

IAF / TECHNICAL ASSURANCE WORKBOOK

Digital Systems Integrity

Assessment checklist

SOURCE-REFERENCED / INTERACTIVE PDF

First Edition | Technical Working Draft
Technical review and pilot use; source adoption remains pending.

ORGANIZATION / CLIENT

ASSESSMENT REFERENCE

ASSESSMENT DATE / PERIOD

LEAD ASSESSOR / TEAM

SITE / LOCATION

ASSESSED OBJECT / SYSTEM / CONFIGURATION

ASSESSMENT PURPOSE AND CLAIMED SCOPE

295

check records

28

mapped sections

40

source pages

Scope, applicability & evidence rules

INTEGRITY PROFILE: IP1 / IP2 / IP3 AND RATIONALE

VEHICLES, ASSETS, SOFTWARE, MODELS AND RELEASE BASELINE

TRUST BOUNDARIES, PRIVILEGED SERVICES AND DEPENDENCIES

REGIONS, SUPPORTED LIFECYCLE AND DEPLOYMENT CONDITIONS

THREAT / RISK REGISTER AND ANNEX C PARAMETERS

ANNEX B VERIFICATION CATALOGUE AND TEST AUTHORIZATION

APPLICABILITY REGISTER / EXCLUSIONS / APPROVING REVIEWER

STANDARD-SPECIFIC ASSESSMENT RULE

Declare the IP1/IP2/IP3 profile and asset/configuration boundary. Verify applicable DSI requirements, Annex B tests and the Annex C parameter schedule. Missing mandatory evidence prevents a positive conclusion for the affected scope.

HOW TO COMPLETE EACH CHECK

Pass	All applicable source conditions are met by identified evidence.
Fail	An applicable requirement or required protective gate is not met.
Not demonstrated	Evidence is absent, incomplete, invalid or inconclusive; this is not a pass.
Not applicable	The trigger is absent and the rationale and reviewer are recorded.

Source schedules, methods and record templates are assessed for correct application. For adverse conditions, verify prevention or effective closure. Do not treat illustrative values as mandatory limits. No result is preselected and no overall result is calculated.

Requirement map

Checklist identifiers are workbook record numbers. Source clause numbers, native requirement IDs and PDF page references are preserved separately. Several records may address one source clause.

SOURCE SECTION	CHECKS	PDF PAGE
1 Scope and intended outcomes	3	5
2 Interpretation and mandatory rules	6	6
4 Scope declaration and integrity profiles	9	7
5 Governance and engineering accountability	7	9
6 Threat analysis and risk decisions	17	11
7 Asset identity and digital configuration	7	15
8 Architecture and trust boundaries	8	17
9 Identity cryptography and trust renewal	11	19
10 Secure software development	8	22
11 Build and release provenance	7	24
12 Supplier and service dependencies	6	26
13 OTA and other update integrity	12	27
14 Cloud mobile applications and remote operations	7	30
15 Privacy and responsible data use	12	32
16 Cyber resilience and safe recovery	8	35
17 Vulnerability handling and corrective updates	8	37
18 Monitoring incident response and evidence	8	39
19 Artificial intelligence and adaptive software integrity	10	41
20 Connected interfaces and automated mobility	9	43
21 Production diagnostics repair and transfer	7	46
22 Support continuity and end of life	7	47
23 Verification and technical assessment	9	49
24 Conformity decisions and change control	9	51
25 Digital integrity passport and transparency	6	54
26 Performance review and technology evolution	6	55
Annex A Required evidence register	28	57
Annex B Minimum verification catalogue	33	64
Annex C Acceptance parameters and response limits	27	76

Source control & use of the workbook

CONTROLLED SOURCE

IAF_Digital_Systems_Integrity_First_Edition_Corporate(1).pdf

First Edition | Technical Working Draft

Source length: 40 pages. Checklist revision: 1.0, dated 15 September 2026.

SOURCE SHA-256

b4db89c703f79f1a901c6b802d3f4f7e7fe61ddaea241064f5f491bb5ccde2c4

INTERPRETATION AND COVERAGE

This workbook reproduces source requirement text and source schedule entries as assessment criteria. Long clauses and schedules may have several separately numbered check records. A clause is not complete until every applicable record and required source condition has been dispositioned.

Read each record with its complete source clause, definitions, referenced methods, numerical rules and applicability conditions. The source document controls if an extraction, layout or interpretation issue is found. Record the discrepancy and resolve it before a positive conclusion.

Normative annexes in the source are included where applicable. Informative annexes are reading aids and do not independently create conformity obligations. Context-only main clauses and definitions without assessment duties are read with the requirements.

Assign responsibility for each applicable record in the controlled applicability register. Duties addressed to IAF or an assessment body must be reviewed against that role. They are not automatically duties of a manufacturer, operator or other applicant.

Record document/test IDs, revision, sample/configuration, measured result and limit where relevant. Explain every Fail, Not demonstrated and Not applicable result. Add a finding ID for any required action.

Text areas are sized for concise entries and limit input to reduce hidden content. Use the continuation sheet or an identified external evidence record for longer notes. Save a local copy, reopen it and check entered values before issuing the completed workbook.

Every Fail or unresolved critical gate requires the relevant scope to remain blocked. An observation is not a substitute for a failed requirement. A positive pilot conclusion is not certification, a product authorization or permission to use an IAF mark.

INFORMATIVE READING SUPPORT

Annex D, Annex E, Annex F

Requirements & evidence

1 | Scope and intended outcomes

CHECK 0001 | DSI-01-01

Source p. 4

Scope and intended outcomes

The organization shall demonstrate that digital assets perform only authorized functions within the declared operating conditions and that security controls do not introduce unacceptable hazards. A valid signature, authenticated connection or successful test alone shall not be treated as evidence that an action is safe or its content is correct.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0002 | DSI-01-02

Source p. 4

Scope and intended outcomes

The lifecycle shall include concept, sourcing, design, development, verification, production, release, deployment, operation, repair, ownership transfer, repurposing, support termination and disposal. For existing products, unavailable historical evidence shall be identified and addressed through reconstruction and verification; it shall not be presumed to exist.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0003 | DSI-01-03

Source p. 4

Scope and intended outcomes

The organization shall identify applicable market obligations and contractual duties separately and reconcile them with the engineering controls. A conformity claim under this standard shall not be represented as vehicle market authorization, comprehensive functional safety approval, or a guarantee against all attacks. Mechanical crashworthiness, general driving performance and overall environmental performance are outside the assessment except where digital behaviour influences them. Artificial intelligence integrity requirements address controlled development and use; they do not by themselves establish that an automated driving function is safe in all conditions.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

2 | Interpretation and mandatory rules

CHECK 0004 | 2

Source p. 4

Interpretation and mandatory rules

"Shall" establishes a requirement. "Shall not" establishes a prohibition. "Should" expresses a recommendation. "May" expresses permission. "Can" describes a capability or possibility. Requirements identified by DSI numbers and Annexes A, B and C are normative. Annexes D, E and F are informative; their examples do not establish additional conformance obligations.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0005 | DSI-02-01

Source p. 4

Interpretation and mandatory rules

The organization shall maintain a clause-level applicability statement covering every numbered requirement and every applicable test in Annex B. Each entry shall state applicable or not applicable, the responsible owner, the implementation, the evidence identifier and the assessment result.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0006 | DSI-02-02

Source p. 4

Interpretation and mandatory rules

A not-applicable decision shall identify the absent function, interface or activity and the evidence establishing its absence. Outsourcing, supplier confidentiality, low production volume, cost and lack of evidence shall not alone justify non-applicability. The assessor shall challenge omissions against actual architecture and behaviour.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0007 | DSI-02-03

Source p. 5

Interpretation and mandatory rules

An alternative implementation shall satisfy the same mandatory outcome and acceptance criteria with equivalent or stronger evidence. It shall be justified, reviewed independently of its design author, and recorded before release. This provision shall not waive a numerical minimum, prohibited behaviour, release gate or independent review requirement.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0008 | DSI-02-04

Source p. 5

Interpretation and mandatory rules

Every organization-selected limit shall be recorded in the parameter declaration of Annex C before testing. The declaration shall include units, operating conditions, uncertainty, justification, owner and approval. A value shall not be relaxed after a failed test without an engineering change assessment and repetition of affected tests.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0009 | DSI-02-05

Source p. 5

Interpretation and mandatory rules

"All" and "100 percent" shall apply to the documented in-scope population, whose completeness shall be verified. Sampling shall not silently redefine the population. An unresolved applicability decision or missing mandatory evidence shall prevent a conformant decision for the affected scope.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

4 | Scope declaration and integrity profiles

CHECK 0010 | DSI-04-01

Source p. 6

Scope declaration and integrity profiles

The scope declaration shall identify legal entity, engineering sites, operational responsibilities, product families, hardware variants, software releases, regions, deployment environments, associated services and supported lifecycle stages. It shall show all external dependencies capable of affecting an in- scope claim.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0011 | DSI-04-02

Source p. 6

Scope declaration and integrity profiles

The organization shall identify the claim as a complete vehicle platform, defined subsystem, component, service, or organizational process. A component or process result shall not be promoted as complete vehicle conformity. Integration assumptions shall be delivered with every partial-scope result.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0012 | DSI-04-03 | part 1/4

Source p. 6

Scope declaration and integrity profiles

Integrity profiles shall be assigned using the criteria below. All profiles shall implement applicable baseline requirements. A higher profile increases assurance depth; it does not imply that another profile may omit necessary controls.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0013 | DSI-04-03 | source schedule row | part 2/4

Source p. 6

IP1

Profile: IP1

Assignment criteria: No credible route to essential-function interference, high-impact privacy harm or fleet propagation; boundaries are demonstrated.

Additional assurance: Independent internal review and baseline verification.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0014 | DSI-04-03 | source schedule row | part 3/4

Source p. 6

IP2

Profile: IP2

Assignment criteria: Connected services, remote functions, valuable credentials or sensitive personal data; compromise can cause material harm without meeting IP3 criteria.

Additional assurance: Assessment team independent of the delivery team; adversarial integration tests.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0015 | DSI-04-03 | source schedule row | part 4/4

Source p. 7

IP3

Profile: IP3

Assignment criteria: Credible influence on essential functions, remote actuation, automated driving authority, release- signing roots or fleet-wide privileged operations.

Additional assurance: Organizationally independent technical assessment; all relevant high-consequence attack paths exercised; recovery and fleet containment exercises.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0016 | DSI-04-04

Source p. 7

Scope declaration and integrity profiles

The highest applicable profile shall govern a shared trust boundary or common control unless isolation is demonstrated. A gateway, build service or identity system that can undermine an IP3 function shall receive IP3 assurance for that dependency even if it is located outside the vehicle.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0017 | DSI-04-05

Source p. 7

Scope declaration and integrity profiles

The scope shall declare whether OTA, AI, V2X, charging control, remote driving, biometrics, third- party applications, digital keys and continuous learning are present. The corresponding conditional requirements shall apply whenever their triggering capability exists, including dormant capabilities activatable after sale.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0018 | DSI-04-06

Source p. 7

Scope declaration and integrity profiles

The organization shall reassess scope and profile after every material change. An integration supplier shall receive the assumptions needed to reassess its own risk, including support limitations and known residual vulnerabilities.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

5 | Governance and engineering accountability

CHECK 0019 | DSI-05-01

Source p. 7

Governance and engineering accountability

Senior management shall appoint an accountable digital integrity owner with authority to stop release or deployment and obtain remediation resources. Product security, safety, privacy, software release and operations responsibilities shall be assigned with named deputies and escalation routes.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0020 | DSI-05-02

Source p. 7

Governance and engineering accountability

The organization shall maintain a lifecycle integrity plan defining deliverables, review gates, staffing, competence, supplier responsibilities, test environments, operating resources and support funding. Release pressure shall not override unresolved mandatory gates.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0021 | DSI-05-03

Source p. 7

Governance and engineering accountability

Personnel performing threat analysis, secure development, cryptography, privacy assessment or adversarial testing shall demonstrate competence appropriate to their tasks through assessed work, supervised practice or relevant experience. Competence shall be reviewed when duties or technologies materially change.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0022 | DSI-05-04

Source p. 7

Governance and engineering accountability

Authoring, approval and deployment authority shall be separated for production signing, trust- root changes and fleet-wide commands. At least two independently authenticated persons shall approve these actions, except for pre-authorized automated actions restricted by tested policy and independent limits.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0023 | DSI-05-05

Source p. 7

Governance and engineering accountability

Risk acceptance shall state affected assets, consequences, alternatives, constraints, owner, review date and invalidating triggers. No individual shall approve their own unreviewed risk analysis. Risk acceptance shall not authorize noncompliance with a mandatory prohibition.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0024 | DSI-05-06

Source p. 7

Governance and engineering accountability

Evidence shall be protected against unauthorized alteration, deletion and backdating. Access shall follow least privilege, with recorded changes and a retention schedule covering the support period and any longer applicable duty. Personal data within evidence shall be minimized and managed separately from technical retention needs.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0025 | DSI-05-07

Source p. 8

Governance and engineering accountability

Internal audits shall examine implementation and actual product behaviour at least once per 12 months. IP3 operations shall additionally review privileged access, exposure and open risks at least once per 6 months. Management shall track corrective actions to verified closure.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

6 | Threat analysis and risk decisions

CHECK 0026 | DSI-06-01

Source p. 8

Threat analysis and risk decisions

Threat analysis shall begin before architecture approval and cover assets, users, attackers, interfaces, data flows, dependencies, privileges, physical access and credible misuse throughout the lifecycle. Assumptions about connectivity, trust, vehicle state and access duration shall be explicit.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0027 | DSI-06-02

Source p. 8

Threat analysis and risk decisions

Analysis shall consider remote and local attackers, malicious insiders, compromised suppliers, stolen service tools, hostile tenants, compromised authorized accounts and attacks using valid credentials. It shall include simultaneous failures, common dependencies and loss of trusted time or revocation services.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0028 | DSI-06-03 | part 1/9

Source p. 8

Threat analysis and risk decisions

Consequences shall be rated separately for physical safety, privacy, operation, financial harm and fleet propagation. The highest justified consequence shall drive treatment. Low financial impact shall not offset serious physical or privacy harm.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0029 | DSI-06-03 | source schedule row | part 2/9

Source p. 8

I1 Limited

Impact: I1 Limited

Decision meaning: Reversible inconvenience with no meaningful essential-function, sensitive-data or fleet effect.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0030 | DSI-06-03 | source schedule row | part 3/9

Source p. 8

I2 Material

Impact: I2 Material

Decision meaning: Recoverable service disruption, limited data harm or material repair and financial consequences.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0031 | DSI-06-03 | source schedule row | part 4/9

Source p. 8

I3 Severe

Impact: I3 Severe

Decision meaning: Potential serious injury contribution, severe personal-data harm, sustained essential-service disruption or substantial fleet propagation.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0032 | DSI-06-03 | source schedule row | part 5/9

Source p. 8

I4 Extreme

Impact: I4 Extreme

Decision meaning: Potential fatal or multiple serious injuries, systemic fleet loss of control, or irreversible and widespread severe harm.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0033 | DSI-06-03 | source schedule row | part 6/9

Source p. 8

F1 Constrained

Feasibility: F1 Constrained

Required reasoning: Several demonstrated independent barriers and demanding access or resources; assumptions remain defensible.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0034 | DSI-06-03 | source schedule row | part 7/9

Source p. 8

F2 Plausible

Feasibility: F2 Plausible

Required reasoning: Specialist capabilities or restricted access are required and reasonably obtainable.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0035 | DSI-06-03 | source schedule row | part 8/9

Source p. 8

F3 Accessible

Feasibility: F3 Accessible

Required reasoning: A motivated attacker can obtain the required access and resources with limited barriers.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0036 | DSI-06-03 | source schedule row | part 9/9

Source p. 8

F4 Demonstrated

Feasibility: F4 Demonstrated

Required reasoning: Reproducible exploitation exists or credible active exploitation affects the relevant configuration.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0037 | DSI-06-04

Source p. 8

Threat analysis and risk decisions

The initial priority shall be the impact number multiplied by the feasibility number: 1 to 3 Low, 4 to 7 Moderate, 8 to 11 High, and 12 to 16 Critical. I4 scenarios shall be at least High. An actively exploited path to essential-function control, production signing or uncontrolled privileged fleet actions shall be Critical regardless of the product. These categories are treatment priorities, not quantitative probabilities.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0038 | DSI-06-05

Source p. 8

Threat analysis and risk decisions

Uncertainty shall be recorded and investigated. Where an uncertain assumption can conceal I3 or

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0039 | I4

Source p. 8

Threat analysis and risk decisions

harm, the assessment shall use the more conservative credible case until evidence resolves it. Absence of public exploitation shall not establish infeasibility.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0040 | DSI-06-06

Source p. 9

Threat analysis and risk decisions

Treatment shall define preventive, detective, containment and recovery controls; link each control to verification evidence; and re-evaluate the complete attack path after implementation. Reducing exposure by disabling a feature shall include checks that it cannot be reactivated without authorization.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0041 | DSI-06-07

Source p. 9

Threat analysis and risk decisions

A release shall contain no known Critical residual scenario and no uncontained, credibly exploitable High residual scenario. Other High residual scenarios shall require demonstrated independent barriers, a time-limited treatment plan and independent approval. A safety or privacy prohibition elsewhere in this standard shall still prevail.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0042 | DSI-06-08

Source p. 9

Threat analysis and risk decisions

Threat analysis shall be updated before material changes, after relevant incidents and when assumptions or attack capabilities change. A periodic review shall occur at least every 12 months, and every 6 months for IP3 scopes.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

7 | Asset identity and digital configuration

CHECK 0043 | DSI-07-01

Source p. 9

Asset identity and digital configuration

The organization shall maintain a controlled inventory of in-scope hardware, software, firmware, models, datasets, calibrations, keys, certificates, services and externally reachable interfaces. Each item shall have an identifier, owner, version or configuration, dependency links and lifecycle status.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0044 | DSI-07-02

Source p. 9

Asset identity and digital configuration

Each release shall include a machine-processable software inventory reconciled with the delivered executable content. Unknown components, binary-only dependencies and incomplete dependency depth shall be explicitly recorded and investigated; they shall not disappear from the inventory because source code is unavailable.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0045 | DSI-07-03

Source p. 9

Asset identity and digital configuration

The inventory shall link executable artifacts to their origin, intended function, supported versions, known vulnerability disposition and deployment population. Cryptographic and AI inventories shall capture the additional fields required by Clauses 9 and 19.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0046 | DSI-07-04

Source p. 9

Asset identity and digital configuration

Released software, policy, model and configuration states shall be identifiable on the product or through a protected service interface. A vehicle identifier shall not be treated as an authentication secret. Publicly readable identifiers shall not grant remote access.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0047 | DSI-07-05

Source p. 9

Asset identity and digital configuration

Unauthorized configuration drift shall be detected at boot, update or a justified runtime checkpoint. The response shall be compatible with the current safety state; immediate shutdown shall not be assumed to be safe.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0048 | DSI-07-06

Source p. 9

Asset identity and digital configuration

Inventory coverage shall include 100 percent of in-scope executable deployment units and production signing identities. The organization shall reconcile build records, deployment manifests and observed instances before release and after material changes.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0049 | DSI-07-07

Source p. 9

Asset identity and digital configuration

Each software inventory shall identify its author, generation time, format and version, generation context, generation tool and version, product baseline, component names, producers, versions, identifiers, digests with algorithm names, license information and dependency relationships. It shall state coverage and unknown values explicitly and shall be authenticated against unauthorized alteration. Changes to the inventory shall be versioned and reconciled with the actual delivered content.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

8 | Architecture and trust boundaries

CHECK 0050 | DSI-08-01

Source p. 10

Architecture and trust boundaries

The architecture shall document trust domains and allowed flows among external interfaces, infotainment, diagnostics, body functions, energy management, motion control, safety functions and backend services. Undocumented cross-domain access shall be denied by default.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0051 | DSI-08-02

Source p. 10

Architecture and trust boundaries

A less trusted domain shall not directly authorize essential-function actuation. Commands crossing the boundary shall be authenticated where technically applicable, explicitly authorized, checked for freshness and constrained by a local integrity envelope independent of the requesting service.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0052 | DSI-08-03

Source p. 10

Architecture and trust boundaries

Every shared compute platform shall enforce separation of privileges, memory, storage, communications and resource consumption. Resource exhaustion and malicious tenants shall be tested against the scheduling and timing limits of essential functions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0053 | DSI-08-04

Source p. 10

Architecture and trust boundaries

Externally supplied data shall be validated for size, structure, range, sequencing, freshness and semantic plausibility before use. Validation shall account for malformed, authenticated-but-false and inconsistent inputs.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0054 | DSI-08-05

Source p. 10

Architecture and trust boundaries

Development ports, diagnostic functions and unused services shall be removed, disabled or access-controlled in production. A production debug session shall require specific authorization, bounded scope and duration, and a durable activity record.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0055 | DSI-08-06

Source p. 10

Architecture and trust boundaries

Safety-related fallback and containment shall not share a single unmitigated compromise path with the control they supervise. Common power, timing, memory, identity and update dependencies shall be analyzed and tested.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0056 | DSI-08-07

Source p. 10

Architecture and trust boundaries

A single compromised user account, service credential or externally connected component shall not permit unrestricted commands across the entire declared fleet. Fleet segmentation and independent authorization boundaries shall limit the declared blast radius.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0057 | DSI-08-08

Source p. 10

Architecture and trust boundaries

Executable boot stages and security-relevant startup configuration shall be verified against authorized integrity evidence before use. The chain of verification shall begin from a protected trust basis and shall include recovery paths. Runtime loading of privileged code shall apply equivalent authorization and integrity checks; verification failure shall invoke the validated state-aware response.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

9 | Identity cryptography and trust renewal

CHECK 0058 | DSI-09-01

Source p. 10

Identity cryptography and trust renewal

Devices, workloads, service personnel and privileged users shall have distinct authenticated identities appropriate to their function. Production devices shall not use a fleet-wide shared authentication secret. Public trust anchors may be shared where their compromise and renewal are controlled.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0059 | DSI-09-02

Source p. 10

Identity cryptography and trust renewal

Keys shall be generated using demonstrably adequate randomness, assigned to defined purposes, protected in storage and use, rotated or renewed as needed, and destroyed when retired. Export of high- value private keys shall be prevented or subject to an independently approved and tested protection mechanism.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0060 | DSI-09-03

Source p. 10-11

Identity cryptography and trust renewal

The organization shall maintain a cryptographic profile containing algorithms, parameter strengths, purposes, libraries, implementation versions, key locations, validity periods, trust chains, revocation behaviour and known limitations. Secrecy of an algorithm shall not be the basis of its claimed strength.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0061 | DSI-09-04

Source p. 11

Identity cryptography and trust renewal

Privileged remote administration shall use phishing-resistant multifactor authentication or a demonstrated equivalent protecting against credential replay and origin impersonation. Machine identities shall use short-lived or equivalently controlled credentials with narrow permissions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0062 | DSI-09-05

Source p. 11

Identity cryptography and trust renewal

Interfaces shall prevent unauthorized downgrade, identity substitution and replay. Nonces, sequence values and trusted freshness mechanisms shall remain sound through reboot, sleep, clock correction and power loss.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0063 | DSI-09-06

Source p. 11

Identity cryptography and trust renewal

Trust-root compromise shall have a documented recovery path that does not rely solely on the compromised signing authority. Recovery shall authenticate a replacement authority, limit affected scope, prevent replay and preserve a recoverable product state.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0064 | DSI-09-07

Source p. 11

Identity cryptography and trust renewal

The organization shall assess long-lived confidentiality and signature trust against foreseeable changes in computational capability, including quantum computation. The assessment shall distinguish data collected now for future decryption from future forgery of software and identity credentials.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0065 | DSI-09-08

Source p. 11

Identity cryptography and trust renewal

IP2 and IP3 designs shall provide and test a migration path for cryptographic algorithms, key formats and trust anchors. Testing shall include larger messages, memory and timing effects, mixed-fleet interoperability, refusal of downgrade and interrupted migration. Where replacement is physically impossible, a declared compensating architecture and lifecycle replacement plan shall be required.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0066 | DSI-09-09

Source p. 11

Identity cryptography and trust renewal

Experimental cryptography shall not become the sole production protection of an IP3 boundary without independent analysis, implementation validation and operational recovery evidence. A claim of quantum readiness shall identify the exact tested migration capability and remaining limitations.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0067 | DSI-09-10

Source p. 11

Identity cryptography and trust renewal

Sensitive data and security-relevant communications shall use confidentiality and integrity protection appropriate to their threat exposure in transit and at rest. Key material shall be separated from protected content, and secrets shall not appear in ordinary logs or diagnostic output. Designs that cannot encrypt a legacy link shall enforce independently verified access and integrity boundaries and shall document the remaining exposure.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0068 | DSI-09-11

Source p. 11

Identity cryptography and trust renewal

For high-value hardware trust boundaries, the threat model shall consider physical extraction, fault injection, side-channel leakage and unauthorized debug access according to credible attacker access. Applicable protection claims shall have representative hardware testing or independent evaluation evidence covering the actual implementation and operating conditions.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

10 | Secure software development

CHECK 0069 | DSI-10-01

Source p. 11

Secure software development

Each security, privacy and resilience requirement shall be traceable to design decisions, implementation items, verification cases and release approval. Requirements affecting essential functions shall also link to the relevant hazard analysis.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0070 | DSI-10-02

Source p. 11

Secure software development

Source repositories shall enforce authenticated access, protected branches, review before integration and recorded changes. Security-sensitive code and policy changes shall receive review by a competent person other than the author.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0071 | DSI-10-03

Source p. 12

Secure software development

The organization shall maintain coding rules covering memory safety, input handling, concurrency, integer behaviour, error handling, privilege use and secret handling. New externally exposed or IP3 code shall use memory-safe implementation where practicable; exceptions shall identify the constrained code, reason, compensating controls and specific tests.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0072 | DSI-10-04

Source p. 12

Secure software development

Development shall include automated source analysis, dependency analysis, secret detection and appropriate dynamic tests. Tool limitations and false-negative risks shall be documented. Unresolved findings shall be dispositioned using Clause 6 rather than hidden through tool exclusions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0073 | DSI-10-05

Source p. 12

Secure software development

Test strategy shall include negative, boundary, misuse, fault-injection and adversarial scenarios alongside correct operation. Security testing shall cover generated code, configurations, scripts and infrastructure definitions, not only compiled application code.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0074 | DSI-10-06

Source p. 12

Secure software development

AI-assisted code shall be subject to the same ownership, review, origin checks and verification gates as other code. Untrusted generated instructions shall not receive privileged build or deployment authority merely because they originate from an assistant.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0075 | DSI-10-07

Source p. 12

Secure software development

Production secrets and identifiable customer records shall not be placed in development data or model prompts without a specific approved need and equivalent protection. Test datasets shall minimize exposure and shall be access-controlled and deleted according to their declared retention.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0076 | DSI-10-08

Source p. 12

Secure software development

Every discovered defect with a security effect shall be assessed for root cause, related components and regression risk. Confirmed defects shall generate regression checks where repeatable testing is possible.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

11 | Build and release provenance

CHECK 0077 | DSI-11-01

Source p. 12

Build and release provenance

The build process shall bind source versions, dependencies, build instructions, toolchain versions, configuration and resulting artifacts into an integrity-protected provenance record. Only approved inputs shall enter a production build.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0078 | DSI-11-02

Source p. 12

Build and release provenance

Build workers shall be isolated from untrusted submissions and production signing authority. Temporary access shall expire, environments shall be reset between trust contexts, and unauthorized outbound access shall be restricted.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0079 | DSI-11-03

Source p. 12

Build and release provenance

Release signing shall occur only after the recorded gates are satisfied. The signing service shall verify the artifact identity and approval state itself; it shall not rely solely on a caller-supplied assertion that testing passed.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0080 | DSI-11-04

Source p. 12

Build and release provenance

IP3 release artifacts shall be independently rebuilt or independently verified against protected provenance, approved inputs and executable content. Where reproducible output is not feasible, the reason and an alternative content-verification method shall be recorded and tested.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0081 | DSI-11-05

Source p. 12

Build and release provenance

Artifact stores shall prevent substitution, unreviewed overwrite and unauthorized deletion. Distribution shall preserve the approved artifact digest and metadata from signing to installation.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0082 | DSI-11-06

Source p. 12

Build and release provenance

The organization shall test compromise of a build worker, dependency source and ordinary release account. The tests shall demonstrate that these compromises alone cannot authorize an unrestricted IP3 release.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0083 | DSI-11-07

Source p. 13

Build and release provenance

Emergency releases shall preserve identity, authorization, integrity, essential regression and recovery checks. Deferred nonessential tests shall be recorded with deadlines and completed before the release is treated as fully verified.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

12 | Supplier and service dependencies

CHECK 0084 | DSI-12-01

Source p. 13

Supplier and service dependencies

Procurement shall assign requirements for secure development, asset transparency, vulnerability notification, update delivery, support duration, incident cooperation, evidence access and retirement. Responsibilities shall extend to relevant subcontractors.

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

CHECK 0085 | DSI-12-02

Source p. 13

Supplier and service dependencies

The integrator shall assess supplier evidence for the delivered version, configuration and use conditions. Supplier attestations shall not replace integration tests or transfer accountability for the complete vehicle claim.

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

CHECK 0086 | DSI-12-03

Source p. 13

Supplier and service dependencies

Dependency inventories shall include executable components, hosted services, model providers, remote administration, signing services and infrastructure control planes. A supplier replacement or service relocation shall trigger a material-change assessment.

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

CHECK 0087 | DSI-12-04

Source p. 13

Supplier and service dependencies

The organization shall establish an actionable response to supplier discontinuation, insolvency, loss of access, signing compromise and support termination. Options shall include replacement, escrow where suitable, service migration, constrained operation or controlled retirement; feasibility shall be demonstrated before dependency acceptance.

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

Requirements & evidence

CHECK 0088 | DSI-12-05

Source p. 13

Supplier and service dependencies

Confidential evidence may be examined under controlled access, but insufficient assessor access shall be recorded as an evidence gap. The assessor shall not infer conformity from inaccessible claims.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0089 | DSI-12-06

Source p. 13

Supplier and service dependencies

Shared or reused components shall be tracked across affected vehicle families. A relevant vulnerability shall trigger population analysis and coordinated remediation across all affected releases, including branches maintained by different suppliers.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

13 | OTA and other update integrity

CHECK 0090 | DSI-13-01

Source p. 13

OTA and other update integrity

Every change delivered to a product shall be governed as an update when it can alter behaviour, authorization, privacy or a risk assumption. This shall include firmware, applications, AI models, calibrations, feature flags, policy, maps used for control and trust credentials, regardless of delivery channel.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0091 | DSI-13-02

Source p. 13

OTA and other update integrity

An integrity-protected update manifest shall identify the artifact, digest, authorized signer, target hardware, allowed source states, resulting state, dependencies, security epoch, validity constraints, installation conditions, recovery method and release approval. Ambiguous targets shall be rejected.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0092 | DSI-13-03

Source p. 13

OTA and other update integrity

Before installation, the receiving system shall verify authenticity, authorization, completeness, freshness, compatibility, available energy, storage and required operating conditions. A package that passes signature verification but fails any required check shall not be activated.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0093 | DSI-13-04

Source p. 13

OTA and other update integrity

Essential-function software shall not be activated during an unsafe vehicle state. Concurrent installation while driving shall be permitted only where isolation, scheduling, power effects and activation controls have been validated for that operating state.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0094 | DSI-13-05

Source p. 14

OTA and other update integrity

Multi-component updates shall maintain a defined compatible state across interruption, restart and partial completion. The update design shall implement transactional activation or an equivalent validated mechanism preventing incompatible component combinations from controlling the vehicle.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0095 | DSI-13-06

Source p. 14

OTA and other update integrity

A failed update shall preserve a validated recoverable state. Recovery may restore a previously approved compatible version or use an approved recovery image. Recovery shall not silently cross below the security epoch or reactivate a known prohibited state.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0096 | DSI-13-07

Source p. 14

OTA and other update integrity

The organization shall test energy interruption, communication loss, storage exhaustion, corrupted packages, stale metadata, wrong targets, revoked authority, incomplete dependencies and failure during each state transition. Annex B defines minimum acceptance evidence.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0097 | DSI-13-08

Source p. 14

OTA and other update integrity

Fleet deployment shall use staged cohorts, predeclared monitoring criteria and automatic or independently authorized pause controls. Cohort size, expansion conditions, observation duration and acceptable failures shall be justified before rollout. A laboratory success shall not alone authorize immediate deployment to the entire fleet.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0098 | DSI-13-09

Source p. 14

OTA and other update integrity

The user or operator shall receive understandable information on purpose, expected duration, vehicle availability, necessary actions, effects on functions and applicable scheduling choices. Changes to optional data use shall require renewed choice where that choice is the processing basis.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0099 | DSI-13-10

Source p. 14

OTA and other update integrity

Deployment records shall distinguish offered, downloaded, verified, installed, activated, failed, recovered and unreachable devices. "Delivered" shall not be counted as "successfully activated." Unreachable devices shall remain visible in the outstanding-risk population.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0100 | DSI-13-11

Source p. 14

OTA and other update integrity

Update refusal, subscription expiry or loss of connectivity shall not secretly disable essential functions. Where continued use becomes unsafe, the organization shall communicate and implement a validated risk response appropriate to vehicle state.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0101 | DSI-13-12

Source p. 14

OTA and other update integrity

Workshop, removable-media and emergency updates shall satisfy the same authorization, target verification, integrity and recovery outcomes as OTA. Physical access shall not itself authorize arbitrary firmware installation.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

14 | Cloud mobile applications and remote operations

CHECK 0102 | DSI-14-01

Source p. 14

Cloud mobile applications and remote operations

Backend services and mobile applications able to read vehicle data or issue commands shall be included in the platform threat model. Authorization shall be checked for each object, vehicle, tenant and operation; possession of an identifier or a valid session shall not grant unrestricted access.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0103 | DSI-14-02

Source p. 14

Cloud mobile applications and remote operations

Remote commands shall be restricted by function, vehicle, operating state, duration and requester role. Commands shall expire, resist replay and be rejected when sequence or state makes execution unsafe. The vehicle shall enforce its local integrity envelope even when the backend is authenticated.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0104 | DSI-14-03

Source p. 14

Cloud mobile applications and remote operations

Tenant and fleet isolation shall be verified using hostile requests from ordinary users, compromised support accounts and service identities. Rate limits shall protect both service availability and vehicle-side resources.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0105 | DSI-14-04

Source p. 15

Cloud mobile applications and remote operations

Mobile applications shall protect credentials and sensitive local records, bind enrollment to verified authority, and revoke access when devices are lost or accounts are transferred. An application update shall not silently broaden vehicle permissions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0106 | DSI-14-05

Source p. 15

Cloud mobile applications and remote operations

Administrative access shall be time-bounded, logged and periodically reviewed. Break-glass access shall require a defined emergency reason, minimum scope, prompt independent review and revocation when the emergency ends.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0107 | DSI-14-06

Source p. 15

Cloud mobile applications and remote operations

Cloud configuration changes, infrastructure deployments and remote feature activations shall pass change control. Separate approval and fleet limits shall apply to commands with common-mode consequences, including immobilization, unlocking and energy dispatch.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0108 | DSI-14-07

Source p. 15

Cloud mobile applications and remote operations

Loss of a region, identity provider, communication carrier, time source or payment service shall be analyzed as a dependency failure. Recovery tests shall establish that essential vehicle behaviour is not dependent on restoring a commercial account or optional subscription.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

15 | Privacy and responsible data use

CHECK 0109 | DSI-15-01

Source p. 15

Privacy and responsible data use

Every personal-data flow shall have a specified purpose, data categories, affected persons, justified processing basis, recipients, access rules, retention limit and deletion method. Linkable vehicle identifiers, location histories, recordings and inferred behaviour shall be treated as personal data where they can relate to a person.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0110 | DSI-15-02

Source p. 15

Privacy and responsible data use

Collection shall be limited to what is necessary for the stated purpose. The design shall evaluate local processing, lower precision, shorter retention and derived features before transmitting raw location, audio, video or biometric information.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0111 | DSI-15-03

Source p. 15

Privacy and responsible data use

Optional analytics, advertising, profiling and secondary model training shall be disabled by default until the required affirmative choice or other demonstrated applicable authority exists. A choice for an optional purpose shall not be bundled with access to an unrelated essential function.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0112 | DSI-15-04

Source p. 15

Privacy and responsible data use

Information shall be accessible to drivers, passengers, rental users and other affected persons through means appropriate to the interaction. Notices and controls shall identify material sensor activity, data sharing and changes in purpose without relying solely on a lengthy account document.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0113 | DSI-15-05

Source p. 15

Privacy and responsible data use

Where processing relies on consent, withdrawal shall be as easy as granting it and shall stop future optional processing at the next applicable processing point. Withdrawal shall be propagated to recipients and offline devices through a controlled mechanism. Data retention on another justified basis shall be explained and restricted.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0114 | DSI-15-06

Source p. 15

Privacy and responsible data use

Access, correction, export, restriction and deletion requests shall be authenticated proportionately and processed through a tracked workflow within applicable deadlines. Identity verification shall not collect excessive additional data. Backup restoration shall reapply deletion and restriction records before renewed use.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0115 | DSI-15-07

Source p. 15

Privacy and responsible data use

Occupant monitoring and biometric systems shall restrict raw recordings, templates and inferred sensitive attributes. Children, incidental passengers and bystanders shall be considered in the impact assessment. Safety monitoring shall not automatically justify commercial reuse.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0116 | DSI-15-08

Source p. 16

Privacy and responsible data use

Ownership transfer, return of a rented vehicle and removal of a shared driver shall revoke prior digital keys, remote access, pairing and personal profiles. Reset shall be verified in the vehicle, applications and relevant backend services; the former owner shall not retain location access.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0117 | DSI-15-09

Source p. 16

Privacy and responsible data use

Precise location and remote access features shall be assessed for stalking, coercive control and unauthorized household access. Removal of a shared user shall prevent covert continued access. Notifications shall be designed so they do not expose a vulnerable person's new location or create additional foreseeable harm.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0118 | DSI-15-10

Source p. 16

Privacy and responsible data use

Data processors and onward recipients shall receive purpose and retention restrictions. Cross- border hosting and access shall be evaluated against applicable duties, and material changes shall trigger renewed assessment. This standard shall not be used to presume that a transfer is permitted.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0119 | DSI-15-11

Source p. 16

Privacy and responsible data use

Claims of anonymity shall be supported by reidentification analysis using realistic auxiliary information. Pseudonymous data shall not be presented as anonymous merely because direct names are removed.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0120 | DSI-15-12

Source p. 16

Privacy and responsible data use

Privacy verification shall trace seeded test data through collection, transmission, access, retention, export and deletion. Privacy settings shown to users shall match observed traffic and stored records under connected, disconnected and reset conditions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

16 | Cyber resilience and safe recovery

CHECK 0121 | DSI-16-01

Source p. 16

Cyber resilience and safe recovery

For each essential function, the organization shall define its authorized operating envelope, tolerated disruption, failure-detection needs, fallback behaviour and maximum safe response time. These parameters shall be derived from hazard and operational analysis rather than a universal network timeout.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0122 | DSI-16-02

Source p. 16

Cyber resilience and safe recovery

The product shall retain the essential capability needed to reach or maintain a justified safe state during loss of cloud, network, positioning, identity or payment services. A remote-dependent automated service shall locally perform its validated contingency response; continued autonomous travel shall not be assumed safe.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0123 | DSI-16-03

Source p. 16

Cyber resilience and safe recovery

Security controls shall not cause an unsafe reboot, sudden loss of steering or braking, unsafe energy interruption, trapping of occupants or uncontrolled actuator command. Containment shall be state- aware and verified with the relevant engineering disciplines.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0124 | DSI-16-04

Source p. 16

Cyber resilience and safe recovery

The architecture shall bound resource starvation, repeated reconnection, crash loops, malicious event floods and corrupted stored states. Failure of optional services shall not exhaust resources reserved for essential functions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0125 | DSI-16-05

Source p. 16

Cyber resilience and safe recovery

Recovery assets shall have protected integrity, appropriate separation and a tested restoration path. Recovery shall re-establish trusted software, configuration, identity and restrictions; simply restarting a compromised state shall not count as recovery.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0126 | DSI-16-06

Source p. 16

Cyber resilience and safe recovery

Fleet exercises shall test simultaneous credential revocation, control-plane outage and compromised update distribution. Measured containment shall remain within the predeclared blast radius and shall not require unsafe commands to unaffected vehicles.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0127 | DSI-16-07

Source p. 17

Cyber resilience and safe recovery

The organization shall define detection, containment, restoration and evidence-preservation times in Annex C. Safety response shall complete within its engineered time budget. Administrative incident deadlines shall not be used as permissible delay for an immediate vehicle safety response.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0128 | DSI-16-08

Source p. 17

Cyber resilience and safe recovery

Resilience testing shall include degraded power, temperature and communication conditions within the declared product limits. A design that only recovers with ideal power and uninterrupted connectivity shall not support a broader claim.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

17 | Vulnerability handling and corrective updates

CHECK 0129 | DSI-17-01

Source p. 17

Vulnerability handling and corrective updates

A publicly accessible vulnerability reporting channel shall remain available throughout support. Reports shall receive an identifier, secure handling, acknowledgement and a stated coordination process. The organization should support responsible research through clear testing boundaries and constructive communication.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0130 | DSI-17-02

Source p. 17

Vulnerability handling and corrective updates

Every credible report shall be triaged against deployed and supported configurations, including reachability, required privileges, compensating controls and fleet scope. A generic severity label or component name match shall not replace product-specific analysis.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0131 | DSI-17-03

Source p. 17

Vulnerability handling and corrective updates

Response clocks shall begin at credible awareness, including actionable supplier notice or internal detection. Classification and clock-start decisions shall be recorded. Reclassification shall not reset elapsed time or conceal a missed deadline.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0132 | DSI-17-04

Source p. 17

Vulnerability handling and corrective updates

The organization shall meet the triage, interim-control and correction-plan deadlines in Annex C. When no safe interim control is available, the condition shall remain unresolved and shall be escalated immediately; a documented explanation shall not convert a failed requirement into conformity.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0133 | DSI-17-05

Source p. 17

Vulnerability handling and corrective updates

A correction shall undergo proportionate regression, compatibility, security and recovery testing. Remediation priority shall consider the danger of both exploitation and deployment. An unsafe patch shall not be installed merely to meet an administrative deadline.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0134 | DSI-17-06

Source p. 17

Vulnerability handling and corrective updates

Advisory information shall identify affected products, practical mitigations, available updates, user actions and remaining limitations without unnecessarily enabling exploitation. Disclosure timing shall consider active harm, remediation availability and applicable reporting duties.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0135 | DSI-17-07

Source p. 17

Vulnerability handling and corrective updates

Closure shall require evidence that the affected state is removed or effectively contained in the relevant population. Unreachable vehicles, declined installations and unsupported branches shall be separately reported with their residual exposure.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0136 | DSI-17-08

Source p. 17

Vulnerability handling and corrective updates

Recurring vulnerabilities shall trigger root-cause improvement in architecture, development or supplier controls. A successful patch shall not close a systemic process failure without evidence of corrective action.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

18 | Monitoring incident response and evidence

CHECK 0137 | DSI-18-01

Source p. 17

Monitoring incident response and evidence

Monitoring shall cover threats relevant to the scope, including unauthorized commands, identity anomalies, boot integrity failures, update rejection, cross-domain access and abnormal fleet activity. Collected telemetry shall be proportionate and shall not depend on continuous raw cabin recording.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0138 | DSI-18-02

Source p. 18

Monitoring incident response and evidence

Security events shall have reliable ordering, source identity, integrity protection and access controls. Where trusted clock time is unavailable, the system shall record clock uncertainty and preserve event sequence rather than fabricate precise timing.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0139 | DSI-18-03

Source p. 18

Monitoring incident response and evidence

Monitoring pipelines shall detect their own loss of coverage and resist forged, suppressed or duplicated events. The organization shall test alert delivery under service failure and shall distinguish "no event observed" from "no monitoring available."

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0140 | DSI-18-04

Source p. 18

Monitoring incident response and evidence

An incident plan shall assign technical command, safety decisions, privacy decisions, communications, supplier coordination and operational recovery. IP3 scopes shall maintain an on-call response capability able to act at any time.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0141 | DSI-18-05

Source p. 18

Monitoring incident response and evidence

Response actions shall preserve essential functions, restrict further compromise and protect necessary evidence. Collection tools shall not overwrite relevant records or expose unrelated personal information without a justified need.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0142 | DSI-18-06

Source p. 18

Monitoring incident response and evidence

Notification workflows shall identify affected users, partners and competent authorities where applicable, record the basis and deadline, and preserve the content sent. The standard's engineering deadlines shall not replace shorter applicable notification duties.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0143 | DSI-18-07

Source p. 18

Monitoring incident response and evidence

The organization shall exercise a complete incident scenario at least every 12 months, and every 6 months for IP3 scopes. Exercises shall include an unavailable primary responder, a supplier handoff, a safety- sensitive decision and recovery verification.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0144 | DSI-18-08

Source p. 18

Monitoring incident response and evidence

A post-incident review shall reconstruct events and assumptions, assess containment performance and assign improvements with owners and due dates. Public or customer statements shall distinguish confirmed facts, current uncertainty and planned actions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

19 | Artificial intelligence and adaptive software integrity

CHECK 0145 | DSI-19-01

Source p. 18

Artificial intelligence and adaptive software integrity

Each deployed model shall have an identified owner, version, intended function, authority, operating limits, input assumptions, dependencies and monitoring plan. The model record shall distinguish development data, evaluation data and live operational inputs.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0146 | DSI-19-02

Source p. 18

Artificial intelligence and adaptive software integrity

Training and evaluation assets shall have documented provenance, authorization for use, transformation history and access controls. Data contamination, duplicate evaluation items and dependence between training and testing shall be investigated before performance evidence is accepted.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0147 | DSI-19-03

Source p. 18

Artificial intelligence and adaptive software integrity

The organization shall evaluate poisoning, adversarial inputs, model substitution, extraction, privacy leakage and manipulation of external content according to the model's role. Results shall include unsuccessful and inconclusive cases, relevant limitations and the defended operating envelope.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0148 | DSI-19-04

Source p. 18

Artificial intelligence and adaptive software integrity

A generative model or agent shall not have direct unrestricted authority over motion control, safety settings, production signing or fleet-wide commands. A separate policy enforcement mechanism shall validate identity, intent, permissions, command parameters and operating state before any authorized action.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0149 | DSI-19-05

Source p. 18

Artificial intelligence and adaptive software integrity

External text, retrieved content, diagnostic files and sensor-derived instructions shall be treated as untrusted data. Tests shall establish that such content cannot grant new permissions, reveal protected credentials or override the independent action boundary.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0150 | DSI-19-06

Source p. 19

Artificial intelligence and adaptive software integrity

A model update, prompt-policy change, retrieval-source change or tool-permission change shall undergo impact analysis and applicable release gates. Model drift shall not be used as an explanation for unapproved changes to safety or privacy authority.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0151 | DSI-19-07

Source p. 19

Artificial intelligence and adaptive software integrity

Continuous or federated learning shall be limited to a prevalidated adaptation envelope with protected provenance, participant controls, poisoning defenses, monitoring and a tested rollback or freeze capability. Adaptation outside that envelope shall be treated as a new release. IP3 actuation policy shall not self-expand its authority in service.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0152 | DSI-19-08

Source p. 19

Artificial intelligence and adaptive software integrity

AI performance and robustness limits shall be declared by scenario and relevant operating conditions before testing. A single average accuracy shall not conceal failure in a safety-relevant subgroup, rare condition or hostile-input category.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0153 | DSI-19-09

Source p. 19

Artificial intelligence and adaptive software integrity

When uncertainty, drift or input conditions exceed the approved envelope, the system shall use its validated fallback, request appropriate human involvement or stop the affected function safely. Human intervention shall not be credited unless the person has sufficient information, competence and response time.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0154 | DSI-19-10

Source p. 19

Artificial intelligence and adaptive software integrity

Reproducing a decision shall use the available model version, relevant configuration and minimum necessary input record. Claims of explanation shall state their limits and shall not substitute for evidence that prohibited actions are prevented.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

20 | Connected interfaces and automated mobility

CHECK 0155 | DSI-20-01

Source p. 19

Connected interfaces and automated mobility

Each external mobility interface shall document its trust assumptions, authorized operations, message limits and failure response. Scope shall include charging, V2X, positioning, digital keys, remote assistance, teleoperation and third-party applications where present.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0156 | DSI-20-02

Source p. 19

Connected interfaces and automated mobility

Authenticated V2X messages shall be checked for freshness, location consistency and plausibility before they influence driving. A valid sender credential shall not establish that a claimed road event is true. Essential decisions shall use corroboration or a validated conservative response.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0157 | DSI-20-03

Source p. 19

Connected interfaces and automated mobility

Positioning and time-dependent functions shall detect or tolerate spoofed, delayed, conflicting or unavailable signals within declared limits. The organization shall test behaviour when the apparent position remains plausible but slowly diverges.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0158 | DSI-20-04

Source p. 19

Connected interfaces and automated mobility

Charging and bidirectional energy functions shall authenticate relevant parties, separate payment from physical protection, bound power requests and validate command freshness. A compromised charging service shall not override local thermal, electrical or vehicle-state limits.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0159 | DSI-20-05

Source p. 19

Connected interfaces and automated mobility

Digital keys shall support verified enrollment, role-limited sharing, expiration, revocation and ownership transfer. Proximity-based access shall consider relay and ranging manipulation. Emergency entry and occupant egress shall remain compatible with safety needs.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0160 | DSI-20-06

Source p. 19

Connected interfaces and automated mobility

Remote driving or assistance shall distinguish advice from control authority, identify the responsible operator, define latency and link-quality limits, and record authority transfer. Loss of link or uncertain authority shall trigger the locally executable validated contingency response.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0161 | DSI-20-07

Source p. 20

Connected interfaces and automated mobility

Cooperative manoeuvres, platooning and shared perception shall not permit a compromised participant to issue unchecked motion commands to peers. Membership change, conflicting messages and abrupt participant withdrawal shall be tested.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0162 | DSI-20-08

Source p. 20

Connected interfaces and automated mobility

Third-party applications and aftermarket devices shall receive the minimum permitted data and functions. Installation, permission changes, removal and revocation shall preserve domain isolation and shall not bypass update control.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0163 | DSI-20-09

Source p. 20

Connected interfaces and automated mobility

Satellite and future communication services shall remain external dependencies subject to the same identity, freshness, denial-of-service and outage analysis. A new communication technology shall not be presumed trusted because it is novel or has greater bandwidth.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

21 | Production diagnostics repair and transfer

CHECK 0164 | DSI-21-01

Source p. 20

Production diagnostics repair and transfer

Production processes shall provision device identities and approved software through controlled stations with authenticated operators, protected credentials and traceable records. Production and engineering test identities shall be separated.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0165 | DSI-21-02

Source p. 20

Production diagnostics repair and transfer

End-of-line checks shall verify approved executable state, unique device credentials, production access settings and required security functions. Any repair to provisioning shall be logged and reverified before release.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0166 | DSI-21-03

Source p. 20

Production diagnostics repair and transfer

Service tools shall authenticate the tool and authorized operator as appropriate, limit functions to the job, and expire access. Service credentials shall not become transferable master keys for all vehicles.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0167 | DSI-21-04

Source p. 20

Production diagnostics repair and transfer

Replacement components shall be checked for identity, compatibility, approved state and key handling. Reused or remanufactured modules shall undergo data sanitization, secure enrollment and removal of previous ownership links.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0168 | DSI-21-05

Source p. 20

Production diagnostics repair and transfer

Authorized independent repair shall have a controlled access route appropriate to the operation and applicable duties. Security restrictions shall be technically justified, proportionate and documented; repair access shall not grant unrelated personal data or unrestricted remote control.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0169 | DSI-21-06

Source p. 20

Production diagnostics repair and transfer

Resale, lease return, fleet reassignment and export shall trigger a documented handover process covering profiles, remote permissions, digital keys, installed state and support information. Security defects shall not be hidden by resetting visible notifications.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0170 | DSI-21-07

Source p. 20

Production diagnostics repair and transfer

Field modifications and retrofit equipment shall be assessed for new attack paths, electrical effects, data access and update compatibility. The integrity passport shall be updated where the assessed baseline changes.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

22 | Support continuity and end of life

CHECK 0171 | DSI-22-01

Source p. 20

Support continuity and end of life

Before supply, the organization shall declare a security support period or end date, covered products and services, update channels, responsible contact and the method for notifying users of changes. The commitment shall be supportable by supplier contracts, capability and resources.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0172 | DSI-22-02

Source p. 21

Support continuity and end of life

Security support for essential functions and previously supplied security protections shall not be conditional solely on purchasing optional entertainment, analytics or convenience services. Any paid service boundary shall be clearly described without undermining the declared product support commitment.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0173 | DSI-22-03

Source p. 21

Support continuity and end of life

End-of-support planning shall assess installed population, expected remaining use, unresolved vulnerabilities, dependency retirement and feasible protective measures. A notice alone shall not resolve a continuing high-consequence technical risk.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0174 | DSI-22-04

Source p. 21

Support continuity and end of life

Support termination notice shall be provided at least 12 months before the declared end date unless an unforeseeable event prevents that notice. An exception shall trigger immediate notification, management escalation and a risk-managed continuity response. An existing commitment shall not be shortened solely by issuing such a notice.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0175 | DSI-22-05

Source p. 21

Support continuity and end of life

The retirement plan shall provide an approved terminal configuration, controlled disconnection, replacement route, restricted mode or other justified protection. Disabling connectivity shall be checked for effects on emergency, safety, energy and recovery functions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0176 | DSI-22-06

Source p. 21

Support continuity and end of life

Decommissioning shall revoke identities and remote access, erase or cryptographically render inaccessible personal and secret data, close service accounts and update the asset record. Reintroduction into service shall require controlled re-enrollment.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0177 | DSI-22-07

Source p. 21

Support continuity and end of life

Support records and recovery instructions needed by authorized maintainers shall remain accessible for the declared period. Changes of corporate ownership, supplier or service operator shall preserve assigned obligations or establish a documented successor arrangement.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

23 | Verification and technical assessment

CHECK 0178 | DSI-23-01

Source p. 21

Verification and technical assessment

The verification plan shall map every applicable mandatory requirement to document review, inspection, analysis, test or a justified combination. Annex B shall be treated as a minimum test catalogue, supplemented by product-specific threat and hazard cases.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0179 | DSI-23-02

Source p. 21

Verification and technical assessment

Test items shall represent the production hardware, software, configuration, access controls and associated services. Differences from production shall be listed with their effect on validity. A disabled security control shall not be used to obtain an otherwise unrepresentative passing result.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0180 | DSI-23-03

Source p. 21

Verification and technical assessment

The plan shall define preconditions, stimuli, environmental limits, expected outcomes, measurement methods, uncertainty, pass criteria, stopping conditions and safe recovery. Adversarial tests shall be authorized and isolated from uncontrolled public-road or customer effects.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0181 | DSI-23-04

Source p. 21

Verification and technical assessment

Interface coverage shall include every distinct exposed interface class and every materially different trust boundary. Sampling of product variants shall be justified by architectural equivalence, with all exceptions and worst-case variants tested. IP3 high-consequence paths shall not be omitted solely because they are difficult to reproduce.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0182 | DSI-23-05

Source p. 21

Verification and technical assessment

Test results shall record exact versions, actual observations, timestamps, tools, configuration, operator, evidence artifacts and deviations. Test procedures shall be repeatable by a competent assessor without relying on undocumented personal knowledge.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0183 | DSI-23-06

Source p. 22

Verification and technical assessment

Simulations shall document model validity and differences from physical systems. Physical timing, energy interruption and hardware isolation claims shall include representative hardware evidence; simulation alone shall not establish them.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0184 | DSI-23-07

Source p. 22

Verification and technical assessment

Failed or inconclusive mandatory cases shall be investigated and rerun after correction. A result shall not be changed to pass by deleting the failed stimulus or excluding a newly discovered attack path without a valid scope change and complete reassessment.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0185 | DSI-23-08

Source p. 22

Verification and technical assessment

Review independence shall match the assigned profile. IP3 assessment shall be conducted by an organizationally independent team with no responsibility for designing or approving the assessed release. A commercial relationship shall be disclosed and managed so it does not control technical conclusions.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0186 | DSI-23-09

Source p. 22

Verification and technical assessment

Competence records shall cover the scope actually assessed, including automotive state behaviour, software, communications, privacy and cryptography as relevant. Specialists shall be involved when a general assessor cannot validate a material claim.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

24 | Conformity decisions and change control

CHECK 0187 | DSI-24-01

Source p. 22

Conformity decisions and change control

A conformant decision shall require a complete scope and applicability statement, satisfied mandatory requirements, passed applicable mandatory tests, acceptable residual risk, a complete evidence index, required independent review and a signed decision. No weighted score shall compensate for a failed requirement.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0188 | DSI-24-02

Source p. 22

Conformity decisions and change control

Findings shall be classified as Critical when they create immediate or uncontrolled severe harm or a prohibited release condition; Major when a required system or control is absent or ineffective; and Minor when a limited required element is deficient without established systemic failure. Severity shall govern response priority, not permission to leave a requirement unmet.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0189 | DSI-24-03

Source p. 22

Conformity decisions and change control

Any unresolved mandatory nonconformity shall prevent a new conformant decision. Observations and recommendations that do not establish a failed requirement may remain open if clearly separated from nonconformities.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0190 | DSI-24-04

Source p. 22

Conformity decisions and change control

An assessment result shall identify scope, profile, versions, evidence baseline, assessor, decision authority, date, conditions, support status and next planned review. This standard shall not impose a universal fixed certificate term. Continued claims shall depend on maintained conditions and reassessment triggers.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0191 | DSI-24-05

Source p. 22

Conformity decisions and change control

A material change shall trigger an impact analysis before deployment. A delta assessment shall identify what changed, what evidence remains valid and what must be repeated. Changes to trust roots, essential-function authority, AI adaptation limits, major suppliers or the support model shall require independent review.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0192 | DSI-24-06

Source p. 22

Conformity decisions and change control

An active claim shall be restricted, suspended or withdrawn when a critical condition, material unassessed change, unsupported configuration or evidence failure invalidates it. Affected parties shall be informed without presenting a historical result as the current condition.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0193 | DSI-24-07

Source p. 22

Conformity decisions and change control

Restoration shall require verified corrective action, relevant repeat testing and a new recorded decision. Merely submitting an action plan shall not restore a suspended claim.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0194 | DSI-24-08

Source p. 23

Conformity decisions and change control

Public claims shall distinguish self-declaration, independently assessed results and certification under a separately approved scheme. Use of an IAF conformity mark shall require explicit authorization under that scheme; preparation of this standard does not grant mark use.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0195 | DSI-24-09

Source p. 23

Conformity decisions and change control

Complaints and appeals shall be recorded and reviewed by competent persons independent of the contested decision. Security-sensitive details shall be protected while the reasons for the outcome remain reviewable by authorized parties.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

25 | Digital integrity passport and transparency

CHECK 0196 | DSI-25-01

Source p. 23

Digital integrity passport and transparency

A conformity claim shall have a digital integrity passport identifying the accountable organization, assessed object, claim type, scope, profile, baseline versions, decision date, support commitment and current status. The passport may use any machine-processable format satisfying the required semantics.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0197 | DSI-25-02

Source p. 23

Digital integrity passport and transparency

The passport shall link to a controlled evidence index without publicly exposing private keys, exploit details, personal records or confidential architecture. A public view and a restricted technical view shall be separated.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0198 | DSI-25-03

Source p. 23

Digital integrity passport and transparency

Passport updates shall be authenticated and versioned. Historical decisions shall remain distinguishable from the current state. A stale or unverifiable passport shall not be displayed as proof of current conformity.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0199 | DSI-25-04

Source p. 23

Digital integrity passport and transparency

An offline status display shall identify the last verified time and its freshness limit. When that limit is exceeded, status shall be shown as unknown rather than automatically conformant or automatically unsafe.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0200 | DSI-25-05

Source p. 23

Digital integrity passport and transparency

The public view shall state relevant feature dependencies, security contact, available updates, support end and significant restrictions in understandable language. It shall not publish individual vehicle location or personal ownership history.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0201 | DSI-25-06

Source p. 23

Digital integrity passport and transparency

Passport information shall be exportable in a documented format so authorized assessors and successor support providers can interpret it without dependence on one service operator.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

26 | Performance review and technology evolution

CHECK 0202 | DSI-26-01

Source p. 23

Performance review and technology evolution

The organization shall monitor inventory completeness, critical and high exposure, deployment success, unreachable population, containment performance, recovery outcomes, privacy-control failures and open corrective actions. Metrics shall have defined denominators, observation windows and treatment of missing data.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0203 | DSI-26-02

Source p. 23

Performance review and technology evolution

Metrics shall be reported by affected configuration and risk class where aggregation can conceal harm. A high average update success rate shall not conceal an unrecoverable essential-function failure in a small vehicle population.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0204 | DSI-26-03

Source p. 23

Performance review and technology evolution

Threat and technology review shall examine changes in compute capability, communication systems, software architecture, autonomous agents, synthetic data, sensing, remote control and energy coordination. It shall occur at least every 12 months and before introducing a materially new capability.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0205 | DSI-26-04

Source p. 24

Performance review and technology evolution

A new capability shall be assessed through its actual authority, dependencies, failure modes and evidence needs. Where existing test methods cannot substantiate its integrity envelope, deployment authority shall be constrained until suitable verification exists.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0206 | DSI-26-05

Source p. 24

Performance review and technology evolution

The organization shall maintain a forward compatibility and migration plan for cryptography, supported interfaces, recovery tooling and evidence formats. The plan shall identify irreversible hardware constraints and the point at which replacement becomes necessary.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0207 | DSI-26-06

Source p. 24

Performance review and technology evolution

Claims such as continuous trust, autonomous resilience or future readiness shall state the measured capability, operating conditions, validated limits and date. Predictions shall not be presented as tested performance, and automated monitoring shall not be presented as proof that no compromise exists.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

Annex A | Required evidence register

CHECK 0208 | Annex A | part 1/28

Source p. 25

Required evidence register

The accountable organization shall maintain the following evidence for applicable activities. Evidence may be combined in one controlled system if each required content item remains identifiable. Every record shall identify its owner, version, approval state, scope, access classification and retention rule. The register shall link each individual DSI requirement and Annex B test to actual evidence, rather than only to a generic policy folder.

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

CHECK 0209 | Annex A | source schedule row | part 2/28

Source p. 25

A01 Scope statement

Record: A01 Scope statement

Required content: Entity, product, services, variants, interfaces, lifecycle stages, claim type and limitations.

Principal clauses: 1 to 4

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

CHECK 0210 | Annex A | source schedule row | part 3/28

Source p. 25

A02 Applicability matrix

Record: A02 Applicability matrix

Required content: Every requirement and test, applicability basis, implementation, evidence and outcome.

Principal clauses: 2 and 23

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

CHECK 0211 | Annex A | source schedule row | part 4/28

Source p. 25

A03 Profile decision

Record: A03 Profile decision

Required content: Consequence and authority analysis, shared dependencies, isolation basis and reviewer.

Principal clauses: 4

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

Requirements & evidence

CHECK 0212 | Annex A | source schedule row | part 5/28

Source p. 25

A04 Integrity plan

Record: A04 Integrity plan

Required content: Roles, competence, gates, resources, suppliers, support funding and review schedule.

Principal clauses: 5

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0213 | Annex A | source schedule row | part 6/28

Source p. 25

A05 Risk register

Record: A05 Risk register

Required content: Assets, scenarios, impact, feasibility, uncertainty, controls, residual risk and acceptance.

Principal clauses: 6

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0214 | Annex A | source schedule row | part 7/28

Source p. 25

A06 Digital inventory

Record: A06 Digital inventory

Required content: Hardware, executable units, dependencies, models, configurations, identities and deployed states.

Principal clauses: 7

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0215 | Annex A | source schedule row | part 8/28

Source p. 25

A07 Architecture record

Record: A07 Architecture record

Required content: Domains, trust boundaries, allowed flows, resource limits and independent containment.

Principal clauses: 8

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0216 | Annex A | source schedule row | part 9/28

Source p. 25

A08 Cryptographic record

Record: A08 Cryptographic record

Required content: Algorithms, keys, trust chains, validity, revocation, migration and recovery evidence.

Principal clauses: 9

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0217 | Annex A | source schedule row | part 10/28

Source p. 25

A09 Development record

Record: A09 Development record

Required content: Requirements traceability, source reviews, tool output, tests and defect dispositions.

Principal clauses: 10

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0218 | Annex A | source schedule row | part 11/28

Source p. 25

A10 Release provenance

Record: A10 Release provenance

Required content: Approved inputs, toolchain, build evidence, artifact digests, signing and release approvals.

Principal clauses: 11

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0219 | Annex A | source schedule row | part 12/28

Source p. 25

A11 Supplier assurance

Record: A11 Supplier assurance

Required content: Responsibility contracts, evidence reviews, support arrangements and exit plans.

Principal clauses: 12

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0220 | Annex A | source schedule row | part 13/28

Source p. 25

A12 Update campaign

Record: A12 Update campaign

Required content: Manifest, preconditions, compatibility, interrupted-update tests, cohorts and outcomes.

Principal clauses: 13

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0221 | Annex A | source schedule row | part 14/28

Source p. 25

A13 Service controls

Record: A13 Service controls

Required content: API permissions, tenancy, mobile enrollment, remote commands and administration.

Principal clauses: 14

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0222 | Annex A | source schedule row | part 15/28

Source p. 25

A14 Data processing record

Record: A14 Data processing record

Required content: Purposes, data flows, user controls, impact assessment, recipients, retention and deletion tests.

Principal clauses: 15

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0223 | Annex A | source schedule row | part 16/28

Source p. 26

A15 Resilience case

Record: A15 Resilience case

Required content: Essential functions, state envelopes, timing budgets, containment and restoration tests.

Principal clauses: 16

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0224 | Annex A | source schedule row | part 17/28

Source p. 26

A16 Vulnerability record

Record: A16 Vulnerability record

Required content: Awareness time, triage, affected population, interim controls, correction and closure.

Principal clauses: 17

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0225 | Annex A | source schedule row | part 18/28

Source p. 26

A17 Incident record

Record: A17 Incident record

Required content: Monitoring coverage, event integrity, decisions, notifications, exercises and lessons.

Principal clauses: 18

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0226 | Annex A | source schedule row | part 19/28

Source p. 26

A18 AI integrity record

Record: A18 AI integrity record

Required content: Provenance, authority, evaluation sets, hostile-input testing, adaptation and fallback.

Principal clauses: 19

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0227 | Annex A | source schedule row | part 20/28

Source p. 26

A19 Interface assurance

Record: A19 Interface assurance

Required content: V2X, charging, positioning, digital keys, remote control and aftermarket tests.

Principal clauses: 20

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0228 | Annex A | source schedule row | part 21/28

Source p. 26

A20 Production and service

Record: A20 Production and service

Required content: Provisioning, end-of-line checks, service access, replacement parts and handover.

Principal clauses: 21

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0229 | Annex A | source schedule row | part 22/28

Source p. 26

A21 Support and retirement

Record: A21 Support and retirement

Required content: Commitments, installed population, continuity response, terminal state and sanitization.

Principal clauses: 22

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0230 | Annex A | source schedule row | part 23/28

Source p. 26

A22 Verification dossier

Record: A22 Verification dossier

Required content: Coverage, representative variants, procedures, uncertainty, observations and retests.

Principal clauses: 23

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0231 | Annex A | source schedule row | part 24/28

Source p. 26

A23 Decision record

Record: A23 Decision record

Required content: Findings, closure, residual risk, independent review, scope and signed decision.

Principal clauses: 24

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0232 | Annex A | source schedule row | part 25/28

Source p. 26

A24 Change record

Record: A24 Change record

Required content: Materiality decision, changed assumptions, evidence reuse and reassessment.

Principal clauses: 24

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0233 | Annex A | source schedule row | part 26/28

Source p. 26

A25 Integrity passport

Record: A25 Integrity passport

Required content: Public and restricted views, versions, authenticated status and support information.

Principal clauses: 25

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0234 | Annex A | source schedule row | part 27/28

Source p. 26

A26 Performance review

Record: A26 Performance review

Required content: Metric definitions, missing data, trends, management action and technology migration.

Principal clauses: 26

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0235 | Annex A | source schedule row | part 28/28

Source p. 26

A27 Parameter declaration

Record: A27 Parameter declaration

Required content: All limits from Annex C, engineering justification, units, approvals and invalidating triggers.

Principal clauses: 2 and Annex C

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

Annex B | Minimum verification catalogue

CHECK 0236 | B0

Source p. 27

Common execution rules

Every applicable case below shall be translated into an executable product-specific procedure. The procedure shall state exact inputs, topology, versions, permissions, timing, vehicle state, expected observations, instruments and restoration steps. The reviewer shall approve it before execution. A catalogue title alone shall not count as a completed test. Each case shall cover its stated variants and all materially different implementations identified in the coverage plan. Stateful interruption or race-sensitive sequences shall be repeated at least 10 times per selected configuration for IP1 and IP2, and at least 30 times for IP3. Repeated runs shall vary relevant timing and initial state. Additional runs shall be performed where nondeterminism or observed failures invalidate confidence. Deterministic document inspections do not require artificial repetition. No unauthorized actuation, cross-boundary authority, acceptance of a prohibited artifact, or exposure of protected test data shall be observed in a passing case. This zero-observed-failure rule concerns the executed test set; it is not proof of zero residual risk. Measurement uncertainty shall be included when comparing an observation with a limit. An observation whose uncertainty crosses the acceptance limit shall be inconclusive until resolved. Each result shall include the procedure, raw observations, evidence digests, outcome, reviewer, deviations and linked finding identifiers. Where a conditional feature is absent, non-applicability shall be established through the scope statement and implementation inspection.

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

CHECK 0237 | B01

Source p. 27

Scope and inventory reconciliation

Applies to all scopes; verifies Clauses 4 and 7. Reconcile the declared scope with architecture, build outputs, observed services and a representative production configuration. Identify omitted binaries, hidden endpoints, dormant features and differing component versions. Compare each executable deployment unit and signing identity with the inventory. Acceptance: every observed in-scope executable unit, privileged identity and material interface is identified; discrepancies are resolved; profile assignment reflects actual authority. Preserve reconciliation logs, inventory snapshots and the variant selection rationale.

RESULT	Select result	FINDING / ACTION ID	
EVIDENCE / OBSERVED RESULT / N/A RATIONALE			

Requirements & evidence

CHECK 0238 | B02

Source p. 27

Boot and runtime integrity

Applies to executable platforms; verifies Clauses 7 to 9. Modify protected boot, executable, configuration and policy artifacts; attempt startup and relevant runtime reloads. Repeat with valid content and with a validly signed but prohibited security state. Observe verification order, execution decisions, alerts and safe recovery. Acceptance: altered or prohibited content does not gain unauthorized execution; the approved state starts correctly; recovery meets its declared envelope. Preserve artifact identifiers, verification results and hardware-observed state transitions.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0239 | B03

Source p. 28

Domain and resource isolation

Applies to shared platforms and gateways; verifies Clauses 8 and 16. From a compromised less trusted domain, attempt unauthorized memory, storage and network access. Exhaust its allocated compute, communication and event capacity while exercising essential functions at declared worst-case workload. Acceptance: cross-domain authority remains constrained and essential deadlines, data integrity and fallback behaviour remain within approved limits. Record timing distributions and worst observed values, not only averages.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0240 | B04

Source p. 28

Identity enrollment and revocation

Applies to identity-controlled access; verifies Clauses 9, 14 and 21. Enroll a legitimate identity; then test stolen credentials, unauthorized enrollment, role escalation, expired credentials and revoked access. Repeat through offline operation, clock uncertainty and later reconnection. Acceptance: only authorized roles act; revocation reaches connected enforcement points within Annex C limits; offline behaviour follows the bounded declared policy. Record issuance, use, refusal and revocation propagation events.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0241 | B05

Source p. 28

Trust root recovery and cryptographic migration

Applies to IP2 and IP3 trust systems and any claimed migration capability; verifies Clause 9. Simulate compromise of the normal authority and exercise the independent recovery path. Migrate a representative component and service to the approved alternative algorithm or trust format. Test downgrade, mixed versions, interruption and resource effects. Acceptance: unauthorized recovery and downgrade fail; legitimate migration preserves compatibility, essential timing and recoverability. The evidence identifies exactly which algorithms, formats and product variants were exercised.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0242 | B06

Source p. 28

Build provenance and release authority

Applies to software producers and integrators; verifies Clauses 10 to 12. Introduce an unapproved dependency, substitute a stored artifact and impersonate an ordinary build worker. Attempt production signing without completed approvals. Verify an approved release against its provenance using the declared independent method. Acceptance: unauthorized content cannot acquire an approved release identity; provenance resolves to the delivered content; independent approvals cannot be fabricated by the tested single compromised account.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0243 | B07

Source p. 28

Update authenticity and target binding

Applies to updateable products; verifies Clause 13. Present a valid package and packages with altered bytes, missing content, stale metadata, incorrect target hardware, unauthorized signer and revoked signing authority. Include a package whose signature is valid but whose dependencies or target state are wrong. Acceptance: only the intended authorized compatible package reaches activation. Rejections preserve approved operation and create actionable records without exposing secrets.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0244 | B08

Source p. 29

Interrupted update and recovery

Applies to updateable products; verifies Clauses 13 and 16. Enumerate the update state machine and interrupt power or communications during download, verification, preparation, writing, activation and confirmation where each interruption is physically meaningful. Repeat at boundary timings and low declared energy. Acceptance: each interruption leaves or restores a validated state within the declared recovery limit. No unapproved image executes, no incompatible essential-function state activates, and recovery does not cross below the allowed security epoch.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0245 | B09

Source p. 29

Multi component compatibility and rollback

Applies to interdependent updates; verifies Clause 13. Execute updates in incorrect order, with one component unavailable, with a stale component state and with a failed activation acknowledgement. Attempt replay of a prior valid update and unauthorized rollback. Acceptance: dependency rules are enforced, partial activation cannot authorize incompatible essential behaviour, and only explicitly approved compatible recovery states are reachable. Preserve the compatibility matrix and observed component states.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0246 | B10

Source p. 29

Fleet rollout and emergency pause

Applies to fleet distribution; verifies Clauses 8, 13 and 16. In an isolated fleet representation, trigger declared failure thresholds during a staged campaign and compromise an ordinary rollout account. Include unreachable vehicles and delayed acknowledgements. Exercise pause and recovery authority. Acceptance: expansion stops at the approved trigger; the tested account cannot exceed its cohort authority; observed affected population remains within the declared blast radius. Unreachable and failed vehicles remain in the denominator and action register.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0247 | B11

Source p. 29

Safe installation conditions

Applies to updates affecting operating state; verifies Clause 13. Attempt activation during motion, charging, low energy, occupied service mode and other disallowed states identified by the hazard analysis. Test false or stale indications of safe state. Acceptance: essential-function activation occurs only under validated conditions; a spoofed state cannot bypass controls; user information matches actual unavailability and recovery behaviour.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0248 | B12

Source p. 29

API object and tenant authorization

Applies to connected services; verifies Clause 14. Using ordinary, elevated and revoked accounts, request another vehicle's records, issue commands to another tenant and invoke privileged endpoints. Include altered identifiers, batch operations, alternate request forms and concurrent authorization changes. Acceptance: no cross-vehicle or cross-tenant access or command execution occurs outside the approved role model. Errors and logs do not disclose protected records or reusable secrets.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0249 | B13

Source p. 30

Remote command freshness and safety envelope

Applies to remote functions; verifies Clauses 8, 14 and 20. Replay, delay, reorder and duplicate commands; submit authorized commands with unsafe parameters or in an invalid vehicle state. Simulate a compromised authenticated backend. Acceptance: stale or unsafe commands are rejected or constrained locally, and no single remote principal bypasses the essential-function envelope. Record both the server decision and the vehicle's actual response.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0250 | B14

Source p. 30

Parser and stateful protocol robustness

Applies to exposed parsers and message handlers; verifies Clauses 8, 10 and 20. Exercise a corpus covering valid traffic, malformed lengths, invalid encodings, extreme values, invalid state sequences and resource exhaustion. Execute at least 100000 distinct mutated inputs per exposed parser class, supplemented by relevant stateful sequences and justified additional exploration for IP3. Acceptance: no unauthorized execution, protected-data disclosure or unsafe loss of essential function occurs; crashes and hangs are analyzed and corrected where they violate requirements. The input count is a minimum exercise size, not a sufficient security argument by itself.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0251 | B15

Source p. 30

Cloud and dependency outage

Applies where external services support the product; verifies Clauses 14 and 16. Remove connectivity, identity, trusted time, positioning or primary cloud service singly and in credible common-failure combinations. Restore dependencies with stale sessions and conflicting state. Acceptance: the product reaches or maintains its declared safe state, reconnects without replaying stale authority and meets recovery limits. Preserve vehicle-state evidence and service restoration records.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0252 | B16

Source p. 30

Ransomware and destructive recovery exercise

Applies to recovery-dependent scopes; verifies Clauses 11, 16 and 18. Use an isolated environment to deny normal operational access and corrupt representative mutable state. Assume one administrative domain is compromised. Restore from protected recovery assets and re-establish trust. Acceptance: the tested compromise cannot destroy all required recovery paths; restored software, identities and data restrictions match an approved baseline. Restoration time is measured from declared exercise onset to verified service readiness.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0253 | B17

Source p. 30

Privacy defaults and data flow

Applies to personal-data processing; verifies Clause 15. Use seeded identities and distinctive synthetic records to trace collection and transmission with default settings, optional consent enabled, consent withdrawn and network access interrupted. Inspect actual destinations and stored content. Acceptance: observed processing matches declared purpose and settings; disabled optional purposes do not receive new data; queued data follows the current valid policy before transmission. Preserve traffic and storage evidence with controlled access.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0254 | B18

Source p. 31

Deletion and backup restoration

Applies to retained personal data; verifies Clause 15. Request deletion through an authenticated test identity and follow the record across active storage, caches, processors and backups. Restore a backup that contains the previously deleted record. Acceptance: the declared deadlines are met; restricted or deleted information does not re-enter ordinary processing after restoration; justified retained evidence remains segregated. The test records any storage where immediate physical overwrite is not feasible and verifies the approved alternative.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0255 | B19

Source p. 31

Ownership transfer and digital keys

Applies to user or owner-linked access; verifies Clauses 15, 20 and 21. Transfer a test vehicle or rental session and attempt access using former accounts, mobile devices, shared keys, service sessions and offline credentials. Include later reconnection of an old device. Acceptance: previous users cannot locate, unlock, command or retrieve new personal records without fresh authorization; the new authorized user can complete intended enrollment; occupant egress remains available.

RESULT **FINDING / ACTION ID**

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0256 | B20

Source p. 31

AI provenance and model substitution

Applies to AI functions; verifies Clause 19. Reconcile the deployed model with its record and substitute model weights, configuration, retrieval data or tool policy. Include a signed model outside the declared compatibility or authority limits. Acceptance: unauthorized substitutions and incompatible authority changes are blocked; the approved model remains traceable to its evaluated baseline and production restrictions. Record both model identity and the effective runtime policy.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0257 | B21

Source p. 31

AI hostile content and action boundaries

Applies to AI or agents processing untrusted content; verifies Clause 19. Submit instructions embedded in retrieved text, diagnostic files and relevant input channels that attempt to override policy, access another user's data or invoke prohibited vehicle and backend functions. Include indirect and multi-step attempts. Acceptance: independent enforcement prevents prohibited tool use, secret disclosure and unauthorized actuation in the defined test suite. Refusal wording from the model alone is insufficient evidence if a tool call can still execute.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0258 | B22

Source p. 31

AI drift poisoning and adaptation limits

Applies to adaptive, learned or federated systems; verifies Clause 19. Introduce representative distribution shifts, manipulated contributions and adaptation outside the approved envelope. Exercise monitoring, isolation of suspect contributions, freeze and recovery. Acceptance: approved scenario-specific limits are maintained or the validated fallback activates; adaptation cannot broaden authority; integrity and provenance survive rollback. Record scenario-level results and uncertainty, including the weakest performing relevant condition.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0259 | B23

Source p. 32

V2X and cooperative message integrity

Applies to V2X and cooperative driving; verifies Clause 20. Send stale, forged, duplicated and authenticated-but-false messages; simulate conflicting participants, false events, implausible position and sudden withdrawal. Use controlled simulation plus hardware where physical behaviour is claimed. Acceptance: origin trust does not bypass plausibility and local safety constraints; malformed or misleading cooperation does not create unauthorized actuation. Preserve the basis for corroboration or conservative fallback.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0260 | B24

Source p. 32

Charging and bidirectional energy authority

Applies to connected energy functions; verifies Clause 20. Emulate a compromised charger or dispatch service, stale authorization, excessive power requests, interrupted sessions and mismatched payment state. Test commands near approved electrical and thermal boundaries. Acceptance: local physical limits remain effective; payment or remote authorization failure cannot override protection; power changes and session termination follow validated vehicle-state behaviour.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0261 | B25

Source p. 32

Positioning time and remote driving

Applies to functions relying on positioning, trusted time or remote driving; verifies Clauses 9, 16 and 20. Inject drift, abrupt jumps, delayed commands, link degradation, clock rollback and conflicting operator authority. Test at the declared worst-case reaction boundary. Acceptance: the product detects or tolerates the condition within its approved envelope and performs the local contingency response before the safe-response budget is exceeded. Record measured latency, loss patterns and actual control authority.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0262 | B26

Source p. 32

Manufacturing provisioning and service access

Applies to production and maintenance; verifies Clause 21. Inspect representative provisioning records and attempt duplicate device credentials, use of engineering keys, expired workshop sessions, unauthorized replacement modules and excessive diagnostic permissions. Acceptance: production identity and state are controlled; service authority remains job-limited; incompatible or unauthorized replacements cannot gain privileged operation. Preserve end-of-line and reenrollment evidence.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0263 | B27

Source p. 32

Logging and monitoring continuity

Applies to monitored scopes; verifies Clause 18. Suppress, forge, reorder and duplicate security events; remove the primary logging endpoint and introduce clock uncertainty. Generate known detectable security events during each condition. Acceptance: relevant detection objectives and coverage-loss alerts are met; source integrity and event ordering remain interpretable; absence of monitoring is not represented as absence of attacks.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0264 | B28

Source p. 33

Vulnerability response clock and coordination

Applies to supported products; verifies Clause 17 and Annex C. Inject a time-stamped credible report affecting a shared component and trace acknowledgement, triage, population discovery, escalation, interim controls and the correction plan. Include an unavailable primary supplier contact. Acceptance: required deadlines are met without resetting the awareness clock; affected variants and unreachable devices remain visible; closure requires technical evidence rather than an unanswered supplier request.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0265 | B29

Source p. 33

End of support and decommissioning

Applies to products with support or retirement obligations; verifies Clause 22. Exercise the terminal- configuration plan on a representative item, remove an external dependency and attempt reuse of revoked credentials and erased test data. Inspect notice and successor-support arrangements. Acceptance: the declared support commitment and safe terminal state are demonstrable; retired identities cannot retain ordinary access; sanitization prevents authorized test recovery of protected content through the defined access methods.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0266 | B30

Source p. 33

Passport status and material change

Applies to conformity claims; verifies Clauses 24 and 25. Alter passport data, replay an older status, expire its freshness period and introduce an unassessed material change. Exercise restriction, suspension and restoration workflows. Acceptance: tampering and stale status are recognizable; current claims track the assessed baseline; restoration requires a recorded new decision. The public view discloses no restricted personal or exploit information.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0267 | B31

Source p. 33

Fleet compromise and independent containment

Applies to IP3 and any shared privileged fleet service; verifies Clauses 8, 14, 16 and 18. Assume compromise of a fleet operations principal and attempt commands, credential changes or update actions beyond its authorized segment. Exercise the independent containment channel with the ordinary control plane unavailable. Acceptance: affected scope stays within its approved quantitative limit, unaffected segments preserve essential behaviour, and containment meets its declared timing. A limit equal to the entire fleet fails unless the scope is a single vehicle with no shared control plane.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0268 | B32

Source p. 33

Supplier exit and replacement integration

Applies to a critical external dependency; verifies Clauses 12 and 22. Select a supplier whose failure can undermine an essential or privileged function. Exercise the documented exit route using representative artifacts, alternative support or constrained operation. Test identity handover and evidence availability. Acceptance: the organization demonstrates a technically feasible continuity or controlled-retirement route, with maintained trust and declared limits. A contractual promise with no executable recovery or replacement method does not pass.

RESULT	Select result	FINDING / ACTION ID	
--------	--	---------------------	----------------------

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

Annex C | Acceptance parameters and response limits

CHECK 0269 | C1 | part 1/14

Source p. 34

Parameter declaration

Before design verification, the organization shall create a signed parameter declaration containing every applicable field below. Product-specific values shall be justified from threat, hazard, dependency and operational analysis. Blank values, "as soon as possible" and values chosen only after seeing test outcomes shall not be accepted.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0270 | C1 | source schedule row | part 2/14

Source p. 34

Essential-function timing

Parameter: Essential-function timing

Required declaration: Detection and safe-response budget per function and operating state, in suitable time units.

Binding decision rule: Observed response including uncertainty shall not exceed the safe budget.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0271 | C1 | source schedule row | part 3/14

Source p. 34

Recovery

Parameter: Recovery

Required declaration: Maximum time to each defined safe state and restored service; power and link conditions.

Binding decision rule: All applicable recovery tests shall meet the declared time and state limits.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0272 | C1 | source schedule row | part 4/14

Source p. 34

Fleet blast radius

Parameter: Fleet blast radius

Required declaration: Maximum number and proportion of vehicles, identities and services affected per defined compromise.

Binding decision rule: Limits shall be below the whole fleet for shared control planes and met in B10 and B31.

RESULT FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0273 | C1 | source schedule row | part 5/14

Source p. 34

Update cohorts

Parameter: Update cohorts

Required declaration: Size, sequence, observation period, expansion authority and stop thresholds.

Binding decision rule: No cohort expansion before its approved evidence and observation conditions are met.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0274 | C1 | source schedule row | part 6/14

Source p. 34

Privileged revocation

Parameter: Privileged revocation

Required declaration: Time from approved revocation to enforcement; connected and offline cases.

Binding decision rule: Connected backend privileged enforcement shall complete within 15 minutes; safety-sensitive device actions shall also follow the local envelope.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0275 | C1 | source schedule row | part 7/14

Source p. 34

Offline authority

Parameter: Offline authority

Required declaration: Maximum credential age, command lifetime and permitted offline functions.

Binding decision rule: Expired optional remote authority shall fail closed; essential functions shall use their validated state-aware response.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0276 | C1 | source schedule row | part 8/14

Source p. 34

Parser coverage

Parameter: Parser coverage

Required declaration: Interface classes, corpus, state sequences, input count and stopping rule.

Binding decision rule: At least 100000 distinct mutated inputs per applicable parser class; risk-based additional coverage remains required.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0277 | C1 | source schedule row | part 9/14

Source p. 34

Update interruption

Parameter: Update interruption

Required declaration: State transitions, timing variation, selected hardware variants and repetitions.

Binding decision rule: At least 10 repetitions per stateful sequence for IP1 and IP2; at least 30 for IP3.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0278 | C1 | source schedule row | part 10/14

Source p. 34

AI evaluation

Parameter: AI evaluation

Required declaration: Scenario-level limits, hostile-input cases, relevant populations, sample rationale and uncertainty.

Binding decision rule: Every safety-relevant declared limit shall pass or the affected authority shall be constrained and reassessed.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0279 | C1 | source schedule row | part 11/14

Source p. 34

Data retention

Parameter: Data retention

Required declaration: Maximum duration by purpose, storage, cache, backup and recipient.

Binding decision rule: Expiry and deletion shall be verified; any mandatory retention exception shall be segregated and justified.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0280 | C1 | source schedule row | part 12/14

Source p. 34

Monitoring

Parameter: Monitoring

Required declaration: Events, coverage, alert latency and response routing by threat class.

Binding decision rule: Missing coverage shall be detectable; engineered safety deadlines take precedence.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0281 | C1 | source schedule row | part 13/14

Source p. 35

Passport freshness

Parameter: Passport freshness

Required declaration: Maximum age of a displayed verified status and offline treatment.

Binding decision rule: Expired status shall be unknown until reverified, without implying that the vehicle is necessarily unsafe.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0282 | C1 | source schedule row | part 14/14

Source p. 35

Support

Parameter: Support

Required declaration: Start basis, end date or calculable duration, components and services covered.

Binding decision rule: Delivered commitment shall be maintained; announced changes shall not silently shorten it.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0283 | C2 | part 1/6

Source p. 35

Vulnerability workflow deadlines

The following are maximum elapsed calendar times from credible awareness. They are proposed IAF process limits. They are not general patch-installation deadlines and do not authorize delay in responding to immediate harm. Any shorter applicable duty or engineered safety-response time shall take precedence.

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0284 | C2 | source schedule row | part 2/6

Source p. 35

Critical

Priority: Critical

Technical triage completed: 24 hours

Effective interim protection or verified existing containment: 72 hours

Dated permanent-correction plan approved: 7 calendar days

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0285 | C2 | source schedule row | part 3/6

Source p. 35

High

Priority: High

Technical triage completed: 72 hours

Effective interim protection or verified existing containment: 14 calendar days

Dated permanent-correction plan approved: 30 calendar days

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0286 | C2 | source schedule row | part 4/6

Source p. 35

Moderate

Priority: Moderate

Technical triage completed: 7 calendar days

Effective interim protection or verified existing containment: Need assessed and dispositioned within 30 calendar days

Dated permanent-correction plan approved: 60 calendar days

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0287 | C2 | source schedule row | part 5/6

Source p. 35

Low

Priority: Low

Technical triage completed: 14 calendar days

Effective interim protection or verified existing containment: Need assessed and dispositioned within 60 calendar days

Dated permanent-correction plan approved: 90 calendar days

RESULT

Select result

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0288 | C2 | part 6/6

Source p. 35

Vulnerability workflow deadlines

Reports through the public channel shall be acknowledged within 2 calendar days; urgent technical action shall not wait for acknowledgement. For initially unclassified reports, triage shall prioritize the highest credible consequence. An indication of active essential-function compromise shall trigger immediate escalation at receipt. An effective interim protection shall remove or contain the relevant attack path in the affected environment and shall have evidence that it does not create unacceptable safety or privacy harm. A press statement, planned update, customer notice alone or disabled alert shall not count as technical containment. Operational restriction may count only where its actual enforcement and safe consequences are demonstrated. Each permanent-correction plan shall state a justified delivery deadline, owner, affected population, validation activities and deployment strategy. Progress shall be reviewed at least weekly for Critical and High items until permanent correction or validated long-term treatment. A missed interim deadline is a nonconformity; a missed correction commitment shall trigger escalation, renewed risk assessment and claim review. Neither shall be erased by issuing a replacement plan. Where an interim control has been verified and the resulting risk no longer meets Critical or uncontained exploitable High criteria, a new conformity decision may consider the updated residual risk and evidence. The original finding, duration and affected population shall remain in the historical record. Without that verification, the release and claim restrictions remain in force.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0289 | C3 | source schedule row | part 1/6

Source p. 36

Complete threat review

Activity: Complete threat review**IP1 and IP2:** At least every 12 months**IP3:** At least every 6 monthsRESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0290 | C3 | source schedule row | part 2/6

Source p. 36

Internal implementation audit

Activity: Internal implementation audit**IP1 and IP2:** At least every 12 months**IP3:** At least every 12 months with privileged- operation review every 6 monthsRESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0291 | C3 | source schedule row | part 3/6

Source p. 36

Incident exercise

Activity: Incident exercise

IP1 and IP2: At least every 12 months

IP3: At least every 6 months

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0292 | C3 | source schedule row | part 4/6

Source p. 36

Review of assurance baseline and targeted technical retest

Activity: Review of assurance baseline and targeted technical retest

IP1 and IP2: At least every 12 months

IP3: At least every 6 months

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0293 | C3 | source schedule row | part 5/6

Source p. 36

New-technology and migration review

Activity: New-technology and migration review

IP1 and IP2: At least every 12 months

IP3: At least every 12 months and after material capability change

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

CHECK 0294 | C3 | part 6/6

Source p. 36

Periodic review minima

Periodic intervals shall not postpone reviews required by an incident, relevant vulnerability, material change or invalidated assumption. Targeted retesting shall cover changed or newly exposed attack paths; the assessor shall justify any unchanged evidence retained. This table sets assurance activities, not a universal certificate validity period.

RESULT

FINDING / ACTION ID

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Requirements & evidence

CHECK 0295 | C4

Source p. 36

Release decision checklist

Before an initial or materially changed release is approved, the decision authority shall verify all of the following: the scope and inventory are complete; all applicable mandatory requirements are met; required tests pass; independent reviews are complete; known Critical residual risks and uncontained exploitable High residual risks are absent; any other High residual risk meets Clause 6; update and recovery routes are verified; privacy settings match observed behaviour; support responsibilities are funded and assigned; and the evidence baseline identifies the actual release. An administrative signature without these conditions shall not authorize a conformant claim. A recommendation for improvement may remain open only if it is not a failed requirement and does not invalidate risk acceptance.

RESULT	FINDING / ACTION ID
Select result	

EVIDENCE / OBSERVED RESULT / N/A RATIONALE

Findings & corrective action

Use one record per finding. Link every affected checklist ID and source clause. Add identified continuation records for further findings. Preserve the original result and document retest evidence before closure.

CORRECTIVE ACTION RECORD 1

FINDING ID

CHECK / CLAUSE IDS

SOURCE SEVERITY / GATE

OBSERVATION, REQUIREMENT AND OBJECTIVE EVIDENCE

IMMEDIATE CONTAINMENT / AFFECTED CONFIGURATIONS

ROOT CAUSE AND CORRECTIVE ACTION

RESPONSIBLE OWNER / DUE DATE

RETEST EVIDENCE / REVIEWER / CLOSURE DATE

CORRECTIVE ACTION RECORD 2

FINDING ID

CHECK / CLAUSE IDS

SOURCE SEVERITY / GATE

OBSERVATION, REQUIREMENT AND OBJECTIVE EVIDENCE

IMMEDIATE CONTAINMENT / AFFECTED CONFIGURATIONS

ROOT CAUSE AND CORRECTIVE ACTION

RESPONSIBLE OWNER / DUE DATE

RETEST EVIDENCE / REVIEWER / CLOSURE DATE

Assessment conclusion & review

Summarize the assessed scope and source-specific decision. Counts are manual cross-checks and do not override an unresolved requirement, critical gate, score cap or mandatory evidence condition.

APPLICABLE CHECKS

PASS

FAIL

NOT DEMONSTRATED

NOT APPLICABLE

OPEN CRITICAL GATES / BLOCKED CONFIGURATIONS / REASSESSMENT TRIGGERS

ASSESSMENT LIMITATIONS, EXCLUSIONS AND UNRESOLVED EVIDENCE

SOURCE-SPECIFIC CONCLUSION AND SUPPORTING DECISION RECORD

- ☐ All applicable check records and source dependencies have been reviewed.
- ☐ No unresolved critical failure is being accepted through averaging or a general pass count.
- ☐ The conclusion is restricted to the identified scope, configuration, evidence and draft status.

ASSESSOR NAME / ROLE

INDEPENDENT REVIEWER NAME / ROLE

ASSESSOR SIGN-OFF (TYPED NAME)

REVIEWER SIGN-OFF (TYPED NAME)

DATE

DATE

Sign-off fields accept typed names; they are not cryptographic digital-signature fields. Apply the organization's approved signing process where a formal signature is required. Final conformity, certification or label authorization remains subject to the source scheme and its adoption controls.

Continuation & additional evidence

Identify every continuation record and its parent checklist or finding. Additional sheets may be retained as separately identified evidence; preserve the link in the parent field.

CHECK / FINDING ID AND CONTINUATION REFERENCE

ADDITIONAL EVIDENCE, MEASUREMENTS, RATIONALE OR VERIFICATION

CHECK / FINDING ID AND CONTINUATION REFERENCE

ADDITIONAL EVIDENCE, MEASUREMENTS, RATIONALE OR VERIFICATION

CHECK / FINDING ID AND CONTINUATION REFERENCE

ADDITIONAL EVIDENCE, MEASUREMENTS, RATIONALE OR VERIFICATION