TISAX®

Trusted Information Security Assessment Exchange

TECHNICAL GUIDE

TISAX® Assessment

DEKRA On the safe side.

In today's digitized business environment, information security has become an increasingly critical prerequisite for manufacturers, supplies and service providers cooperating across the automotive value chain. The Trusted Information Security Assessment Exchange (TISAX®) provides members a standardized information security status to be shared among partners working throughout the automotive industry.

Contents

1. TISAX® overview and benefits

Goals

TISAX® has been developed specifically for the automotive industry and aims to ensure the recognized integrity of your information security system. The TISAX® platform provides members standardized assessment of their information security status to be shared with partners working throughout the value chain. Your achieved protection class is conveniently registered on a dedicated digital platform and provided to selected members requesting your TISAX® status. Partners in the TISAX® assessment include:

- The ENX association
- An authorized audit provider
- A participant company applying for certification

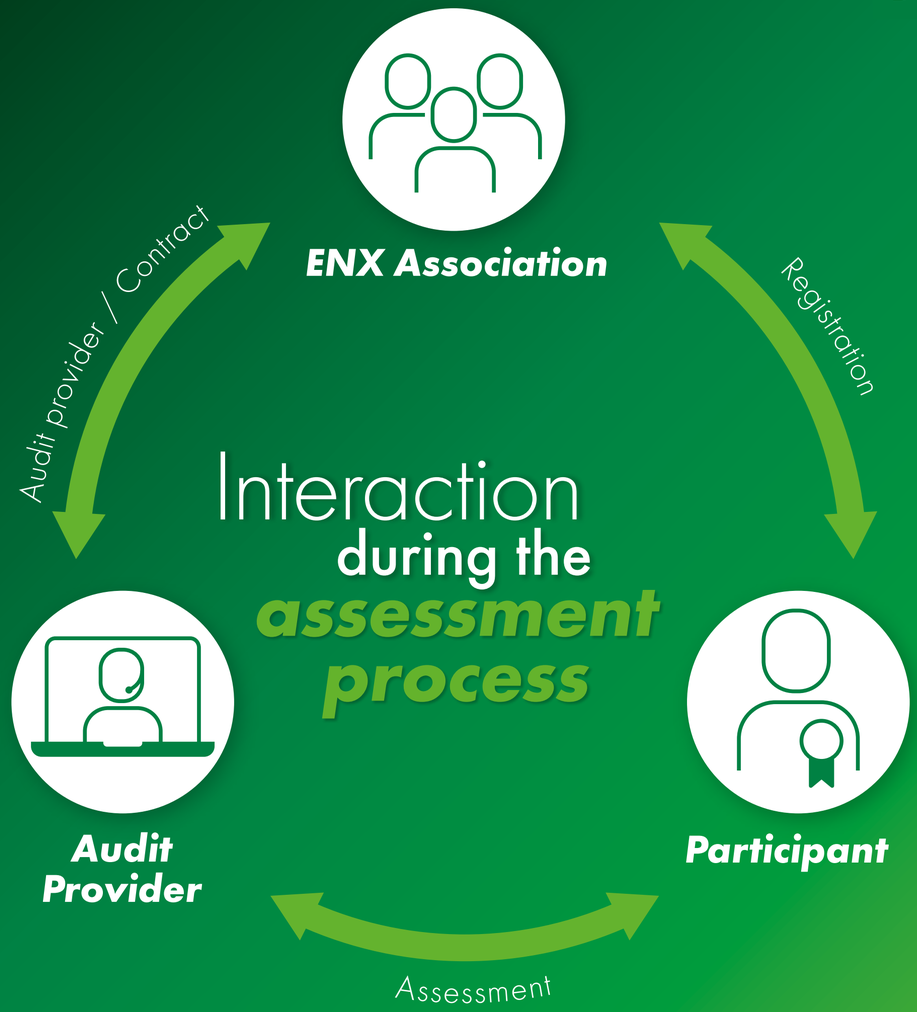
TISAX® certification is valid for a period of three years. Registered partners share confidential information and need to be absolutely sure that others are continuously handling information according to established TISAX® standards. Based on assessment results, the information security status of each registered participants is available on the online platform. No TISAX® member has automatic access to the assessment results and the status of others. Selected partners with which information is shared are determined by each TISAX® participant on a case-by-case basis.

TISAX®, VDA and ENX

Established in early 2017, the TISAX® testing and exchange mechanism was founded on the German Association of the Automotive Industry (VDA) catalog of ISA (Information Security Assessment) requirements.

Founded in 2000, the ENX Association is a legally-independent union of companies and national associations including Audi, BMW, Bosch, Continental, Daimler, DGA, Ford, Magna, PSA Peugeot Citroën, Renault, Volkswagen ANFAC (Spain), GALIA (France), SMMT (UK) and VDA (Germany) which supervises the performance of certified service providers, operates central ENX network services and supports providers with efficient solutions.

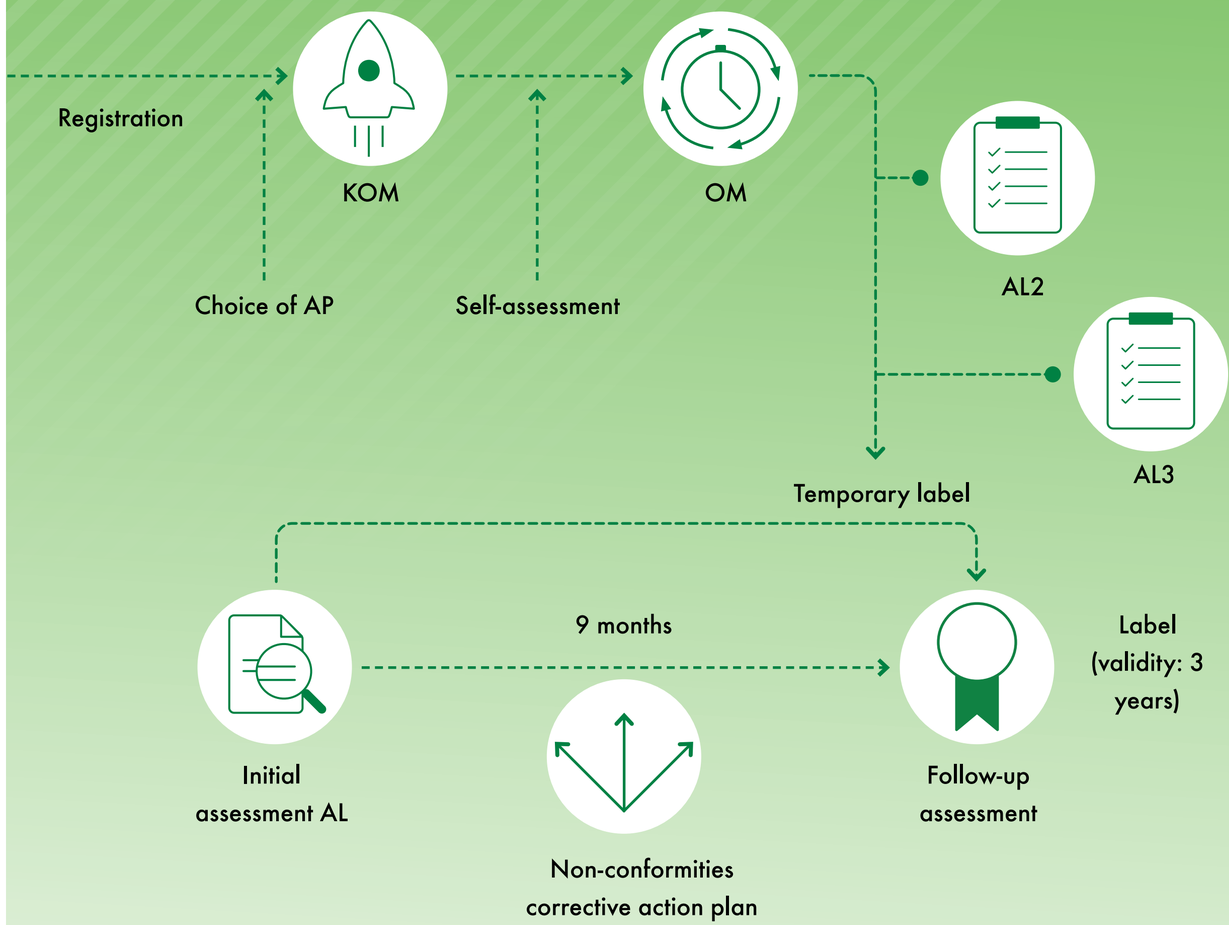
At its core, TISAX® aims to establish standardized labeling based on criteria common within the automotive industry. TISAX® has been developed to provide a community environment in which the performance and security of IT and IS systems can be shared.



Phases of TISAX® certification

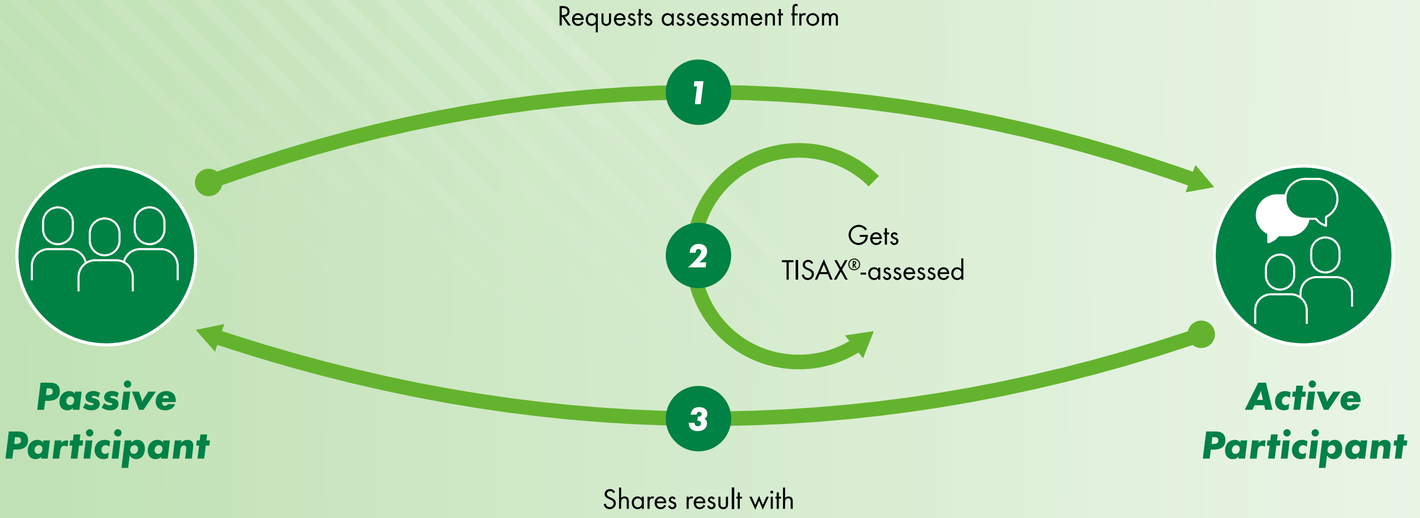
1. Registration on the TISAX® platform
2. Selection of an audit provider
3. Preliminary verification of label/scope assessment, information protection class, and simplified group assessment (if possible)
4. Execution and signing of the contract
5. Self-assessment (Assessment Level 1)
6. Off-site audit (review of Assessment Level 1 according to documentation and label/scope confirmation or Assessment Level 2) optional
7. On-site audit (Assessment Level 3)
8. Label validation
9. Audit information shared with exclusive TISAX® partners designated by the audited member company

TISAX®
Assessment Flow Chart



KOM = Kick-off-meeting OM = Opening meeting AL = Assessment level AP = Audit Provider

Roles of participation



Benefits of TISAX® certification

In addition to the added value of your recognized information security status, TISAX® certification provides you the following advantages:

- Increased credibility with a certified information security system
- Cross-company recognition among TISAX® members
- Strong strategies for effective risk management
- Transparency through harmonized VDA ISA catalog
- Sharper focus on customer needs and expectations
- Internationally recognized listing on the TISAX® online platform
- Complete control over who can access your assessment results
- TISAX® assessment every three years eliminating time and money spent on multiple checks

2. Roles of participation

Member organizations participating in the exchange model may adapt either a passive or an active role according to each particular circumstance:

Passive participant (e.g. OEM, automotive manufacturer): Calls for another company such as a supplier to undergo assessment and requests access to the assessment results.

Active participant (e.g. supplier): Either orders assessment or is called on by an OEM or customer to undergo assessment.
The active participant then provides selected partners access to the assessment results.

The three steps of participation:

1. **Registration**
Your selected TISAX® provider gathers information about your company and determines the scope of your assessment.

2. **Assessment**
Assessment(s) is conducted by an approved TISAX® audit provider.

3. **Exchange**
Assessment results and certification(s) are exclusively shared with designated partners.

Step 1
Clients can register on the TISAX® platform and are required to follow a specific process to obtain a "participant number". During the online TISAX® registration process candidates must:

- Provide contact details and billing information
- Accept TISAX® terms and conditions
- Define the scope of the information security assessment

The audit scope is based on VDA ISA catalog. Audit duration is calculated according to the determined scope and cannot be precalculated based solely on the structure of the organization.

Step 2

Assessment is broken into four sub-steps:

- **Assessment preparation**

The extent of preparation depends on the current maturity level of information security management system and must be based on VDA ISA catalog requirements.

- **Audit provider selection**

Participants choose their preferred partner from the list of approved TISAX® audit providers.

- **Information security assessment(s)**

The audit provider conducts assessment based on a scope determined by the requirements of the requesting partner. Each assessment process consists of at least an initial audit, with additional actions necessary for those who do not immediately pass.

- **Assessment result sharing**

Upon the completion of a successful audit, the report and results are shared at the approval of the active participant.

Step 3

Results are entered on the TISAX® platform to be exclusively shared with designated partners on a case-by-case basis. The content of your TISAX® report is structured in levels and only you are authorized to decide the level at which your partner will have access. TISAX® and ENX publication of the results and assessment label on the TISAX® digital platform make your certification official.

3. TISAX® scopes of assessment

Scopes of assessment available to you:

- **Standard Scope**

Applied in the majority of cases, the standard scope is pre-defined to include all resources and processes used in collecting, storing, and managing digital information.

- **Customized Extended Scope**

Tailored to meet your needs beyond standard scope perimeters.

- **Customized Narrowed Scope**

Tailored to meet only specific needs in a reduction of the standard scope (no label can be issued).

TISAX® certification culminates with an achieved assessment label symbolizing the assessment result. There are four different label categories that can be required by various partners. Defined at the beginning of the process, assessment objectives are audited and assigned the appropriate assessment level status upon successful completion of the audit. Degrees of "high" or "very high" define the achieved protection level in each category.

TISAX® assessment scope and duration are determined on a case-by-case basis according to the list of criteria to be met, defined protection objectives, ISMS complexity, and the number of affected locations.

VDA ISA criteria catalog	Protection Level (PL)	TISAX® Assessment objective	Assessment Level
Information security	high	Information with high protection level	AL 2
	very high	Information with very high protection level	AL 3
Prototype protection		Handling of prototypes with high protection level (for further information please see chapter 9)	AL 3
Data protection	high	Datenschutz nach §11 BDSG („Auftragsdatenverarbeitung")	AL 2
	very high	Data protection with special categories of personal data, data protection according to German §11 BDSG ("Auftragsdatenverarbeitung"), special categories according to German §3 section (9) BDSG ("Besondere Arten")	AL 3

4. Established VDA ISA requirements

VDA ISA assessment includes a generic questionnaire on information security and three additional specific topic modules:

- Prototype protection: Originally covered by VDA PTS, the module has been revised to follow the same structure as the main catalog.
- Connections to third parties: The module describes the specific requirements suppliers and service providers should consider when renting space meant to host on-premise partner network connections.
- Data protection: This module is applied to service providers mandated to process information according to Article 28 of the European General Data Protection Regulation (GDPR).

5. Registered TISAX® subscriber

Access to TISAX® is available to registered subscribers via the online TISAX® portal. Registration is the prerequisite to choosing an approved TISAX® auditor from the list of authorized service providers. A single organization may register several locations and have a group assessment carried out if needed. After assessment based on VDA ISA requirements, active participants can provide information to be shared with their designated TISAX® partners.

TISAX® uses the VDA ISA questionnaire created by the German Automotive Industry Association (VDA) which is based on essential aspects of the internationally recognized ISO / IEC 27001 standard regulating information security management systems (ISMS).

ENX monitors adherence to TISAX® procedure which includes specific requirements for ENX TISAX® audit service providers to

safeguard the quality of implementation and assessment results. ENX therefore executes contracts with all authorized audit service providers and registered participants. TISAX® standardization and quality control ensures your certification is recognized among TISAX® members throughout the automotive industry value chain.

6. ISO 27001 vs. TISAX®

TISAX® assessment is based on the VDA Information Security Assessment (VDA ISA) test catalogue, which in turn is based on ISO/IEC 27001 or ISO/IEC 27002 requirements extended to include automobile-specific requirements such as prototype protection, or the integration of third parties or data protection.

A company that has successfully passed the TISAX® procedure is not automatically certified according to ISO 27001. ISO 27001 certification must be carried out separately.

See the table below for the main differences:

	ISO 27001:2013	TISAX®
Audit frequency	Annually	Every three years
Proof	Certificate	Electronic label (only available in the ENX data base)
International recognition	Yes	Only in the automotive industry at this time
Dealing with deviations	Major deviations must be closed before the certificate is issued	All major and minor deviations must be closed before the label is issued

7. Defined TISAX® protection and assessment levels

As the operator of the TISAX® program, the ENX Association has clearly defined protection and assessment levels. TISAX® differentiates between two protection levels which define the appropriate security for the type of information being reviewed. Levels of security range from:

- **High:** Potential damage would be substantial, of a mid-term nature and not limited to a single entity.
- **Very high:** Potential damage would be threatening to the continued existence of the business, of a long-term nature and not limited to a single company.

TISAX® also differentiates among three assessment levels (AL) which define assessment depth and method for the three categories of information:

- **Information with normal protection level:**
  Assessment Level 1: Self-assessment. Assessment Level 1 results are not normally referenced in TISAX®, but may be requested for general use.
- **Information with high protection level:**
  Assessment Level 2. Audit conducted by an independent approved service provider using the self-assessment as a basis together with various documents and a telephone interview (on-site inspection may be required).

- **Information with very high protection level:**
  Assessment Level 3: Audit conducted by an independent approved service provider on the basis of documentation and an on-site inspection.

8. Test marks and labels

Appropriate labeling corresponding to the protection and assessment classification levels is a prerequisite for the proper handling of information. In addition to the creator, both recipients and processors of information must know, understand, and apply the associated classification level requirements during handling.

Labeling is particularly critical when transmitting confidential and strictly confidential information across company boundaries.

In addition to uniform information classification and corresponding document labeling, the Information Security Working Group also demands uniform labeling for IT applications. When opening digital information such as e-mail or an attached file, a color clue can provide an important indicating feature to visually signal the classification level of a digital information. A clear reference such as a colored bar can support universal understanding of the classification level regardless of language-specific differences.

9. Assessment objectives for TISAX® prototype protection

Assessment objective	Information
Protection of prototype parts and components	Applies to companies that manufacture, store or provide vehicles or components classified as vulnerable on their own premises.
Protection of prototype vehicles	Applies to companies that manufacture, store use customer-provided vehicles classified as requiring protection at their own premises.
Handling of test vehicles and components	Applies to companies that conduct tests and test drives with customer-provided vehicles classified as requiring protection.
Protection of prototypes during events and film or photo shootings	Applies to companies that conduct presentations or events and film and photo shootings with customer-provided vehicles, components or parts classified as requiring protection.

About DEKRA

Since our founding over 90 years ago, DEKRA has been providing services to ensure the highest of safety standards. With passion, expertise and 45,000 employees worldwide, we think ahead to address the safety challenges of the future. We promote safe human interaction with technology and the environment and strive to meet today's security demands with regard to digitalization. On the road, at work and at home – our skilled DEKRA experts work to increase safety across all key areas of life.

→ Would you like more information?

→ Contact us!

Do you require a TISAX® assessment for your company?

Contact our experts now!

Contact us!