TISAX: the standard for information security in the automotive industry

Article by Daniel Wuhrmann

After an extended development process, the German Automotive Industry Association (VDA) created a new industry standard in 2017 based on the ISO/IEC 27001 standard.

TISAX: Trusted Information Security Assessment Exchange

TISAX is designed to offer complete information security for all stages of the supply chain while at the same time simplifying the recognition process for external providers. Following the two-year pilot testing phase in 2016 and 2017, as of 2018, there is no longer any alternative to the TISAX label in the medium term for businesses which intend to work with or for automotive companies. TISAX is operated by the ENX Association, an association of European automotive manufacturers, suppliers and associations which was engaged by VDA as a neutral body.

The TISAX process

The entire TISAX process consists of three steps: registration, the actual assessment and the exchange of the assessment results.

It is particularly important to define the scope and goals of the assessment when registering for TISAX, as these form the basis for the actual assessment in the second stage of the process. In defining the scope of the assessment, a distinction is made between the standard scope and a custom (extended or narrowed) scope. Only assessment results from the standard scope of the assessments are (generally) accepted by other TISAX participants, while a narrowed scope is not suitable for the TISAX label and an extended scope is accepted only insofar as it includes standard-scope assessment results. In addition to the scope, the goals of the assessment are also defined upon registration. These goals determine the applicable requirements for the participant’s information security management system (ISMS) and are to be determined depending on the type of data which is to be processed and its level of protection. Types of assessment goals may include information security, prototype protection, data protection and protection upon involvement of third parties,
and may entail a high or very high level of protection in each case. The higher the level of protection for the individual data, the higher the assessment level and the more intensive the assessment will be, ranging from self-reporting by the participant and document-based assessments to on-site assessments.

The actual assessment in the second stage of the process begins with a VDA self-assessment by the participant (preparatory assessment). This is performed using the questionnaire which has been developed for this purpose, whose assessment is implemented using a maturity level model (Level 0 – Level 5).

The results of the assessment are summarized and compared against the target maturity levels. Only after this self-assessment is performed is a TISAX-accredited assessment service provider selected in order to perform and supervise an information security assessment (ISA) or assessments based on the assessment scope and the self-assessment. This assessment begins in each case with an "initial assessment"; if this initial assessment reveals that the participant is conforming (i.e. that it adheres to requirements and actual ISMS), it leads directly to an official TISAX report and the issuance of a TISAX label. Otherwise, if the results of the initial assessment are not "conforming" and reveal a "major non-conformity," the assessment service provider will prepare a plan of action based on the initial assessment and a subsequent assessment is performed once the participant completes this plan of action. The preparation and execution of plans of action and subsequent assessments are then to be repeated until the participant meets the requirements and is issued a TISAX label, or until the maximum duration of nine months is reached. If no TISAX label is issued in this nine-month period, a new initial assessment is required.

Once the participant receives a TISAX label, its assessment results are exchanged on the ENX portal's exchange platform, in the final stage of the TISAX process. TISAX labels can generally assumed to be valid for three years, beginning with the time of the initial assessment.

---

About us:
reuschlaw Legal Consultants advise companies active on a national and international scale in more than 30 countries in the areas of product liability, product safety law, recall management, insurance law, cybersecurity and data protection, compliance management and contract law.

Company contact: Melanie Schuh | Head of Marketing & Communications | T: +49 30 / 2332895 0 | E: melanie.schuh@reuschlaw.de