VDA ISA and TISAX[1] Model

The VDA (German Association of the Automotive Industry) first set up its "Information Security" working group more than ten years ago. It has gradually developed a catalog of questions about information security (the Information Security Assessment, or VDA ISA), which is based on major aspects of International Standard ISO/IEC 27001. Version 3.0 of the Assessment has been available since the beginning of 2017 and can be downloaded from the following website:

https://www.vda.de/en/topics/safety-and-standards/information-security/information-security-requirements

During recent years this has more or less become an industry standard for information security. At present it consists of one basic component plus additional modules for prototype protection, connections to third parties (e.g. project offices and project areas) and data protection (Section 11 of the Federal Data Protection Act (BDSG) on commissioned processing of data), which can be used during audits. Other modules are developed and added to the catalog as required.

The VDA ISA is used by the member companies both for their own internal purposes and to audit suppliers and service providers that handle sensitive information from these companies. In the past these audits, especially those of service providers and suppliers, were frequently conducted by the company itself. Consequently a service provider or supplier could be audited repeatedly at fairly short intervals. The responsible VDA bodies have now put the substantive and formal prerequisites in place for establishing a common auditing and exchange mechanism (TISAX) in the automotive industry for the Information Security Assessment (ISA) and, in addition, for avoiding multiple (repeated) audits. The TISAX model was constructed to be as universal as possible and therefore also applicable in other sectors.

The concept developed for this purpose has been undergoing pilot testing since May 2016. TISAX is operated by the ENX[2] Association that has been commissioned by the VDA to carry out implementation as a neutral body. TISAX enables competition between accredited audit providers, and through standardization and quality assurance it enables mutual recognition of audit results among the TISAX participants. These audit providers carry the audits out based on the ISA elaborated by the VDA members.

TISAX participants are all companies wishing to either request audits or make audit results available via TISAX. There are two possible roles for participants: that of accessing information (requesting an audit result), and that of providing information (supplying an audit result). A participating company may be audited at the request of another participant, or else make its own arrangements for an Assessment. Following the Assessment by an accredited audit provider, the results are made available to the requesting party. Furthermore, the audited company can choose to make its audit results available to other TISAX participants in varying levels of detail, thus avoiding additional audits for other interested participants with the same security

---

[1] **T**rusted **I**nformation **S**ecurity **A**ssessment e**X**change
[2] **E**uropean **N**etwork e**X**change

requirements. Duplicate and multiple audits are therefore a thing of the past, which helps all those involved to save time and money.

The ENX Association acts as a governance organization. It gives accreditation to the audit providers and monitors the quality of implementation and Assessment results. The legal basis for this control function is the "ENX Triangle of Governance," a contractual framework that consists of contracts between ENX and each accredited auditor, and the "Participation General Terms and Conditions" (GTC) agreed between ENX and each participant. During registration participants agree to be bound by the GTC. This ensures that ultimately the results have the desired quality and objectivity, and that the process preserves the rights and obligations of the participants and satisfies the demands of the requesting parties.

Mutual recognition of audit results requires participants to register for TISAX. In order to register, you must fill out a registration form that you can request from the ENX Association by e-mail: **tisax@enx.com** or by telephone: **+49 69 986692-777**. Further information is also available at: www.enx.com/tisax.

The TISAX model provides for IT security assessments by audit providers in accordance with a VDA standard, and helps avoid redundant audits.

"Information Security" working group