Apptega

GUIDE

TISAX 6.0.3 Compliance Guide

Understanding and Implementing Information Security Requirements for the Automotive Industry

Current as of November 2025

1. Introduction

The Trusted Information Security Assessment Exchange (TISAX) provides a standardized, accredited framework for evaluating and exchanging assurance about information security within the automotive and mobility sectors. Developed by the German Association of the Automotive Industry (VDA) and operated by the ENX Association, TISAX enables original equipment manufacturers (OEMs), suppliers, and service providers to demonstrate a consistent level of protection for sensitive engineering and production information.

TISAX 6.0.3 builds upon the VDA Information Security Assessment (ISA) catalog and incorporates alignment with ISO/IEC 27001 and 27002 principles. It expands these standards with industry-specific requirements for prototype protection, supplier assurance, and secure data-sharing across extended supply chains. The framework is structured into nine domains—IS1 through IS7, PP8, and DP9—each containing detailed controls and sub-controls that define measurable expectations for policy, process, and technical safeguards.

TISAX focuses on three key assessment modules:

- **Information Security (IS) –** the foundation for all participants, defining the governance, risk management, and operational controls that establish a secure baseline for information handling.
- **Prototype Protection (PP) –** ensuring that physical and digital prototypes are safeguarded through controlled environments, custody tracking, and event security.
- **Data Protection (DP) –** demonstrating compliance with privacy, confidentiality, and personal-data requirements consistent with GDPR and related laws.

Unlike a one-time certification, TISAX emphasizes continuous improvement. Each participating organization develops and maintains an Information Security Management System (ISMS) that evolves with new risks, technologies, and business relationships. The TISAX assessment process applies a maturity-based model (0–5) to evaluate not only whether controls exist but how effectively and consistently they operate in practice. The resulting TISAX label, valid for three years, communicates the organization's verified level of assurance to authorized partners through the ENX portal.

This compliance guide translates the TISAX 6.0.3 requirements into a practical implementation roadmap. It is written for organizations seeking to design, operate, and sustain a compliant ISMS capable of achieving or maintaining a valid TISAX label. Each section provides context, intent, implementation steps, evidence expectations, and maturity guidance so that stakeholders—from executives to technical managers—can understand what must be done and how to demonstrate conformity during an audit. By following this guide, companies can establish a repeatable compliance program that reduces audit friction, protects proprietary information, and strengthens trust across the automotive ecosystem.

1A. Beginner Quick-Start (First 30—90 Days)

Establishing TISAX compliance requires careful planning and sustained execution. Many organizations underestimate the effort to transition from informal security practices to a structured ISMS that meets the expectations of TISAX auditors. This section provides a pragmatic onboarding framework for the first three months of activity. Each phase focuses on achievable deliverables that collectively build a credible foundation for certification.

First 30 Days (Establish Governance and Scope)

- The initial month focuses on building accountability and defining scope. Begin by appointing an ISMS Owner, an executive sponsor, and identifying key stakeholders across IT, HR, Legal, Engineering, and Procurement.
- Document the organizational boundaries and information assets included in the TISAX assessment—typically one or more sites, data environments, and supplier interfaces.
- Select the appropriate Assessment Level (AL1–AL3) based on data sensitivity and customer requirements, and confirm which modules apply (Information Security, Prototype Protection, Data Protection).
- Acquire the official VDA ISA 6.0.3 catalog, and perform an initial gap analysis against current controls.
- Create a central evidence repository—such as a secured SharePoint or GRC system—to store all policies, procedures, and audit artifacts.

Days 31—60 (Develop Core Policies and Implement Foundations)

- Once governance is in place, shift attention to formalizing documentation and baseline controls.
- Draft and approve foundational policies including Information Security, Access Control, Incident Response, Risk Management, Supplier Security, and Prototype Handling.
- Define a RACI matrix that clarifies roles and decision authority across departments.
- Introduce mandatory awareness training for all employees, emphasizing confidentiality and prototype-handling expectations.
- Deploy quick-win controls that raise immediate security posture—multi-factor authentication, endpoint protection, asset inventory, secure backups, and controlled visitor management.
- Simultaneously, begin developing the risk register, logging vulnerabilities and assigning mitigation owners.

Days 61—90 (Validate Readiness and Prepare for Assessment)

- The final month is dedicated to validating effectiveness and preparing for external evaluation.
- Conduct a self-assessment using the ISA questionnaire and maturity scoring model.
- Complete risk assessments and document treatment plans.
- Schedule and hold a management review covering risk status, resource allocation, and ISMS objectives.
- Identify and engage an accredited audit provider for AL2 or AL3 as appropriate.
- Finalize all policy approvals and ensure the evidence repository contains current documents and records mapped to each control domain.

By the end of the first 90 days, the organization should have:

- A defined ISMS scope and governance structure.
- Approved core policies and assigned roles.
- Completed gap and risk assessments.
- A functioning evidence repository and training program.
- Documented readiness to undergo the formal TISAX assessment process.
- Vendor controls initiated
- **Evidence:** library functioning

This 90-day framework creates momentum and demonstrates executive commitment to security maturity—both critical factors in achieving and sustaining a TISAX label.

2. Understanding TISAX and Assessment Levels

The TISAX framework uses a structured maturity and assurance model to evaluate how effectively an organization manages information security. Rather than a binary pass/fail audit, TISAX measures consistency, documentation quality, and continuous improvement. The result is a TISAX label, which communicates the organization's verified assurance level to customers and partners through the ENX portal.

Assessment Levels (AL1 — AL3)

Each assessment level represents the depth of validation required and the sensitivity of information involved.

Assessment Level 1 — Self-Assessment

Intended for organizations handling low-sensitivity information or performing internal benchmarking. The organization completes the ISA questionnaire, self-scores each control on the 0–5 maturity scale, and records supporting evidence. External validation is not required, but the process establishes a baseline for future improvements.

Assessment Level 2 — Remote Audit

Used when exchanging confidential information that does not involve physical prototypes or highly sensitive engineering data. An accredited TISAX audit provider reviews submitted documentation remotely, performs interviews, and verifies representative evidence. The auditor assigns maturity ratings and identifies corrective actions with defined remediation timelines.

Assessment Level 3 — On-Site Audit

Reserved for organizations handling highly confidential, prototype, or personal data. Auditors perform on-site inspections, evaluate physical and technical controls, interview personnel, and verify process execution. This level demonstrates the highest degree of assurance and is typically required by OEMs for design, testing, or production collaboration.

Maturity Model (0—5)

TISAX assesses each control on a six-point scale representing process discipline and effectiveness:

Level	Description	Typical Evidence
0	Not Implemented	No control or documentation exists.
1	Initial	Activities are informal or ad hoc.
2	Managed	Policies and procedures are documented but inconsistently applied.
3	Defined	Controls are standardized and enforced across the organization.
4	Quantitatively Controlled	Metrics and automation drive proactive management.
5	Optimized	Continuous improvement integrated into business strategy.

Assessment Levels and Maturity Levels are related but distinct: the assessment level defines how the audit is performed, while maturity levels define how well the controls operate.

Typical targets: **AL1 → Level 2, AL2 → Level 3, AL3 → Level 4.**

Relationship to ISO/IEC 27001

TISAX builds on ISO/IEC 27001's ISMS framework but tailors it to automotive requirements. Organizations already certified to ISO 27001 can reuse governance, risk, and compliance artifacts, yet must extend their ISMS to cover:

- Prototype Protection (physical and digital custody)
- Supplier Information Security Assurance
- Data Protection (GDPR-aligned controls)

Auditors often map TISAX domains IS1–IS7, PP8, and DP9 to corresponding ISO Annex A controls, simplifying integration while ensuring that automotive-specific expectations are met.

Assessment Cycle and Label Validity

A TISAX label is valid for three years. Organizations must conduct annual internal reviews to maintain compliance, track maturity trends, and prepare for re-assessment. Major organizational or infrastructure changes—such as mergers, relocations, or new prototype activities—should trigger an interim evaluation.

Information Exchange via ENX

After successful validation, assessment results are uploaded to the ENX portal, where the organization controls who can view its results. This trusted exchange mechanism eliminates redundant audits between business partners and promotes a consistent, transparent security posture across the automotive ecosystem.

3. Policy Areas & Practices

Effective information-security governance begins with well-defined, documented policies that establish expectations across all domains of control. TISAX 6.0.3 treats policy management as the backbone of the Information Security Management System (ISMS): each domain—from access management to prototype protection—must have an approved policy that is maintained, communicated, and traceable to operational procedures and evidence. Auditors review not only whether a policy exists but whether it is current, reviewed on schedule, and demonstrably implemented within daily operations.

A complete policy framework should define purpose, scope, ownership, and review intervals. Each document must link to measurable procedures, assign control owners, and include revision history. Alignment with the TISAX ISA domains ensures that every requirement is governed by an explicit rule set, avoiding overlap or omissions. Policies should be version-controlled, digitally signed, and stored in a secure, read-only repository accessible to all employees. Annual review cycles confirm continued adequacy and trigger updates when organizational or regulatory conditions change.

Domain	Policy Focus	Example Supporting Documents
IS1 – Policies and Organization	Governance, accountability, and overall ISMS structure	ISMS Charter • Information Security Policy • Policy Register
IS2 – Human Resources Security	Personnel vetting, onboarding, and disciplinary processes	HR Security Policy • Code of Conduct • Screening Procedure
IS3 – Physical Security	Facility access, visitor control, environmental safety	Physical Security Policy • Access Badge Procedure • CCTV Retention Plan
IS4 – Identity & Access Management	Account provisioning, authentication, privilege control	Access Control Policy • Password Standard • Privileged Access Procedure
IS5 – IT / Cyber Security	Hardening, patching, monitoring, backups, malware defense	System Configuration Baseline • Patch Management Procedure • SIEM Runbook
IS6 – Supplier Relationships	Third-party security, contract clauses, performance review	Supplier Security Policy • Vendor Risk Procedure • Due-Diligence Checklist
IS7 – Compliance and Audit	Regulatory tracking, audit execution, corrective action	Compliance Register • Audit Program • CAPA Process
PP8 – Prototype Protection	Custody, event security, transport, destruction	Prototype Handling Policy • Chain-of-Custody Form • Event Security Plan
DP9 – Data Protection	GDPR alignment, privacy impact assessments, breach response	Data Protection Policy • RoPA Template • Incident Notification Procedure

To maintain maturity, the organization should operate a Policy Register listing every policy, its owner, last approval date, and next review. A Change Control Procedure must govern how policies are updated, communicated, and acknowledged by employees. Many organizations automate acknowledgments through learning-management or intranet systems to capture evidence that staff have read and understood the content.

Auditors will typically sample policies across several domains to ensure consistency in language, structure, and version control. Discrepancies—such as outdated templates or unapproved revisions—indicate immaturity in ISMS governance. Mature programs integrate policy compliance into onboarding and annual refresher training, ensuring awareness becomes a measurable control rather than a static document review.

- **Evidence: Examples:** policy register, approval signatures, communication records, employee acknowledgments.
- **Common Failures:** missing approval metadata, outdated versions, or policies stored in uncontrolled locations.
- **Maturity Goal:** Level 3 (Defined) for AL2 and Level 4 (Quantitatively Controlled) for AL3, where policy management is automated and metrics (e.g., review-cycle completion) drive improvement.

4. RACI Matrix

Effective governance requires unambiguous accountability. The RACI (Responsible, Accountable, Consulted, Informed) model is a foundational tool in TISAX for mapping decision authority, execution responsibility, and stakeholder communication across all domains of the ISMS. Without a maintained RACI matrix, even well-written policies can fail in execution because teams are unclear who must act, approve, or report. Auditors routinely request this artifact early in the assessment to confirm that every control has an identifiable owner.

Each role must be documented in the ISMS Charter and reflected in job descriptions or committee terms of reference. The matrix should be reviewed at least annually—or whenever the organization restructures—to ensure continued accuracy. In mature programs, updates are synchronized with HR systems and approval workflows so that organizational charts and RACI assignments remain aligned.

Domain	CISO	ISMS Owner	IT Operations	HR	Legal / Privacy	Procurement	Site Management	Prototype Lead
IS1 Policies & Organization	**A**	**R**	C	I	I	I	I	I
IS2 HR Security	C	R	I	**A**	I	I	I	I
IS3 Physical Security	C	R	C	I	I	I	**A**	R
IS4 Identity & Access Mgmt	C	R	**A**	I	I	I	I	I
IS5 IT / Cyber Security	C	R	**A**	I	I	I	I	I
IS6 Supplier Relationships	C	R	I	I	I	**A**	I	I
IS7 Compliance & Audit	C	R	I	I	**A**	I	I	I
PP8 Prototype Protection	C	R	C	I	I	I	**A**	**A**
DP9 Data Protection	C	R	I	I	**A**	I	I	I

Key: R – Responsible A – Accountable C – Consulted I – Informed

To maintain maturity, organizations should establish a version-controlled “RACI Register” showing who approved the current matrix and when it was last validated. Each control owner listed must understand their obligations, and evidence of awareness—such as committee minutes or acknowledgment records—should be stored in the ISMS repository.

- **Evidence: Examples:** signed RACI Register, organizational chart, meeting minutes confirming review.
- **Common Failures:** undefined ownership for cross-functional processes, outdated matrices not reflecting personnel changes.
- **Maturity Goal:** Level 3 (Defined) for AL2 and Level 4 (Quantitatively Controlled) for AL3, where responsibility mapping is system-linked and updated automatically with organizational changes.

5. Maturity Model (0—5)

The TISAX maturity model defines how effectively an organization implements, measures, and improves its information-security controls. Rather than viewing compliance as a binary state, the model recognizes that capability evolves over time. Assessors evaluate not only whether a control exists but also how consistently it operates, how well it is measured, and how improvement is driven.

Maturity ratings provide transparency between business partners and help prioritize remediation. Higher maturity levels correspond to stronger governance discipline, broader adoption, and greater automation. Organizations should maintain a maturity-tracking dashboard within their ISMS to visualize current and target levels across all domains.

Level	Description	Core Characteristics	Typical Evidence
0 – Not Implemented	No control, process, or documentation exists.	Reactive or unaware posture.	Absence of policy or procedure; no record of activity.
1 – Initial	Ad hoc and unstructured activities.	Success depends on individual effort; no formal assignment of roles.	Emails, informal checklists, personal notes.
2 – Managed	Policies and procedures exist but are inconsistently applied.	Partial coverage; limited evidence of training or review.	Draft policies, some logs, limited audit trail.
3 – Defined	Controls are standardized and enforced organization-wide.	Roles clearly assigned; activities documented and repeatable.	Approved policies, training records, audits, management reviews.
4 – Quantitatively Controlled	Metrics and automation drive proactive management.	Performance indicators monitored; data-driven improvements.	Dashboards, trend reports, KPI analyses, corrective-action logs.
5 – Optimized	Continuous improvement embedded in culture and strategy.	Predictive analytics, benchmarking, and lessons learned used for prevention.	Executive KPIs, process-maturity audits, annual strategic reviews.

Applying the Model

Each control in the ISA catalog is scored independently from 0 to 5. Auditors validate self-assessments by reviewing supporting evidence and conducting interviews. The goal is not to achieve “perfect 5s,” but to demonstrate that controls are mature enough to manage risk relative to the assessment level:

- **AL1** organizations should target Level 2 (Managed).
- **AL2** organizations should target Level 3 (Defined).
- **AL3** organizations should target Level 4 (Quantitatively Controlled).

Continuous Improvement

Maturity levels should be tracked quarterly through internal audits and management reviews. Progress from one level to the next is usually driven by formalizing processes, adding metrics, and integrating controls into business operations.
At higher levels, automation and data analytics replace manual oversight, allowing security performance to be measured with the same rigor as production or quality KPIs.

- **Evidence: Examples:** self-assessment scores, trend reports, management review minutes, corrective actions.
- **Common Failures:** static maturity levels with no improvement plan; unsubstantiated self-ratings without evidence.
- **Maturity Goal:** Maintain organization-wide Level 3 minimum; plan progression toward Level 4 through automation and metrics integration.

6. IS1 Policies and Organization

Overview

The Policies and Organization domain forms the foundation of every Information Security Management System (ISMS). It defines how governance is established, how roles are assigned, and how leadership ensures that the system remains effective and continually improved. All subsequent domains in TISAX depend on the strength of this governance layer.

An organization must prove that its information security policies are formally documented, approved, communicated, and aligned with business objectives. It must also demonstrate that management provides resources, defines responsibilities, and monitors ISMS performance through metrics and reviews.

1.1 Information Security Policies

Establish and maintain a documented, approved, and communicated set of information-security policies aligned with TISAX and organizational strategy.

Minimums

- Master Information Security Policy approved by executive management.
- Sub-policies addressing each TISAX domain (Access Control, Risk Management, Incident Response, Supplier Security, etc.).
- Defined review cycle and version control.

Implement

Create a centralized policy register listing all policies, owners, and review dates. Use consistent templates that include purpose, scope, responsibilities, and references. Publish policies on a secure internal portal with read-only access. Communicate updates through onboarding and annual awareness programs. Require electronic acknowledgment from employees to verify understanding.

- **Evidence:** Policy register, approval signatures, acknowledgment logs.
- **Acceptance: Policies:** current, accessible, and understood by employees during interviews.
- **Common Failures:** Outdated or unapproved policies; lack of employee communication records.
- **Maturity (0–5):** 0 none → 5 fully integrated policy-management automation.
- **Internal QA:** Annual policy audit with documented corrective actions.
- **Documentation: :** Information Security Policy, Policy Register, Communication Plan.

1.2 Organization of Information Security

Intent

Define an organizational framework for governing information security across business units.

Minimums

- Designated CISO or ISMS Owner with authority and resources.
- Steering Committee including IT, HR, Legal, Procurement, and Operations.
- Defined escalation and decision-making processes.

Implement

Document reporting lines and responsibilities in the ISMS Charter. Hold quarterly committee meetings reviewing KPIs, risks, and incidents. Ensure security is represented in corporate scorecards. Assign deputies to maintain continuity during absences.

- **Evidence:** ISMS Charter, committee minutes, organizational chart, KPI reports.
- **Acceptance:** Clear accountability and active management oversight.
- **Common Failures:** Inactive committees or undefined roles.
- **Maturity (0–5):** 0 none → 5 governance embedded in corporate planning cycle.
- **Internal QA:** Annual charter review.
- **Documentation: :** ISMS Charter, Organizational Chart, Meeting Minutes.

1.3 Asset Management

Intent

Identify and classify all information assets to ensure appropriate protection.

Minimums

- Comprehensive asset inventory including hardware, software, and data.
- Classification scheme (e.g., Confidential, Internal, Public).
- Assigned owners responsible for asset protection.

Implement

Establish a central Configuration Management Database (CMDB) or inventory spreadsheet. Include asset ID, owner, location, classification, and review frequency. Label physical assets and secure storage areas. Reconcile inventories quarterly and remove obsolete entries.

- **Evidence:** Asset register, labels, reconciliation reports.
- **Acceptance:** All critical assets classified and owned.
- **Common Failures:** Shadow IT, missing data classification, untracked cloud resources.
- **Maturity (0–5):** 0 none → 5 automated CMDB integration.
- **Internal QA:** Quarterly inventory audit.
- **Documentation:** Asset Management Policy and Procedure.

1.4 Information Security Risk Management

Intent

Identify, evaluate, and treat risks to confidentiality, integrity, and availability.

Minimums

- Documented risk-assessment methodology aligned with ISO 27005.
- Formal risk register with owners and status tracking.
- Defined risk appetite approved by management.

Implement

Conduct risk assessments at least annually or after significant changes. Calculate likelihood × impact, prioritize treatment plans, and assign responsibilities. Link risks to controls and incidents for trend analysis. Report residual risk to leadership for acceptance.

- **Evidence:** Risk register, treatment plans, risk reports.
- **Acceptance:** Residual risks within approved tolerance.
- **Common Failures:** Outdated registers, no linkage to controls.
- **Maturity (0–5):** 0 none → 5 predictive analytics for risk forecasting.
- **Internal QA:** Quarterly risk review.
- **Documentation:** Risk Management Policy and Register.

1.5 Assessments and ISMS Review

Intent

Verify ISMS effectiveness through audits and management reviews.

Minimums

- Documented internal audit program covering all domains.
- Annual management review evaluating performance and resources.

Implement

Schedule audits based on risk and previous findings. Track nonconformities in a CAPA system. Summarize results and recommendations for executive approval. Use management reviews to set objectives and allocate resources for improvement.

- **Evidence:** Audit reports, CAPA register, review minutes.
- **Acceptance:** Findings closed on time and documented.
- **Common Failures:** Unresolved nonconformities or missing management reviews.
- **Maturity (0–5):** 0 none → 5 integrated audit metrics dashboard.
- **Internal QA:** Annual audit effectiveness evaluation.
- **Documentation:** Internal Audit Plan, CAPA Tracker, Review Report.

1.6 Incident and Crisis Management

Intent

Ensure prompt detection, response, and recovery from information-security incidents.

Minimums

- Documented Incident Response Plan (IRP).
- Defined incident classification and escalation criteria.
- Crisis management team with clear communication protocols.

Implement

Train staff to report incidents immediately to the ISMS Owner or IT helpdesk. Document investigations, containment, root-cause analysis, and lessons learned. Conduct annual incident-response exercises simulating cyber and prototype events. Integrate incident metrics into management reviews and risk updates.

- **Evidence:** Incident tickets, post-incident reports, exercise records.
- **Acceptance:** Incidents classified and resolved within defined SLA; corrective actions tracked to closure.
- **Common Failures:** Unreported events, no follow-up analysis, inconsistent logging.
- **Maturity (0–5):** 0 none → 5 continuous monitoring and automated response.
- **Internal QA:** Annual IRP exercise review.
- **Documentation:** Incident Response Plan, Crisis Management Manual, Lessons-Learned Report.

7. IS2 Human Resources Security

Overview

Human resources security ensures that individuals who access information systems understand and fulfill their security responsibilities before, during, and after employment. This domain focuses on minimizing insider risk, embedding security awareness, and ensuring departures or transfers are handled securely and consistently. Auditors often trace personnel records, training logs, and disciplinary actions to verify that human factors are adequately managed within the ISMS.

2.1 Pre-Employment Screening

Intent

Ensure candidates for employment, contractors, and third-party users are subject to background verification proportional to the organization’s risk.

Minimums

- Background checks conducted in accordance with local law and job criticality.
- Verification of identity, education, and employment history.
- Confidential handling of results and retention per privacy rules.

Implement

Develop a formal background-screening procedure defining when checks occur, who performs them, and what documentation is required. Require signed confidentiality and acceptable-use agreements prior to granting access to systems. Engage third-party agencies where allowed by law.

- **Evidence:** Screening logs, signed agreements, privacy notices.
- **Acceptance:** All personnel screened and cleared prior to access.
- **Common Failures:** Incomplete verification, missing documentation, or privacy violations.
- **Maturity (0–5):** 0 none → 5 automated HR integration with digital records.
- **Internal QA:** Annual audit of screening compliance.
- **Documentation:** Pre-Employment Screening Procedure, Confidentiality Agreement Template.

2.2 Onboarding and Security Training

Intent

Embed security awareness from the start of employment and ensure all staff understand their responsibilities.

Minimums

- Mandatory onboarding security orientation.
- Completion of annual refresher training.
- Tracking of completion through HR systems.

Implement

Develop an online or instructor-led security-training program covering acceptable use, phishing awareness, data-classification rules, and incident reporting. Integrate the module into onboarding workflows so that new hires must complete it before system access is activated.

- **Evidence:** Training completion logs, training materials, acknowledgment records.
- **Acceptance:** 100 % completion for active staff.
- **Common Failures:** No refresher training or lack of completion tracking.
- **Maturity (0–5):** 0 none → 5 adaptive training based on risk behavior analytics.
- **Internal QA:** Quarterly training completion review.
- **Documentation:** Security Awareness Policy, Training Program Guide.

2.3 During Employment

Intent

Ensure that security responsibilities remain clear and enforced throughout employment.

Minimums

- Role-based access rights reviewed at least annually.
- Disciplinary process defined for policy breaches.
- Managers accountable for security conduct within teams.

Implement

Require annual policy acknowledgments and periodic privilege reviews. HR and IT collaborate to ensure promotions, transfers, or role changes trigger access reviews. Include security KPIs in performance evaluations.

- **Evidence:** Role-review reports, acknowledgment confirmations, disciplinary logs.
- **Acceptance:** Ongoing compliance and timely remediation of issues.
- **Common Failures:** Stale access privileges, inconsistent policy enforcement.
- **Maturity (0–5):** 0 none → 5 continuous monitoring of user behavior and alerts.
- **Internal QA:** Semi-annual access review.
- **Documentation:** Employee Lifecycle Procedure, Disciplinary Policy.

2.4 Termination or Change of Employment

Intent

Ensure security responsibilities and access rights are properly managed during termination or reassignment.

Minimums

- Formal offboarding checklist.
- Immediate revocation of system and physical access.
- Return of assets and retrieval of credentials.

Implement

Coordinate HR and IT to synchronize terminations. Remove or disable accounts within 24 hours of notice. Collect badges, keys, laptops, and mobile devices. Conduct exit interviews reminding employees of confidentiality obligations.

- **Evidence:** Offboarding checklists, access-removal tickets, signed acknowledgments.
- **Acceptance:** No active accounts for terminated staff.
- **Common Failures:** Delayed access removal or unreturned assets.
- **Maturity (0–5):** 0 none → 5 automated identity-lifecycle management.
- **Internal QA:** Quarterly termination audit.
- **Documentation:** Offboarding Procedure, Access Revocation Form.

2.5 Security Culture and Behavior

Intent

Foster a culture where security is viewed as a shared responsibility.

Minimums

- Regular awareness campaigns and internal communications.
- Reporting channels for security concerns.
- Recognition programs encouraging positive behavior.

Implement

Run quarterly campaigns with topics aligned to current threats. Use internal newsletters, posters, and intranet banners. Recognize employees who demonstrate exemplary compliance behavior. Conduct anonymous surveys to measure awareness.

- **Evidence:** Campaign materials, survey reports, recognition logs.
- **Acceptance:** Improved awareness scores and engagement metrics.
- **Common Failures:** Static campaigns or no measurement of impact.
- **Maturity (0–5):** 0 none → 5 data-driven culture analytics.
- **Internal QA:** Annual culture assessment.
- **Documentation:** Security Culture Program Plan.

8. IS3 Physical Security

Overview

Physical security under TISAX focuses on preventing unauthorized physical access, damage, and interference to facilities, equipment, and information. It ensures that controls around buildings, secure areas, visitor management, and environmental protection are robust and consistently applied. Assessors often review access logs, CCTV retention, and data center safeguards to confirm these controls are operating effectively.

3.1 Physical Access Control

Intent

Ensure access to buildings and secure areas is restricted to authorized personnel only.

Minimums

- Access granted only to authorized personnel.
- Badge- or key-based access control systems in place.
- Visitor registration and escort procedures.

Implement

Deploy electronic access systems integrated with HR records to automatically revoke access upon termination. Maintain visitor logs and require visible identification badges. Conduct periodic audits comparing system access records to employment lists. Secure sensitive areas such as data centers, server rooms, and prototype storage behind multi-factor access barriers (badge + PIN or biometric).

- **Evidence:** Access logs, visitor logs, badge assignment reports.
- **Acceptance:** No unauthorized entries; visitor management effective.
- **Common Failures:** Shared badges, unrecorded visitors, inactive card removal delays.
- **Maturity (0–5):** 0 none → 5 integrated, biometric, and monitored access systems.
- **Internal QA:** Semi-annual access control validation.
- **Documentation:** Physical Access Policy, Visitor Management Procedure.

3.2 Secure Areas and Zoning

Intent

Define and control secure areas based on risk and data sensitivity.

Minimums

- Segregated zones (public, restricted, secure).
- Clear physical boundaries and signage.
- Access reviewed and approved by management.

Implement

Classify each facility zone by sensitivity. Implement perimeter fences, locked doors, and access-controlled corridors. Apply zoning to office layouts and manufacturing floors. Display warning signage. Restrict photography or recording devices within secure areas.

- **Evidence:** Floor plans, zoning diagrams, approval forms.
- **Acceptance:** Physical zones established and enforced.
- **Common Failures:** Inconsistent labeling or lack of secure segregation.
- **Maturity (0–5):** 0 none → 5 risk-based zoning with automated controls.
- **Internal QA:** Annual zoning verification.
- **Documentation:** Secure Area Design Standard, Zoning Map.

3.3 Equipment Security

Intent

Protect equipment and media from loss, damage, theft, or compromise.

Minimums

- Fixed and mobile assets secured at all times.
- Secure disposal or reuse procedures in place.
- Protection from power loss, fire, and water damage.

Implement

Install uninterruptible power supplies (UPS) and environmental sensors (temperature, humidity, smoke). Enforce workstation-lock policies. Securely store laptops and removable media in locked drawers. Require chain-of-custody documentation for prototype materials.

- **Evidence:** Asset logs, UPS test records, disposal certificates.
- **Acceptance:** No loss or damage incidents unaccounted for.
- **Common Failures:** Unsecured laptops, improper disposal.
- **Maturity (0–5):** 0 none → 5 continuous monitoring of environmental factors.
- **Internal QA:** Quarterly asset-security inspection.
- **Documentation:** Equipment Security Policy, Disposal Procedure.

3.4 Environmental and Facility Protection

Intent

Ensure facilities have environmental safeguards preventing system outages or data loss.

Minimums

- Fire detection and suppression systems.
- Backup power and surge protection.
- Climate control and regular maintenance.

Implement

Install redundant HVAC, smoke detectors, and sprinkler systems. Test backup generators quarterly. Maintain service contracts for critical infrastructure. Implement alarm systems monitored 24/7 by security teams or external services.

- **Evidence:** Maintenance logs, test reports, vendor SLAs.
- **Acceptance:** Operational safety systems verified and tested.
- **Common Failures:** Expired maintenance contracts, untested systems.
- **Maturity (0–5):** 0 none → 5 predictive environmental monitoring with analytics.
- **Internal QA:** Annual environmental controls audit.
- **Documentation:** Facility Maintenance Log, Fire Safety Plan, Generator Test Records.

3.5 Prototype Handling Security

Intent

Protect physical prototypes and confidential automotive materials against theft or unauthorized disclosure.

Minimums

- Designated prototype security zones.
- Controlled storage and access logs.
- Transport and disposal protocols.

Implement

Develop and enforce prototype storage standards aligned with NDAs and manufacturer agreements. Maintain chain-of-custody logs for prototype transfers. Enforce escort rules for visitors during prototype events or photography restrictions.

- **Evidence:** Custody logs, event security checklists, storage access lists.
- **Acceptance:** No untracked prototype exposure incidents.
- **Common Failures:** Unlogged transfers or inadequate escorting.
- **Maturity (0–5):** 0 none → 5 integrated prototype traceability system.
- **Internal QA:** Post-event audits and reconciliation.
- **Documentation:** Prototype Protection Policy, Handling Register.

9. IS4 Identity & Access Management

Overview

Identity and Access Management (IAM) ensures that access to systems, applications, and information is strictly controlled based on user identity, business need, and authorization level. Under TISAX 6.0.3, IAM requirements ensure that only legitimate, verified individuals access the right systems at the right time, with full traceability and prompt revocation when access is no longer required. Assessors focus heavily on role-based access control, privilege review, authentication mechanisms, and evidence of timely account deactivation.

4.1 User Registration and Deregistration

Intent

Ensure that user accounts are created, modified, and deleted in a controlled and auditable manner.

Minimums

- Documented account provisioning and deprovisioning process.
- Unique user IDs; no shared accounts.
- Timely removal of access for terminated or transferred employees.

Implement

Integrate IAM processes with HR workflows. Accounts are created only after documented management approval and completion of security onboarding. Use identity-governance tools to automate provisioning and deactivation. Regularly reconcile active accounts against HR records.

- **Evidence:** Access request forms, provisioning logs, reconciliation reports.
- **Acceptance:** 100% account alignment with HR data.
- **Common Failures:** Orphaned accounts, generic IDs, delayed removals.
- **Maturity (0–5):** 0 none → 5 full lifecycle automation with certification workflow.
- **Internal QA:** Monthly reconciliation audit.
- **Documentation:** User Access Management Procedure, Deprovisioning Checklist.

4.2 User Access Provisioning

Intent

Ensure that users receive only the minimum access necessary for their duties.

Minimums

- Role-based access control (RBAC) defined for each function.
- Management approval required for all privileged roles.
- Access reviewed at least quarterly.

Implement

Document job roles with predefined access entitlements. Implement segregation of duties between requesters and approvers. Automate workflows through ticketing or IAM tools. Conduct quarterly reviews comparing privileges to job functions.

- **Evidence:** Role definitions, approval logs, review reports.
- **Acceptance:** Access levels match job requirements with management verification.
- **Common Failures:** Over-privileged accounts or missing review evidence.
- **Maturity (0–5):** 0 none → 5 adaptive access provisioning using analytics.
- **Internal QA:** Quarterly access certification.
- **Documentation:** Access Control Policy, RBAC Matrix, Review Report.

4.3 Privileged Access Management

Intent

Control, monitor, and audit privileged access to critical systems.

Minimums

- Dedicated privileged accounts separated from standard ones.
- Multi-factor authentication (MFA) for administrative access.
- Session logging and approval for elevated access.

Implement

Deploy Privileged Access Management (PAM) solutions to control and record admin sessions. Require just-in-time access where feasible. Store credentials in a secured, encrypted vault with check-in/check-out tracking.

- **Evidence:** PAM logs, MFA configuration screenshots, approval records.
- **Acceptance:** No unmonitored administrative access.
- **Common Failures:** Shared admin accounts, disabled logging, weak MFA.
- **Maturity (0–5):** 0 none → 5 continuous privileged-session monitoring.
- **Internal QA:** Semi-annual PAM review.
- **Documentation:** Privileged Access Policy, PAM Configuration Guide.

4.4 Authentication and Password Management

Intent

Ensure secure authentication processes protect systems and data.

Minimums

- Strong password policies aligned with industry standards.
- MFA enforced for remote and privileged users.
- Periodic password rotation and complexity requirements.

Implement

Define a password policy specifying minimum length, complexity, reuse restrictions, and change intervals. Enforce MFA for all remote and sensitive systems. Integrate authentication logs into the SIEM for anomaly detection.

- **Evidence:** Authentication logs, password policy, MFA configuration.
- **Acceptance:** MFA implemented and effective; no weak-password findings.
- **Common Failures:** Default credentials, missing MFA enforcement.
- **Maturity (0–5):** 0 none → 5 adaptive authentication based on behavioral analytics.
- **Internal QA:** Quarterly password compliance audit.
- **Documentation:** Password Policy, MFA Implementation Plan.

4.5 Access Review and Recertification

Intent

Verify regularly that all access rights remain appropriate.

Minimums

- Formal access-review process performed quarterly.
- Results documented and approved by management.
- Remediation tracked for discrepancies.

Implement

Automate user-access certification through IAM or GRC platforms. Distribute review reports to managers and require electronic acknowledgment. Track remediation actions to completion. Integrate review status into compliance dashboards.

- **Evidence:** Review reports, remediation logs, manager approvals.
- **Acceptance:** All excessive privileges identified and removed.
- **Common Failures:** Missed reviews or incomplete follow-up.
- **Maturity (0–5):** 0 none → 5 real-time access analytics and auto-remediation.
- **Internal QA:** Quarterly review completeness check.
- **Documentation:** Access Review Procedure, Certification Reports.

4.6 Logging and Monitoring of Access

Intent

Provide accountability for all user and admin activities through centralized logging and analysis.

Minimums

- System and application logs collected and retained.
- Alerts for unauthorized or unusual access patterns.
- Integration with SIEM or monitoring platforms.

Implement

Implement log forwarding from key systems to a centralized SIEM. Define correlation rules for privileged actions and failed logins. Retain logs for at least 12 months or per contractual requirements. Conduct regular reviews of anomalies.

- **Evidence:** SIEM dashboards, log samples, alert reports.
- **Acceptance:** Unauthorized access attempts detected and investigated.
- **Common Failures:** Disabled logging or excessive log retention gaps.
- **Maturity (0–5):** 0 none → 5 predictive anomaly detection and response.
- **Internal QA:** Monthly SIEM rule audit.
- **Documentation:** Logging and Monitoring Policy, SIEM Operations Guide.

10. IS5 IT / Cyber Security

Overview

The IT / Cyber Security domain ensures that all systems and networks are hardened, monitored, and maintained to prevent unauthorized access or disruption. It encompasses the lifecycle of technical security — from configuration to ongoing monitoring — and demonstrates how the organization enforces baseline standards and responds to emerging threats. Assessors expect consistent technical implementation aligned with policy requirements, traceable maintenance records, and evidence of continuous improvement.

5.1 Configuration Management

Intent

Establish secure configurations for all IT systems, applications, and network components to reduce vulnerabilities.

Minimums

- Documented baseline configurations.
- Standardized build procedures and change control.
- Periodic configuration audits.

Implement

Define system hardening standards referencing CIS Benchmarks or vendor baselines. Use automated configuration management tools (e.g., Ansible, SCCM) to deploy secure settings. Record deviations with risk justification and approval. Conduct quarterly configuration drift analyses and report exceptions to management.

- **Evidence:** Configuration baselines, audit logs, deviation reports.
- **Acceptance:** All critical systems aligned with approved baselines.
- **Common Failures:** Untracked configuration changes, inconsistent patch states.
- **Maturity (0–5):** 0 none → 5 automated compliance enforcement via CM tools.
- **Internal QA:** Quarterly baseline validation.
- **Documentation:** Configuration Management Policy, Hardening Standards.

5.2 Patch and Vulnerability Management

Intent

Ensure vulnerabilities are identified, assessed, prioritized, and remediated within defined timelines.

Minimums

- Documented patch management policy.
- Routine vulnerability scanning of systems and networks.
- Defined remediation timeframes based on severity.

Implement

Deploy automated vulnerability scanning tools to identify and classify findings. Maintain a patch calendar coordinated with IT operations. Document risk acceptance for deferred patches. Correlate vulnerabilities with asset criticality and track closure metrics.

- **Evidence:** Scan reports, patch deployment logs, risk-acceptance records.
- **Acceptance:** No high-severity vulnerabilities exceeding defined SLA.
- **Common Failures:** Missed patches, no documented approvals for deferrals.
- **Maturity (0–5):** 0 none → 5 predictive vulnerability management integrated with threat intelligence.
- **Internal QA:** Monthly patch compliance review.
- **Documentation:** Patch Management Procedure, Vulnerability Register.

5.3 Malware Protection

Intent

Prevent, detect, and respond to malware infections across all systems.

Minimums

- Endpoint protection software installed and active.
- Centralized monitoring and signature updates.
- Regular scanning and incident response procedures.

Implement

Deploy enterprise-grade antivirus and endpoint-detection-and-response (EDR) solutions. Enforce automatic signature updates and alerting. Integrate with the SIEM for correlation and escalation. Conduct periodic phishing simulations and response testing.

- **Evidence:** Antivirus console reports, alert logs, incident tickets.
- **Acceptance:** No unmanaged endpoints or expired protection.
- **Common Failures:** Outdated definitions, alert fatigue, no escalation path.
- **Maturity (0–5):** 0 none → 5 AI-driven threat detection and automated remediation.
- **Internal QA:** Quarterly endpoint compliance audit.
- **Documentation:** Malware Protection Policy, EDR Configuration Standard.

5.4 Network and Perimeter Security

Intent

Protect networks and communications through layered defense and continuous monitoring.

Minimums

- Firewalls, intrusion detection/prevention systems (IDS/IPS).
- Network segmentation based on data classification.
- Secure remote access using VPN and MFA.

Implement

Define network security architecture diagrams identifying trust zones. Configure firewalls with “deny by default” rules. Monitor network flows through IDS/IPS and capture logs for review. Encrypt data in transit using TLS 1.2+ or IPSec. Enforce least privilege for remote connectivity.

- **Evidence:** Firewall rule sets, VPN logs, architecture diagrams.
- **Acceptance:** Secure segmentation and active monitoring verified.
- **Common Failures:** Overly permissive firewall rules, outdated firmware.
- **Maturity (0–5):** 0 none → 5 fully segmented, monitored, and adaptive network defense.
- **Internal QA:** Biannual firewall rule audit.
- **Documentation:** Network Security Policy, Architecture Diagram, VPN Procedure.

5.5 Backup and Recovery Controls

Intent

Ensure data and system backups are available, tested, and protected against loss or corruption.

Minimums

- Backup schedule covering all critical systems.
- Offsite or immutable storage.
- Regular restore tests.

Implement

Use centralized backup solutions with encryption and retention policies. Test restores quarterly to validate recovery objectives. Protect backup credentials and restrict access to authorized personnel. Document RPO (Recovery Point Objective) and RTO (Recovery Time Objective) alignment.

- **Evidence:** Backup logs, restore test results, offsite storage reports.
- **Acceptance:** Successful restore test completion within target time.
- **Common Failures:** Unverified restores or unencrypted backups.
- **Maturity (0–5):** 0 none → 5 automated validation and immutable storage.
- **Internal QA:** Quarterly backup verification.
- **Documentation:** Backup and Recovery Policy, Restore Test Plan.

5.6 Secure Software and System Maintenance

Intent

Maintain systems securely throughout their lifecycle.

Minimums

- Supported software versions only.
- Secure change control and maintenance logs.
- Secure disposal of decommissioned assets.

Implement

Enforce change-management processes requiring impact analysis, approvals, and testing. Maintain vendor support lists and upgrade schedules. Securely wipe or destroy media before disposal. Document lifecycle states for all assets in the CMDB.

- **Evidence:** Change tickets, maintenance records, disposal certificates.
- **Acceptance:** All systems supported and securely maintained.
- **Common Failures:** Unsupported software, untracked decommissioning.
- **Maturity (0–5):** 0 none → 5 lifecycle automation with patch and asset integration.
- **Internal QA:** Semi-annual lifecycle compliance audit.
- **Documentation:** System Maintenance Procedure, Change Management Log.

11. IS6 Supplier Relationships

Overview

Supplier security under TISAX is critical because third parties often process sensitive product, prototype, or customer data. The objective is to ensure suppliers adhere to the same security requirements that apply internally. The organization must implement a structured vendor-management program covering selection, onboarding, monitoring, and offboarding. Assessors will expect documented due diligence, contractual clauses referencing TISAX or equivalent standards, and evidence of ongoing compliance oversight.

6.1 Supplier Risk Assessment

Intent

Identify and evaluate security risks associated with suppliers and service providers before engagement.

Minimums

- Formal risk assessment process for all third parties.
- Categorization by criticality and data sensitivity.
- Defined acceptance criteria before contract signing.

Implement

Establish a supplier risk-tiering framework (e.g., critical, high, medium, low). Assess each supplier's security posture using questionnaires aligned with TISAX or ISO/IEC 27001 controls. Require supporting evidence such as SOC 2, ISO certificates, or assessment results. Document risk treatment actions and approvals.

- **Evidence:** Completed questionnaires, risk evaluation forms, supplier inventory.
- **Acceptance:** All suppliers assessed prior to contract execution.
- **Common Failures:** Missing documentation or outdated risk ratings.
- **Maturity (0–5):** 0 none → 5 automated risk scoring integrated with procurement systems.
- **Internal QA:** Annual supplier risk re-evaluation.
- **Documentation:** Supplier Risk Assessment Procedure, Vendor Inventory.

6.2 Supplier Contracts and Security Clauses

Intent

Ensure contracts include enforceable information-security and confidentiality clauses.

Minimums

- Standardized contract templates with security provisions.
- NDAs required before sharing confidential data.
- Defined requirements for incident reporting and audit rights.

Implement

Work with legal and procurement teams to maintain a standard security addendum applicable to all vendors. Include breach notification timelines, data-protection clauses, and audit access language. Verify that high-risk suppliers have signed agreements before onboarding.

- **Evidence:** Executed contracts, NDA repository, contract templates.
- **Acceptance:** All active suppliers under valid agreements with security clauses.
- **Common Failures:** Missing clauses or unsigned NDAs.
- **Maturity (0–5):** 0 none → 5 contract automation with mandatory clause validation.
- **Internal QA:** Annual contract review sampling.
- **Documentation:** Standard Security Addendum, NDA Template, Supplier Contract Matrix.

6.3 Supplier Monitoring and Performance Management

Intent

Continuously monitor supplier compliance and performance against security requirements.

Minimums

- Scheduled assessments or audits for critical suppliers.
- Reporting mechanisms for security incidents.
- Documented remediation plans and tracking.

Implement

Conduct annual or biannual supplier reviews based on criticality. Require suppliers to provide updated certifications or audit reports. Monitor performance metrics such as SLA compliance and incident history. Escalate recurring issues to procurement and ISMS leadership for remediation or contract reconsideration.

- **Evidence:** Supplier audit reports, remediation logs, KPI dashboards.
- **Acceptance:** Suppliers maintain compliance; corrective actions tracked to closure.
- **Common Failures:** Lack of follow-up after findings; no performance measurement.
- **Maturity (0–5):** 0 none → 5 continuous supplier risk intelligence feeds.
- **Internal QA:** Quarterly critical-supplier reviews.
- **Documentation:** Supplier Monitoring Procedure, Audit Plan, Remediation Tracker.

6.4 Supplier Offboarding and Contract Termination

Intent

Ensure the secure disengagement of suppliers and protection of organizational information upon contract termination.

Minimums

- Formal offboarding checklist.
- Revocation of system and physical access.
- Return or certified destruction of data and assets.

Implement

Coordinate with IT and Legal to verify completion of all offboarding steps. Remove supplier accounts, retrieve credentials, and obtain written confirmation of data destruction. Archive termination documentation for audit evidence.

- **Evidence:** Offboarding checklists, destruction certificates, email confirmations.
- **Acceptance:** No residual access or retained data by former suppliers.
- **Common Failures:** Missing destruction evidence or delayed account removal.
- **Maturity (0–5):** 0 none → 5 automated access revocation through vendor systems integration.
- **Internal QA:** Post-termination audit sampling.
- **Documentation:** Supplier Termination Procedure, Data Destruction Certificate.

12. IS7 Compliance & Audit

Overview

The Compliance and Audit domain ensures that the organization meets all applicable legal, regulatory, and contractual obligations related to information security and privacy. It validates that internal controls are working as designed and that corrective actions are identified, tracked, and closed. In the TISAX framework, compliance is not a one-time exercise but a sustained state of readiness supported by transparent documentation and evidence-based reviews.

7.1 Legal and Regulatory Compliance

Intent

Identify, document, and maintain awareness of all applicable legal and regulatory requirements affecting information security and privacy.

Minimums

- Compliance register maintained and reviewed quarterly.
- Legal and privacy representatives involved in ISMS oversight.
- Defined processes for monitoring regulatory updates.

Implement

Establish a compliance register listing all applicable laws, standards, and contractual obligations (e.g., GDPR, IP protection laws, automotive regulations). Assign ownership for each requirement. Subscribe to regulatory updates or industry bulletins. Document compliance evaluations and action plans.

- **Evidence:** Compliance register, meeting minutes, action-tracking logs.
- **Acceptance:** Current, complete, and actively managed compliance register.
- **Common Failures:** Outdated entries or missing evidence of monitoring.
- **Maturity (0–5):** 0 none → 5 automated regulatory intelligence integration.
- **Internal QA:** Quarterly review and update confirmation.
- **Documentation:** Compliance Register, Legal Review Log.

7.2 Internal Audits and Self-Assessments

Intent

Evaluate the effectiveness of the ISMS through systematic, independent internal audits and self-assessments.

Minimums

- Annual audit plan approved by management.
- Auditors independent of audited areas.
- Documented nonconformities and corrective actions.

Implement

Develop a risk-based internal-audit schedule covering all domains over a two-year cycle. Train internal auditors in TISAX and ISO audit techniques. Use structured checklists to ensure consistent evidence collection. Present findings to management with root-cause analysis and remediation plans.

- **Evidence:** Audit plans, reports, CAPA logs, management review minutes.
- **Acceptance:** All planned audits completed with documented follow-up.
- **Common Failures:** Unclosed findings or incomplete corrective actions.
- **Maturity (0–5):** 0 none → 5 fully automated audit lifecycle in GRC tool.
- **Internal QA:** Annual auditor competence review.
- **Documentation:** Internal Audit Procedure, CAPA Tracker, Audit Reports.

7.3 External Assessments and Certifications

Intent

Maintain readiness for third-party TISAX assessments and other certifications.

Minimums

- Defined process for external audit coordination.
- Repository of prior assessment reports and responses.
- **Evidence:** tracking for all corrective actions.

Implement

Assign an Assessment Coordinator to manage scheduling, evidence collection, and liaison with auditors. Conduct mock assessments to test readiness. Maintain centralized documentation, cross-referenced to TISAX control IDs. Track and verify closure of external findings before re-assessment.

- **Evidence:** Assessment schedules, evidence repository, closure reports.
- **Acceptance:** No overdue external corrective actions.
- **Common Failures:** Missing evidence or fragmented documentation.
- **Maturity (0–5):** 0 none → 5 integrated certification-tracking dashboard.
- **Internal QA:** Annual mock audit validation.
- **Documentation:** Assessment Readiness Plan, External Audit Tracker.

7.4 Corrective and Preventive Actions (CAPA)

Intent

Ensure nonconformities and audit findings are addressed effectively and lead to sustainable improvement.

Minimums

- Documented CAPA process with defined responsibilities.
- Root-cause analysis performed for each nonconformity.
- Verification of effectiveness before closure.

Implement

Log all findings into a centralized CAPA tracker. Assign owners and due dates. Require root-cause analysis and define preventive measures. Track completion and validate effectiveness through re-audits. Report CAPA metrics to leadership monthly.

- **Evidence:** CAPA logs, follow-up reports, closure confirmations.
- **Acceptance:** All findings closed within target timelines.
- **Common Failures:** Recurring issues or superficial corrective actions.
- **Maturity (0–5):** 0 none → 5 predictive issue management using trend analysis.
- **Internal QA:** Monthly CAPA status review.
- **Documentation:** CAPA Procedure, Root Cause Template, Corrective Action Log.

13. PP8 Prototype Protection

Overview

The Prototype Protection domain addresses the automotive industry’s need to safeguard sensitive vehicle designs, parts, and test data throughout development and pre-release stages. TISAX requires demonstrable controls for the handling, storage, transport, and presentation of prototypes—whether physical objects, CAD files, or digital data. Compliance protects intellectual property, brand reputation, and contractual trust among OEMs, suppliers, and engineering partners.

8.1 Prototype Security Governance

Intent

Establish governance structures and procedures to manage prototype security across all stages of design, testing, and disposal.

Minimums

- Documented Prototype Protection Policy.
- Defined roles and responsibilities for prototype handling.
- Approved facilities and secure storage areas.

Implement

Develop a cross-functional prototype governance committee including Engineering, Security, and Supply Chain. Define end-to-end prototype lifecycle stages (creation, transfer, testing, return, destruction). Assign a Prototype Security Officer responsible for oversight and compliance reporting. Conduct annual awareness training specific to prototype confidentiality.

- **Evidence:** Governance charter, training logs, policy documents.
- **Acceptance:** Formal governance established with active oversight.
- **Common Failures:** No centralized responsibility or inconsistent practices across departments.
- **Maturity (0–5):** 0 none → 5 enterprise-wide governance with automated tracking.
- **Internal QA:** Annual prototype governance audit.
- **Documentation:** Prototype Protection Policy, Governance Charter.

8.2 Secure Storage and Facility Controls

Intent

Protect physical prototypes and related materials within secure facilities.

Minimums

- Restricted access areas with controlled entry logs.
- CCTV coverage for all storage zones.
- Separation of prototype areas from standard production or office zones.

Implement

Designate restricted prototype rooms with badge and video monitoring. Maintain 24/7 CCTV recording retention for a minimum of 30 days. Label storage units clearly as confidential. Enforce a “no personal device” rule inside prototype areas. Review access logs monthly.

- **Evidence:** Access logs, CCTV retention reports, facility blueprints.
- **Acceptance:** Secure zones validated and monitored without unauthorized entry.
- **Common Failures:** Shared keys, expired CCTV retention, or unlabeled materials.
- **Maturity (0–5):** 0 none → 5 AI-driven intrusion detection and automated visitor alerts.
- **Internal QA:** Monthly facility access reconciliation.
- **Documentation:** Secure Area Layout, CCTV Audit Report, Storage Control Checklist.

8.3 Transport and Logistics of Prototypes

Intent

Ensure prototypes and related materials are securely transported between locations.

Minimums

- Approved logistics providers with signed NDAs.
- Chain-of-custody documentation for every transfer.
- Secure packaging and labeling procedures.

Implement

Implement a transport policy requiring sealed, tamper-evident containers. Assign escorts for high-value transfers. Require supplier and driver identity verification. Maintain chain-of-custody forms including pickup and delivery timestamps. Review carrier compliance annually.

- **Evidence:** Transport manifests, custody logs, carrier contracts.
- **Acceptance:** End-to-end custody documentation available for every shipment.
- **Common Failures:** Missing forms, unverified drivers, or unsecured vehicles.
- **Maturity (0–5):** 0 none → 5 GPS-tracked shipments with automated custody updates.
- **Internal QA:** Quarterly logistics-security review.
- **Documentation:** Prototype Transport Procedure, Custody Log Template.

8.4 Events, Testing, and Public Exposure

Intent

Protect prototypes during exhibitions, road tests, and media events.

Minimums

- Defined approval process for public display.
- Non-disclosure and photography restrictions enforced.
- Trained event staff and controlled participant access.

Implement

Require event risk assessments before prototype exposure. Enforce restricted photography zones and NDAs for all attendees, including media. Maintain visitor lists and escort logs. Store covered prototypes when inactive. Perform debriefs post-event to document compliance.

- **Evidence:** Event risk assessments, NDAs, attendee logs, photographs.
- **Acceptance:** No prototype leakage incidents or unauthorized images.
- **Common Failures:** Weak event supervision or missing NDA controls.
- **Maturity (0–5):** 0 none → 5 real-time media-monitoring and alerting.
- **Internal QA:** Post-event review and incident report.
- **Documentation:** Event Security Plan, NDA Forms, Debrief Report.

8.5 Destruction and End-of-Life Handling

Intent

Ensure prototypes and related confidential materials are irreversibly destroyed after use.

Minimums

- Documented destruction process and approval.
- Secure disposal vendor contracts with certifications.
- Verification of destruction.

Implement

Label items for destruction and track them through signed approval forms. Contract certified disposal vendors who provide certificates of destruction. Document destruction videos or photos for high-value prototypes. Maintain records for at least five years or per OEM agreement.

- **Evidence:** Destruction logs, vendor certificates, photo documentation.
- **Acceptance:** All prototypes verified destroyed; no residual materials retained.
- **Common Failures:** Missing certificates or undocumented partial destruction.
- **Maturity (0–5):** 0 none → 5 fully audited digital destruction workflow.
- **Internal QA:** Annual destruction audit.
- **Documentation:** Prototype Destruction Procedure, Vendor Certification File.

14. DP9 Data Protection

Overview

The Data Protection domain establishes the organizational and technical safeguards required to ensure lawful processing of personal data. TISAX integrates GDPR principles directly into its assessment model, requiring documented evidence of consent management, data-subject rights, lawful processing bases, and breach-notification procedures. Auditors evaluate the company's ability to demonstrate accountability—meaning every processing activity must be explainable, risk-assessed, and compliant with both contractual and legal obligations.

9.1 Governance and Accountability

Intent

Ensure clear governance for privacy and data-protection compliance.

Minimums

- Appointment of a qualified Data Protection Officer (DPO).
- Defined roles for privacy management, incident response, and training.
- Documented Data Protection Policy reviewed annually.

Implement

Establish a privacy-governance committee chaired by the DPO. Integrate privacy considerations into all projects through a "privacy-by-design" review step. Maintain a privacy compliance calendar covering audits, training, and DPIA schedules.

- **Evidence:** DPO appointment letter, policy document, committee minutes.
- **Acceptance:** DPO formally designated and active oversight documented.
- **Common Failures:** Unclear accountability or missing governance documentation.
- **Maturity (0–5):** 0 none → 5 integrated privacy management platform.
- **Internal QA:** Annual DPO report review.
- **Documentation:** Data Protection Policy, Governance Charter, Privacy Calendar.

9.2 Lawful Basis for Processing

Intent

Ensure all personal data processing activities have a clearly documented lawful basis.

Minimums

- Data mapping identifying processing purposes and bases.
- Consent, contract, legal obligation, legitimate interest, or vital interest recorded.
- Periodic review of processing justifications.

Implement

Maintain a Record of Processing Activities (RoPA) mapping each data type, purpose, and lawful basis. Conduct annual validations to ensure accuracy. Require explicit consent where necessary and store consent evidence securely.

- **Evidence:** RoPA entries, consent forms, validation logs.
- **Acceptance:** All processing documented with legitimate legal bases.
- **Common Failures:** Missing justification or unverified consent storage.
- **Maturity (0–5):** 0 none → 5 automated processing-basis management with dynamic updates.
- **Internal QA:** Annual RoPA audit.
- **Documentation:** RoPA Register, Consent Policy, Validation Report.

9.3 Data-Subject Rights Management

Intent

Enable and document fulfillment of individual rights requests under GDPR or equivalent laws.

Minimums

- Procedure for access, rectification, erasure, and portability.
- Defined response timelines (typically 30 days).
- Secure identity-verification method.

Implement

Create a centralized privacy-request portal or workflow. Train staff to identify and escalate requests promptly. Track requests to completion and record evidence of fulfillment. Conduct mock rights-request exercises annually to test readiness.

- **Evidence:** Rights-request logs, response templates, verification records.
- **Acceptance:** All rights fulfilled within deadlines and logged.
- **Common Failures:** Delayed responses or no tracking of requests.
- **Maturity (0–5):** 0 none → 5 automated privacy-request management integrated with ticketing systems.
- **Internal QA:** Quarterly rights-request audit.
- **Documentation:** Data-Subject Rights Procedure, Request Tracker, Response Templates.

9.4 Data Breach Management

Intent

Detect, report, and mitigate personal-data breaches promptly and effectively.

Minimums

- Incident-response process aligned with GDPR Articles 33–34.
- Notification to authorities within 72 hours when required.
- Root-cause analysis and mitigation tracking.

Implement

Integrate breach-response steps into the ISMS Incident Response Plan. Establish decision criteria for notification triggers. Maintain communication templates for authorities and affected individuals. Conduct annual breach-simulation exercises.

- **Evidence:** Incident logs, notification forms, post-incident reports.
- **Acceptance:** Breach responses timely and compliant with legal obligations.
- **Common Failures:** Late notifications or incomplete records.
- **Maturity (0–5):** 0 none → 5 fully integrated breach-response automation with metrics dashboards.
- **Internal QA:** Annual breach-response drill.
- **Documentation:** Breach Notification Procedure, Incident Register, Lessons-Learned Report.

9.5 Data Retention and Disposal

Intent

Ensure personal data is retained only as long as necessary and securely deleted thereafter.

Minimums

- Data-retention schedule approved by Legal and DPO.
- Secure deletion or anonymization processes.
- Documentation of retention exceptions.

Implement

Create and maintain a data-retention matrix mapping data types to retention periods and deletion methods. Automate deletion through data-lifecycle tools where possible. Verify destruction via certificates or deletion logs.

- **Evidence:** Retention matrix, deletion logs, certificates of destruction.
- **Acceptance:** No data retained beyond approved limits.
- **Common Failures:** Undefined retention periods or manual deletion without verification.
- **Maturity (0–5):** 0 none → 5 automated lifecycle-based data-retention management.
- **Internal QA:** Annual retention-policy audit.
- **Documentation:** Data Retention Policy, Disposal Log, Retention Schedule.

9.6 Privacy Impact Assessments (DPIA)

Intent

Evaluate and mitigate privacy risks for high-risk processing activities.

Minimums

- Defined DPIA procedure and criteria for triggering assessments.
- Documented results with approval and follow-up actions.
- Integration with project-management lifecycle.

Implement

Mandate DPIAs for new systems, applications, or vendors processing sensitive data. Use standardized templates to assess purpose, necessity, proportionality, and residual risk. Require DPO review and management approval before go-live.

- **Evidence:** Completed DPIA forms, approval signatures, mitigation logs.
- **Acceptance:** DPIAs conducted timely and approved before processing starts.
- **Common Failures:** DPIAs performed post-implementation or missing mitigation follow-up.
- **Maturity (0–5):** 0 none → 5 automated DPIA workflow integrated with system-change approvals.
- **Internal QA:** Annual DPIA quality review.
- **Documentation:** DPIA Procedure, Risk Register, Mitigation Tracker.

15. Training & Awareness Program

Overview

A robust training and awareness program ensures that security and privacy principles become embedded in daily operations rather than existing only in documentation. TISAX emphasizes that personnel behavior is one of the most significant risk factors affecting information confidentiality, integrity, and availability. Organizations must maintain continuous, measurable education programs tailored to different job functions, roles, and risk levels.

15.1 Program Structure and Objectives

Intent

Establish a formal, documented security and privacy awareness program for all personnel, including contractors and suppliers.

Minimums

- Annual training plan approved by management.
- Role-based modules (e.g., developers, HR, executives, IT).
- Defined success metrics (completion rate, quiz scores, survey feedback).

Implement

Develop and publish a Training & Awareness Policy describing scope, audience, frequency, and methods. Use an LMS or similar tool to assign courses and track completion. Refresh modules annually and when new risks emerge. Maintain attendance logs and report completion metrics to leadership.

- **Evidence:** Training policy, completion reports, evaluation metrics.
- **Acceptance:** ≥ 95% completion rate and active management oversight.
- **Common Failures:** One-time or generic training without engagement measurement.
- **Maturity (0–5):** 0 none → 5 adaptive, behavior-based learning with analytics.
- **Internal QA:** Annual review of training effectiveness.
- **Documentation:** Training & Awareness Policy, Annual Plan, Completion Dashboard.

15.2 Specialized and Technical Training

Intent

Provide advanced instruction for personnel performing high-risk or technical functions.

Minimums

- Defined curriculum for system administrators, developers, SOC staff, and incident responders.
- Alignment with evolving threat landscape and regulatory changes.
- Certification or documented proof of participation.

Implement

Create specialized courses such as secure coding, privileged access management, and vulnerability handling. Require certification (e.g., CompTIA Security+, ISO 27001 Lead Implementer, GDPR Practitioner) for designated staff. Maintain training records within HR systems.

- **Evidence:** Certificates, attendance records, training matrix.
- **Acceptance:** Key roles trained and certified as required.
- **Common Failures:** No refresher training or outdated materials.
- **Maturity (0–5):** 0 none → 5 integrated career-path and skills matrix.
- **Internal QA:** Annual certification tracking review.
- **Documentation:** Skills Matrix, Training Record, Certification Register.

15.3 Awareness Campaigns and Communication

Intent

Foster ongoing awareness beyond mandatory training through internal campaigns and communication.

Minimums

- Quarterly awareness campaigns.
- Topics aligned with observed incidents or risk trends.
- Measurable employee engagement.

Implement

Run interactive campaigns using newsletters, posters, intranet posts, and phishing simulations. Include leadership messages reinforcing accountability. Use surveys or knowledge tests to measure impact. Reward positive participation to strengthen engagement.

- **Evidence:** Campaign materials, metrics reports, simulation results.
- **Acceptance:** Active participation and demonstrable knowledge improvement.
- **Common Failures:** Static campaigns or lack of management visibility.
- **Maturity (0–5):** 0 none → 5 data-driven, risk-based awareness cycle.
- **Internal QA:** Quarterly campaign evaluation.
- **Documentation:** Awareness Campaign Plan, Communications Archive.

15.4 Supplier and Contractor Awareness

Intent

Ensure external parties accessing company systems or facilities understand and comply with security requirements.

Minimums

- Supplier orientation or acknowledgment requirement.
- Periodic training for third-party staff working onsite.
- Documented evidence of participation.

Implement

Incorporate awareness clauses into supplier contracts. Provide simplified onboarding modules for contractors. Require acknowledgment of security rules before access is granted. Maintain a central record of all supplier participants and completion rates.

- **Evidence:** Signed acknowledgments, supplier completion logs, LMS reports.
- **Acceptance:** All supplier staff trained and documented.
- **Common Failures:** Untrained contractor access or incomplete records.
- **Maturity (0–5):** 0 none → 5 supplier portal integration with training verification.
- **Internal QA:** Semi-annual supplier training audit.
- **Documentation:** Supplier Training Record, Orientation Checklist.

15.5 Continuous Improvement and Metrics

Intent

Measure training effectiveness and use results to improve content, methods, and frequency.

Minimums

- Defined KPIs (completion, comprehension, incident reduction).
- Annual effectiveness report to management.
- Process for updating materials based on results.

Implement

Collect and analyze performance data from quizzes, phishing simulations, and post-training surveys. Adjust modules to address weak areas. Present annual reports to management summarizing trends and recommended improvements.

- **Evidence:** KPI dashboards, annual effectiveness report, updated materials.
- **Acceptance:** Program continuously refined and demonstrably effective.
- **Common Failures:** Static content or no lessons-learned integration.
- **Maturity (0–5):** 0 none → 5 continuous improvement driven by analytics.
- **Internal QA:** Annual effectiveness assessment.
- **Documentation:** Training Effectiveness Report, Updated Curriculum.

16. Assessment Preparation & Continuous Improvement

Overview

TISAX certification demands an organization not only achieve compliance once but demonstrate sustained effectiveness and continuous improvement of its ISMS. Assessment readiness is therefore an ongoing operational discipline involving evidence collection, internal testing, management reviews, and data-driven improvement actions. Organizations that maintain continuous readiness reduce audit friction, strengthen resilience, and preserve trust with partners and OEMs.

16.1 Assessment Planning

Intent

Establish a structured plan for TISAX assessment readiness and coordination.

Minimums

- Annual or biennial assessment calendar aligned with TISAX certification cycles.
- Designated Assessment Coordinator responsible for evidence preparation.
- Clearly defined assessment scope and participating sites.

Implement

Document an annual assessment plan detailing timelines, responsible personnel, and deliverables. Maintain readiness checklists for each domain (IS1–IS7, PP8, DP9). Conduct pre-assessment workshops with control owners to validate evidence completeness.

- **Evidence:** Assessment plan, readiness checklists, meeting minutes.
- **Acceptance:** Assessment conducted within planned schedule with no delays.
- **Common Failures:** Unclear scope or missing readiness evidence.
- **Maturity (0–5):** 0 none → 5 continuous assessment lifecycle with automated tracking.
- **Internal QA:** Annual audit-preparation review.
- **Documentation:** Assessment Plan, Domain Readiness Checklists.

16.2 Evidence: Management and Traceability

Intent

Ensure all audit evidence is current, traceable, and mapped to control requirements.

Minimums

- Central evidence repository with version control.
- Cross-reference matrix linking evidence to ISA controls.
- Secure storage and retention policy.

Implement

Use a centralized GRC platform or secure document repository to store evidence by control ID. Maintain metadata (owner, date, control reference, version). Validate evidence quarterly to ensure freshness. Archive outdated documents and maintain version history.

- **Evidence: Evidence:** matrix, repository screenshots, version logs.
- **Acceptance:** 100% traceability between controls and supporting evidence.
- **Common Failures:** Disorganized files or outdated versions presented during audit.
- **Maturity (0–5):** 0 none → 5 fully automated evidence lifecycle within ISMS.
- **Internal QA:** Quarterly evidence verification.
- **Documentation:** **Evidence:** Management Procedure, Control-Evidence: Matrix.

16.3 Internal Readiness Audits

Intent

Conduct periodic internal reviews simulating TISAX assessments.

Minimums

- Self-assessments covering all control domains annually.
- Findings logged and tracked to closure.
- Independent validation by ISMS or audit function.

Implement

Perform mock assessments at least six months before formal TISAX audits. Engage subject-matter experts from IT, HR, and Engineering. Use the official ISA questionnaire for scoring consistency. Present readiness scores and improvement actions to leadership.

- **Evidence:** Self-assessment reports, corrective-action logs, readiness metrics.
- **Acceptance:** Gaps identified and closed before external audit.
- **Common Failures:** No pre-assessment validation or recurring nonconformities.
- **Maturity (0–5):** 0 none → 5 predictive readiness analytics using historical trends.
- **Internal QA:** Semi-annual internal readiness review.
- **Documentation:** Self-Assessment Report, Gap Analysis Tracker.

16.4 Continuous Improvement Cycle

Intent

Implement an iterative process to drive continuous enhancement of the ISMS.

Minimums

- Defined improvement objectives and KPIs.
- Root-cause analysis performed for incidents and findings.
- Results integrated into management reviews.

Implement

Use PDCA (Plan–Do–Check–Act) or equivalent frameworks. Identify recurring weaknesses through audit data, incidents, and risk trends. Prioritize corrective actions and monitor implementation progress. Link lessons learned to training updates, procedures, and metrics.

- **Evidence:** Improvement plans, KPI dashboards, management-review records.
- **Acceptance:** Demonstrated reduction in recurring issues and measurable maturity growth.
- **Common Failures:** No follow-through on improvement actions.
- **Maturity (0–5):** 0 none → 5 continuous improvement embedded in governance culture.
- **Internal QA:** Annual improvement-cycle review.
- **Documentation:** Continuous Improvement Plan, KPI Tracker, Lessons-Learned Register.

16.5 Management Reviews and Strategic Alignment

Intent

Ensure that leadership remains actively engaged in reviewing ISMS performance and aligning it with business strategy.

Minimums

- Management reviews conducted at least annually.
- Inputs include audit results, incident trends, and KPIs.
- Documented outputs with assigned actions.

Implement

Hold structured management-review meetings involving executive leadership, CISO, and key process owners. Present data-driven dashboards summarizing control effectiveness and improvement initiatives. Record decisions, resource allocations, and strategic changes.

- **Evidence:** Management-review minutes, presentations, action logs.
- **Acceptance: Evidence:** of active leadership oversight and strategic decision-making.
- **Common Failures:** Superficial reviews or missing follow-up.
- **Maturity (0–5):** 0 none → 5 management integration into enterprise scorecards.
- **Internal QA:** Annual review-validation audit.
- **Documentation:** Management Review Agenda, Action Tracker, Performance Dashboard.

17. Quick Reference Summary

Overview

The Quick Reference Summary provides a condensed view of TISAX 6.0.3 requirements across all domains. It helps compliance teams quickly identify where specific controls reside, what kind of measures they require (administrative, technical, or physical), and what practical actions demonstrate conformity. This table can be used as a mapping tool during internal readiness reviews or management presentations to illustrate comprehensive coverage.

Domain / Control Family	Type	Example Measures and Artifacts
IS1 – Policies and Organization	Administrative	Information Security Policy • ISMS Charter • Risk Register • Policy Register
IS2 – Human Resources Security	Administrative	Background Checks • Training Logs • Offboarding Checklists • Confidentiality Agreements
IS3 – Physical Security	Physical	Access Logs • CCTV Retention Reports • Visitor Management Records • Facility Zoning Map
IS4 – Identity & Access Management	Technical	Access Control Lists • MFA Configurations • PAM Logs • Role-Based Access Reviews
IS5 – IT / Cyber Security	Technical	Patch Reports • SIEM Dashboards • Network Diagrams • Backup Verification Logs
IS6 – Supplier Relationships	Administrative	Supplier Assessments • Contract Clauses • Audit Reports • Destruction Certificates
IS7 – Compliance & Audit	Administrative	Compliance Register • Audit Plans • CAPA Logs • Management Review Reports
PP8 – Prototype Protection	Physical / Administrative	Chain-of-Custody Forms • Event Security Plans • Destruction Certificates
DP9 – Data Protection	Administrative / Technical	RoPA Register • DPIA Reports • Breach Notifications • Consent Records
Training & Awareness Program	Administrative	Annual Plan • Training Metrics • Awareness Campaign Records
Assessment & Continuous Improvement	Administrative	Assessment Checklists • Evidence Matrix • Improvement Plans • Management-Review Actions

Usage Tip:

For each TISAX control, ensure at least one current and one historical evidence item are available in the repository. During audits, cross-reference these artifacts directly to ISA questionnaire sections to prove control maturity and ongoing effectiveness.

18. Operating Model & Governance

Overview

The TISAX Operating Model establishes how information security governance is structured, sustained, and improved. It clarifies who makes decisions, how compliance performance is monitored, and how responsibilities are delegated across functions. A strong operating model ensures that the organization's ISMS operates as a continuous cycle of policy enforcement, risk management, measurement, and review—not as a one-time certification activity.

18.1 Governance Framework

Intent

Define the organizational framework and committees that oversee TISAX compliance and information security governance.

Minimums

- Designated ISMS Owner accountable to executive management.
- Information Security Steering Committee with cross-departmental representation.
- Defined meeting cadence and documented agendas.

Implement

Establish a formal ISMS Steering Committee chaired by the CISO or ISMS Owner. Include members from IT, HR, Legal, Operations, Procurement, and Engineering. Conduct quarterly meetings to review audit results, KPIs, incidents, and improvement actions. Document all minutes and decisions.

- Evidence: Committee charter, meeting minutes, decision logs.
- Acceptance: Regular governance meetings held with measurable outputs.
- Common Failures: Inactive committees or undocumented follow-up.
- Maturity (0–5): 0 none → 5 data-driven governance integrated into enterprise planning.
- Internal QA:Annual governance-effectiveness review.
- Documentation: Governance Charter, Meeting Schedule, Action Tracker.

18.2 Roles and Responsibilities

Intent

Define and communicate roles, responsibilities, and authority for managing and maintaining the ISMS.

Minimums

- Role descriptions documented and approved by HR.
- Deputies assigned for continuity.
- Responsibilities communicated through job descriptions or internal manuals.

Implement

Create a Responsibility Matrix (RACI) mapping control ownership and accountability. Publish this matrix within the ISMS documentation library. Update assignments annually or during personnel changes. Ensure all owners complete awareness training specific to their responsibilities.

- **Evidence:** RACI matrix, signed responsibility acknowledgments, HR records.
- **Acceptance:** All roles clearly defined, communicated, and active.
- **Common Failures:** Overlapping or unclear authority lines.
- **Maturity (0–5):** 0 none → 5 dynamic assignment linked to organizational systems.
- **Internal QA:** Annual review of RACI accuracy.
- **Documentation:** Responsibility Matrix, HR Role Description File.

18.3 Integration with Business Strategy

Intent

Ensure that information-security objectives align with the organization’s broader business and risk strategy.

Minimums

- Security goals linked to corporate KPIs.
- Security risk considered in business decision-making.
- Reporting line to executive leadership.

Implement

Integrate ISMS metrics and TISAX maturity goals into enterprise performance reviews. Present quarterly updates to the executive board on risk status, audit results, and improvement plans. Embed security representation in project-portfolio governance and procurement approvals.

- **Evidence:** Strategy presentations, KPI dashboards, board minutes.
- **Acceptance:** Security formally represented in business planning processes.
- **Common Failures:** Reactive compliance disconnected from strategic priorities.
- **Maturity (0–5):** 0 none → 5 strategic integration with business objectives.
- **Internal QA:** Annual strategy-alignment review.
- **Documentation:** Security Strategy Plan, KPI Dashboard, Board Briefing Pack.

18.4 Communication and Reporting

Intent

Ensure that security performance and TISAX status are communicated effectively throughout the organization.

Minimums

- Defined reporting schedule and recipients.
- Metrics summarized in accessible dashboards.
- Escalation process for significant risks or incidents.

Implement

Publish monthly or quarterly ISMS performance dashboards. Report open risks, audit findings, and training metrics to leadership and control owners. Maintain a security communication channel for staff updates. Ensure key metrics are communicated across departments using standardized formats.

- **Evidence:** Reports, dashboards, risk summaries, communications logs.
- **Acceptance:** Timely, accurate, and transparent reporting to all stakeholders.
- **Common Failures:** Unclear escalation or inconsistent reporting cadence.
- **Maturity (0–5):** 0 none → 5 automated dashboards and alerting workflows.
- **Internal QA:** Quarterly communication-effectiveness audit.
- **Documentation:** ISMS Dashboard, Communication Matrix, Escalation Procedure.

18.5 Program Sustainability and Resource Management

Intent

Ensure adequate staffing, funding, and tools are maintained for ongoing TISAX compliance.

Minimums

- Annual ISMS budget.
- Defined resource plan (people, tools, training).
- Formal management approval of resource allocations.

Implement

Include ISMS costs in the organization's annual operating plan. Maintain an updated resource register including tools, software licenses, and personnel assigned to compliance functions. Conduct annual gap analyses to identify capability shortfalls and request additional resources.

- **Evidence:** Budget records, resource plan, staffing reports.
- **Acceptance:** Resources available to meet all compliance obligations.
- **Common Failures:** Underfunded ISMS or lack of full-time security staff.
- **Maturity:** (0–5) 0 none → 5 self-sustaining program integrated with enterprise budgeting.
- **Internal QA:** Annual resource adequacy review.
- **Documentation:** ISMS Budget, Resource Plan, Gap Analysis Report.

19. Common Audit Findings & Remediation Tips

Overview

TISAX audits follow a structured approach that validates both documentation and practical implementation. Many organizations achieve partial conformity due to procedural gaps, missing evidence, or insufficiently demonstrated control maturity. By understanding common findings and applying targeted remediation strategies, an organization can significantly improve audit performance and sustain compliance throughout the certification cycle.

19.1 Incomplete or Outdated Documentation

Typical Finding

Policies and procedures exist but are outdated, unsigned, or missing revision history.

Root Cause

Lack of centralized version control and unclear document ownership.

Remediation Tip

Implement a controlled documentation process within the ISMS. Maintain a master document list showing owners, approval dates, and next review dates. Automate reminders for policy reviews.

Preventive Control

Quarterly document-control audits and enforced version numbering across all policies.

19.2 Unverified Access and Identity Management

Typical Finding

User accounts remain active after employee termination or access reviews are incomplete.

Root Cause

Manual provisioning and lack of synchronization between HR and IAM systems.

Remediation Tip

Integrate IAM lifecycle with HR systems for automatic account creation and revocation. Perform quarterly access recertifications and remove orphaned accounts immediately.

Preventive Control

Implement least-privilege and segregation-of-duties principles validated through RBAC matrices.

19.3 Insufficient Evidence for Control Implementation

Typical Finding

Policies claim controls exist, but there is little or no evidence demonstrating actual operation.

Root Cause

Evidence not systematically collected, versioned, or mapped to TISAX controls.

Remediation Tip

Maintain an Evidence Matrix linking every TISAX control to specific evidence items (reports, logs, training records). Validate quarterly for completeness.

Preventive Control

Automate evidence capture through GRC or document-management tools.

19.4 Weak Risk Management Practices

Typical Finding

Risk assessments are irregular, incomplete, or unlinked to treatment plans.

Root Cause

Risk process not institutionalized or disconnected from decision-making.

Remediation Tip

Formalize risk assessment frequency (at least annually) and align residual risk acceptance with management approval. Ensure treatment plans include accountability and status tracking.

Preventive Control

Centralize risk management in a digital register linked to incident and audit data.

19.5 Prototype and Data Protection Gaps

Typical Finding

Prototype controls are inconsistent across facilities or data-protection activities lack complete documentation.

Root Cause

Departmental silos or missing coordination between Engineering, Security, and Privacy teams.

Remediation Tip

Standardize prototype-handling procedures and train staff on event-specific protocols. Conduct privacy impact assessments for all systems handling personal or prototype data.

Preventive Control

Annual facility compliance checks and periodic cross-functional workshops.

19.6 Lack of Continuous Improvement Tracking

Typical Finding

Nonconformities are remediated reactively but not analyzed for systemic trends.

Root Cause

Absence of a formal improvement or CAPA framework.

Remediation Tip

Adopt a CAPA process with root-cause analysis, corrective and preventive measures, and effectiveness validation. Report recurring themes in management reviews.

Preventive Control

Use analytics dashboards to monitor CAPA completion rates and recurring issues.

19.7 Limited Leadership Engagement

Typical Finding

Executives delegate ISMS responsibility without active participation in reviews or decision-making.

Root Cause

Security not tied to business metrics or strategic objectives.

Remediation Tip

Integrate ISMS KPIs into corporate scorecards. Schedule quarterly briefings to keep leadership informed about risk posture and TISAX status.

Preventive Control

Establish executive ownership for at least one ISMS objective annually.

19.8 Ineffective Training or Awareness Programs

Typical Finding

Employees complete mandatory courses but fail to apply learned behaviors.

Root Cause

Generic training content and lack of performance feedback.

Remediation Tip

Tailor training to roles and reinforce awareness through ongoing campaigns.
Use phishing simulations and gamified learning to measure behavioral improvement.

Preventive Control

Track awareness metrics (reporting rates, quiz performance) to evaluate program maturity.

19.9 Weak Supplier Oversight

Typical Finding

Suppliers not regularly reassessed or missing evidence of signed security agreements.

Root Cause

Procurement and security processes not integrated.

Remediation Tip

Create a shared Supplier Security Register linking risk ratings, contracts, and audit results. Conduct periodic due diligence reviews.

Preventive Control

Automate supplier-risk tracking within procurement or GRC tools.

19.10 Environmental and Physical Oversight Deficiencies

Typical Finding

Physical or environmental security controls untested or lacking maintenance documentation.

Root Cause

Facility management not integrated into ISMS scope.

Remediation Tip

Conduct regular facility audits covering access controls, CCTV systems, and environmental monitoring. Validate maintenance contracts and renewal logs.

Preventive Control

Include facilities in annual ISMS review and risk assessments.

20. Evidence Checklist and Documentation Map

Overview

The Evidence Checklist and Documentation Map ensures that all controls defined in the TISAX 6.0.3 framework are supported by verifiable and current evidence. A complete and organized documentation set allows auditors to validate conformity efficiently, while enabling internal teams to maintain ongoing readiness.

Each item in this checklist aligns to TISAX domains and specifies document examples typically required during certification or surveillance audits.

20.1 Core ISMS Documentation

Document Type	Purpose	Typical Evidence	Frequency / Owner
Information Security Policy	Defines ISMS scope, objectives, and authority	Signed master document with revision log	Annual / CISO
ISMS Manual	Framework overview and process references	Manual with scope statement and process links	Annual / ISMS Manager
Risk Assessment & Treatment Plan	Identifies and mitigates security risks	Risk register, treatment plan, acceptance forms	Annual / Risk Manager
Statement of Applicability (SoA)	Summarizes applied controls	Signed SoA aligned to ISA controls	Annual / CISO
ISMS Charter & Governance Policy	Defines leadership and oversight structure	Board-approved charter and committee records	Biennial / Governance Lead

20.2 Technical & Operational Documentation

Domain	Key Evidence Documents	Owner / Function
IS4 Identity & Access Management	Access Control Policy, RBAC Matrix, User Recertification Logs, IAM Reports	IT Security
IS5 IT & Cybersecurity Controls	Vulnerability Scans, Patch Logs, Firewall Rulesets, Backup Verification Reports	IT Operations
IS6 Supplier Management	Supplier Risk Assessments, Security Clauses in Contracts, Audit Reports	Procurement / Vendor Risk
IS7 Compliance & Audit	Internal Audit Plan, Audit Reports, CAPA Logs, Management Review Records	Compliance / Audit
PP8 Prototype Protection	Prototype Handling Procedures, Chain-of-Custody Records, Event Security Logs	Engineering / Physical Security
DP9 Data Protection	RoPA Register, DPIAs, Consent Forms, Breach Logs	Privacy Office

20.3 HR & Awareness Documentation

Document Type	Purpose	Evidence Examples
Security Awareness Plan	Defines annual training program	Approved plan and curriculum
Training Completion Records	Verifies user participation	LMS Reports, Certificates
Onboarding & Termination Checklists	Ensures security obligations lifecycle	Signed checklists and HR logs
Confidentiality Agreements	Establishes legal protection	HR Files, NDA Repository

20.4 Physical & Environmental Security Documentation

Control Area	Evidence Examples	Review Frequency
Facility Access Controls	Access Logs, Visitor Registers, Badge Assignment Records	Quarterly
Environmental Monitoring	HVAC / Power Monitoring Logs, Maintenance Reports	Semi-annual
CCTV & Surveillance	Retention Policy, Camera Maintenance Logs	Annual
Equipment Disposal	Destruction Certificates, Chain-of-Custody Reports	As Occurs

20.5 Governance and Management Review Evidence

Governance Element	Evidence Examples	Responsible Function
Management Review Minutes	Meeting Records, Action Items, KPIs	Executive / ISMS
Steering Committee Reports	Dashboards, Risk Summaries, Decisions	Governance / Security
Resource Allocation Records	Budgets, Staffing Plans, Procurement Approvals	Finance / ISMS
Continuous Improvement Plans	KPI Trackers, Lessons Learned Logs	Compliance / QA

20.6 Audit and Certification Evidence

Stage	Typical Evidence Required	Provided To
Self-Assessment (Pre-Audit)	Evidence Matrix, Internal Assessment Reports	Internal Audit / ISMS
External Assessment (Audit Phase)	TISAX Evidence Package, Corrective Action Plan	TISAX Auditor
Surveillance or Renewal Audit	Updated Risk Assessment, CAPA Status Report	Accredited TISAX Body

20.7 Document Control and Retention

- All ISMS documents must include version control, owner, approval signature, and next review date.
- Obsolete documents are to be archived securely and retained for at least three years.
- Document control shall be governed under the ISMS Documentation Policy, with periodic sampling to confirm accuracy.
- Evidence repositories should align with TISAX confidentiality classifications (e.g., “restricted” for prototype or customer data).

21. Definitions

This section provides concise definitions of key terms used throughout the TISAX 6.0.3 Compliance Guide.

Access Control
Restrictions ensuring only authorized users access specific systems, data, or facilities.

Assessment Level (AL)
TISAX assurance levels: AL1 (self-assessment), AL2 (documented/remote or on-site validation), AL3 (deep on-site validation).

Asset
Any information, system, facility, or resource requiring protection.

Confidential Information
Sensitive or restricted information requiring controlled handling.

Corrective and Preventive Action (CAPA)
Steps taken to address and prevent control deficiencies.

Data Protection Impact Assessment (DPIA)
Evaluation of risks to personal data for high-risk processing activities.

Data Subject Rights (DSR)
Individual rights regarding personal information (e.g., access, erasure, correction).

Evidence Matrix
A document linking TISAX controls to required audit evidence.

Incident
Any event that compromises or threatens confidentiality, integrity, or availability.

Information Security Management System (ISMS) — The organizational framework for managing and improving security controls.

Least Privilege
Granting users the minimum access required for job responsibilities.

Management Review
Leadership evaluation of ISMS performance, risks, and improvement needs.

Personal Data
Information identifying or relating to an identifiable individual.

Privacy by Design
Integrating data-protection measures into systems and processes from the outset.

Prototype
Pre-production models, parts, or digital assets requiring heightened protection.

Record of Processing Activities (RoPA)
Inventory documenting personal-data processing purposes, bases, and safeguards.

Remediation
Measures taken to correct audit findings or control gaps.

Residual Risk
Risk remaining after mitigation controls are applied.

Risk Assessment
Identification and evaluation of risks affecting security or privacy.

Security Classification
Categorization of information based on sensitivity (e.g., internal, confidential, restricted).

Stakeholder
Any party with responsibility or involvement in security, privacy, supplier risk, or compliance.

Statement of Applicability (SoA)
Summary of applicable or excluded controls with justifications.

TISAX (Trusted Information Security Assessment Exchange)
Automotive-industry assessment and exchange mechanism for information security, prototype protection, and data protection.

22. References & Resources

Overview

This section provides authoritative source material and recommended resources that support TISAX implementation, continuous improvement, and audit readiness. All URLs are fully visible to ensure accessibility in printed and PDF formats.

22.1 Official TISAX & ENX Resources

ENX Association — TISAX Participant Handbook (Version 6.0.3)
https://enx.com/tisax

ENX Association — ISA (Information Security Assessment) Catalogue (v6.0.3)
https://enx.com/tisax/downloads

ENX — TISAX Assessment & Labeling Process Overview
https://enx.com/tisax/tisax-assessment-process

ENX Approved Audit Providers List
https://enx.com/tisax/auditors

22.2 ISO/IEC Standards

ISO/IEC 27001:2022 — Information Security Management Systems (Requirements)
https://www.iso.org/standard/82875.html

ISO/IEC 27002:2022 — Code of Practice for Information Security Controls
https://www.iso.org/standard/75652.html

ISO/IEC 27017:2015 — Security Controls for Cloud Services
https://www.iso.org/standard/43757.html

ISO/IEC 27701:2019 — Privacy Information Management
https://www.iso.org/standard/71670.html

ISO 21434 — Road Vehicles — Cybersecurity Engineering
https://www.iso.org/standard/70918.html

22.3 Privacy & Data Protection

GDPR Official Text and Guidance
https://gdpr.eu/

ENISA — Cloud Security & Personal Data Protection Guidance
https://www.enisa.europa.eu

EDPB — European Data Protection Board Guidelines
https://edpb.europa.eu

22.4 Cybersecurity Frameworks

NIST SP 800-53 Rev. 5 — Security and Privacy Controls
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST Cybersecurity Framework (CSF 2.0)
https://www.nist.gov/cyberframework

CIS Critical Security Controls v8
https://www.cisecurity.org/controls/v8

OWASP Application Security Verification Standard (ASVS)
https://owasp.org/www-project-application-security-verification-standard/

22.5 Automotive Industry Resources

VDA ISA — Information Security Assessment Catalogue
https://www.vda.de

AIAG Automotive Cybersecurity Resources
https://www.aiag.org

UNECE WP.29 R155 — Vehicle Cybersecurity Regulation
https://unece.org/transport/documents/2021/03/regulations/uniform-provisions-concerning-approval-vehicles-cyber-security

SAE J3061 — Cybersecurity Process Framework
https://www.sae.org/standards/content/j3061_201601/

22.6 Training & Capability Development

ENX TISAX Training & Awareness Programs
https://enx.com/tisax/training

ISO/IEC 27001 Lead Implementer / Lead Auditor Programs
https://www.iso.org

(ISC)² and ISACA Professional Security Certifications (CISSP, CCSP, CISM, CRISC)
https://www.isc2.org
https://www.isaca.org

VDA QMC — TISAX Workshops and Supplier Training
https://www.vda-qmc.de/en/academy

Apptega

Apptega Product Features

- 16+ Security Frameworks
- One-Click Reporting
- Automated Alerts & Notifications
- API & Application Connectors
- Automated Framework Crosswalking
- Real-Time Compliance Scoring
- Restricted Auditor View
- Single Sign-On Connectivity
- Policy & Plan Templates
- Automated Risk Assessments
- Document Repository for Artifacts
- Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com