White Paper
TISAX® Assessment in the Automotive Industry

DEKRA
On the safe side.

The automotive industry has one of the most complex supply chains in the world. Manufacturers and customers demand robust, resilient and consistent information security when data is transferred or exchanged throughout the entire value chain – not only during prototype development. Providing reliable proof of data security has become a prerequisite for participation in the automotive supply chain. TISAX® assessments allow companies to credibly document compliance with relevant information security requirements.

Background

The TISAX® (Trusted Information Security Assessment Exchange) testing and exchange standard is based on the VDA ISA questionnaire, which in turn is derived from the ISO 27001 standard. This questionnaire serves as a self-assessment and has been used by member companies in recent years for internal purposes and for supplier and service provider audits. In practice, this has often resulted in a service provider or supplier who processes sensitive information being audited several times, sometimes at short intervals. The TISAX® model was developed to prevent multiple audits and streamline processes by allowing mutual recognition of information security assessments among the various suppliers in the automotive industry. This means that the test standard can be used not only across companies, but also across industries without the need for additional company-specific questionnaires.

Your advantages

Automotive companies benefit from various advantages with a TISAX® assessment:

- **In the automotive industry, the ENX Association and the VDA launched TISAX® at the beginning of 2017 to facilitate the exchange of proof of information security among manufacturers, suppliers and service providers across companies.**

- The TISAX® platform saves time and money. Double and multiple information security checks are avoided.
- The audited company decides for itself with whom it shares its results.
- TISAX® registration leads to increased security awareness among employees and promotes company values.
- Registered companies can use the platform to ensure that their suppliers and service providers also meet the required level of information security.

Who is affected?

Manufacturers, suppliers and service providers across the automotive supply chain who process sensitive information have an interest in actively using TISAX®. For example, suppliers to the automotive industry must prove compliance with strict information security requirements at regular intervals. In most cases, compliance is based on the VDA ISA (Information Security Assessment) catalog of requirements.

A mutually accepted, robust level of information security in the industry also protects the information provided by suppliers in-house and confirms to customers that sensitive information is handled with care.

The operator of the TISAX® exchange platform is the ENX Association. It has been entrusted with the operation by the VDA as a neutral authority.

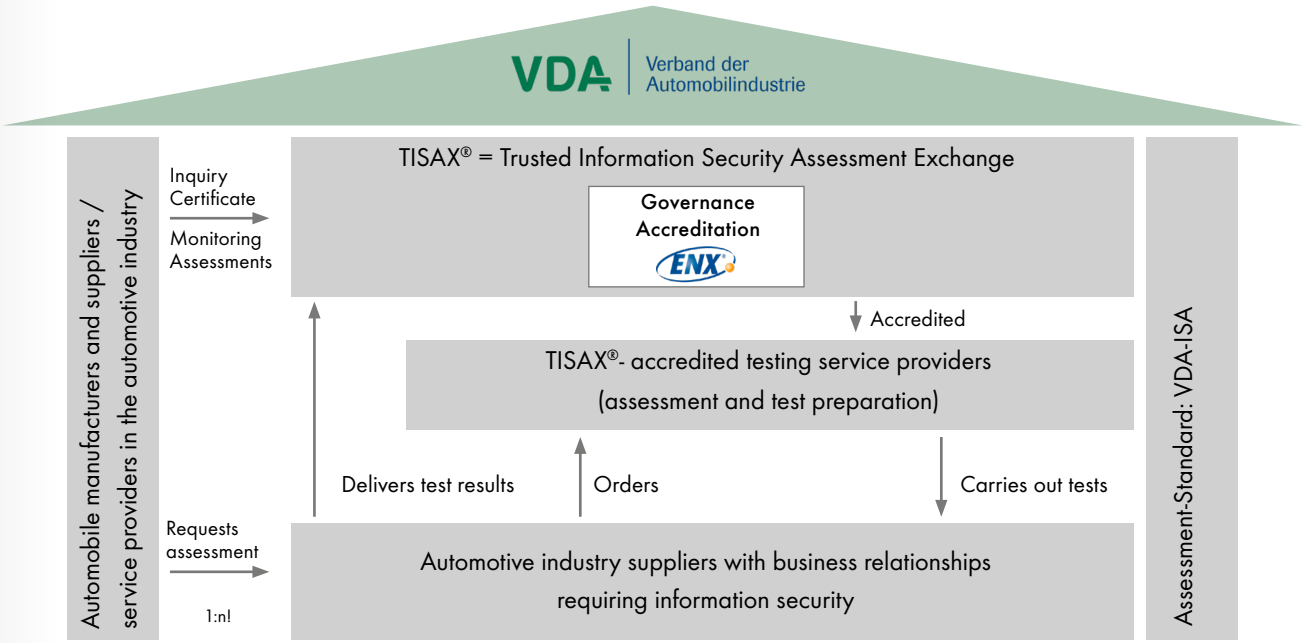
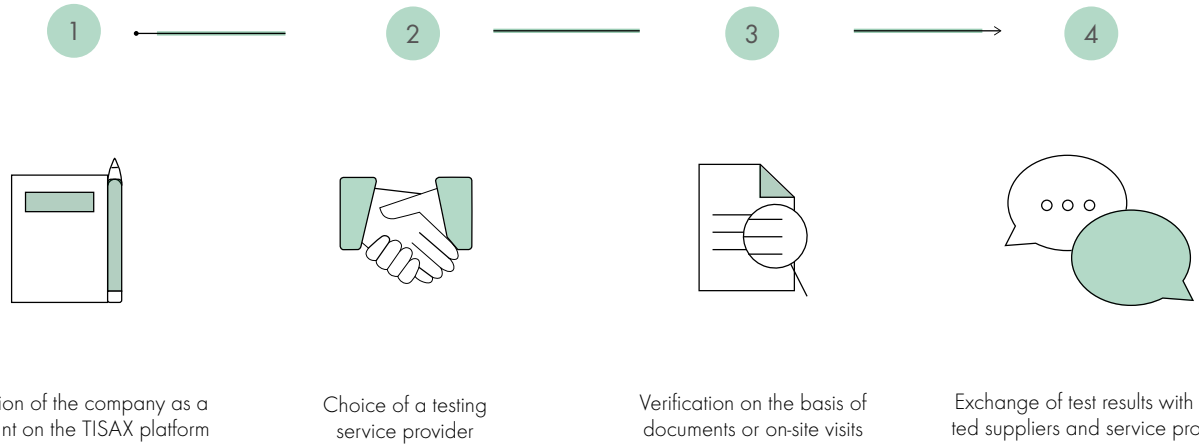


Figure 1: VDA TISAX model. Source: Own presentation according to VDA (2017, https://www.vda.de/de/Search-Results.html?q+model)

TISAX® is more than just a technical checklist

The testing and exchange mechanism is based on the ISA catalog of requirements from the VDA, which eliminates the need for the special requirements and extensive catalogs issued by major automobile manufacturers. Since all ISO standards have the same high-level structure in the first sections, the TISAX® ISA catalog, with its references to ISO 27001, contains essential quality management requirements according to ISO 9001:2015. A robust IT security management system is always based on quality management, and above all on the organizational measures this requires. Thus, companies participating in TISAX® also lay the foundation for a possible later certification according to ISO 27001.

Participation in TISAX® in four steps



The scope of the audit

The basic assessment targets "Information security" and can be extended by the optional modules "Connection to third parties“, "Data protection“ and "Prototype protection.“ The ISA requirements catalog uses a comprehensive spreadsheet displaying different test categories to describe the process by which enterprises determine their level of information security maturity (basic test).

Start with an information security assessment

The VDA recommends starting the self-assessment with the "Information security“ spreadsheet. This questionnaire lists 52 security topics (controls) which the company must use to obtain a comprehensive overview of its own information security status. Each of these topics must be evaluated with a degree of target achievement (from level 0 to 5) in order to obtain an overall assessment.

The catalog of requirements requires a high degree of implementation and maturity in the company, especially for the following security topics:

- **Sensitization and training of employees**
  Awareness measures should include findings from information security incidents.
- **User registration**
  Collective accounts should only be used in exceptional cases, as they make it more difficult to assign user activities unambiguously.
- **Change management**
  An effective change management process leads to a low error rate in implemented changes and thus contributes to safe operations.
- **Protection against malware**
  Current virus signatures are a prerequisite for effective endpoint security.
- **Information security (Backup)**
  Data security must be ensured by double-checking backups via measures such as system restores.
- **Vulnerability tracking (patch management)**
  The prompt installation of patches strengthens systems and applications and thus reduces security gaps in the operating software.
- **Processing information security incidents**
  Information security incidents must be prioritized and dealt with appropriately according to their criticality.

Other security topics/controls are:

- Information security policy
- Information security in projects
- Mobile devices
- Security zones
- Protective measures in the delivery and dispatch area
- Event logging
- Network services
- Non-disclosure agreements
- Requirements for the procurement of information systems
- Security in the software development process
- Efficacy testing

What level have you reached?

Implementation of VDA ISA requirements is assessed by assigning levels of maturity. Depending on the importance of the controls, the target maturity levels vary between level 2 and level 4. However, particularly important requirements require maturity levels of 3 and 4.

- Level 0: The implementation of the requirements is incomplete. No process exists or the process does not achieve the required results.
- Level 1: The necessary requirements have been met according to information security needs. A process exists and has been shown to work, but is not fully documented. Its reliability, therefore, cannot be fully ensured.
- Level 2: The process for achieving the goal is controlled and documented, and evidence (e.g. documentation) is available.
- Level 3: The process to achieve the goal is established and the processes are linked to map existing dependencies. The documentation is up-to-date and maintained.
- Level 4: The requirements from Level 3 are fulfilled. Furthermore, measurements of the results (e.g. KPI) are carried out and make the process predictable.
- Level 5: The requirements from Level 4 are met, and additional resources (e.g. personnel and money) are used to optimize the process. A continuous improvement of the process takes place.

The assessment result

The results of the test catalogs are summarized in an overview and are preformatted for printing. The VDA has developed a clear spider web diagram for the 52 safety topics on the basic information security test in order to show at a glance the degree of maturity determined for the 52 safety topics or their deviations from target controls.

Particularly critical deviations from the target maturity level are shown in red in a traffic light system. "When calculating the overall result, the results of controls that exceed the target degree of maturity are capped and the average is determined. This ensures that the requirements are met across all topics and that there is no compensation for over- and underfulfilled controls," says the VDA's explanation of the test catalog.

Case study

A supplier of simple mechanical components for the automotive industry has worked through the VDA ISA test catalog for the "Information Security" basic test. The supplier determined the degree of maturity achieved for each of the 52 safety topics (18 overriding topics) by analyzing documents and conducting interviews and internal audits.

The following spider diagram shows the overall result, the degree of target achievement and the deviations from the target maturity level.

Overall result: 2.62, Maximum achievable: 3.00

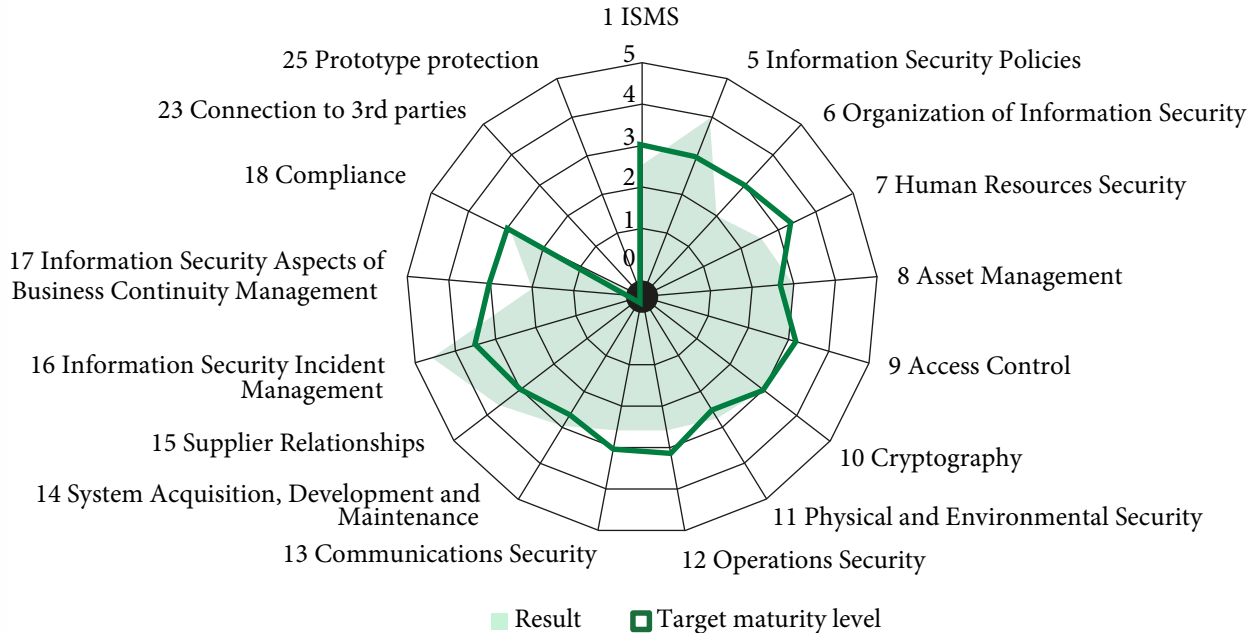


Figure 2: Information Security Assessment. Source: Own illustration based on a fictional customer

The assessment revealed, among other things, that the degree of maturity at various central test points was too low. These low maturity levels are reflected in the spider chart for the ISMS (1), Organization of Information Security (6) and Information Security Aspects of Business Continuity Management (17) categories.

Your Partner

We are authorized to audit companies that process sensitive information for the automotive industry according to the TISAX® standard. The audit is valid for three years.

By participating in TISAX® and undergoing evaluation by our experts, companies open up new opportunities for winning contracts.

Are you interested in a TISAX® assessment to prove the reliability of your information security in the automotive industry? Then request an offer now!

Other services of benefit to you

We can certify other quality, environmental and safety management systems for you, such as ISO 9001, ISO 27001 and ISO 14001 and their combinations. Our portfolio includes more than 40 accreditations! In addition, the DEKRA Group offers comprehensive services related to quality:

- Evaluations for compliance with internal rules, e.g. supplier requirements
- Training and education, e.g. quality management representatives
- Personal certifications, e.g. of your quality manager
- Product testing and certification, e.g. machines, food contact materials and articles

The DEKRA seal of excellence

Setting the pace for superior quality and reliability - across industries and internationally.

The DEKRA seal stands for excellence as an image enhancer and marketing instrument, enabling you to stand out from the competition. Show your customers and business partners that performance is worth the investment. We are happy to provide support.

DEKRA Audit North America
sales.us@dekra.com
www.dekra.us/audits/