del, providing a transparent and comparable view of an organisation's information security capabilities.

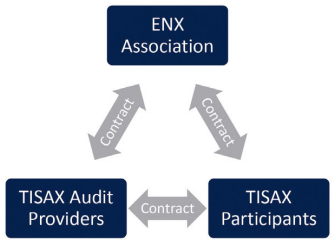
Audit Providers

Assessments within TISAX are performed by independent audit providers approved by ENX. These providers conduct assessments according to standardized requirements and ensure objective and reliable results. Companies are free to choose their audit provider, creating flexibility while maintaining comparability across assessments.

After completing the assessment, results are uploaded to the portal and can be shared securely with business partners. TISAX provides a reliable way to demonstrate compliance with industry-specific security requirements, strengthen trust, and enable secure collaboration across the supply chain.

ENX Governance Framework

The TISAX governance framework combines common requirements with a binding contractual structure between ENX, TISAX Participants, and audit providers. ENX defines the requirements for TISAX assessments, approves audit providers, and oversees their activities to ensure compliance and consistent assessment quality.



ENX monitors Audit Providers through reviews, witness activities, complaint handling, and assessment analysis. This ensures consistency and continuous improvement.

ENX also acts as an independent escalation authority in the event of disagreements between auditees and Audit Providers, facilitating fair and consistent resolutions.

Why TISAX?

- Reduces multiple audits by enabling mutual recognition of results
- Creates a standardized and comparable assessment framework
- Increases trust between manufacturers, suppliers, and partners
- Strengthens information and cybersecurity across supply chains
- Supports scalability in complex global networks
- Enables efficient proof of a functioning Information Security Management System (ISMS)
- Protects sensitive data such as prototypes, business data, and personal information
- Reduces costs and administrative effort

More detailed information about the TISAX process and the registration can be found in the TISAX Participant Handbook on our website and on our YouTube channel. On LinkedIn, we offer more regular bites of updates.

enx.com | ENXAssociation | ENX Association

About ENX Association

ENX is a trust anchor for cross-company data exchange and the protection of sensitive data in the automotive industry, supported by its members and users. Founded in 2000, the ENX Association is an organization of automotive manufacturers, suppliers and national automotive associations. The aim of ENX is to enable and simplify secure and trustworthy collaboration in industrial value-added networks.

Contact us

ENX Association
tisax@enx.com
+49 69 9866927-77
www.enx.com/tisax

Download Flyer

ENX Association 11/2026

TISAX® ENX ASSOCIATION

Assessed once, recognised by many.



Trusted Information Security Assessment Exchange

At a time when cyber attacks are increasing and companies must actively address information security, thousands of organisations across the industry rely on TISAX.

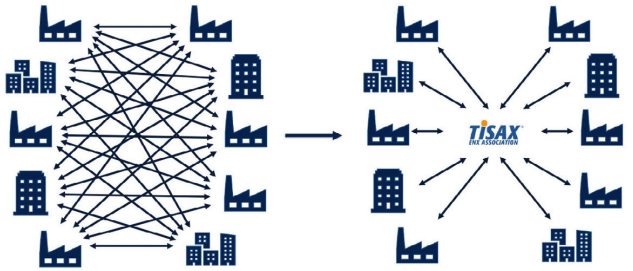
What is TISAX?

TISAX was developed to create a uniform and scalable approach to assess information security posture for the automotive industry. TISAX drives companies to make themselves more resilient and keep their businesses running. It also reinforces protecting customer's design data, production information, customer information, prototypes, and intellectual property.

TISAX is based on the Information Security Assessment (ISA) catalogue which is developed and maintained by the ENX Association and published by the VDA. The ISA supports organisations in identifying risks and implementing controls to prevent incidents, detect threats, minimize impact through effective response, and restore normal operations.

Efficient mechanism to manage security risks in supply chains at scale

To manage risks in the supply chain, organisations can rely on individual supplier audits to evaluate information security. However, this approach is resource-intensive and difficult to scale.



TISAX provides an efficient and scalable mechanism for managing information security risks across complex business ecosystems. By establishing a common assessment and recognition framework, it reduces duplicated effort, increases transparency, and enables organisations to share trusted assessment results across the industry.

A key enabler of this scalability is the TISAX platform, which provides a secure and standardized mechanism for exchanging assessment results between participants. The platform can be integrated into supplier management processes and supports automation, allowing organisations to efficiently manage assessment requests, result sharing, and supplier security oversight at scale.

How does TISAX work?

The TISAX process begins with registration in the ENX Portal. Organisations become TISAX Participants and define their assessment scope, including the relevant locations, processes, information assets, and protection needs that are to be assessed.



Participants then prepare for the assessment by conducting a self-assessment and implementing any necessary improvements. Once prepared, they select a TISAX Audit Provider to conduct the assessment. Depending on the assessment objectives and required Assessment Level, the assessment may range from a review of submitted evidence to extensive on-site evaluation activities.

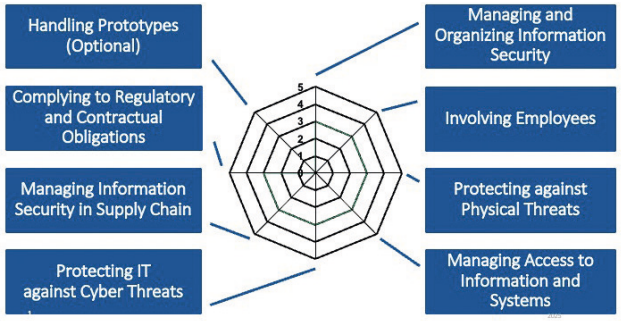
After successful completion, the audit provider uploads the assessment results to the ENX Portal. Based on the assessed objectives, organisations receive TISAX labels that demonstrate conformity with the applicable requirements. Labels are valid for three years.

Organisations remain in full control of their assessment results and can selectively share them with customers and business partners through the ENX Portal. This allows suppliers and service providers to demonstrate their information security capabilities once and reuse the results across multiple business relationships.

Information Security Assessment catalogue (ISA)

The Information Security Assessment (ISA) is the assessment catalogue used for TISAX. Developed by industry experts in ENX Working Groups, it defines the information security requirements that organisations have to implement and demonstrate during a TISAX assessment.

The ISA covers security management and governance, personnel security, physical security, business process and access security, IT and OT security, cybersecurity, supplier security, and compliance. Additional modules address specific requirements for prototype protection and data protection. Rather than focusing solely on IT security, the ISA provides a comprehensive framework that addresses people, processes, facilities, suppliers, and technology across the entire organisation.



Beyond serving as the basis for TISAX assessments, the ISA provides organisations with a practical roadmap for building, operating, and continuously improving their security management system. It helps organisations identify risks, implement appropriate safeguards, and establish a structured and sustainable approach to information security.

During a TISAX assessment, the implementation of ISA requirements is evaluated using a defined maturity mo-