; client notification route; transfer arrangements; appeal route]

Annex H Audit and certification records

Proposed normative minimum information for the roles identified below. Existing forms and digital systems may be used when they preserve all required information and its traceability. The tables are blank working templates; they are not evidence of a completed audit or certification decision.

H1 Record connections and ownership

The certification body shall assign a unique client identifier and unique identifiers for each audit, finding, review and decision. The records shall connect to the applicable scope, site schedule and standard revision. A changed scope shall retain a link to the preceding scope and the approving decision.

The audit leader owns the accuracy of the audit report; the technical reviewer owns the review conclusion; and the decision authority owns the certification decision. The body shall define record custody and approval permissions without transferring these responsibilities to an administrative data-entry function.

Corrections shall preserve the original information or a recoverable change history. The person, date and reason for a material correction shall be recorded. A report amended after a decision shall trigger evaluation of whether that decision remains supported.

H2 Application and audit planning record

Required information	Entry to complete
Client and scope	[Legal entity; site addresses; activity at each location; supplied products or services; scope revision]
Responsibilities and interfaces	[Design; manufacture; service; remote support; external providers; shared functions]
Criteria and applicability	[AQMS edition; applicable customer and mandatory obligations; register revision; disputed decisions]
Programme and timing	[Audit type; objectives; cycle; planned dates; shifts; locations; coverage of previous findings]
Duration calculation	[Approved method revision; personnel basis; baseline; each adjustment; planned competent hours]
Team and independence	[Names; assigned roles and technical domains; authorization check; conflicts and controls]
Methods and access	[On-site or remote activities; sample priorities; technology; language support; access limitations]
Plan approval	[Reviewer; date; accepted plan revision; material changes and reasons]

H3 Audit report record

Required information	Entry to complete
Identification	[Audit identifier; client and scope; criteria; actual dates; report revision]
Execution	[Team and roles; actual competent hours; locations and shifts; methods; deviations from plan]

Required information	Entry to complete
Evidence coverage	[Processes and requirements evaluated; sample identifiers; relevant results; interfaces followed]
Applicability conclusion	[Register evaluated; accepted justifications; disputed omissions; unassessed duties]
Findings	[Finding identifiers; requirements; objective evidence; classifications; urgent communications]
Limitations	[Unavailable evidence; incomplete activities; remote-method limitations; effect on conclusion]
Overall conclusion	[System effectiveness assessment; significant strengths and failures; recommendation and basis]
Closing and issue	[Closing participants; disagreements; response deadlines; report approval and distribution]

A favorable recommendation shall not be described as a certification decision. Where evidence coverage is incomplete, the report shall identify the missing work and shall not silently mark it conforming.

H4 Finding and corrective action record

Required information	Entry to complete
Finding statement	[Identifier; exact requirement; observed evidence; failure; classification and basis]
Notification and dates	[Notification timestamp; reference time zone; containment, plan, implementation and follow-up deadlines]
Correction and protection	[Affected outputs or decisions; immediate action; extent; notifications; owner]
Cause and extent analysis	[Verified causes; failed prevention or detection; similar conditions; unresolved uncertainty]
Corrective action	[Actions linked to causes; responsibility; resources; completion criteria; change validation]
Implementation verification	[Evidence; method; verifier; date; implemented or incomplete conclusion]
Effectiveness verification	[Required operating exposure; actual exposure; recurrence evidence; result; verifier]
Status and certification effect	[Open; plan accepted; implemented with effectiveness pending; closed; reopened; status decision reference]

H5 Use of finding status

The body shall use the status values in H4 consistently. Plan accepted means that proposed action has been judged adequate; it does not mean implemented. Implemented with effectiveness pending is permitted only within the minor-finding conditions and time limits of Clause 14.12. Closed requires the applicable verification and effectiveness evidence.

A finding shall be reopened when new evidence invalidates closure. The original finding, closure decision and new evidence shall remain traceable. Reclassification shall record its reason, authorized reviewer and the applicable deadline consequences; it shall not restart the original clock without an explicit justified rule.

The body shall verify outstanding deadlines before initial certification, surveillance continuation, scope extension, recertification or transfer decisions. A system status label shall not replace the decision maker's review of the actual evidence.

H6 Technical review record

Review question	Entry to complete
Is the scope supported?	[Entity and sites verified; applicability justified; actual coverage sufficient]
Was the audit competent and independent?	[Authorization scope; assignments; conflicts; duration and method adequacy]
Are findings reliable?	[Requirement and evidence connection; classification; extent; unresolved disagreements]
Are closure conditions met?	[Critical and major closure; minor plan or closure basis; deadlines; effectiveness restrictions]
Is more work required?	[Missing evidence; additional audit; clarification request; responsible person and due date]
Review conclusion	[Sufficient for decision or insufficient; reasons; reviewer; independence declaration; date]

H7 Independent certification decision record

Required information	Entry to complete
Decision request	[Grant; continue; extend; reduce; renew; suspend; restore; withdraw; transfer acceptance]
Evidence reviewed	[Audit report; technical review; finding records; scope schedule; additional evidence identifiers]
Outstanding matters	[Minor findings permitted to remain open; protection; follow-up dates; unresolved limitations]
Decision and scope	[Outcome; precise affected scope and sites; reason; conditions; certificate identifier]
Dates and validity	[Decision date; effective date; expiry; original cycle basis; any gap in validity]
Decision authority	[Name; role authorization; independence and conflict checks; approval]
Communication and implementation	[Client notification; public status update; mark-use instruction; follow-up owner]

The body shall reject a positive decision when a required condition is unmet. Administrative completion of this template shall not authorize a certificate. Suspension, restoration and withdrawal shall be supported by the same traceable decision discipline as initial certification.

Annex I Certificate information and status control

Proposed normative annex for certification bodies and the scheme owner. This annex defines minimum information and controls; it does not prescribe a particular software product. Certificate information shall remain distinguishable from assessment personnel authorizations and certification-body authorizations.

I1 Identity and scope information

The certification body shall maintain a unique, non-reused identifier for each certificate and a persistent identifier for the certified legal entity. The record shall distinguish the legal entity name, trading name where used, operating locations, certified activities, standard edition and scope revision.

Each site schedule shall identify the location, activity and link to relevant support functions. A remote support location shall not be represented as an independently certified operational site unless it has its own supported certification scope. Changes to site information shall be controlled through the applicable scope decision.

The body shall retain the previous scope and status history. A certificate number shall not be reassigned to another legal entity to conceal ownership changes, transfer, withdrawal or a break in certification.

I2 Minimum certificate data

Data element	Content and control
Certificate identity	Unique certificate number; issuing body identity; certified legal entity identifier.
Assessed scope	Approved activity description; sites; standard edition; controlled limitations and non-applicability statement.
Decision connection	Decision identifier; responsible authority; decision date; scope revision.
Validity dates	Initial certification date; current issue date; effective date; expiry; previous-cycle connection.
Current status	Valid; Suspended; Withdrawn; Expired; Terminated. Include status effective date and affected scope.
Supersession or transfer	Previous record reference; receiving or previous body where relevant; continuity or validity gap.
Public verification	Current status, issuing body, entity, scope and validity; date or timestamp of last update.
Controlled private record	Audit history; findings; decision evidence; confidential contacts; change and access history.

I3 Status transitions and authority

Valid status shall require a positive authorized decision and a current validity period. Suspended status shall identify the affected scope and restoration conditions. Withdrawn status shall record a decision ending certification for the stated reason. Expired status shall apply when the validity period ends without a timely renewal decision. Terminated status shall identify voluntary or contractual ending where withdrawal for nonconformity is not the basis.

Only authorized personnel shall enter a decision-dependent status change, and the system shall require a traceable decision reference. Automatic expiry may operate from the approved expiry date, provided that the resulting event is logged and cannot be silently reversed by administrative editing.

Restoration from suspension shall require an independent decision under Clause 14.19. Expiry shall not be converted to uninterrupted validity through backdating. Transfer shall retain the history required by Clause 14.20; it is not itself proof of a new full assessment.

For a partially suspended scope, the public result shall show the restriction clearly. A single unqualified Valid label shall not be displayed where it would imply that suspended activities remain certified.

I4 Public verification and updates

The certification body shall make current validity information accessible without requiring purchase of an audit report. Searches or certificate links shall resolve to the authoritative record and display the issuing body, certified entity, scope, status and relevant dates.

A decision changing validity or scope shall be reflected publicly no later than twenty-four continuous hours after its effective time, using the recorded reference time zone and hour-counting rule in Clause 14.11. Until the update is complete, the body shall prevent issuance of a conflicting certificate or confirmation. A known critical restriction shall be communicated promptly to affected parties rather than waiting for routine publication.

Public records shall not disclose personal evaluator files, confidential audit evidence or customer information unnecessary to verify certification. Where public access is interrupted, the body shall provide a controlled alternative verification channel and identify any limitation on freshness. A cached page shall not be presented as guaranteed current.

I5 Integrity access and recovery

The body shall protect certificate records against unauthorized creation, alteration and deletion. Permissions shall distinguish data entry, decision approval and system administration. An administrator shall not create a positive certification decision merely by changing a database field.

Material changes shall retain the previous value, new value, person or controlled system identity, time and reason. Correction of a clerical error shall be distinguishable from a change in certification scope or validity. The body shall periodically reconcile issued certificates and public records against authorized decisions.

The body shall maintain recoverable backups and test restoration at risk-based intervals. Recovery shall include verification of status events and decisions made since the restored copy. During uncertain recovery, the body shall not provide an unsupported assurance of validity.

I6 Scheme register and record exchange

The scheme owner shall define the minimum exchange format and update responsibilities for the scheme register. A body submitting a record shall verify the entity, certificate and decision identifiers, dates and status. Rejected or failed submissions shall be corrected and tracked to completion.

The owner shall reconcile material differences between the scheme register and the issuing body's record. Until resolved, the published result shall communicate the uncertainty or restriction rather than silently selecting the more favorable status.

Record exchange shall preserve confidentiality and the evidence needed for oversight, transfer and client continuity. A technical identifier, verification link or digital signature may support authenticity but shall not replace the underlying competent decision.

I7 Prelaunch acceptance checks

Before live certification records are published, the body and scheme owner shall demonstrate that their controls correctly handle initial grant, partial suspension, restoration without expiry extension, withdrawal, expiry, transfer, a changed site schedule and correction of a clerical error.

Checks shall include an unauthorized status-change attempt, a failed update, a duplicate identifier, conflicting register information and restoration from backup. The result shall identify expected behavior, observed behavior, evidence and unresolved defects. Defects permitting an unsupported Valid result shall be resolved before launch.

All test records shall be marked as test data and separated from public certificate claims. Successful software checks demonstrate record-control behavior only; they do not establish technical conformity of an organization or approval of this draft.

Annex J Pilot cases and expected reasoning

Informative. All organizations, events and evidence packages in this annex are hypothetical. The expected responses are internal interpretations of this working draft for pilot testing, not completed assessments, external-standard interpretations or certification decisions.

J1 Use of the case pack

The pilot coordinator should give assessors the scenario and questions before releasing the expected reasoning. Assessors should record the applicable requirement, evidence sufficiency, classification where justified, necessary action, responsible role and any limit on the conclusion. Two assessors should first work independently under Annex D.

A different answer should be evaluated against the stated facts and exact requirement. Agreement with the expected response is not sufficient when the reasoning is unsupported. If a scenario is incomplete, the assessor should identify the missing fact and explain which conclusion depends on it. The coordinator should not invent additional evidence to make a preferred answer correct.

Cases may support the knowledge and decision exercises in Annex F. They do not replace witnessed practical performance. Before using this public case pack for candidate assessment, the granting organization should develop controlled equivalent variants so that memorizing these responses is not mistaken for demonstrated competence.

J2 Customer design and purchased heat treatment

Scenario. A 40-person supplier machines brackets to customer-controlled drawings. Its contract excludes authority to change the product design. The supplier develops the machining process and buys heat treatment. It marks all of Clause 6 and all special-process controls Not applicable. Provider selection records exist, but heat-treatment qualification and lot acceptance evidence have not been obtained.

Questions. Which omissions can be justified? What evidence is missing? Can a positive conformity conclusion cover the purchased process?

Expected reasoning. Product-design duties may be absent to the extent supported by the contract and actual practice. Process development and retained supplier controls remain relevant. The broad exclusions are unjustified. The assessor should examine the heat-treatment requirements, provider qualification, traceability and acceptance evidence. The missing records do not support a positive conclusion. Classification depends on the demonstrated extent, consequences and remaining controls; the case does not establish an immediate severe-harm threat.

AQMS references: 1.5; 1.6; 6.14; 7.3; 7.6; 8.9; B3.

J3 Measurement evidence used after an equipment failure

Scenario. A laboratory finds that a measuring instrument fails an intermediate check. It stops using the instrument, but releases a report based on earlier measurements without assessing when the error began or which results may be affected. Other equipment records are reliable. No product safety consequence has yet been established.

Questions. What must the laboratory investigate? Does calibration status alone settle the validity of earlier results?

Expected reasoning. The laboratory should control potentially affected work, determine the period and extent of unreliable results and evaluate reports already issued. A previous calibration does not resolve the intervening failure. The assessor should review the instrument history, check results, method sensitivity and release decisions. Classification requires evidence of extent and consequences; neither an automatic minor finding nor an automatic critical finding is justified by the scenario alone.

AQMS references: 5.12; 11.9; 11.10; 11.18; 12.11; 13.12.

J4 Digital release with an incomplete evidence trail

Scenario. A diagnostic software company releases an update using a validation report for the previous version. The update changes a decision threshold. The release record identifies the new software build but does not link it to reviewed change impact or suitable validation evidence. The company argues that it has no factory and therefore Clause 6 does not apply.

Questions. Which activity triggers the requirements? What release evidence is needed? Can physical production be used as the applicability test?

Expected reasoning. Software development and controlled release trigger the relevant duties. Absence of physical assembly does not remove development responsibility. The organization should assess the change, affected configurations and users, and establish suitable verification and validation before relying on the release. The assessor should determine whether this is a single unsupported change or a systemic release-control failure and evaluate the consequence before classification.

AQMS references: 1.4; 4.7; 6.12; 6.13; 6.17; 9.14; 9.19; B4.

J5 Confirmed defeat of a battery safety control

Scenario. During a surveillance audit, verified records and direct observation establish that a battery pack safety interlock has been deliberately bypassed on packs awaiting shipment. The bypass creates a credible immediate threat of severe harm during intended use. Shipment is still scheduled. The responsible manager asks the auditor to wait for the final report.

Questions. What is the finding class? Who must act immediately? What happens to affected certification?

Expected reasoning. The stated facts meet the critical definition. The audit leader should communicate promptly to responsible management and the certification body. The organization should initiate protective action immediately. The body should suspend affected certification once the critical finding is confirmed. The initial containment evidence is due within twenty-four hours of notification. These actions do not replace control of affected packs or any applicable external notification duty.

AQMS references: 3.7; 4.11; 9.10; 13.12; 13.13; 14.11; 14.12.

J6 Minor action implemented without sufficient operating exposure

Scenario. A minor finding is notified at day zero. Its plan is accepted by day thirty. The correction and permanent action are verified at day seventy-five. Only one relevant service transaction has since occurred, while the approved effectiveness criteria require a broader operating sample. Protective controls remain adequate. The certificate remains within its validity period.

Questions. What finding status is appropriate? May the body report the finding as closed? What limits apply to follow-up?

Expected reasoning. The record may state Implemented with effectiveness pending if the conditions in 14.12 are met. It should not state Closed. The body should record the required exposure, protection and follow-up date, no later than day one hundred eighty after notification. If effectiveness remains unsupported at that limit, the affected scope is suspended. This allowance cannot be used for a critical or major finding.

AQMS references: 12.14; 14.12; H4; H5.

J7 Major finding overdue during surveillance

Scenario. A major surveillance finding is formally notified at day zero. The plan arrives on day ten. At the end of day sixty, the certification body has neither verified implementation nor obtained evidence supporting closure. The client asks for a new due date because a contractor is unavailable. Its certificate would otherwise remain valid for another year.

Questions. Does plan acceptance preserve certification? Can the deadline be reset for contractor availability?

Expected reasoning. An accepted plan is not closure. Under the proposed scheme rule, an overdue major finding results in suspension of affected certification. The body should record and communicate the decision and restoration conditions. Contractor availability does not create an automatic extension. The organization remains responsible for protective controls and corrective action. The suspension period is separate from the original finding period and does not extend certificate expiry.

AQMS references: 12.13; 14.11; 14.12; 14.18; 14.19.

J8 Recertification decision after expiry

Scenario. A recertification audit finishes before expiry, but the required independent decision is not completed until five days after expiry. The body proposes retaining uninterrupted validity because the audit recommendation was positive. No separate rule authorizing uninterrupted status exists.

Questions. What is the status during the gap? Which dates belong in the record?

Expected reasoning. The certificate expires on its stated date. A positive recommendation is not a decision. The body should assess evidence currency and any required additional work, then record the actual decision date and a validity period beginning only from the positive decision. The gap should remain visible in history and public information. A backdated decision or deletion of the expiry event would be inconsistent with the draft.

AQMS references: 14.13; 14.16; H7; I2; I3.

J9 Transfer with unavailable audit history

Scenario. A client presents a certificate shown as valid on the issuing body's public record and requests transfer. It provides no prior audit report or finding history. The receiving body cannot establish whether important corrective actions remain open. A salesperson proposes accepting the transfer from the certificate image alone.

Questions. Is public validity enough? What work is needed before accepting a transfer?

Expected reasoning. Public validity supports authenticity and current status but does not establish the full transfer basis. The receiving body should obtain sufficient history, assess unresolved concerns and perform additional assessment or treat the request as a new application where necessary. It should not erase

previous deadlines or restart the cycle simply because information is unavailable. Acceptance requires competent independent review and decision.

AQMS references: 14.20; H6; H7; I6.

J10 Auditor consultancy and a technical scope gap

Scenario. An experienced manufacturing auditor helped implement a client's quality system eighteen months ago. The body proposes assigning that person to audit the same client's battery software controls. The auditor has a current mechanical-process authorization but no demonstrated battery-software competence.

Questions. Are experience and a current authorization enough? Can an expert remove both concerns?

Expected reasoning. The consultancy restriction prevents the client assignment within the stated two-year minimum period. Independently, the technical authorization does not cover the proposed work. Adding an expert does not remove the personal impartiality restriction or automatically authorize the auditor for a new domain. The body should select an eligible competent team and assess any new authorization through Annex F.

AQMS references: 13.5; 13.17; 13.18; 14.4; F2; F5; F6.

J11 Deliberate alteration of certification evidence

Scenario. An authorized body is found to have deliberately changed an audit report to conceal a supported major finding and obtain a positive certification decision. The alteration and its material effect on the decision are verified. The scheme owner has not yet determined whether other files are affected.

Questions. How should the oversight finding be treated? Does every client certificate automatically become invalid?

Expected reasoning. The deliberate material falsification meets the critical evidence-integrity principle. The scheme owner should immediately restrict or suspend the affected authorization and require protection against unsupported decisions. It should investigate the extent across files and assess affected certificates individually. The evidence supports neither automatic invalidation of every unrelated client nor an assumption that every existing certificate remains reliable.

AQMS references: 13.12; 14.4; G5; G6; G7.

J12 Conflicting certificate status records

Scenario. A body makes a supported suspension decision. Its own controlled record says Suspended, but a failed update leaves the scheme register showing an unqualified Valid result. The discrepancy is known. An administrator offers to delete the failed submission message and wait until the next monthly reconciliation.

Questions. What must be corrected? Who owns the certification decision? What should the public result communicate?

Expected reasoning. The discrepancy should be tracked to correction and the public result should not continue to imply unsupported validity. The issuing body remains responsible for its decision and the scheme owner for its register controls. The failure record and history should be preserved. The body should provide a controlled verification alternative where necessary and meet the proposed public-update limit. Administrative editing cannot reverse a suspension.

AQMS references: 14.18; H1; I3; I4; I5; I6.

J13 Logistics and repair responsibilities in one company

Scenario. One company stores replacement parts and repairs vehicles at a second location. The warehouse has traceable preservation and dispatch controls. At the repair site, there is no defined authorization or verification for returning vehicles to use. Management submits a logistics-only scope statement although the proposed certificate advertising includes vehicle repair.

Questions. What is wrong with the scope? Can good warehouse performance cover the repair activity?

Expected reasoning. The claimed scope and assessed activities are inconsistent. Repair requires its own applicable service, competence and return-to-use controls. Warehouse performance cannot establish repair conformity. The scope claim should be corrected and relevant repair activity assessed before inclusion. The absence of a required return-to-use control should be evaluated as a possible systemic failure, with safety consequence determined from the actual repairs and exposure.

AQMS references: 1.3; 5.5; 10.5; 10.9; 10.14; 14.6; 14.10; 14.22.

J14 Audit time exhausted before critical process coverage

Scenario. A pilot audit reaches its allocated time before reviewing a technically significant process. Two trainees have attended throughout. The lead auditor proposes counting their attendance as extra auditor days and recording all planned requirements as covered. The trainees did not independently collect or evaluate evidence.

Questions. Can attendance increase completed competent time? How should the coverage gap affect the conclusion and duration analysis?

Expected reasoning. Trainee presence does not create independent auditor time. The leader should identify incomplete work, revise the plan and limit the conclusion until sufficient evidence is obtained. The duration record should preserve planned and actual productive time and the unfinished tasks. The pilot should investigate whether the baseline, adjustments, assignment or access assumptions caused the shortfall.

AQMS references: 13.4; 13.14; 14.7; D4; D5; K3; K5.

J15 Independent response and reconciliation record

Field	Entry to complete
Case and assessor	[Case identifier and revision; assessor; role; date; independent first response]
Facts and missing information	[Facts relied on; uncertainty; evidence needed for a firmer conclusion]
Requirement and applicability	[Exact AQMS reference; responsible role; applicability decision and reason]
Finding and consequence	[Conformity or failure; justified classification; protective action; scope affected]
Dates and status	[Notification basis; relevant deadlines; finding and certificate status; decision authority]
Comparison and disposition	[Initial disagreement; evidence or wording issue; resolution; revision and retest needed]

Annex K Audit duration validation and approval

Proposed normative development requirements for the scheme owner, subject to approval of the completed standard. This annex defines how an operational duration method shall be validated and controlled. It does not convert the pilot starting points in Annex D into an approved certification rule.

K1 Validation responsibility and intended use

The scheme owner shall identify the person responsible for developing the duration method and appoint an independent technical reviewer. The validation plan shall define the intended scope, audit types, organization profiles, sites, shifts, technical domains and methods to which the proposed calculation will apply.

The method shall separately address readiness assessment, initial implementation audit, surveillance, recertification, scope extension and special audits. Evidence for one audit type shall not automatically establish the adequacy of another. A surveillance or recertification percentage shall not be adopted without a task and coverage basis.

The owner shall freeze each candidate method revision before collecting comparison data. A changed calculation shall retain its prior revision, reason for change and effect on previously planned or completed pilot work.

K2 Definition of time and populations

The duration method shall distinguish evidence-collection time, preparation, travel, reporting, technical review, decision and follow-up. It shall state which categories the calculation covers and how competent parallel work is counted. An auditor day shall have a defined number of working hours.

The personnel basis shall define inclusion of temporary workers, contractors, part-time staff, shared support and multiple shifts. Allocation across sites shall prevent double counting while preserving the need to assess shared interfaces. A reduction for repeated work shall require evidence that the remaining time covers relevant variation and abnormal conditions.

Calendar duration and total auditor time shall be recorded separately. Observers, interpreters, trainees and technical experts shall not automatically be counted as independently productive auditors. Where an expert performs a distinct necessary technical task, the method shall record that task and its relationship to auditor evidence evaluation.

K3 Task and coverage record

For each pilot, the planning record shall identify the processes and requirements to be evaluated, necessary technical domains, site and shift coverage, expected samples, intended methods and known constraints. It shall connect each significant task to a competent assigned person and planned time.

During execution, the team shall record actual productive time, tasks completed, additional tasks identified and work remaining. It shall identify interruptions and delays separately from productive assessment. The record shall explain whether a shortfall resulted from underestimated scope, technical complexity, access, poor preparation or inefficient execution.

Completion shall mean sufficient evidence for the defined assessment objective, not merely elapsed time or a checked agenda item. If a task remains unassessed, its time allocation shall not be treated as validated. The pilot report shall retain the resulting limitation on conclusions.

K4 Duration observation template

Task or component	Planned basis	Actual result to record
Population and scope	[Personnel count; activities; sites; shifts; support; technologies]	[Verified differences and effect on the calculation]
Baseline	[Method revision; band or task estimate; competent hours]	[Hours used; coverage achieved; assumptions tested]
Additions and reductions	[Each adjustment; specific task; reason; approval]	[Observed need; duplicate allowance; missing task]
Specialist work	[Domain; assigned competence; expert and auditor interaction]	[Distinct productive hours; evaluation completed]
Remote or on-site work	[Method by task; evidence access; travel excluded]	[Method success; access limitations; extra work]
Coverage shortfall	[Expected tasks and samples]	[Unassessed work; cause; additional hours needed]
Other effort	[Preparation; reporting; review; decision; follow-up]	[Actual hours by category; kept separate from audit time]

K5 Analysis of sufficiency and burden

The validation team shall compare planned and actual time with achieved coverage for each profile and audit type. It shall examine underestimation of technically significant tasks, unnecessary duplicated work and differences between assessors. An average time across dissimilar scopes shall not be the sole basis for a common rule.

The analysis shall distinguish a participant's incomplete implementation from insufficient audit time. Additional time spent investigating a material failure may still be necessary even if the candidate baseline was suitable for normal conditions. The operational rule shall state how such additional work is authorized and recorded.

Commercial price and a desire to shorten visits shall not establish adequacy. Equally, unused time shall be examined for unjustified allowances or inefficient planning. The objective shall be sufficient competent evidence collection with a documented basis, rather than maximizing or minimizing time alone.

K6 Acceptance and limitations

The technical reviewer shall accept a proposed duration rule only when its scope, inputs, baseline, adjustments, minimum conditions and exception process are clear and supported by representative observed work. Every material shortfall in the validation set shall have a disposition and appropriate retest or additional evidence.

The decision shall identify the profiles and audit types for which validation is sufficient and those for which evidence remains incomplete. A profile lacking support shall receive an explicitly limited task-based assessment route with technical review or remain outside the operational rule until validated. It shall not be assigned an untested automatic reduction.

A rule that allowed required safety, technical or independence checks to be omitted shall not be accepted merely because most other tasks were completed. The reviewer shall examine consequential outliers and shall not conceal them in an aggregate completion rate.

K7 Approval and controlled introduction

The scheme owner shall approve the operational method through its defined authority after independent technical review. The approval record shall identify the revision, permitted use, evidence set, open limitations, effective date, training needs and transition from any previous method.

Before use, authorized bodies shall receive the approved rule and demonstrate that relevant planners and reviewers can apply it correctly to representative cases. The owner shall resolve material interpretation differences before permitting the affected calculation to support certification.

Approval of a duration method shall not by itself authorize publication of the standard, accreditation claims or certification-body operation. The other launch conditions in Clause 14 and Annex E shall remain applicable.

K8 Validation and approval record

Field	Entry to complete
Candidate method	[Identifier; revision; owner; intended profiles and audit types]
Evidence set	[Pilot identifiers; observed scopes; assessor competence; time and coverage records]
Analysis	[Underestimation; excessive allowance; variation; access effects; consequential outliers]
Changes and retests	[Rule changed; evidence supporting change; comparable retest; result]
Independent review	[Reviewer and independence; accepted scope; limitations; unresolved issues]
Approval	[Approve; approve limited use; return for revision; authority; reason; effective date]
Introduction and monitoring	[Training; interpretation checks; transition; review triggers; responsible owner]

K9 Monitoring after introduction

The scheme owner shall monitor actual time, coverage limitations, additional audit requests, complaints and consistency of duration calculations after introduction. It shall compare observed results with the assumptions used for validation and investigate material departures.

New technologies, substantially different activities, repeated shortfalls or changes to required coverage shall trigger an impact review. The owner shall issue controlled adjustments or require a task-based estimate with technical review where the existing rule is not demonstrably suitable.

Changes shall identify whether they affect planned audits, current certification programmes or the reliability of completed assessments. The owner shall define proportionate action and shall not silently rewrite the historical calculation used for an earlier decision.

K10 Current development status

Editorial note. At WD 0.7, Annex D contains candidate starting values and this annex contains the proposed validation method. No real pilot observations, independent approval or operational duration validation have been completed in this document. Tables K4 and K8 remain blank templates. Their existence is not evidence of successful validation.

Annex L Technical review and sector challenge register

Informative review instrument. This annex defines questions and evidence routes for reviewing the draft. It does not add product acceptance limits, establish external-standard equivalence or record completed independent sector reviews. Existing numbered requirements remain the assessment criteria.

L1 Review method

The technical reviewer should examine each requirement as a combination of responsible party, applicability condition, required action, expected outcome and verifiable evidence. The reviewer should identify whether a competent organization can understand and implement it without an unstated decision rule.

Review should follow an actual or explicitly hypothetical activity from customer commitment to delivery and feedback. The reviewer should challenge both unjustified omissions and requirements applied to absent activities. A proposed correction should state the practical consequence and identify the exact text to change.

The tables below are an initial review map. They are not a substitute for reviewing every applicable subclause or for testing sector-specific obligations. Record Untested where evidence is unavailable. Do not infer complete coverage from a row containing a familiar subject title.

L2 Clause review map

Clause	Question to resolve	Evidence route
1 Scope and application	Can the legal entity, sites, actual activities and retained outsourced duties be identified without relying on a commercial category?	Scope, contracts, activity flow and Annex A decisions; challenge mixed operations using B and J.
2 Definitions	Does each defined term support a consistent operational decision without importing a different scheme's meaning?	Compare use in requirements, reports and case responses; record terms with competing interpretations.
3 Management	Do decisions, authority and resources support conformity when delivery or cost pressures conflict?	Trace an escalated concern to management action, resource commitment and authorized restart.
4 Planning and risk	Are foreseeable failure, change, interruption and recovery connected to actual controls?	Trace a significant risk through treatment, continuity exercise, change approval and recovery evidence.
5 Resources and people	Can competence, equipment suitability, information integrity and authorization be demonstrated for critical tasks?	Sample a person, instrument and digital decision from qualification to actual use and review.
6 Development	Are requirements, risks, outputs, verification, validation and transfer connected for the assigned responsibility?	Follow a released product or service configuration, including a change and unresolved development issue.
7 Providers	Are purchased results controlled through appropriate specification, qualification, monitoring and acceptance?	Follow an external process or technical service through the supplier chain and a failure response.
8 Operations	Do working controls match actual production or service execution and react effectively to abnormal conditions?	Observe setup, changeover, special process, traceability, deviation and release as relevant.

Clause	Question to resolve	Evidence route
9 Technology	Are the relevant technical categories triggered by supplied function, and are acceptance criteria sourced for the actual market and application?	Technical specification, configuration, risk evidence and verification; identify controls outside the current draft.
10 Services	Are intake, execution, handover and field actions controlled across the organization's service responsibilities?	Follow a service order or field case through diagnosis, parts, competence, return to use and feedback.
11 Conformity evidence	Can a result be reconstructed and shown suitable for the acceptance decision?	Method, item identity, equipment, uncertainty where relevant, technical records and report review.
12 Performance	Do reliable data and management review lead to effective action rather than administrative closure?	Trace an adverse trend to cause analysis, resources, implementation and sufficient effectiveness evidence.
13 Assessment	Can competent independent assessors obtain sufficient evidence and reach defensible conclusions?	Audit plan, authorization, samples, findings, limitations and independent case comparisons.
14 Certification	Does every status decision have sufficient evidence, competent independent authority and controlled dates?	Trace application to decision and public status; test open findings, expiry, suspension and transfer.

L3 Review of the annexes

Annex A should be tested for justified requirement selection and retained responsibilities. Annex B should be tested against businesses with more than one activity. Annex C supports independent review of AQMS requirements and evidence. Annex D should produce real observations when executed; planned work is not proof of validation.

Annex E should remain a traceable review and publication record. Annexes F and G should be tested for competence, independence, authorization scope and the feasibility of monitoring. Annexes H and I should allow reconstruction of a decision and prevent misleading certificate status.

Annex J should challenge judgment without replacing observed competence. Annex K should connect a proposed duration calculation with actual coverage and limitations. Annexes L and M support review and disposition; they do not establish that independent validation has occurred.

L4 Sector challenge questions

Activity	Specific challenge	Relevant starting points
Vehicle and component integration	Are interface failures and responsibilities across purchased hardware, software and final integration adequately controlled?	6.2; 6.9; 9.3; 9.5; 9.15
Materials and special processes	Can batch variation, process qualification and the limits of final testing be evaluated without treating inspection as proof of every process condition?	7.6; 8.9; 8.12; 9.6; 11.5
Battery charging and stored energy	Do the requirements address the actual operating states, protective functions, transport and service interfaces within the supplied scope?	9.9 to 9.13; 10.7 to 10.9; 11

Activity	Specific challenge	Relevant starting points
Software AI and connected services	Are version changes, operating limits, data validity, security and post-release performance sufficiently testable?	5.18; 9.14 to 9.19; 10.16
Production equipment	Are installation, commissioning, software interfaces and transfer of maintenance information covered by the supplier's responsibility?	6.18; 9.21; 10.7; 10.10
Laboratory and inspection services	Can evidence support the stated result while accreditation and product certification remain separately justified claims?	11.2 to 11.19; 1.7; 14.1
Distribution repair and remanufacture	Do provenance, incoming condition, preservation, repair limits and return-to-use evidence remain connected?	7.10; 9.20; 10.6 to 10.14
Assessment and certification	Can a small body maintain independence and competence without bypassing review, oversight or record controls?	13.5; 14.13; F1; G2; H6; H7; I3

L5 Customer and market requirement traceability

The reviewer should select a relevant customer or market obligation and identify its source, revision, effective date, applicability, internal owner, affected output and implementation evidence. The review should test how a changed obligation reaches development inputs, suppliers, operations and acceptance decisions.

Where two obligations appear inconsistent, the record should identify the conflict and the authorized resolution. A general AQMS conformity statement should not be treated as resolution of an unverified product approval, test method, customer-specific requirement or market authorization.

The source comparison should distinguish an obligation absent from the AQMS text but controlled through Clause 1.7 from an essential system control missing from the draft itself. The latter may require a standard revision; the former may require correct implementation and a clearly stated scope limitation.

L6 Requirement level review record

Field	Entry to complete
Review identity	[Reviewer; competence and independence basis; date; draft revision; sector or activity]
Exact requirement	[Clause or subclause; responsible role; applicability condition; action and intended result]
Evidence examined	[Live evidence or hypothetical case; identifiers; method; limits and missing information]
Review result	[Supported by examined evidence; wording issue; coverage gap; intentional difference; Untested]
Practical consequence	[Effect on safety, conformity, assessment consistency, burden or certification claim]
Proposed disposition	[Exact revised text or action; reason; related clauses; necessary retest]
Decision and follow-up	[Decision authority; outcome; owner; target date; closure evidence and independent review]

Annex M Draft review findings and technical disposition

Informative editorial record for WD 0.8. The findings below result from an internal consistency review of the working text and its hypothetical case pack. They are not findings from an independent audit or an executed organizational pilot.

M1 Wording changes made in this revision

Item	Issue identified	Disposition and remaining check
R8 01 Public update interval	I4 used one business day without identifying a business calendar; holiday treatment could therefore vary.	I4 now uses twenty-four continuous hours and the recorded time basis. Confirm feasibility and critical-event communication during pilot execution.
R8 02 Body authorization expiry	G8 prohibited backdated renewal but did not explicitly state operating restrictions and client-continuity action when authorization expires.	G8 now stops new certification decisions in the expired scope and applies G7 continuity controls. Test client-file access and transfer arrangements.
R8 03 Review status clarity	Development completion could be mistaken for independent sector validation or a completed technical review.	Annex L uses explicit evidence limits and Untested. M2 retains unresolved launch dependencies rather than marking them closed.

M2 Open technical and publication issues

Open item and priority	Required evidence or decision	Accountable role to appoint
O8 01 Technical evidence High	Complete AQMS requirements review, sector evidence and independent technical assessment under Annex C.	Technical review lead and sector reviewers
O8 02 Sector coverage High	Independent review across the activities in L4; actual evidence or explicitly identified gaps for each advertised scope.	Technical review authority
O8 03 Duration validation High	Observed task and time records under K4, analysis of shortfalls, retests and approved operational method under K8.	Duration method owner and independent reviewer
O8 04 Numerical rules High	Pilot evidence supporting audit frequency, response periods, authorization cycles, site coverage and public update timing; justified revisions where needed.	Scheme technical authority
O8 05 Oversight readiness High	Demonstrated competence and independence for body authorization, witnessing, appeals, record access and client continuity.	Scheme owner
O8 06 Record system readiness High	Successful I7 checks and reconciliation of decisions, issued certificates and public status; no unsupported Valid result.	Register owner and certification bodies
O8 07 Publication and transition High	Exact approved text, legal scheme-owner identity, publication authority, effective dates, transition and controlled distribution.	Governing approval authority

Open item and priority	Required evidence or decision	Accountable role to appoint
O8 08 Usability and burden Medium	User feedback on integrated evidence, small-organization role combinations, language clarity and duplicated record requests.	Pilot coordinator and drafting lead

Priority identifies review urgency and consequence. It is not an audit nonconformity classification. No owner has been appointed and no listed issue has been closed by this document; role names identify the responsibility that needs to be assigned.

M3 Comment handling and technical decisions

Each comment should receive a unique identifier, exact affected requirement, evidence basis, practical consequence and proposed wording or action. The review coordinator should retain the original comment even when it is combined with a related issue. A combined disposition should preserve the link to every originating comment.

The decision authority should record Accept, Accept with revision, Reject with reason or Defer with an explicit dependency. Accepted text should be checked for effects on related clauses, forms, cases and certification claims. A deferred issue affecting a publication gate should remain visibly open.

Closure should require the revised text or action, review evidence and any necessary retest. A response sent to the commenter is not itself technical closure. A person responsible for the change should not be the sole independent verifier where safety, impartiality or decision validity is affected.

M4 Review of the hypothetical case reasoning

The internal review compared the thirteen scenarios in J2 to J14 with the draft references stated in each case. The expected responses preserve the distinction between absent activities and retained outsourced responsibility, between implementation and effectiveness, and between an audit recommendation and a certification decision.

Cases J2 to J4 and J13 deliberately require further evidence before a final severity classification. J5 and J11 state the facts needed to support critical treatment. J6 and J7 apply different minor and major action rules. J8 and J9 preserve expiry and transfer history. J10, J12 and J14 address assignment restrictions, record consistency and insufficient competent time.

This comparison is an editorial reasoning check, not an independent agreement study or observed assessor assessment. The reviewer responses and reconciliation record in J15 remain to be produced during execution. No assessor pass result, agreement percentage or completed pilot outcome is reported.

M5 Hypothetical check of the revised public update rule

Illustrative facts: a suspension takes effect at 16:00 in the recorded reference time zone on day zero. The next day is a local holiday. Under revised I4, the public update is due no later than 16:00 on day one; the holiday does not stop the twenty-four-hour period. Urgent communication of a known critical restriction remains required without waiting for that outer limit.

Expected evidence: the independent suspension decision, effective timestamp, recorded time zone, update event, public result and any failure response. If the update fails, the body should preserve the error, use a

controlled alternative verification route where needed and correct the discrepancy. A favorable cached status cannot be treated as the authoritative current decision.

M6 Hypothetical check of body authorization expiry

Illustrative facts: a body's scheme authorization expires before renewal is decided. Several client certificates are still within their stated validity periods. Under revised G8, the body cannot make new grants, scope extensions or recertification decisions in the expired scope. It cannot backdate renewal to conceal the gap.

The scheme owner should activate G7, examine the basis and support arrangements for affected clients, maintain accurate public authorization information and control any transfer or continuing protective work. Expiry of the body's authorization does not by itself prove either conformity or nonconformity of every client. Each certificate's support and necessary action require evaluation.

Expected evidence: the authorization history, expiry event, work restrictions, affected-client population, continuity decisions, record access and notifications. These are expected records for a future exercise, not completed operational events.

M7 Handoff for independent review

The review package should consist of this exact draft revision, the completed applicability and sector review records when available, the source baseline, proposed numerical rules, open issue register and controlled pilot instructions. Reviewers should receive a clear account of what has and has not been verified.

The next evidence-producing activities are independent sector review, independent requirements review, real pilot execution and duration validation. Additional drafting may resolve identified gaps, but it should not substitute for those activities or change their status to complete. Publication remains subject to the gates in Annex E.

Annex N Field pilot execution and evidence records

Informative implementation instrument for the pilot protocol in Annex D. This annex supplies a sequence and record fields for obtaining real observations, comparing judgments and preparing a technical disposition. It does not change assessment requirements or approve a numerical pass threshold. At WD 0.9, no participants, assessors, completed observations or pilot results are recorded.

N1 Pilot sequence and controlled baseline

The pilot coordinator should first assign a pilot identifier and freeze the document revision, participant scope, applicable requirements, planned tasks and evaluation questions. The baseline should include the relevant records from Annexes A, H, J, K and L. An identifier should connect these records; existing forms may be used without copying the same evidence into every annex.

The sequence is preparation, readiness confirmation, observation, independent comparison, technical disposition and targeted retest. A stage should proceed only when its necessary inputs are available. A delay or incomplete stage should retain its actual status; scheduled work should not be recorded as performed.

A changed requirement or duration hypothesis should receive a new baseline identifier. Earlier observations should retain their original criteria. The technical reviewer should determine which results remain relevant and which need retesting before combining results across revisions.

N2 Pilot initiation record

Record field	Information to enter
Identity and purpose	[Pilot ID; coordinator; participant alias; activity; specific questions to test]
Frozen criteria	[AQMS revision and file checksum; applicable subclauses; duration method revision; case pack revision]
Operating boundary	[Sites; shifts; products or services; technologies; outsourced work; remote support; actual responsibilities]
Assigned people	[Lead assessor; second reviewer; technical specialists; independent disposition reviewer; competence and conflict records]
Evidence arrangements	[Access agreement; permitted observation; confidentiality restrictions; evidence custodian; retention and deletion arrangements]
Execution plan	[Dates; competent hours by task; relevant operational opportunities; participant contact; interruption and escalation route]
Readiness decision	[Proceed; revise plan; or defer; reasons; missing inputs; responsible person; dated decision]

N3 Participant selection and coverage gaps

The coordinator should maintain one participant register showing the actual activities covered, organizational scale, independent scope, sites, shifts and operating maturity. Selection should follow D2, including its proposed development targets. Several activities at one participant may contribute different evidence, but they should not be counted as several independent organizations.

The coverage register should distinguish planned participation, access agreed, observed live, assessed by simulation and not evaluated. Record withdrawals and unavailable evidence with their reasons. The completed series should retain this history so that difficult or unsuccessful participants cannot silently disappear from the reported results.

For each activity in D2 and each relevant challenge in L4, the coordinator should identify the observation that supports coverage or retain an explicit gap. Diversity of activities does not establish statistical representativeness. Conclusions should state the populations, operating conditions and technologies actually examined.

N4 Readiness and observation controls

Before observation, the lead assessor should verify access to the selected activity, competence for the planned tasks, the applicability register and the evidence needed to trace at least one relevant transaction. A new or dormant activity may support a preparedness exercise; it should not be reported as demonstrated routine operation. Missing inputs should lead to a revised plan or a recorded evidence gap.

The team should observe ordinary work and available abnormal conditions without creating hazards or disrupting product controls. A pilot exercise should not introduce defects into customer products, defeat protective controls or authorize release. Simulated records should be clearly marked and kept outside operational acceptance and public certificate systems.

If observation identifies a credible immediate safety or evidence-integrity concern, the lead assessor should notify the designated responsible manager promptly, preserve the relevant evidence and pause affected pilot work where necessary. The organization retains responsibility for its operational response. The pilot record should capture the response and any limit on further observation; it should not imply that the pilot team has issued or suspended a certificate.

N5 Observation record

Use one record per connected observation or evidence trail. Record facts before interpretation and link the exact requirement to each conclusion. Where one trail supports several requirements, identify the separate conclusions without duplicating the underlying record.

Record field	Information to enter
Observation identity	[Pilot ID; observation ID; observer; date and time; site and shift; activity or transaction]
Requirement and purpose	[Exact subclause; applicable responsibility; question being tested; related Annex A entry]
Evidence basis	[Live observation; historical operational record; interview corroborated by identified evidence; or simulation]
Facts and references	[Observed condition; relevant sample and selection reason; traceable source IDs; version; access restrictions]
Assessment outcome	[Conforming evidence; Nonconformity; Not applicable verified; or Not evaluated under D6; supporting reason]
Drafting implication	[No wording issue identified; ambiguity; missing control; contradictory control; or burden concern; link to L6 and M3]

Record field	Information to enter
Time and follow-up	[Linked K4 task record; incomplete work; additional evidence needed; responsible person; intended review date]

N6 Evidence limits and record custody

An interview may explain a process but should not, by itself, prove that a required control operates effectively. A sample should identify the available population, selection method and important limits, including unavailable shifts or records. Do not generalize a single successful transaction to unobserved products or operating conditions.

Use aliases in consolidated analysis and retain identifiable evidence only where necessary and authorized. A restricted record may be represented by a controlled reference and a sufficiently detailed observation, provided an authorized reviewer can verify the conclusion. If verification is prevented, record the limitation rather than replacing evidence with assurance language.

The custodian should protect original observations and reviewer responses against silent amendment. Corrections should retain the previous entry, author, date and reason. Retention, access and eventual disposal should follow the agreed pilot arrangements and applicable obligations.

N7 Independent judgment comparison

The coordinator should give the two reviewers the same frozen evidence package and questions, using D7 and J15. Each reviewer should record an initial conclusion before discussion or access to the other response. The comparison should identify differences in applicability, selected requirement, evidence sufficiency, classification, required action and decision consequences separately.

Preserve initial responses after reconciliation. The comparison record should explain whether a difference arose from wording, incomplete or unequal evidence, technical competence, overlooked facts or a permitted judgment range. A reconciled answer should identify its evidential basis; agreement reached through discussion should not be reported as initial independent agreement.

N8 Comparison and reconciliation record

Record field	Information to enter
Common package	[Pilot and case IDs; exact evidence version; questions; access conditions; response cut-off]
Independent responses	[Reviewer IDs; separately dated initial decisions; reasoning; evidence limitations]
Difference	[Decision dimension; exact disagreement; possible effect on safety, applicability, finding or certification conclusion]
Resolution basis	[Relevant requirement and facts; additional evidence where needed; unresolved issue; independent technical disposition]
Required follow-up	[Competence action; wording proposal; additional observation; or no change with reason; linked issue ID]

Record field	Information to enter
Retest	[Revised baseline; new or retained case and justification; independent responses; result; remaining limitation]

N9 Evaluation measures and interpretation

The coordinator should report counts and denominators alongside every percentage. Planned but unobserved tasks, verified non-applicable requirements and simulations should be visible separately. A percentage describes the specified dataset; it is not a conformity score or an approval threshold.

Requirement coverage may be calculated as applicable requirement units with an evidence-based assessment outcome divided by the applicable requirement units planned for evaluation. Conforming evidence and supported nonconformities both count as evaluated; Not evaluated does not. Verified non-applicable units are reported separately and excluded from that denominator. Freeze the counting unit before execution so that splitting clauses does not inflate the result.

Initial agreement should be calculated separately for each judgment dimension as matching independent response pairs divided by all pairs with two usable initial responses for that dimension. Report missing or unusable pairs separately. Two identical Not evaluated responses may represent agreement about insufficiency, but should not count as successful conformity evaluation.

Compare planned and actual competent hours by task using K4, and report remaining work and coverage achieved. A time ratio below one does not demonstrate efficiency when required work is incomplete. Track participant preparation and duplicate evidence requests separately from auditor productive hours.

For each consequential disagreement, record whether it remains unresolved, was resolved by evidence, required a wording change or required a competence action. No average coverage or agreement result should override an unresolved issue that could permit unsafe release or an unsupported conformity decision. This annex introduces no universal percentage for pilot success.

N10 Pilot result and technical disposition

Each completed pilot report should state what the observed evidence supports, what remains untested and what additional work is needed. Use the report structure below to bring together existing records. An organization's implementation failure should not automatically be attributed to a defect in the standard; conversely, repeatable ambiguity between competent reviewers should not be dismissed as a participant failure without investigation.

Report element	Required content for review
Baseline and coverage	[Pilot ID; revision; actual activities, locations and dates; selection basis; deviations from plan; live and simulated coverage]
Observed results	[Linked N5 evidence trails; applicable units planned and evaluated; outcomes; missing evidence and limitations]
Assessment consistency	[N8 comparisons; initial agreement by dimension with denominators; consequential disagreements and their disposition]

Report element	Required content for review
Time and burden	[K4 records; planned and actual competent hours; incomplete tasks; participant preparation; duplicate requests and causes]
Change proposals	[Exact affected text; evidence and practical consequence; linked L6 or M3 issue; proposed wording or implementation action]
Retest evidence	[Changed baseline; tasks repeated; independent review; results; unresolved matters and linked M2 items]
Conclusion and review	[Supported conclusions and limits; recommendation for more work or technical disposition; reviewer identity and dated decision]

N11 Retest and series review

A retest should target the reason for the change and its effects on related requirements. Where a reviewer has already seen the expected answer, the coordinator should use a new equivalent case where practicable or disclose the learning effect. A repeated answer to the same coached case does not demonstrate independent generalization.

The series review should combine pilot evidence without concealing variation between sectors, small and large organizations, live and simulated activities, or draft revisions. It should identify which proposed duration assumptions and numerical rules have relevant observations and which remain untested. Short pilots cannot establish multi-year effectiveness of certification or authorization cycles; those claims need appropriate historical evidence, justified provisional controls and subsequent monitoring.

The independent technical reviewer should evaluate the series against D9, K and the gates in E2. A completed report is a submission for disposition, not approval to launch. Limitations affecting the advertised scope should lead to further evidence or an explicit scope revision before the corresponding claim is made.

N12 Status at this development stage

WD 0.9 adds the field execution instruments in this annex. The registers and report fields are uncompleted templates. Their preparation does not close the open technical items in M2, validate the candidate days in D4 or authorize any certification decision.

The next operational step is to appoint the pilot roles, secure participants and evidence access, and complete N2 for each intended pilot. Independent requirements review remains a separate open workstream under Annex C and E2. Actual results should be entered only after the corresponding work has occurred.

Annex O Organizational implementation and readiness guide

Informative guidance for an organization implementing the applicable AQMS requirements. This annex connects scope selection, existing controls, improvement actions and operational evidence. It supplements Clauses 1 to 13 without prescribing a separate management system, fixed implementation period or additional conformity criteria. Certification roles remain governed by Clause 14 and the relevant normative annexes. Use of this guide during draft development does not establish certification eligibility.

O1 Establish the implementation boundary

Top management should name an implementation coordinator and confirm the legal entity, locations, activities and responsibilities to be addressed. The coordinator should establish the chosen AQMS revision and prepare or update the applicability register under Clause 1 and Annex A. Existing customer, market and contractual obligations should remain in force throughout implementation.

The team should follow how work actually moves from an accepted commitment through development where applicable, purchasing, execution, acceptance and feedback. It should include support functions and external interfaces that affect those outcomes. The sector profiles in Annex B provide starting points; each omission still needs a decision at the relevant requirement level.

Implementation may be organized by process or location. Phasing should identify the boundary of each phase and its dependencies. It should not be used to present an unimplemented applicable requirement as Not applicable or to imply that a whole organization has completed implementation when only a pilot area has been examined.

O2 Reuse effective existing controls

For each applicable requirement, identify the process that fulfils it, the accountable owner and evidence of actual operation. Existing instructions, engineering records, software systems and integrated management arrangements may provide this evidence. Their titles and numbering need not match AQMS clause numbers.

An existing certificate or a familiar procedure title should not replace review of the underlying control. Examine the required action, responsibility, conditions and evidence, including differences in scope. Keep an effective control where it fulfils the requirement; change only what is missing, unreliable or inconsistent with the intended outcome.

A shared document may support several clauses. The organization should preserve a clear link from each requirement to the relevant part of that document and the associated operating records. Avoid copying identical information into separate quality manuals, forms and departmental spreadsheets solely to reproduce the structure of the standard.

O3 Process implementation record

The following fields may be integrated into an existing process description. They connect process ownership under 3.6 with implementation evidence; they do not require a new form for every clause.

Field	Information to record
Process and boundary	[Process name; owner; locations; start and end points; activities and outputs]
Requirements and inputs	[Applicable AQMS references; customer and market obligations; accepted inputs and their sources]

Field	Information to record
Controls and resources	[Methods; equipment; competence; permissions; current instructions; supplier controls]
Interfaces and decisions	[Sending and receiving roles; acceptance conditions; release authority; escalation and change route]
Evidence and performance	[Operating record references; measures and definitions; review frequency and responsible person]
Abnormal operation	[Stop or restriction criteria; containment; continuity arrangements; restart verification]

O4 Assess gaps using evidence

The coordinator should distinguish a requirement that is not understood, a control that has not been established, a control that exists but is not used, and a control whose effectiveness is unverified. These conditions need different actions. Unavailable evidence should remain visible until a competent person resolves the uncertainty.

For implementation tracking, use Not started, In progress, Implemented awaiting verification, and Verified against the stated criteria. These labels describe action progress only. They do not replace the applicability decisions in Annex A, the assessment outcomes in D6 or the finding classifications in Clause 13.

Where an assessment establishes a nonconformity, retain its classification, required response and closure rules in the relevant finding record. An implementation plan should not reset those deadlines or convert an overdue finding into an ordinary improvement action.

O5 Gap and action record

Field	Information to record
Gap identity	[Action ID; exact requirement; process; affected sites, outputs or responsibilities]
Current evidence	[Existing control and record references; observed weakness; uncertainty; finding ID if applicable]
Risk and immediate response	[Potential consequence; urgency; containment or restriction needed; escalation owner]
Action and dependencies	[Specific change; accountable owner; resources; required prior actions; planned completion date]
Verification basis	[Expected operating evidence; acceptance criteria; competent verifier; observation opportunity]
Progress and closure	[Status under O4; actual completion date; verification result and evidence; remaining work; management decision]

O6 Prioritize and resource the work

Top management should address gaps that threaten safety, mandatory obligations, release validity or evidence integrity before treating lower-consequence improvements as the principal implementation objective. If several actions depend on a common prerequisite, the plan should show that dependency and provide interim controls for exposed work.

Priorities should reflect consequences and operational exposure as well as effort. The number of closed actions alone does not show readiness: several completed administrative tasks cannot compensate for an unresolved release-control failure. The coordinator should report delayed actions, the reason, current exposure and the decision required from management.

Target dates should follow the complexity of the change and the next valid operating opportunity, while respecting applicable deadlines. This guide sets no universal thirty-, sixty- or ninety-day implementation programme. Any revised target should preserve the original date, reason, approval and effect on dependent work.

O7 Assign competence and preserve independence

Process owners should determine who needs new knowledge, practical skills or decision authority because of the planned changes. Training attendance should be followed by an appropriate assessment under Clause 5, such as observed execution, a relevant work sample or demonstrated handling of an abnormal condition. Authorization should match the tasks actually demonstrated.

Small organizations may combine coordination and operational roles where the underlying requirements permit it. They should still arrange competent independent assessment where required, including internal audit independence under 13.5. An external resource may support this function when its competence, scope and conflicts are controlled.

If the only available verifier developed the control being examined, management should evaluate whether the assigned review requires independence and arrange another competent person where it does. A role combination should be justified against the relevant requirement rather than accepted solely because the organization is small.

O8 Put changed controls into operation

Before a changed control becomes effective, the owner should confirm the approved version, trained and authorized personnel, necessary resources and readiness of connected processes. A change affecting a supplier, customer interface or shared support function should include the receiving party and any required approval.

The introduction plan should identify the effective point by date, batch, configuration or other suitable boundary. Superseded instructions should cease to be available for unintended use, while historical records retain the version under which work occurred. Where old and new configurations coexist, their acceptance criteria and traceability should remain distinguishable.

Observe initial use and any representative abnormal condition that can be evaluated safely. If the change does not achieve the intended result, contain affected outputs, identify the cause and decide whether to correct, restrict or reverse the change. Reversal should be controlled and should not restore an unsafe or otherwise unacceptable condition.

O9 Verify implementation and effectiveness

The verifier should compare actual operation with the predefined criteria in O5. Approval of a procedure demonstrates that a document was authorized; it does not demonstrate that people use it correctly or that the process achieves its intended outcome. Verification should consider relevant shifts, locations, variants and outsourced interfaces.

Where operation is infrequent, identify the next suitable observation opportunity and any alternative evidence that can support a limited conclusion. Simulations may demonstrate preparedness, but their limits should be recorded. An item awaiting sufficient evidence should remain open for effectiveness review rather than receive an unsupported closure.

Internal audits should follow Clause 13 and management review should follow 12.8 to 12.10. Together they should establish whether the implementation has produced a functioning system, which weaknesses remain and what resources or decisions are needed. They should also examine whether corrective actions have reached similar processes where the same cause may exist.

O10 Management readiness review

Management should use the following questions to review the defined implementation scope. A Yes response should reference evidence. No or Not yet demonstrated responses should identify the remaining action and its consequence; the table is not a percentage-based certification score.

Review question	Evidence to reference
Is the scope accurate and applicability justified?	[Approved scope; Annex A decisions; actual activity and responsibility checks]
Are process owners and interfaces effective?	[Assignments; sampled handovers; acceptance and escalation evidence]
Are relevant people and resources ready?	[Competence assessments; authorizations; equipment and information readiness]
Do controls operate through delivery and feedback?	[Representative work trails; release evidence; supplier and field-response records]
Have gaps and adverse findings been addressed?	[O5 actions; finding records; containment; verification and unresolved risks]
Have independent audit and management review informed the decision?	[Audit coverage and results; management decisions; follow-up responsibilities]

O11 Readiness decision and subsequent change

The management record should identify the scope and revision reviewed, evidence considered, unresolved matters, operational restrictions where needed and the responsible decision maker. The conclusion may authorize the next internal implementation phase, require further work or request an external assessment when an approved scheme permits it. It should not be labelled a certification decision.

After implementation, material changes in scope, technology, suppliers, customer obligations or the standard baseline should trigger an impact review. Identify affected applicability decisions, process controls, competence, records and assessment plans. Preserve the relationship between the old and new baselines and verify the changed arrangements.

Formal publication, external recognition and certification launch remain subject to Clause 14 and Annex E. Organizational readiness under this guide does not close the scheme development issues in M2.

O12 Illustrative use in a mixed service organization

Hypothetical example: a vehicle service business performs repairs and also develops diagnostic software. It begins with one activity map linking service intake, diagnosis, software development, purchased parts, repair execution and return to use. The applicability review considers both service and software responsibilities, rather than selecting requirements solely from the business label.

The gap review identifies that technicians cannot reliably determine which approved software version was used for a completed job. The organization links an action to the applicable configuration, traceability and service-record requirements. It assigns an owner, controls the affected work, changes the job record and verifies that the version is captured and recoverable during actual use.

The same controlled job record may support several requirements when each connection is clear. A hypothetical entry or a completed training session would not establish that the revised control works. The organization would need operating evidence and any necessary corrective-action effectiveness review before closing the action. This example illustrates the method and records no completed implementation.

Annex P Standard maintenance and transition control

Proposed normative requirements for the scheme owner and the other roles expressly identified below. This annex implements the maintenance responsibilities in 14.2. It governs the handling of changes to AQMS and its binding scheme rules; it does not establish an effective date or authorize publication of this working draft. Initial launch remains subject to Clause 14 and Annex E.

P1 Maintenance responsibility and input

The scheme owner shall appoint a maintenance coordinator and identify the technical review and approval authorities. The coordinator shall maintain a register of interpretation requests, proposed changes, reported errors and emerging implementation concerns. An item shall identify its origin, affected requirement and revision, practical consequence, supporting evidence and current disposition.

Input shall be accessible to affected organizations, assessment personnel and other relevant stakeholders. Federation membership or a commercial relationship shall not be a prerequisite for submitting a technical concern. The coordinator shall protect confidential evidence while providing sufficient information for competent review.

The scheme owner shall review maintenance needs at least annually and following a significant safety concern, recurring assessment inconsistency or material external-source change. This annual interval is an original AQMS proposal requiring validation. Review shall consider pilot and oversight evidence, appeals, operational performance, technology changes and the burden of implementation. A review need not result in a revision when the evidence supports retaining the existing text.

P2 Classification of proposed changes

The technical reviewer shall classify each proposal by its effect on obligations and decisions, rather than by its length or requested title. An editorial correction shall correct presentation without changing the required action, applicability, acceptance basis or decision consequence. An interpretation shall explain an existing requirement without adding or removing an obligation. A substantive amendment shall change a requirement, scope condition, assessment criterion or binding decision rule.

Where a proposed interpretation would make previously acceptable conduct unacceptable, introduce new required evidence or change a certification consequence, it shall be processed as a substantive amendment. A frequently asked question, training slide, private response or website explanation shall not introduce a binding requirement outside the controlled change process.

The reviewer shall record the classification and its reasoning. Uncertainty about the effect shall be resolved through impact review before approval. Related proposals may be combined, provided their individual origins and dispositions remain traceable.

P3 Technical and operational impact review

Before approval, the technical review authority shall evaluate affected clauses, annexes, definitions, forms, case material and operational systems. The review shall identify changes needed in organizational controls, personnel competence, assessment time, body authorization, public status information and existing agreements.

The review shall distinguish a change in an external source from a change adopted into AQMS. A revised external standard shall not silently amend AQMS. Applicable customer and mandatory obligations shall continue to be managed under 1.7, independently of the AQMS revision schedule.

For a substantive proposal, the scheme owner shall obtain input from affected activity groups and competent assessors. The review plan shall specify consultation scope, response period and the evidence needed to test the proposal. The duration and extent shall be justified by the consequence and complexity of the change. An unresolved consequential concern shall retain its disposition and any restriction on approval.

Material changes to assessment judgments or duration rules shall receive targeted validation using the relevant controls in Annexes D, J, K, L and N. Reuse of previous evidence shall have a recorded relevance assessment. Drafting completion or consensus alone shall not substitute for evidence of operational feasibility.

P4 Approval and authoritative publication

The approving authority shall consider the exact proposed text, technical review, consultation dispositions, validation evidence and transition plan. Persons with an unresolved material conflict shall not control the approval decision. The approval record shall identify the decision, authority, date, conditions and document version or checksum.

The scheme owner shall publish an authoritative version with its identifier, approval date, effective date, change description and relationship to superseded material. Publication and effectiveness shall be distinguished. A consolidated text shall identify amendments incorporated into it so that users can establish the applicable criteria for a given date.

Approved interpretations shall identify the affected requirement and the limits of the explanation. They shall be available on equal terms to affected parties. A private technical answer shall not become an undisclosed assessment criterion. Superseded material shall remain retrievable for historical decision review and shall be marked to prevent unintended current use.

P5 Change decision record

Required field	Information to retain
Identity and basis	Change ID; origin; affected AQMS version and provisions; evidence and reason
Classification	Editorial correction, interpretation or substantive amendment; effect and justification
Impact and review	Affected activities and roles; competence, duration and system changes; reviewers and conflicts
Consultation and validation	Comments and dispositions; examined evidence; test results; unresolved concerns and limitations
Approved text	Exact replacement or explanatory text; linked provisions; approval authority and decision date
Release and transition	Publication identifier; effective date; transition notice; superseded material; monitoring responsibility

P6 Transition planning

For each substantive amendment, the scheme owner shall approve a transition plan before it takes effect. The plan shall identify affected organizations, certification bodies and assessment roles; the old and new criteria; implementation evidence; and the dates governing assessment and certification decisions.

The plan shall address applications already accepted, audits planned or in progress, completed audits awaiting decision, valid certificates, recertification, transfers and open findings. It shall state when earlier criteria may still be used and when transition verification is required. It shall also define the status consequence if transition is not completed by the applicable limit and the authorized decision process for that consequence.

A transition arrangement shall not automatically extend certificate expiry, body authorization or an existing finding deadline. Where an approved change affects an open finding, the certification body shall retain the original requirement and evidence, review whether the finding remains valid and document any revised action or deadline with its authorized basis. Historical records shall not be rewritten to conceal the earlier decision.

The scheme owner shall justify the transition period against implementation effort, competence development, assessment capacity and the risk of continued use of the earlier criteria. A body shall not grant a private extension inconsistent with the published plan. Changes to the plan shall follow controlled approval and communication.

P7 Implementation by affected parties

The certification body shall identify affected clients, personnel, assessment plans and decision procedures. It shall communicate the approved change and applicable transition conditions, evaluate required competence, and retain evidence that assigned personnel can apply the revised criteria.

An affected applicant or certified organization shall evaluate the change against its scope, update relevant controls and applicability decisions, and provide the required implementation evidence within the approved transition arrangements. Existing integrated records may be used. The organization shall not claim that receiving the change notice establishes implementation.

The certification body shall verify transition to the extent prescribed by the approved plan and make the required independent decision. It shall record the criteria actually used for each assessment and decision and update certificate and public status information under Annex I where necessary. A scheduling entry or attendance at training shall not by itself demonstrate completed transition.

P8 Transition verification record

Required field	Information to retain
Affected scope	Organization or body; sites and activities; existing certificate or authorization where relevant
Applicable change	Approved change ID; old and new criteria; relevant dates and published transition conditions
Implementation	Affected controls and personnel; actions completed; outstanding work and operating restrictions
Verification	Competent evaluator; method; evidence sampled; actual criteria; findings and limits
Decision and status	Decision authority and date; outcome; validity or scope consequences; public update reference

Required field	Information to retain
Follow-up	Open actions and deadlines; responsible roles; closure evidence; link to retained history

P9 Urgent protective changes

Where credible evidence identifies an immediate serious threat to safety or decision integrity, the scheme owner shall assess the need for an urgent controlled measure. The decision shall identify the evidence, affected scope, responsible parties, action, effective time and communication route. It shall distinguish enforcement of an existing obligation from introduction of a new temporary requirement.

An urgent new requirement shall remain a substantive change. The approval authority shall document why the normal consultation sequence cannot be completed before protective action, obtain competent review and define a review deadline and expiry or replacement condition. The measure shall be limited to the justified scope and shall not remain indefinite through repeated unexplained extensions.

The scheme owner shall review comments and operating evidence after issue and decide whether to confirm, revise or withdraw the measure through the controlled process. Withdrawal of the measure shall not erase decisions or operational events that occurred while it applied. Known failures under previously applicable requirements shall continue to receive the necessary response.

P10 Language consistency and maintenance effectiveness

The scheme owner shall identify the authoritative language version and control authorized translations through competent technical review. Differences affecting meaning shall be registered, assessed for their effect on prior and current decisions, and corrected with appropriate notification. An affected body shall resolve uncertainty about assessment criteria before issuing a conclusion that depends on the disputed wording.

The maintenance coordinator shall monitor receipt of binding changes, completion of required transition work, recurring interpretation disputes and unintended consequences. The review shall identify whether the published instructions were understood and consistently applied, and whether corrective changes are needed.

The scheme owner shall retain change and transition records sufficient to reconstruct which requirements applied to an assessment or decision. Completion of these records shall not imply external endorsement or equivalence. At WD 0.11, this annex contains proposed controls; no operational amendment, transition deadline or urgent measure has been approved by this document.

Development notes

Informative editorial record. This section is maintained during drafting and is not part of the proposed conformity requirements.

Continuation sequence

Stage	Content to be added to this same document
1 completed for review	Clauses 1 to 5 and Annex A. Common requirements, definitions and applicability controls.
2 completed for review	Clauses 6 to 8. Development stages, technical reviews, product and process approval, supplier controls, production and special processes.
3 completed for review	Clauses 9 to 11. Product and technology categories, services, aftersales, test, calibration, measurement and acceptance.
4 completed for review	Clauses 12 to 14. Performance, internal and external audits, auditor and expert competence, certification decisions, surveillance and appeals.
5 drafted for review	Internal consistency corrections; sector guide; technical evidence review; pilot protocol and publication gates. Actual pilots and technical review remain open.
6 drafted for review	Annexes F to I: qualification, body authorization and oversight, audit and decision records, certificate information controls.
7 drafted for review	Annex J hypothetical cases and expected reasoning; Annex K duration validation method and records. No actual pilot validation completed.
8 drafted for review	Annexes L and M: review map, sector questions, editorial findings and open issues; revised I4 and G8.
9 drafted for review	Annex N: field pilot planning, observation, independent comparison, measurement and result records. Execution remains pending.
10 drafted for review	Annex O: organizational implementation, process and gap records, competence, verification and readiness review.
11 drafted for review	Annex P: change classification, approval, publication, transition and urgent protective measures; linked to 14.2.
Validation pending	Independent sector review, technical evidence review, real pilot evidence and final technical dispositions before publication approval.

Subjects reserved for technical review

The completed draft requires review of technical thresholds, role independence, audit duration methods, nonconformity classification, closure periods and certification eligibility. The proposed intervals and deadlines in Clauses 12 to 14 are original AQMS design choices requiring representative pilot validation before publication.

Coverage review will include vehicle and component production, materials, special processes, services, equipment, software, AI, batteries, charging, laboratories, logistics and aftersales. Reviewers will test whether the applicability method allows justified exclusions without removing essential responsibilities.

Annex C defines the technical evidence and review records supporting this independent AQMS draft. Reviewers should evaluate completeness, applicability, clarity and operational effectiveness against the intended automotive scope. Open technical gaps and pilot limitations remain subject to resolution before publication approval.

Proposed rule rationale and launch gates

Annual review and audit coverage are proposed to prevent prolonged blind spots. Three-year authorization and certification periods combine periodic full reassessment with annual monitoring. The two-year consultancy restriction provides a minimum separation period while requiring evaluation of continuing conflicts. The twenty-four-hour, fifteen-day, thirty-day, sixty-day, ninety-day and one-hundred-eighty-day response limits distinguish immediate protection, planning, implementation and status control; they do not override shorter mandatory duties.

Pilot review must test these limits in small service providers, laboratories, software organizations and complex manufacturing groups. Review must also test the feasibility of annual operational-site assessment and the independence arrangements for small bodies. The scheme owner must approve the operational duration method under 14.7, validate the body authorization and oversight arrangements drafted in Annex G, and establish transition rules and publication authority before launch. Annex D proposes numerical starting points and Annex K defines their validation route. No operational audit-day table is approved.

Review comment record

Reviewers should identify the clause, the issue, the practical consequence, the proposed wording and the supporting reason. Each accepted change should be traceable to a disposition. Open comments affecting safety, scope or certification conclusions should be resolved before approval.

Comment	Clause	Issue and proposed change	Disposition
[ID]	[Clause]	[Issue, evidence and replacement wording]	[Accepted, revised, rejected or open; reason]