

TISAX ISA v6

TISAX ISA v6 is an assessment framework for evaluating and demonstrating information security and data protection across automotive supply chains.



What it is

TISAX ISA v6 — Trusted Information Security Assessment Exchange is an information security assessment framework that supports organizations in evaluating and demonstrating cybersecurity, data protection, and compliance within the automotive industry. The framework establishes consistent criteria for assessing the maturity and effectiveness of security controls across supply chains.

Developed and maintained by the ENX Association, TISAX is tailored to the needs of automotive manufacturers, suppliers, and service providers worldwide. It covers key domains such as information security management, risk assessment, data privacy, and third-party supplier oversight, ensuring alignment with requirements often found in ISO/IEC 27001 and other recognized standards.

At a glance

PUBLISHER ENX Association	TYPE Framework	VERSION TISAX ISA v6
EFFECTIVE June 2023	DOMAIN Cybersecurity	FAMILY TISAX
REGION Germany	INDUSTRY Automotive	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY High		

Source: <https://portal.enx.com/en-us/TISAX/downloads/>

Why it matters

- **Strengthen cybersecurity governance** Establish clear criteria and accountability to ensure effective information security management throughout the automotive value chain.
- **Enhance regulatory alignment** Facilitate consistent compliance with data protection laws and industry standards, streamlining regulatory reporting and certification processes.
- **Improve supplier risk oversight** Enable comprehensive due diligence and continuous monitoring of third-party partners to reduce cybersecurity and privacy risks.
- **Increase audit transparency** Allow organizations to reliably demonstrate control effectiveness and share assessment results with trusted partners, reducing redundant audits.

How SmartSuite supports TISAX ISA v6

ISA Requirement Library

Organize information security, data protection, and prototype protection requirements.

Scope and Site Readiness Tracking

Define in-scope locations and processes with clear ownership and boundaries.

Evidence Collection and Audit Trail

Centralize policies, procedures, and operating proof aligned to ISA requirements.

Corrective Actions and Remediation

Track findings, root cause, actions, and verification through closure.

Supplier and Partner Controls

Manage partner requirements, evidence requests, and ongoing oversight.

Assessment Readiness Reporting

Report status, gaps, and readiness across sites and requirement areas.

Common framework mappings

[CIS Controls v8.1](#)[ISO 27001:2022](#)[ISO 27002:2022](#)[ISO 27701](#)[ISO/SAE 21434](#)[NIST CSF 2.0](#)[NIST 800-53 Rev.5](#)[UNECE R155](#)

Official resources

TISAX Participant Handbook

Provides detailed guidance on participation in TISAX assessments and compliance processes.

enx.com/handbook/TISAX%20Participant%20Handbook.pdf

TISAX Assessment Guide

Describes the assessment process and requirements for achieving TISAX certification.

enx.com/handbook/tisax-participant-handbook.html

TISAX Exchange Platform Introduction

Outlines how to use the TISAX Exchange platform for managing assessment results.

portal.enx.com/en-US/TISAX

Frequently asked questions

What is TISAX ISA v6 used for?

TISAX ISA v6 is used to assess and demonstrate an organization's information security posture within the automotive industry. It provides a standardized framework for evaluating security controls, data protection, and regulatory compliance across manufacturers, suppliers, and service providers.

Is TISAX ISA v6 certification required?

TISAX certification is not legally mandated but is often required by automotive manufacturers and OEMs as a prerequisite for doing business within the sector. Certification demonstrates adherence to information security requirements aligned with industry expectations.

What is the scope of a TISAX assessment?

The TISAX assessment scope is defined by the organization and includes the business units, information systems, and processes relevant to the assessment objectives. The scope should clearly specify locations, assets, and data flows that are subject to evaluation.

What are the key concepts or artifacts required for TISAX compliance?

Key artifacts for TISAX compliance include a defined information security management system (ISMS), documented risk assessments, asset inventories, access control policies, evidence of implemented controls, and third-party management documentation.

How do organizations implement TISAX ISA v6?

Organizations implement TISAX by conducting gap analyses, mapping the ISA control catalog to their existing controls, remediating weaknesses, and preparing documentation and evidence for the assessment. They may conduct a self-assessment before engaging an accredited TISAX auditor for official evaluation.

How does TISAX ISA v6 relate to other frameworks such as ISO 27001?

TISAX ISA v6 is closely aligned with ISO/IEC 27001, using similar principles such as risk management and control assessment. However, TISAX is tailored specifically for the automotive industry, with additional requirements for data protection and supplier security.

What are the ongoing compliance requirements for TISAX?

Maintaining TISAX compliance requires regular review of controls, periodic risk assessments, updates to policies, continuous monitoring for incidents, and timely remediation of identified issues. Organizations must also undergo re-assessments within cycles defined by their TISAX label.

How would SmartSuite support TISAX ISA v6?

SmartSuite supports TISAX ISA v6 by providing mapped control libraries, a centralized risk register, and workflow tools for policy governance and evidence collection. It streamlines compliance tracking, enables remediation assignment, supports audit readiness with dashboards and checklists, and generates consolidated reports for ongoing monitoring.

License included / downloadable: No TISAX documentation and the ISA catalog are published by the ENX Association. Access to the full assessment catalog typically requires participation in the TISAX program. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/tisax-isa-v6-trusted-information-security-assessment-exchange