

Corporate recognition assessment checklist

100 corporate controls | 10 software/service profiles | 8 technology domains | 8 internal directives

Use the exact Standard edition and approved applicability map. Record objective evidence, limitations and findings. This checklist does not itself grant recognition or certify an additional IAF text.

LEGAL ENTITY / HUBS / FAMILY SCOPE / CASE ID

ASSESSMENT TYPE, PROFILES/DOMAINS AND SCOPE SCHEDULE VERSION

AUDITORS, TECHNICAL COMPETENCE, CONFLICTS AND DATES

IAF CONSTITUTION, SDR EDITION AND ADDITIONAL CLAIMED IAF TEXT MAPS

ORIGINAL EVIDENCE, CASE POPULATIONS, HUB COVERAGE AND FAMILY DEMONSTRATIONS

SEPARATE IAF OPERATOR ASSURANCE AND APPROVED APPLICABILITY RECORD

Decision rules, scope and evidence

Results

Met = supported fulfilment. Minor = isolated lapse. Major = systemic/consequential failure. Critical = serious harm or severe integrity loss. Pending = unresolved evidence. NA = inherent non-applicability accepted with reasons; missing resources or evidence is not NA.

Initial recognition

Six months of implemented controls, completed internal audit/review and three real release/change events per family/responsible hub. All applicable requirements must be Met and findings effectively closed. No duplicate targets, invented trivial events, conditional initial grant or compensating score.

Active recognition

An isolated Minor may remain open at most 90 calendar days only with protected safety, validity and integrity. Major: immediate containment, 30-day closure target and suspension review if unresolved. Critical: immediate protective-suspension review.

Hub and family coverage

Every hub assessed; physical technical facilities visited annually. Remote-only offices require independent adequacy approval. Demonstrate all families initially/at renewal; annually all consequential, changed/adverse families plus ceil square root of remaining families, rotating within three years. Three events per family/hub; expand for risk.

Independent decision

Three uninvolved competent panel members participate; at least two affirmative reasoned votes are required and all initial gates remain mandatory. Recognition term is at most three years, with surveillance by months 12 and 24; no automatic extension.

Fair response and urgent duty

Allow 15 calendar days for factual response and 30 days for an appeal after decision notice. Serious incidents require IAF notice within 48 hours of awareness. Protect safety and evidence immediately; response or appeal does not suspend necessary protection.

Requirement map and applicability record

ENTITY / SCOPE / CASE REFERENCE

--

Corporate baseline SDR-01 to SDR-25 | 100 requirements

Software/service profiles DEV to DAT | 40 requirements

Technology domains T01 to T08 | 32 requirements

Internal directives IR01 to IR08 | 32 requirements

The organization demonstrates its duties; IAF operator duties require independent programme-assurance evidence. Additional IAF claims need complete separate clause maps and any required separate programme decision.

SELECTED PROFILES/DOMAINS, ACTUAL RESPONSIBILITIES AND EXCLUDED SCOPE

--

ACCEPTED NA BY REQUIREMENT, EXACT REASON, EVIDENCE AND REVIEWER

--

IAF OPERATOR ASSURANCE AND ADDITIONAL IAF TEXT EVALUATION REFERENCES

--

Requirement assessment | SDR-01.01 to SDR-01.03

ENTITY / SCOPE / CASE REFERENCE

SDR-01.01 | ESSENTIAL GATE

Standard p. 7

Accountable holder

Identify the legal entity or legally operating sole enterprise responsible for software, digital services, contracts and recognition claims. Record ownership, jurisdiction and authority to bind the holder. A project name, repository, marketplace listing or informal contributor group alone shall not establish accountable corporate responsibility.

Evidence: Legal identity, ownership and authorised undertaking.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-01.02 | ESSENTIAL GATE

Standard p. 8

Bounded activities

Define software/service families, lifecycle roles, delivering hubs, deployment modes, intended users, supported configurations and exclusions. Separate developer, integrator, distributor, operator and customer responsibilities. Recognition shall not automatically cover affiliates, every product version or customer deployments outside the approved boundary.

Evidence: Controlled entity, hub, family and responsibility schedule.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-01.03

Standard p. 8

Permissions and obligations

Determine actual market, software, data, professional and contractual obligations for each activity and territory. Verify required permissions and third-party rights. IAF recognition shall not be presented as vehicle homologation, statutory software approval, permission to access a vehicle or a waiver of applicable duties.

Evidence: Obligation and permission register with current evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-01.04 to SDR-02.02

ENTITY / SCOPE / CASE REFERENCE

SDR-01.04

Standard p. 8

Corporate versus product assurance

Apply Corporate Recognition to demonstrated organisational controls for stated activities. Identify product families as scope descriptors, not individually certified products. A customer shall be able to distinguish current corporate status from a release's technical evidence, known limitations, support state and separate acceptance decision.

Evidence: Public wording and corporate/release boundary.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-02.01

Standard p. 8

Executive responsibility

Assign an executive or proprietor accountable for quality, security, safety interfaces, ethical conduct, resources and truthful claims. Establish escalation, deputies and management review. Commercial pressure shall not override an unresolved release blocker, evidence-integrity concern or necessary customer protection.

Evidence: Mandate, decisions and resourcing evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-02.02 | ESSENTIAL GATE

Standard p. 8

Technical stop authority

Give competent technical and security owners authority to stop an unsafe or unsupported release, isolate compromised pipelines and require further validation. Define who may lift a hold and the evidence required. Sales approval or deadline pressure shall not substitute for technical acceptance.

Evidence: Authority matrix, actual holds and reasoned clearance.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-02.03 to SDR-03.01

ENTITY / SCOPE / CASE REFERENCE

SDR-02.03

Standard p. 8

Distributed control

Identify development hubs, remote teams, contractors, acquired products and operating partners. Establish enforceable duties for source access, competence, confidentiality, release controls, incident notice and support continuity. Branding or a shared platform shall not imply control over independent suppliers or unrelated work.

Evidence: Control agreements and distributed responsibility map.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-02.04

Standard p. 8

Independence of challenge

Separate consequential change creation from competent verification and release challenge. Small organisations may use external competent reviewers under controlled access. Review fees may be outcome-independent; self-approval, reciprocal rubber stamping or undisclosed material interests shall not establish effective independent challenge.

Evidence: Reviewer assignment, competence and actual challenge.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-03.01

Standard p. 9

Controlled adoption

Adopt this Standard by an authorised decision, identifying edition, scope, owners and effective implementation. Maintain a requirement-level map of actual practice and original evidence. A published policy or statement of intent shall not be treated as demonstrated operation.

Evidence: Adoption decision and complete evidence map.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-03.02 to SDR-03.04

ENTITY / SCOPE / CASE REFERENCE

SDR-03.02

Standard p. 9

Additional IAF claims

List each additional IAF quality text claimed as implemented, with exact title, edition, approval status and clause-level evaluation. Resolve conflicts and incomplete drafts transparently. This programme shall not automatically confer another IAF approval or validate an unassessed additional claim.

Evidence: Additional-text register and separate evaluations.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-03.03 | ESSENTIAL GATE

Standard p. 9

Operating history and events

For initial or new family/hub scope demonstrate at least six months of implemented controls, completed internal audit and management review, and three actual completed release/change events per family/responsible hub. Events shall show real delivery or service operation; demonstrations and invented minor changes shall not meet the gate.

Evidence: Dated history, actual event population and completed reviews.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-03.04

Standard p. 9

Applicability and gaps

Evaluate all common controls, selected profiles and triggered domains. NA requires an absent inherent trigger with reasoned review; outsourcing, low volume, confidentiality or missing evidence is not itself NA. Record unresolved conclusions and unsupported future scope honestly rather than converting them to a pass.

Evidence: Applicability, gaps and approved exclusions.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-04.01 to SDR-04.03

ENTITY / SCOPE / CASE REFERENCE

SDR-04.01

Standard p. 9

Role-specific competence

Define competence for architecture, development, test, security, safety interfaces, data, AI, operations and release authority. Verify relevant experience through work samples and practical challenge. Qualifications and tool access alone shall not authorise consequential technical decisions outside demonstrated capability.

Evidence: Role matrix, verified work and challenge results.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-04.02

Standard p. 9

Supervision and continuity

Control trainee and contributor tasks, independent authority and supervision. Maintain deputies for critical roles and review capacity, fatigue and on-call workload. Departure of a key engineer or supplier shall trigger capability and access review rather than leaving obsolete authority active.

Evidence: Authorisation, supervision and continuity records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-04.03

Standard p. 9

Learning effectiveness

Plan development from actual defects, new threats, technology changes and competence gaps. Verify learning in work or technical challenge, not attendance alone. Reassess after prolonged inactivity or serious error and restrict unsupported roles until competence is demonstrated.

Evidence: Development plan and effectiveness checks.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-04.04 to SDR-05.02

ENTITY / SCOPE / CASE REFERENCE

SDR-04.04 | ESSENTIAL GATE

Standard p. 10

Integrity and protected challenge

Prohibit fabricated test results, hidden defects, misleading benchmarks, unauthorised source use and retaliatory treatment of good-faith reporters. Protect technical dissent and distinguish an honest error from deliberate falsification. Maintain accessible confidential escalation and impartial investigation.

Evidence: Ethics rules, reports and fair investigation evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-05.01

Standard p. 10

Clear intended use

Agree deliverables, deployment context, interfaces, performance claims, responsibilities, acceptance criteria and exclusions before commitment. Separate prototype, evaluation and production use. A demonstration or marketing benchmark shall not imply fitness for an unvalidated vehicle, fleet, environment or safety function.

Evidence: Contract, intended-use and acceptance baseline.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-05.02

Standard p. 10

Commercial transparency

State licensing, subscriptions, material dependencies, service limits, data ownership, export/exit provisions and support commitments intelligibly. Obtain authority for material changes and avoid hidden disabling of purchased safety-relevant functions. Recognition shall not imply IAF guarantees solvency or every transaction.

Evidence: Customer terms, change consent and remedy controls.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-05.03 to SDR-06.01

ENTITY / SCOPE / CASE REFERENCE

SDR-05.03

Standard p. 10

Rights and provenance

Verify rights to source code, datasets, models, documentation and incorporated components, including redistribution and support obligations. Record provenance and unresolved restrictions. Public availability does not itself permit unrestricted commercial use, training use or disclosure of confidential content.

Evidence: Rights inventory and verified contribution terms.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-05.04

Standard p. 10

Complaints and remedy

Provide accessible support and complaints channels, triage consequential failures and preserve user evidence. Explain responsibilities and actual remedy limits without using recognition to dismiss a complaint. Verify correction or agreed disposition and examine systemic effects across customers and versions.

Evidence: Complaint, support and verified-remedy records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-06.01 | ESSENTIAL GATE

Standard p. 10

Consequence classification

Classify each family and material change by credible safety, security, privacy, financial and operational consequences, including foreseeable misuse and integration effects. Identify indirect impact from engineering or test tools. A non-embedded tool can still influence a safety-critical decision.

Evidence: Consequence rationale and interface analysis.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-06.02 to SDR-06.04

ENTITY / SCOPE / CASE REFERENCE

SDR-06.02

Standard p. 10

Risk and threat analysis

Assess hazards, misuse, adversarial access, dependency failure and operational degradation across the lifecycle. Identify controls, verification and residual uncertainty with accountable owners. A numerical risk score shall not conceal a known unacceptable consequence or override a mandatory release gate.

Evidence: Risk/threat register and verified controls.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-06.03

Standard p. 11

Assurance plan

Plan requirements, architecture, verification, validation, independent review, deployment and monitoring proportionate to consequence. Define objective acceptance and stop criteria before testing. Changes to criteria after results shall be justified and independently reviewed, not used to erase a failure.

Evidence: Versioned assurance plan and criteria changes.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-06.04 | ESSENTIAL GATE

Standard p. 11

Unacceptable residual risk

Do not release or continue an affected service with an uncontained credible serious-harm condition, known uncontrolled critical exploitation or materially invalid safety evidence. Identify the competent risk authority and lawful protective action. A customer waiver or executive signature shall not make an unacceptable technical condition conforming.

Evidence: Release blockers, containment and reasoned risk decisions.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-07.01 to SDR-07.03

ENTITY / SCOPE / CASE REFERENCE

SDR-07.01

Standard p. 11

Verifiable requirements

Specify functional behaviour, timing, accuracy, availability, security, privacy, accessibility, support and failure responses as relevant to intended use. Identify assumptions and local obligations. Avoid vague requirements such as secure or reliable without an observable acceptance basis.

Evidence: Reviewed requirements and measurable acceptance criteria.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-07.02 | ESSENTIAL GATE

Standard p. 11

Bidirectional evidence

Trace consequential requirements to design, implementation, verification, validation and released configuration, and trace material defects back to affected requirements and users. Preserve links through change. A completed percentage in a dashboard shall not replace the actual evidence behind the claim.

Evidence: Requirement-to-release and defect-impact traces.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-07.03

Standard p. 11

Interface contracts

Define data types, units, ranges, timing, trust boundaries, error handling and compatibility at material interfaces. Verify both ends where responsibility is shared. A passing isolated component test shall not establish integrated vehicle or ecosystem correctness.

Evidence: Interface specifications and integration evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-07.04 to SDR-08.02

ENTITY / SCOPE / CASE REFERENCE

SDR-07.04

Standard p. 11

Change impact

Assess proposed changes across requirements, architecture, data, dependencies, deployed variants and customer commitments. Review regression needs and approval effects before release. Small code size or a configuration-only label shall not be treated as evidence of low consequence.

Evidence: Change impact and regression scope decisions.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-08.01

Standard p. 11

Separation and least privilege

Define trust boundaries, process/data separation and necessary privileges. Isolate development, test and production appropriately, and protect consequential controls from untrusted input. Document why shared components or credentials cannot create uncontrolled cross-system or cross-tenant consequences.

Evidence: Architecture, privilege and isolation verification.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-08.02 | ESSENTIAL GATE

Standard p. 12

Safe degraded behaviour

Define and validate behaviour on lost connectivity, bad data, partial update, overload, dependency loss and resource exhaustion. Coordinate software responses with actual vehicle or service safety needs. A generic restart or rollback shall not be assumed safe for every physical state.

Evidence: Failure/degraded-mode analysis and validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-08.03 to SDR-09.01

ENTITY / SCOPE / CASE REFERENCE

SDR-08.03

Standard p. 12

Secure usable defaults

Provide protective defaults, individual access and understandable configuration. Avoid universal embedded secrets and unnecessary exposure. Explain material trade-offs and dangerous settings without shifting all foreseeable security responsibility to users who cannot reasonably control the underlying design.

Evidence: Default configuration and usability/security review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-08.04

Standard p. 12

Maintainability and portability

Design for supported updates, diagnosability, migration, evidence export and declared exit needs. Control proprietary dependencies and undocumented interfaces. Portability claims shall be tested against actual data, configuration and service constraints rather than inferred from an export button.

Evidence: Maintainability, migration and exit tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-09.01 | ESSENTIAL GATE

Standard p. 12

Source and privileged access

Use individual identities, strong authentication and least privilege for repositories, build systems, production and signing operations. Review privileged access and revoke promptly on departure or compromise. Shared uncontrolled accounts shall not authorise consequential changes.

Evidence: Access register, review and revocation evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-09.02 to SDR-09.04

ENTITY / SCOPE / CASE REFERENCE

SDR-09.02

Standard p. 12

Environment integrity

Control developer tools, build runners, test infrastructure and infrastructure definitions. Separate trusted execution from untrusted contributions and limit credentials exposed to automation. Record approved versions and detect material drift or unauthorised administrative change.

Evidence: Environment baseline and drift/access monitoring.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-09.03

Standard p. 12

Secret lifecycle

Inventory sensitive credentials and cryptographic material, protect storage/use, rotate when warranted and test revocation. Prevent secrets entering source, logs, test datasets or customer packages. A secret removed from the latest file may remain exposed in history and requires impact review.

Evidence: Secret scanning, custody and rotation records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-09.04

Standard p. 12

Remote and supplier access

Bound remote administration and contractor access by purpose, duration, identity and authorised systems. Log consequential activity and provide emergency revocation. Supplier convenience shall not create unrestricted standing access to customer vehicles, production tenants or confidential engineering data.

Evidence: Remote-access approvals and session evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-10.01 to SDR-10.03

ENTITY / SCOPE / CASE REFERENCE

SDR-10.01

Standard p. 13

Controlled code change

Identify author, purpose, affected requirements, review and approved baseline for material code or configuration changes. Protect branches and release references from unauthorised alteration. Emergency changes shall remain traceable and subject to the defined minimum assurance and retrospective process review.

Evidence: Change records and protected source history.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-10.02

Standard p. 13

Independent code review

Have competent persons other than the author review consequential code and configuration changes, including generated contributions. Focus on logic, security, failure behaviour and integration, not style alone. Automated checks assist but shall not substitute for required human technical judgment.

Evidence: Review comments, corrections and approval identity.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-10.03

Standard p. 13

Defensive implementation

Validate inputs, boundaries, errors, resource use and state transitions appropriate to the application. Treat untrusted external data, generated content and dependency outputs according to their actual trust level. Preserve unresolved concerns and escalate before release where consequence is material.

Evidence: Implementation checks and adverse-input tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-10.04 to SDR-11.02

ENTITY / SCOPE / CASE REFERENCE

SDR-10.04

Standard p. 13

Generated code and reuse

Identify generated or reused code, source, rights, assumptions and necessary verification. Review the actual result and its dependency implications. Tool reputation, a successful compilation or apparent similarity to trusted code shall not establish correctness or acceptable licensing.

Evidence: Generated/reused contribution and verification record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-11.01 | ESSENTIAL GATE

Standard p. 13

Component visibility

Maintain a release-linked inventory of incorporated components, versions, origins, dependency relationships and relevant rights, including firmware, containers, models and material datasets. Record unknowns and completeness limits. A generic inventory detached from the delivered artifact shall not establish its actual composition.

Evidence: Version-linked component inventory and reconciliation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-11.02

Standard p. 13

Supplier control

Evaluate critical suppliers for technical capability, security, support, rights, change notice and evidence access. Verify received outputs proportionately to consequence and preserve accountability for outsourced work. Procurement approval alone shall not establish technical fitness.

Evidence: Supplier evaluation, agreements and received-output checks.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-11.03 to SDR-12.01

ENTITY / SCOPE / CASE REFERENCE

SDR-11.03

Standard p. 13

Dependency change

Monitor material dependency changes, vulnerabilities, support loss and compromised sources. Pin or otherwise control accepted versions and verify provenance. An automatic update shall not bypass regression or consequence review merely because it originates upstream.

Evidence: Dependency monitoring and controlled update evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-11.04

Standard p. 14

Unknown and abandoned components

Assess unsupported, unmaintained or unverifiable components against actual exposure and replacement options. Establish compensating controls, deadlines and customer communication where appropriate. Do not claim complete visibility or long-term support when essential dependencies remain unknown.

Evidence: Exception, replacement and affected-release review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-12.01 | ESSENTIAL GATE

Standard p. 14

Source-to-artifact provenance

Link released artifacts to approved source, dependency set, toolchain, settings, build identity and authorised changes. Protect the evidence from unauthorised alteration. A file hash identifies bytes but does not alone prove trusted origin or correct behaviour.

Evidence: Build provenance and source/artifact reconciliation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-12.02 to SDR-12.04

ENTITY / SCOPE / CASE REFERENCE

SDR-12.02

Standard p. 14

Build reproducibility

Make builds reproducible where feasible and define controlled verification of unavoidable nondeterminism. Retain sufficient instructions and dependencies for competent reconstruction. Explain differences rather than claiming bit-for-bit reproducibility without testing it.

Evidence: Rebuild or justified-equivalence evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-12.03

Standard p. 14

Signing and trust lifecycle

Authenticate release artifacts and protect signing authority proportionate to risk. Control key custody, approval, expiry, revocation and recovery. Signature validity shall be interpreted with trusted identity and policy context; a signed malicious or wrong-target artifact remains unacceptable.

Evidence: Signing approvals, trust verification and recovery tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-12.04

Standard p. 14

Configuration identity

Assign unique versions to software, configuration, models, schemas and feature settings affecting behaviour. Record compatible target hardware and services. A common marketing version shall not conceal materially different deployed configurations or prevent identification of affected populations.

Evidence: Release/configuration manifest and compatibility map.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-13.01 to SDR-13.03

ENTITY / SCOPE / CASE REFERENCE

SDR-13.01

Standard p. 14

Representative testing

Verify requirements with suitable unit, integration, system and operational-context tests, including adverse conditions and relevant variants. Justify coverage gaps and sample limits. High code coverage or a large test count shall not alone establish safe, secure or correct intended behaviour.

Evidence: Test plan, coverage rationale and original results.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-13.02 | ESSENTIAL GATE

Standard p. 14

Original result integrity

Retain actual test inputs, environment, version, timestamps, failures and disposition. Distinguish reruns from original results and prevent selective deletion of inconvenient evidence. A green summary without reviewable source results shall not establish conformity.

Evidence: Original results and failed/rerun traceability.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-13.03

Standard p. 15

Independent validation

For consequential functions, obtain competent validation and release challenge independent of their creation. Verify intended use and integration assumptions rather than only implementation against internal design. Unsupported safety or accuracy claims shall prevent the affected release.

Evidence: Independent validation, queries and resolved blockers.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-13.04 to SDR-14.02

ENTITY / SCOPE / CASE REFERENCE

SDR-13.04

Standard p. 15

Defect and regression control

Classify defects by actual consequence and exposure, define correction/regression needs and verify effectiveness. Record accepted nonblocking limitations with authority and user information. Do not relabel a serious defect as a feature or close it solely because a test was disabled.

Evidence: Defect register, regression evidence and acceptance decisions.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-14.01

Standard p. 15

Tool influence

Identify whether a tool creates, checks, measures or supports consequential outputs and whether its errors can escape downstream detection. Establish task-specific confidence through validation, independent checks or appropriate safeguards. A tool licence or vendor certificate alone shall not validate its intended use.

Evidence: Tool-impact analysis and confidence evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-14.02

Standard p. 15

Measurement validity

Validate units, conversions, timestamps, sampling, precision and uncertainty for the actual decision. Control sensor and data-acquisition interfaces and investigate unreliable results. Software calibration settings shall remain linked to the relevant equipment and configuration.

Evidence: Measurement chain and uncertainty/fitness record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-14.03 to SDR-15.01

ENTITY / SCOPE / CASE REFERENCE

SDR-14.03

Standard p. 15

Models and simulations

Document purpose, input provenance, assumptions, model version, validation, sensitivity and limits. Distinguish measured facts from simulated or predicted results. A realistic digital twin or animation shall not be represented as observed evidence or universal proof of physical performance.

Evidence: Reproducible model package and validation limits.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-14.04 | ESSENTIAL GATE

Standard p. 15

False-pass prevention

Challenge tools with known failures, boundary cases, corrupted data and incompatible versions. Verify that missing evidence cannot silently become a pass. Investigate potentially affected earlier outputs when a tool defect invalidates a consequential acceptance decision.

Evidence: Adverse challenge and prior-output impact review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-15.01 | ESSENTIAL GATE

Standard p. 15

Release gates

Before release verify exact configuration, required evidence, independent approvals, resolved blockers, customer readiness, support and recovery. All mandatory gates shall be satisfied. An emergency schedule, commercial acceptance or majority vote shall not waive a known unacceptable technical condition.

Evidence: Authenticated release decision and complete evidence manifest.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-15.02 to SDR-15.04

ENTITY / SCOPE / CASE REFERENCE

SDR-15.02

Standard p. 16

Deployment control

Identify targets, permissions, sequencing, environment preconditions, staged rollout and stop criteria. Confirm that the actual installed or activated state matches the authorised release. A successful server-side send or closed deployment ticket shall not alone prove successful safe operation.

Evidence: Target inventory, deployment and installed-state evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-15.03

Standard p. 16

Recovery and containment

Validate rollback, roll-forward, isolation or another safe recovery route for relevant failure states. Check data/schema compatibility and physical consequences before reversal. Where rollback is unsafe, establish a validated alternative and communicate the limitation before deployment.

Evidence: Failure rehearsal and safe recovery decision.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-15.04

Standard p. 16

Customer acceptance and limits

Provide accurate release notes, known limitations, configuration requirements, support contacts and necessary user action. Separate supplier release approval from customer integration acceptance. Record unresolved customer-side conditions and prevent claims that the corporate status guarantees every deployment.

Evidence: Release communication and bounded customer acceptance.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-16.01 to SDR-16.03

ENTITY / SCOPE / CASE REFERENCE

SDR-16.01

Standard p. 16

Accessible vulnerability intake

Provide a clear route for good-faith vulnerability reports and coordinated handling, including secure exchange and acknowledgement. Define authorised research boundaries without implying permission for intrusive testing. Do not retaliate against lawful reporting or suppress credible evidence to protect reputation.

Evidence: Intake, triage and coordinated communication records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-16.02 | ESSENTIAL GATE

Standard p. 16

Exposure-based triage

Prioritise vulnerabilities using exploitability, reachability, active exploitation, affected assets and safety/privacy consequences, not a score alone. Investigate unknown exposure promptly. A scanner's absence of findings or disputed severity shall not establish that an affected deployed system is safe.

Evidence: Exposure analysis and accountable response priorities.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-16.03

Standard p. 16

Containment and correction

Act promptly on serious risk, preserve evidence, identify affected versions/users and validate remediation and recovery. Set risk-based dated response commitments with escalation and customer communication. Do not wait for a perfect patch before implementing necessary safe containment.

Evidence: Incident chronology, affected population and verified remedy.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-16.04 to SDR-17.02

ENTITY / SCOPE / CASE REFERENCE

SDR-16.04

Standard p. 16

IAF notification

Notify IAF within 48 hours of awareness of serious harm, material compromise, deliberate falsification or loss of control affecting recognised scope. State known facts and uncertainty and update promptly. This programme clock shall not delay emergency action or earlier applicable reporting duties.

Evidence: Awareness timestamp, initial notice and updates.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-17.01

Standard p. 17

Purpose and authority

Identify lawful purposes, data roles, entitled users and necessary data for development, operation, telemetry and model use. Distinguish vehicle-owner, driver, passenger, employee and customer interests. Possession of a vehicle or dataset shall not automatically confer unrestricted processing or training rights.

Evidence: Data map, authority and bounded purpose record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-17.02

Standard p. 17

Minimisation and privacy design

Minimise personal data, protect sensitive location, images, behaviour and identifiers, and apply suitable separation or de-identification. Test privacy controls across defaults, logs, support access and exports. A general consent statement shall not justify unnecessary collection or hidden secondary use.

Evidence: Privacy design and actual data-flow verification.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-17.03 to SDR-18.01

ENTITY / SCOPE / CASE REFERENCE

SDR-17.03

Standard p. 17

Transfer, retention and rights

Control recipients, hosting, transfers, access and retention according to actual obligations and commitments. Provide workable rights and deletion routes while preserving lawful holds and essential technical evidence. Distinguish removal from a live system from copies, backups and derived datasets.

Evidence: Transfer/retention register and verified request handling.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-17.04

Standard p. 17

Information security

Protect source, customer secrets and evidence with role-based access, suitable authentication, encryption where appropriate and monitored recovery. Verify provider controls and revoke access promptly. A provider claim shall not replace the organisation's own responsibility for its configuration and data handling.

Evidence: Access review, provider assurance and restore evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-18.01 | ESSENTIAL GATE

Standard p. 17

Bounded AI purpose

Define model purpose, consequence, operating domain, human responsibility, prohibited uses and fallback. Distinguish development assistance from deployed decision-making or vehicle control. An AI label or benchmark ranking shall not establish suitability for an automotive safety or professional decision.

Evidence: AI inventory, purpose and consequence boundary.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-18.02 to SDR-18.04

ENTITY / SCOPE / CASE REFERENCE

SDR-18.02

Standard p. 17

Data and model provenance

Record training/evaluation data provenance, rights, representation, transformations, model versions and relevant dependencies. Separate evaluation from training influence and assess leakage and synthetic-data limitations. Explain unavailable provenance and resulting restrictions rather than claiming complete assurance.

Evidence: Data/model lineage and evaluation independence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-18.03

Standard p. 17

Robustness and human control

Validate representative, adverse and out-of-domain behaviour, subgroup performance, uncertainty and override needs. Prevent untrusted content or tool output from silently granting authority to act. Consequential actions require bounded permissions, verified context and appropriate competent human oversight.

Evidence: Robustness, permission and human-control tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-18.04

Standard p. 18

Change, drift and generated content

Monitor material drift, model/provider changes and incorrect generated outputs. Revalidate before consequential use after material change and preserve relevant versions. Verify generated code, facts and references against authentic evidence; label synthetic exhibits and prohibit fabrication presented as observation.

Evidence: Monitoring, revalidation and human verification record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-19.01 to SDR-19.03

ENTITY / SCOPE / CASE REFERENCE

SDR-19.01

Standard p. 18

Service objectives

Define service-level indicators, measurement points, availability, latency, integrity and recovery objectives appropriate to user consequence. Specify exclusions and dependency boundaries transparently. A favourable average shall not hide dangerous tail behaviour or unavailable critical functions.

Evidence: Service objectives and reconciled operational data.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-19.02

Standard p. 18

Tenant and interface protection

Validate tenant isolation, authentication, authorisation, rate limits and interface error handling. Test negative access and cross-account scenarios safely. A successful login or network encryption alone shall not establish that a user may access another vehicle, tenant or privileged action.

Evidence: Isolation and authorisation test evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-19.03 | ESSENTIAL GATE

Standard p. 18

Operational change and observability

Control production changes, detect consequential failures and preserve relevant logs and alerts. Ensure clock context, access and response ownership. Feature flags, infrastructure or data changes affecting behaviour shall receive appropriate change control even without a new binary.

Evidence: Change, telemetry, alert and response evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-19.04 to SDR-20.02

ENTITY / SCOPE / CASE REFERENCE

SDR-19.04

Standard p. 18

Continuity and restore

Exercise dependency loss, region/provider outage, compromised credentials and corrupted data under safe conditions. Demonstrate recovery of correct state and evidence links, not only infrastructure availability. Define customer communication, safe degradation and restart authority.

Evidence: Continuity exercise and restored-state validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-20.01

Standard p. 18

Published support boundary

Define supported versions/configurations, support period, security maintenance, dependencies and end-of-support conditions before commitment. Align foreseeable service life and customer obligations with resources. No single universal support duration shall be implied where actual risk and commitments differ.

Evidence: Support policy, resource plan and customer disclosure.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-20.02 | ESSENTIAL GATE

Standard p. 18

End-of-support protection

Assess consequences before ending support or disabling a dependency used by vehicles or critical tools. Give justified notice, migration or safe alternatives and preserve necessary access to user data. Do not abandon a known serious risk merely because a commercial subscription ended.

Evidence: End-of-support impact and transition evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-20.03 to SDR-21.01

ENTITY / SCOPE / CASE REFERENCE

SDR-20.03

Standard p. 19

Legacy and cryptographic change

Inventory legacy platforms, fragile dependencies and cryptographic exposure, including long-lived vehicle data and trust roots. Plan tested migration with compatibility, safe fallback and resource constraints. A future algorithm claim shall not replace present key custody or practical transition evidence.

Evidence: Legacy inventory and migration validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-20.04

Standard p. 19

Sustainable digital operation

Measure material compute, storage, network and hardware impacts with defined boundaries and useful-work denominators. Improve efficiency without suppressing necessary testing, evidence or safety controls. Substantiate environmental claims and consider accessibility, reparability and extended useful service.

Evidence: Resource baseline, trade-offs and verified improvement.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-21.01

Standard p. 19

Defined indicators

Use reconciled populations, periods, denominators and exclusions for escaped defects, failed changes, vulnerability response, service reliability and customer outcomes. Preserve original commitments and adverse results. Test-count growth or faster release alone shall not be described as improved quality.

Evidence: Metric definitions and source reconciliation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-21.02 to SDR-21.04

ENTITY / SCOPE / CASE REFERENCE

SDR-21.02

Standard p. 19

Internal audit

Audit implemented controls at least annually across included hubs, families and relevant profiles/domains, using independent competent review. Examine actual releases, adverse cases and source-to-deployment traces. A self-completed checklist without objective evaluation shall not establish internal assurance.

Evidence: Audit plan, original samples and findings.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-21.03

Standard p. 19

Management review

At least annually review quality, security, safety interfaces, privacy, customer issues, resources, suppliers, support horizons and new technologies. Record decisions, owners and due dates. A review limited to favourable delivery metrics shall not fulfil the requirement.

Evidence: Review inputs, decisions and action follow-up.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-21.04

Standard p. 19

Corrective effectiveness

Contain failures, investigate evidence-based causes, review affected past releases and verify subsequent effectiveness. Preserve unsuccessful actions and shared causes across products. Training attendance, a new policy or a closed ticket alone shall not prove recurrence has been controlled.

Evidence: Cause, affected-population and effectiveness evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-22.01 to SDR-22.03

ENTITY / SCOPE / CASE REFERENCE

SDR-22.01

Standard p. 19

Evidence access

Provide lawful protected access to original source, build, test, deployment and operational records sufficient for the claimed scope. Minimise confidential copies and agree secure review where needed. If essential evidence cannot be verified, defer or exclude unsupported scope rather than assert unrestricted assurance.

Evidence: Access plan, protected review and limitations.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-22.02

Standard p. 20

Actual technical demonstration

Support assessment of every delivering hub and required product-family demonstrations under IR02. Demonstrate real traceability and failure handling safely, without unauthorised production disruption. A prerecorded marketing demonstration shall not replace sufficient interactive evidence.

Evidence: Coverage, live challenge and sample evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-22.03 | ESSENTIAL GATE

Standard p. 20

Independent recognition gates

Accept competent assessment, uninvolved technical review and the three-person independent decision process. Initial grant requires every applicable requirement Met and all findings effectively closed. Payment, membership, high scores or an important customer shall not override a failed gate.

Evidence: Complete case, closure and independent decision.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-22.04 to SDR-23.02

ENTITY / SCOPE / CASE REFERENCE

SDR-22.04

Standard p. 20

Truthful cooperation

Disclose material defects, incidents, prior adverse decisions and scope changes. Preserve authentic evidence and fair assessor access. Deliberate concealment, fabricated telemetry or selective removal of failed results shall trigger integrity and protective-status review.

Evidence: Disclosure, source integrity and response records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-23.01

Standard p. 20

Annual surveillance

Maintain conformity between assessments and support surveillance by months 12 and 24 of a maximum three-year term. Review every hub annually, physically visit technical facilities and follow approved remote-only office rules. Apply family-demonstration coverage and risk expansion under IR02.

Evidence: Annual hub/family coverage and actual evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-23.02

Standard p. 20

Material change notice

Notify IAF before planned material changes to entity, hubs, families, consequence, lifecycle responsibility, critical suppliers or support commitments. Notify unplanned material changes within five calendar days; serious incidents retain the 48-hour clock. Unsupported extensions remain outside active claims.

Evidence: Change notice, impact and revised scope.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-23.03 to SDR-24.01

ENTITY / SCOPE / CASE REFERENCE

SDR-23.03

Standard p. 20

Renewal and expiry

Apply for renewal at least six months before expiry and complete reassessment and independent decision before the term ends. A pending application, appeal or commercial agreement shall not extend validity. Prepare truthful claim changes and continuing support duties if status expires.

Evidence: Renewal plan and expiry controls.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-23.04

Standard p. 20

Restriction and restoration

Implement restriction, suspension or withdrawal promptly and protect affected customers and evidence. Restore active scope only after competent verification and independent dated decision. Do not backdate status, silently transfer recognition to an acquisition or hide lost capability behind unchanged branding.

Evidence: Protection, verified correction and status history.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-24.01 | ESSENTIAL GATE

Standard p. 21

Exact public claim

Use IAF Corporate Recognition under this programme only for the approved legal holder, hubs and lifecycle activities. State material exclusions and current verification. Do not imply that every software version, AI output, vehicle or customer integration has been certified or endorsed by IAF.

Evidence: Approved wording and bounded public scope.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-24.02 to SDR-24.04

ENTITY / SCOPE / CASE REFERENCE

SDR-24.02

Standard p. 21

Product-facing context

Where a corporate mark appears near a product, interface or report, explain its organisational meaning and distinguish release/support status. Do not present it as a security guarantee, safety seal, model-accuracy rating or permission for automated driving. Review context, not merely artwork dimensions.

Evidence: Placement examples and misleading-implication review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-24.03

Standard p. 21

Licence and removal

Use controlled artwork only under a recorded licence with defined channels, holder and dates. Prohibit sublicensing to unrelated suppliers and correct affected claims after restriction, expiry or scope change. Historical release records shall not be altered to imply continuous current recognition.

Evidence: Licence, monitoring and removal evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-24.04

Standard p. 21

Current verification

Provide a tested current status/scope route and controlled manual fallback. During outage, uncertainty or unknown records report unavailable or unresolved rather than stale active confirmation. Correct deliberate or repeated misuse through fair investigation and proportionate programme action.

Evidence: Verification tests, inquiry and correction records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-25.01 to SDR-25.03

ENTITY / SCOPE / CASE REFERENCE

SDR-25.01

Standard p. 21

Factual response and appeal

Allow 15 calendar days for factual response to draft findings and 30 calendar days to appeal a decision notice. Use independent reasoned review and protect justified confidentiality. Appeal shall not automatically stay necessary protection or extend expiry.

Evidence: Notices, deadlines and independent outcome.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-25.02

Standard p. 21

Protected complaints

Provide accessible routes for programme conduct, integrity, misleading claims and good-faith reporting. Assign uninvolved competent investigators and prohibit retaliation. Distinguish customer remedies from IAF's programme remit; recognition shall not make IAF the guarantor of every commercial dispute.

Evidence: Triage, investigation and verified remedy.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

SDR-25.03

Standard p. 21

IAF operator evidence

IAF shall independently demonstrate assessment competence, impartiality, technical review, decisions and registry control. Applicant declarations shall not substitute for operator evidence. Record the operator-assurance basis and correct material weaknesses affecting recognition decisions.

Evidence: Independent operator audit and case reference.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | SDR-25.04 to DEV-02

ENTITY / SCOPE / CASE REFERENCE

SDR-25.04

Standard p. 22

Controlled development

Review emerging technology, actual failures and stakeholder needs through controlled revisions and published effective dates. Evidence specific acceptance arrangements separately. Global programme design shall not be described as universal legal approval, automatic equivalence or acceptance by every customer or authority.

Evidence: Revision, consultation and substantiated acceptance.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

DEV-01 | ESSENTIAL GATE

Standard p. 22

Accountable lifecycle role

Identify who develops, integrates, releases, distributes, operates and supports each family. Where the applicant does not develop code, demonstrate the controls it actually owns and supplier interfaces it enforces. Do not imply authorship or design control over an unverified third-party product.

Evidence: Lifecycle responsibility and enforceable supplier controls.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

DEV-02

Standard p. 22

Engineering workflow

Maintain controlled work intake, requirements, source/configuration change, review, testing and issue handling appropriate to the actual role. A ticketing system or repository alone shall not demonstrate that mandatory gates are effective.

Evidence: Actual workflow and completed-event traces.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | DEV-03 to EMB-01

ENTITY / SCOPE / CASE REFERENCE

DEV-03

Standard p. 22

Integration responsibility

Assess compatibility, shared assumptions, data contracts and failure propagation when combining components or services. Verify integration in representative configurations rather than assuming that individually accepted parts produce a conforming system.

Evidence: Integration matrix and adverse-interface evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

DEV-04

Standard p. 22

Delivery accountability

Provide accurate deliverables, limitations, support obligations and transition information. Retain source-to-delivery evidence and responsibility after outsourcing or ownership change. A subcontract shall not transfer away the applicant's own obligations to its customer.

Evidence: Delivery package and continuing responsibility.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

EMB-01 | ESSENTIAL GATE

Standard p. 22

Vehicle consequence and configuration

Identify affected vehicle functions, hardware, variants, timing/resource constraints and integration authority. Evaluate indirect safety effects and dependencies. Corporate recognition shall not replace vehicle-level acceptance or permission to operate an automated function.

Evidence: Vehicle interface and configuration assurance.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | EMB-02 to EMB-04

ENTITY / SCOPE / CASE REFERENCE

EMB-02

Standard p. 22

Real-time and fault behaviour

Validate timing, concurrency, resource exhaustion, start-up/shutdown and relevant fault responses under representative load. Explain what simulation or bench tests cannot establish about actual installed behaviour.

Evidence: Timing, load and fault-injection evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

EMB-03

Standard p. 23

Hardware and diagnostics interface

Control hardware/software compatibility, calibration data, diagnostic permissions and service interactions. Prevent unsupported coding or configuration from silently changing safety-relevant behaviour. Identify the installed state reliably for investigation and support.

Evidence: Compatibility, diagnostic and installed-state records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

EMB-04

Standard p. 23

Integration handover

Supply integrators with assumptions, unresolved limitations, verification results and required vehicle-level checks. Record acceptance responsibilities and update impacts. A supplier release shall not be described as approval of the complete vehicle.

Evidence: Integrator package and acceptance boundary.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | ENG-01 to ENG-03

ENTITY / SCOPE / CASE REFERENCE

ENG-01

Standard p. 23

Intended analytical use

Define quantities, populations, configurations and decisions the tool supports, including prohibited extrapolation. Distinguish visualization, calculation and validated prediction. A digital twin label shall not establish correspondence to every physical vehicle state.

Evidence: Intended-use and validity-domain record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

ENG-02 | ESSENTIAL GATE

Standard p. 23

Calculation and model validation

Validate significant equations, units, solvers, data transformations and numerical behaviour with independent reference cases and adverse inputs. Document uncertainty and material assumptions. A plausible picture or stable numerical output is not sufficient validation.

Evidence: Independent benchmark and sensitivity evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

ENG-03

Standard p. 23

Version and collaboration integrity

Preserve model, geometry, parameters, data, tool version and collaborator changes necessary to reconstruct an engineering conclusion. Detect incompatible import/export or silent unit conversions and preserve the original input.

Evidence: Reproducible engineering configuration.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | ENG-04 to TST-02

ENTITY / SCOPE / CASE REFERENCE

ENG-04

Standard p. 23

Decision handover

Explain limits and required independent checks to users, particularly where tool errors can influence safety. Review prior outputs after a consequential tool defect and provide actionable correction information to entitled affected users.

Evidence: User guidance and prior-output impact records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

TST-01 | ESSENTIAL GATE

Standard p. 23

False-pass controls

Validate the complete path from stimulus or acquisition to displayed result and exported report. Test missing, stale, corrupted and wrong-target data. The tool shall not convert an incomplete required test or communication failure into a passing result.

Evidence: End-to-end adverse and known-failure tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

TST-02

Standard p. 24

Measurement chain

Control equipment interfaces, timestamps, sample rates, units, calibration parameters and uncertainty relevant to use. Record software and equipment configuration together. A software-only test shall not establish the fitness of the whole measurement chain.

Evidence: Measurement/configuration and fitness evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | TST-03 to CLD-01

ENTITY / SCOPE / CASE REFERENCE

TST-03

Standard p. 24

Safe diagnostic authority

Restrict write, actuation, coding and security-sensitive functions to authorised users and suitable vehicle conditions. Separate observation from intervention. Recognition shall not authorise bypassing protected functions or unsafe actuation on live vehicles.

Evidence: Role, vehicle authority and safe-function controls.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

TST-04

Standard p. 24

Report authenticity

Preserve original results, failures, alterations, tool versions and issue authority. Prevent unauthorised editing of acceptance decisions and identify corrected reports. A branded report template shall not imply IAF performed or certified the test.

Evidence: Result integrity and report-version trail.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

CLD-01

Standard p. 24

Shared responsibility

Define provider/customer responsibilities for identity, configuration, data, backups, incident response and support. Verify the applicant's actual controls. A hosting provider's assurance shall not cover insecure tenant configuration or application logic automatically.

Evidence: Responsibility map and configured-control evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | CLD-02 to CLD-04

ENTITY / SCOPE / CASE REFERENCE

CLD-02 | ESSENTIAL GATE

Standard p. 24

Tenant and privilege isolation

Test cross-tenant, cross-vehicle and administrative access boundaries safely, including negative cases and support impersonation. Prevent a valid identity from being treated as universal authority across customer accounts.

Evidence: Isolation and authorisation evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

CLD-03

Standard p. 24

Resilient operation

Validate load, overload, dependency loss, regional failure and correct-state recovery. Define service indicators and safe degradation appropriate to vehicle and user needs. An available endpoint with incorrect data shall not count as a successful critical service.

Evidence: Load, failure and state-recovery tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

CLD-04

Standard p. 24

Exit and customer continuity

Demonstrate usable export, migration, retention/deletion and support transition according to commitments. Identify proprietary dependencies and failure of key providers. A subscription ending shall not silently strand safety-relevant vehicle functions or essential customer evidence.

Evidence: Exit rehearsal and continuity plan.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | FLE-01 to FLE-03

ENTITY / SCOPE / CASE REFERENCE

FLE-01

Standard p. 25

Vehicle and user authority

Separate owner, driver, fleet administrator, passenger and service-provider permissions. Verify authority for remote commands, location use and account transfer. A vehicle association or prior login shall not permit all future actions or data use.

Evidence: Role, consent/authority and transfer controls.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

FLE-02 | ESSENTIAL GATE

Standard p. 25

Safe interaction

Assess distraction, accessibility, misleading state displays, command confirmation and lost-connectivity behaviour. Consequential remote actions require verified target and appropriate safe conditions. Do not present stale telemetry as confirmed current vehicle state.

Evidence: Human-interaction and command-safety validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

FLE-03

Standard p. 25

Operational data quality

Validate location, energy, route, charging and scheduling data against intended use, update rate and uncertainty. Explain estimates and incomplete coverage. A planning prediction shall not become an unsupported guarantee of range, arrival or service availability.

Evidence: Data-quality and bounded prediction evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | FLE-04 to OTA-02

ENTITY / SCOPE / CASE REFERENCE

FLE-04

Standard p. 25

Fair service and recovery

Communicate prices/terms, transaction state, cancellations, disputed charges and support routes clearly where applicable. Reconcile interrupted operations and protect user access during account or provider changes.

Evidence: Transaction, user-remedy and recovery records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

OTA-01 | ESSENTIAL GATE

Standard p. 25

Target and package authenticity

Verify authorised package, origin, compatible target, configuration and entitlement before deployment. Detect wrong-target, altered, stale and unauthorised downgrade attempts. Transport encryption alone shall not establish that a package is suitable or permitted.

Evidence: Target/package verification and negative tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

OTA-02

Standard p. 25

Update safety

Validate preconditions, sequencing, power/connectivity interruption and partial-state handling for relevant vehicle configurations. Coordinate with the integrating authority. Do not assume a general reboot or automatic rollback is safe during a physical manoeuvre or schema change.

Evidence: State-specific update and recovery validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | OTA-03 to AIM-01

ENTITY / SCOPE / CASE REFERENCE

OTA-03

Standard p. 25

Campaign accountability

Link campaign, artifacts, target population, consent/notice where needed, installation result and actual activated state. Reconcile offline and failed targets. A successful download shall not be counted as a completed functional update.

Evidence: Campaign and installed-state reconciliation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

OTA-04

Standard p. 26

Compromise and support

Test distribution/signing compromise response, trust revocation, protected recovery and customer communication. Maintain update capability and evidence for the declared support horizon; do not confuse preventing hostile downgrade with preventing a validated recovery path.

Evidence: Compromise exercise and lifecycle support evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

AIM-01 | ESSENTIAL GATE

Standard p. 26

Use and autonomy boundary

Define operating domain, consequence, user role, action permissions and human intervention. Separate research evaluation from production decision authority. A model's apparent reasoning shall not grant unrestricted vehicle, system or financial action permissions.

Evidence: Model/action scope and authorisation design.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | AIM-02 to AIM-04

ENTITY / SCOPE / CASE REFERENCE

AIM-02

Standard p. 26

Evaluation integrity

Use representative and adverse evaluation independent of training influence. Explain subgroup, rare-event and out-of-domain limitations. Benchmark improvement shall not be treated as evidence of safe deployment in a different vehicle, environment or user population.

Evidence: Evaluation design and result limitations.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

AIM-03

Standard p. 26

Agent and retrieval controls

Treat retrieved content, user input and tool responses as potentially untrusted. Validate requested actions against explicit authority and scope, protect secrets and record consequential actions. A generated instruction shall not override higher-level operational permissions.

Evidence: Permission-bound action and adversarial-input tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

AIM-04

Standard p. 26

Lifecycle monitoring

Track model/data/provider versions, drift, incorrect outputs and human overrides. Revalidate material changes and retain a safe fallback or withdrawal route. Correct affected outputs and users when a material model defect is discovered.

Evidence: Monitoring, revalidation and correction evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | CYB-01 to CYB-03

ENTITY / SCOPE / CASE REFERENCE

CYB-01

Standard p. 26

Authorised operation

Bound testing, monitoring and intervention by written authority, target, purpose and safe conditions. Separate defensive tool capability from permission to use it. Recognition shall not authorise intrusion or uncontrolled testing on vehicles or third-party systems.

Evidence: Authorisation and safe assessment scope.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

CYB-02 | ESSENTIAL GATE

Standard p. 26

Detection and protection validity

Measure relevant detection, false-positive/negative and response behaviour using representative and adverse cases. State coverage gaps and blind spots. A clean scan or absence of an alert shall not establish absence of compromise.

Evidence: Validation and bounded detection claims.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

CYB-03

Standard p. 27

Response safety

Evaluate automated isolation, blocking, credential revocation and vehicle-interface actions for secondary consequences. Require suitable approval and recovery for consequential actions. A security response shall not blindly disable a necessary safety function.

Evidence: Response consequence and recovery validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | CYB-04 to DAT-02

ENTITY / SCOPE / CASE REFERENCE

CYB-04

Standard p. 27

Sensitive finding handling

Protect exploit details, credentials and customer evidence, coordinate disclosure and prevent unsupported public accusations. Preserve technical facts and communicate material exposure responsibly. Commercial interests shall not suppress necessary customer protection.

Evidence: Finding custody, disclosure and remedy records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

DAT-01

Standard p. 27

Data provenance and rights

Record source, collection authority, transformations, quality, permitted use and onward-transfer conditions for material datasets. Distinguish observed, inferred, purchased and synthetic data. Marketplace availability shall not itself establish accuracy or lawful reuse.

Evidence: Dataset lineage and rights evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

DAT-02 | ESSENTIAL GATE

Standard p. 27

Integrity of distribution

Verify publisher identity, artifact/data integrity, version and required limitations across distribution channels. Detect substitution, stale packages and misleading listings. A platform listing shall not confer recognition on an unassessed third-party producer.

Evidence: Publisher, package and listing control.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | DAT-03 to T01-01

ENTITY / SCOPE / CASE REFERENCE

DAT-03

Standard p. 27

Interoperability and semantics

Validate schemas, units, identifiers, time context and meaning across integration boundaries, including malformed and incompatible inputs. Syntactic compatibility shall not be treated as semantic correctness or universal interoperability.

Evidence: Contract and semantic compatibility tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

DAT-04

Standard p. 27

Correction and withdrawal

Provide versioned correction, withdrawal and recipient notice for materially wrong data or compromised packages. Preserve affected transaction and access records lawfully. Prevent a removed listing from leaving unsupported copies falsely described as current.

Evidence: Recipient tracing and corrected distribution.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T01-01 | ESSENTIAL GATE

Standard p. 28

Consequence chain

Trace how software or tool error can affect people, vehicles or consequential decisions, including downstream integration. Define assumptions and competent authority; a desktop deployment does not make a safety-influencing tool low risk.

Evidence: Consequence and dependency map.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T01-02 to T01-04

ENTITY / SCOPE / CASE REFERENCE

T01-02

Standard p. 28

Independent assurance

Require competent independent verification and release challenge for consequential functions and changes. Preserve material dissent and unresolved blockers. Automated tests and code-author approval shall not replace the required independent judgment.

Evidence: Review independence and resolved queries.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T01-03

Standard p. 28

Failure and degraded state

Validate foreseeable failures, misuse and safe degraded behaviour in the actual context. Record the limits of bench, simulation and live evidence. Do not claim complete safety from a narrow successful demonstration.

Evidence: Adverse-state and integration validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T01-04

Standard p. 28

Affected-user protection

When evidence becomes invalid, identify earlier releases and outputs relying on it, notify entitled users lawfully and verify necessary correction. A fixed development branch shall not close the impact on deployed systems.

Evidence: Prior-release and user-remedy review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T02-01 to T02-03

ENTITY / SCOPE / CASE REFERENCE

T02-01

Standard p. 28

Threat and exposure

Analyse actual trust boundaries, attacker access, credentials and dependency exposure. Reassess after material change. A generic checklist or scanner severity alone shall not establish the risk of the deployed configuration.

Evidence: Threat model and reachability analysis.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T02-02 | ESSENTIAL GATE

Standard p. 28

Protective architecture

Implement and verify least privilege, individual authentication, isolation, input handling and controlled remote access proportionate to consequence. Protect recovery and signing paths as well as normal operation.

Evidence: Architecture and negative security tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T02-03

Standard p. 28

Coordinated response

Maintain secure vulnerability intake, rapid exposure review, risk-based dated remediation and escalation. Preserve evidence and protect users while a permanent remedy is developed; no arbitrary grace period permits known serious uncontrolled risk.

Evidence: Triage, containment and validated correction.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T02-04 to T03-02

ENTITY / SCOPE / CASE REFERENCE

T02-04

Standard p. 29

Trust renewal

Test credential/key compromise, revocation, re-establishment of trust and affected-artifact identification. Prevent a valid signature from concealing an unauthorised source or unsafe target configuration.

Evidence: Trust-recovery exercise and artifact impact.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T03-01

Standard p. 29

Lawful purpose

Determine data roles, actual authority and permitted use across development, support, telemetry and AI. Separate data subjects and contractual parties. Public or purchased data shall not automatically be available for unrestricted processing.

Evidence: Purpose, authority and rights register.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T03-02

Standard p. 29

Minimised flows

Verify actual collection, logs, access, export and deletion against the intended boundary. Minimise unnecessary identifiers and sensitive content while preserving essential lawful technical evidence.

Evidence: Data-flow and minimisation checks.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T03-03 to T04-01

ENTITY / SCOPE / CASE REFERENCE

T03-03 | ESSENTIAL GATE

Standard p. 29

Protected access

Control privileged and supplier access, tenant separation, transfers and incident response. Use lawful protected review for assessment; confidentiality shall not be used to hide a material contradiction.

Evidence: Access and protected-evidence review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T03-04

Standard p. 29

Lifecycle obligations

Implement retention, rights, lawful holds and end-of-service custody with tested procedures. Explain what deletion means for backups and derived data. Avoid both indefinite unnecessary retention and unsupported destruction of essential evidence.

Evidence: Retention, rights and disposal evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T04-01

Standard p. 29

Bounded model claim

Define task, operating conditions, consequence and human responsibility. State unsupported uses and uncertainty. A general intelligence or accuracy claim shall not replace task-specific validation.

Evidence: Model-purpose and limitation statement.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T04-02 to T04-04

ENTITY / SCOPE / CASE REFERENCE

T04-02

Standard p. 29

Data and evaluation quality

Preserve lineage and rights, assess representation and separate evaluation from training influence. Challenge rare/adverse cases and misleading benchmark selection. Identify synthetic data and its limitations.

Evidence: Independent evaluation and lineage record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T04-03 | ESSENTIAL GATE

Standard p. 30

Action permission

Constrain consequential actions by verified authority, target and safe conditions. Treat retrieved/generated instructions as untrusted data unless explicitly authorised through the control design. Test misuse, prompt manipulation and erroneous tool responses safely.

Evidence: Action-boundary and adversarial tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T04-04

Standard p. 30

Monitoring and revalidation

Detect material drift/provider changes and reassess affected conclusions or deployments. Preserve relevant versions, human overrides and safe fallback. Silent model replacement shall not maintain an unsupported prior assurance claim.

Evidence: Change, drift and corrective action evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T05-01 to T05-03

ENTITY / SCOPE / CASE REFERENCE

T05-01

Standard p. 30

Intended-use validity

Validate method, units, inputs and operating limits for the actual decision. Identify how errors can escape downstream checks. Reputation or visual realism shall not establish fitness for purpose.

Evidence: Tool influence and independent validation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T05-02

Standard p. 30

Uncertainty and sensitivity

Explain material measurement, sampling and model uncertainty, including influential assumptions. Use justified decision rules and preserve inconclusive outcomes rather than forcing a pass.

Evidence: Uncertainty and borderline-case evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T05-03 | ESSENTIAL GATE

Standard p. 30

Reproducible result

Retain inputs, versions, settings, dependencies, original failures and sufficient intermediate results for competent reconstruction. Prevent missing or stale data from appearing as a valid current result.

Evidence: Reproduction and false-pass challenge.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T05-04 to T06-02

ENTITY / SCOPE / CASE REFERENCE

T05-04

Standard p. 30

Retrospective impact

After a consequential tool defect identify affected prior outputs and decisions, assess validity and notify entitled users. Correcting the tool shall not automatically validate old reports.

Evidence: Affected-output analysis and verified remedy.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T06-01

Standard p. 30

Composition and rights

Maintain release-linked components, versions, origins, relationships and rights. Identify inventory gaps and actual material dependencies, including models and data. Do not label a partial inventory complete.

Evidence: Composition reconciliation and limitations.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T06-02 | ESSENTIAL GATE

Standard p. 31

Build trust

Protect the path from approved source through build, artifact, distribution and target verification. Isolate untrusted contributions and sensitive credentials. A signature or hash alone shall not prove a trustworthy build or safe behaviour.

Evidence: Provenance, isolation and verification evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T06-03 to T07-01

ENTITY / SCOPE / CASE REFERENCE

T06-03

Standard p. 31

Supplier continuity

Evaluate critical supplier support, change notice, incident cooperation and exit options. Verify actual received outputs and retain the applicant's own accountability. Unavailable essential supplier evidence requires bounded scope or deferral.

Evidence: Supplier assurance and continuity record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T06-04

Standard p. 31

Compromise response

Identify all affected downstream artifacts and users after a source, dependency or build compromise. Validate clean recovery and communicate limitations. Rebuilding with the same compromised inputs shall not count as remediation.

Evidence: Compromise tracing and clean recovery.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T07-01

Standard p. 31

Service and target identity

Identify production tenants, vehicle/asset targets, actual versions and permissions. Reconcile service-side commands with target-side outcomes. Delivery acknowledgement is not proof of correct installed operation.

Evidence: Inventory and target-state reconciliation.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T07-02 to T07-04

ENTITY / SCOPE / CASE REFERENCE

T07-02 | ESSENTIAL GATE

Standard p. 31

Safe production change

Validate preconditions, staged deployment, stop thresholds and recovery for material changes. Include data, infrastructure and feature flags, not only binaries. Do not use live customers for uncontrolled consequential experiments.

Evidence: Production change and safe rollout evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T07-03

Standard p. 31

Resilience and observation

Test load, dependency loss, stale data, partial failure and state recovery. Monitor user-relevant correctness and tail behaviour with response ownership, not availability alone.

Evidence: Service indicators and failure exercises.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T07-04

Standard p. 31

Customer exit

Provide usable migration, data export, deletion and support transition consistent with obligations. Identify functions that depend on continuing service and protect users against unannounced consequential loss.

Evidence: Exit validation and communicated dependencies.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T08-01 to T08-03

ENTITY / SCOPE / CASE REFERENCE

T08-01

Standard p. 32

Bounded innovation

Define pilot limits, intended use, consequence and evidence needed before production scope. Keep experimental capability outside active claims until implemented, validated and independently assessed.

Evidence: Pilot boundaries and extension gates.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T08-02

Standard p. 32

Long-life support

Assess dependencies, resource constraints, support horizon and migration needs for long-lived vehicles and tools. Preserve necessary evidence and a safe exit plan when suppliers or technologies disappear.

Evidence: Lifecycle and obsolescence plan.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

T08-03 | ESSENTIAL GATE

Standard p. 32

Cryptographic transition

Inventory trust roots, keys and relevant long-lived sensitive data; plan tested migration and revocation with compatibility and recovery. Future-resistant claims shall be evidence-based and shall not substitute for present control.

Evidence: Migration, compatibility and trust-recovery tests.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | T08-04 to IR01-02

ENTITY / SCOPE / CASE REFERENCE

T08-04

Standard p. 32

Responsible progress

Assess accessibility, resource use, human skills and foreseeable misuse of new capability. Measure benefits against a defined baseline and preserve necessary assurance work. Do not market speculative benefits as verified operational results.

Evidence: Impact, benefit and limitation evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR01-01 | ESSENTIAL GATE

Standard p. 32

Adoption before operation

IAF shall record adoption, programme ownership, controlled editions and decision authority before live recognition. Complete launch gates and publish eligibility and process. Prepared documents or pilot participation shall not be represented as an already operational recognition scheme.

Evidence: Adoption, launch approval and operating notice.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR01-02

Standard p. 32

Fair access

Assess eligible organisations consistently regardless of size, geography, membership, sponsorship or commercial importance. Accept legally operating small developers with effective safeguards. Recognition shall not depend on buying consultancy or receiving a favourable commercial recommendation.

Evidence: Eligibility and impartial intake decisions.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR01-03 to IR02-01

ENTITY / SCOPE / CASE REFERENCE

IR01-03 | ESSENTIAL GATE

Standard p. 32

Initial evidence gate

Verify six months of implemented organisation controls, internal audit, management review and three actual completed release/change events per family/delivering hub before initial grant or extension. Governance-only functions demonstrate real oversight cases instead of fictitious client work. Insufficient evidence permits private readiness review only.

Evidence: Actual history, release/change events and assurance records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR01-04

Standard p. 33

Corporate and release boundary

Identify the legal holder, lifecycle responsibilities, families, hubs and support boundaries. Corporate Recognition concerns organisational controls, not certification of each version, AI output or customer integration. Verify competence for actual technical roles without implying a separate personal credential.

Evidence: Holder, family and release-boundary review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR02-01

Standard p. 33

Hub coverage

Assess every delivering hub at initial and renewal and review every hub annually. Physically visit technical facilities handling physical subjects at initial, renewal and annually. A remote-only office may use secure live observation and source review only after an uninvolved reviewer approves adequacy; otherwise require physical access or defer scope.

Evidence: Complete hub map and reasoned visit/remote determination.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR02-02 to IR02-04

ENTITY / SCOPE / CASE REFERENCE

IR02-02 | ESSENTIAL GATE

Standard p. 33

Family and event coverage

Demonstrate every included family at initial/renewal. Annually demonstrate all consequential, new/materially changed and adverse-case families plus $\text{ceil}(\sqrt{N})$ of remaining families, rotating all within three years. Review three actual events per family/responsible hub and challenge relevant role competence; expand for risk.

Evidence: Family coverage, event samples and technical challenges.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR02-03

Standard p. 33

Duration floors

One auditor-day is eight assessment hours excluding travel. Initial/renewal floor is two central days plus one per hub with up to 10 technical personnel, two for 11-50 and three above 50. Add one hub-day per material factor: novel consequential software/AI, continuous multiregion operations, complex critical outsourcing or unresolved systemic risk.

Evidence: Duration, personnel counts and risk additions.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR02-04

Standard p. 33

Adequate observation

Annual floor is one central auditor-day plus one per physical technical facility and half a day per remote-only hub. A physical visit spans at least one full operating day; at least half on-site time covers observation, interviews and witnessing. Do not double-count central/hub hours; add time for sufficient personnel and technical coverage.

Evidence: Actual time, observation and adequacy record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR03-01 to IR03-03

ENTITY / SCOPE / CASE REFERENCE

IR03-01 | ESSENTIAL GATE

Standard p. 33

Assessment team

Appoint at least two competent assessors collectively covering technical governance and the actual technical families, methods and jurisdictions. Verify competence through observed performance. Specialists support accountable assessment and shall not substitute for a missing technical basis.

Evidence: Team competence and assignment record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR03-02 | ESSENTIAL GATE

Standard p. 34

IAF conflict exclusion

Exclude assessors, reviewers and decision-makers with employment, consultancy, ownership or material commercial interests in the case during the preceding 36 months, and longer where residual risk remains. Screen personal interests and separate sales from outcomes. This operator rule is distinct from the organisation's assignment-specific conflict review.

Evidence: Conflict screening and independent resolution.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR03-03

Standard p. 34

Evidence sufficiency

Triangulate original release/change event files, direct technical challenge, observation, client outcomes and adverse evidence. Preserve limitations. Missing essential facts remain Pending or a justified finding; a qualification or client reference alone shall not establish implemented technical quality.

Evidence: Evidence log and contradictory-fact resolution.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR03-04 to IR04-02

ENTITY / SCOPE / CASE REFERENCE

IR03-04

Standard p. 34

Independent technical review

An uninvolved competent reviewer shall verify scope, product/service schedule, applicability, evidence, findings and effective closure before panel referral. Resolve essential gaps and preserve queries. The reviewer shall not become the applicant's consultant or silently rewrite the assessment conclusion.

Evidence: Independent review and resolved queries.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR04-01 | ESSENTIAL GATE

Standard p. 34

Initial grant logic

Every applicable requirement shall be Met and all findings effectively closed before initial grant. Essential safety, integrity, independence, competence and scope gates cannot be offset by scores. NA requires an absent inherent trigger; coherent exclusions shall not conceal a shared failure.

Evidence: Requirement results, exclusions and closed findings.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR04-02

Standard p. 34

Finding classification and clocks

Critical denotes credible serious harm or severe integrity failure; Major systemic or consequential breakdown; Minor an isolated lapse preserving essential assurance. Active Minor closure is due within 90 calendar days; Major requires immediate containment and a 30-day target with suspension review if unresolved. Critical requires immediate protective review. Clocks start at written notice; urgent action starts at awareness.

Evidence: Severity, protection, notice and due dates.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR04-03 to IR05-01

ENTITY / SCOPE / CASE REFERENCE

IR04-03 | ESSENTIAL GATE

Standard p. 34

Independent decision

Three uninvolved competent panel members shall participate in every disposition, with at least two reasoned votes. Grant and restoration also require all applicable gates. Record dissent, exact scope and release-evidence basis, effective/expiry dates and appeal route. Maximum recognition term is three years.

Evidence: Individual votes and authenticated decision.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR04-04

Standard p. 34

Urgent interim suspension

The programme manager and an independent technical lead may authorise proportionate urgent interim suspension. A three-person independent panel shall review it within five business days. Give prompt reasons, affected scope and response route, preserving necessary protection while evidence develops.

Evidence: Interim authority, notice and panel review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR05-01

Standard p. 35

Defined states

Use Applicant, Under Assessment, Corporate Recognition, Restricted, Suspended, Expired and Withdrawn with exact scope and dates. Restricted retains only expressly stated active scope. Restoration is a dated event preserving history; no backdating or silent transfer of personal or corporate coverage is permitted.

Evidence: Status vocabulary and effective history.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR05-02 to IR05-04

ENTITY / SCOPE / CASE REFERENCE

IR05-02

Standard p. 35

Continuing surveillance

Complete surveillance by months 12 and 24 and the annual hub/family coverage in IR02. Renewal is requested at least six months before expiry. Overdue essential coverage requires protective status review; pending renewal or appeal shall not extend the term.

Evidence: Coverage calendar and renewal/status decisions.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR05-03 | ESSENTIAL GATE

Standard p. 35

Current verification

Before launch provide a tested registry and manual fallback showing programme, holder, families, hub scope, version, dates and status. Publish protective changes normally within two business days, sooner for urgent risk. During outage or uncertainty report unavailable/unresolved rather than stale active confirmation.

Evidence: Registry tests, fallback and update history.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR05-04

Standard p. 35

Marks and product claims

License corporate artwork against a valid decision, control product-facing context and monitor misuse. A logo in an application or report shall not imply IAF certification of every release, security guarantee or automated-driving permission. Verify correction after scope change, restriction, suspension or expiry.

Evidence: Licence, product context and removal evidence.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR06-01 to IR06-03

ENTITY / SCOPE / CASE REFERENCE

IR06-01

Standard p. 35

Factual response

Provide evidence-based draft findings and 15 calendar days for factual response, with reasoned extensions where appropriate. Correct supported factual error transparently. Response periods shall not delay necessary urgent protection.

Evidence: Draft report, response and resolution.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR06-02

Standard p. 35

Independent appeal

Allow appeal within 30 calendar days of decision notice. A different three-person competent conflict-free panel decides by at least two reasoned votes. Target outcome within 45 calendar days after complete evidence, explain delay and provide updates. Appeal does not automatically stay protection.

Evidence: Appeal, independent votes and outcome notice.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR06-03

Standard p. 35

Complaint investigation

Provide accessible channels for programme conduct, misleading recognition and technical-integrity concerns. Triage serious risk, assign an uninvolved investigator and protect good-faith reporting. Distinguish technical error, reasonable disagreement and issues outside IAF's remit.

Evidence: Triage, investigation and reasoned response.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR06-04 to IR07-02

ENTITY / SCOPE / CASE REFERENCE

IR06-04

Standard p. 36

Fair disclosure and correction

Give sufficient reasons for meaningful response while protecting justified confidentiality. Correct material procedural or factual error and assess similar cases. IAF shall not imply that recognition makes it the adjudicator or financial guarantor of every client dispute.

Evidence: Disclosure rationale and systemic correction.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR07-01

Standard p. 36

Protected evidence review

Bind IAF personnel and providers to confidentiality, role-based access and lawful transfer controls. Use minimised extracts and protected original review. If essential facts cannot be lawfully verified, defer the affected conclusion rather than claim unrestricted assurance.

Evidence: Access, confidentiality and protected-review record.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR07-02

Standard p. 36

Retention and integrity

Retain organisational release/assurance evidence ten years after last delivery or declared support end, whichever is later; IAF case evidence ten years after expiry/withdrawal. Binding limits and lawful holds apply. Minimise personal data, preserve material corrections and test recovery; long retention does not authorise unnecessary raw telemetry collection.

Evidence: Retention, integrity and lawful exception records.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR07-03 to IR08-01

ENTITY / SCOPE / CASE REFERENCE

IR07-03

Standard p. 36

Incident response

Contain compromise of applicant information or registry integrity, preserve evidence and independently reconcile authoritative records. Notify affected parties under applicable duties. A questionable status record remains unresolved until verified.

Evidence: Incident chronology, reconciliation and notice.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR07-04

Standard p. 36

Traceable decisions

Identify case, role, time, source evidence and authority for every material action. Preserve decisions through staff or platform change. Typed names require supporting authority/authentication; blank templates shall not be presented as issued recognition or approved releases.

Evidence: Case trail and authenticated approvals.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR08-01 | ESSENTIAL GATE

Standard p. 36

Representative pilots

Before live operation complete at least four pilots: a small developer, an engineering/test-tool supplier, a vehicle update operation and a cloud/AI service. Include a failed or contested case. Verify competence, independence, reviewer safeguards, duration, appeal and status correction; close essential gaps before launch.

Evidence: Pilot results and authorised launch decision.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Requirement assessment | IR08-02 to IR08-04

ENTITY / SCOPE / CASE REFERENCE

IR08-02

Standard p. 36

Independent operator assurance

Audit programme operation annually and obtain an independent review at least every three years. Examine competence, conflicts, decision consistency, complaints, protection and registry accuracy. Correct weaknesses and review affected recognition decisions.

Evidence: Annual audit and independent programme review.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR08-03

Standard p. 37

Controlled improvement

Consult relevant technical, customer and user interests, assess emerging methods and actual errors, and publish controlled revisions with effective dates. Guidance and transition notices shall not silently waive essential requirements or invent retrospective conformity.

Evidence: Consultation, impact review and approved changes.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

IR08-04

Standard p. 37

Substantiated global acceptance

Build confidence through transparent scope and verifiable outcomes. Evidence any specific customer, forum, manufacturer or public acceptance separately. Global design and IAF membership shall not be described as universal product approval, legal authority or automatic equivalence.

Evidence: Acceptance evidence and truthful programme claims.

RESULT

Select

FINDING ID

EVIDENCE / RATIONALE / SCOPE LIMITS - USE CONTINUATION FOR DETAIL

Findings, closure and essential gates

ENTITY / SCOPE / CASE REFERENCE

APPLICABLE MODULES, RESULT COUNTS AND ACCEPTED NA REASONS

HISTORY/CASES, RELEASE EVIDENCE, HUB COVERAGE, TECHNICAL CHALLENGE AND ESSENTIAL GATES

FINDINGS, AFFECTED SCOPE, CONTAINMENT, PRIOR-OUTPUT IMPACT AND DEADLINES

VERIFIED CLOSURE, UNRESOLVED EVIDENCE AND COHERENT EXCLUSIONS

ASSESSMENT RECOMMENDATION, LIMITATIONS AND RESPONSIBLE AUDITOR AUTHORIZATION

Independent recognition and exact scope

ENTITY / SCOPE / CASE REFERENCE

FINAL LEGAL ENTITIES, HUBS, SCOPE VERSION AND EVIDENCE MANIFEST

THREE UNINVOLVED PANEL MEMBERS, COMPETENCE, CONFLICTS AND INDIVIDUAL VOTES

ALL APPLICABLE MET; GRANT/DEFER/REFUSE/RESTRICT, REASONS AND DISSENT

EFFECTIVE/EXPIRY WITHIN THREE YEARS AND ANNUAL HUB/FAMILY COVERAGE AND SURVEILLANCE DATES

AUTHORIZED CLAIMS, VERIFICATION, DECISION NOTICE, APPEAL DEADLINE AND SIGNATURE

Continuation and supporting detail

ENTITY / SCOPE / CASE REFERENCE

PARENT FIELD, REQUIREMENT OR RECORD ID / CONTINUATION NUMBER

FULL RESPONSE, SOURCE REFERENCES, RATIONALE AND LIMITATIONS

PREPARED BY / ROLE / DATE / AUTHORIZATION