TISAX for information security in the automotive industry.

TÜV Rheinland tests the level of information security in the automotive industry. The basis is the TISAX test model.

www.tuv.com

TÜVRheinland®
Precisely Right.

INFORMATION SECURITY IN THE AUTOMOTIVE INDUSTRY

Information security also represents a key success factor in the automotive industry: It is important for the exchange of design data in development processes, functional security of manufacturing processes, automated data exchange between networked production systems, as well as for the availability and reliability of production. This also applies to the vehicles themselves which have long been computers on four wheels. As a service provider or supplier of the automotive industry, you must prove to your customers at regular intervals whether you comply with the standardized and specific requirements relating to information security.

OUR WORLDWIDE TEST COMPETENCE

TÜV Rheinland now also tests the level of information security in the automotive industry: The TISAX (Trusted Information Security Assessment Exchange) test model is used as the basis in this respect. TISAX is an intercompany test and exchange mechanism based on the VDA ISA. The Information Security Assessment (ISA) of the German Association of the Automotive Industry (VDA) contains essential features of the Information Security Management System (ISMS) according to ISO 27001.

WARUM SOLLTEN SIE AN TISAX TEILNEHMEN?

All suppliers and service providers of automobile manufacturers and suppliers who process sensitive information from the respective firms should be interested in actively using TISAX in order to meet the requirements of their customers. The results always remain under the control of the customers who are being tested.

WHO IS ALLOWED TO TEST IN ACCORDANCE WITH TISAX?

The so-called TISAX assessments may only be performed by testing organizations accredited in accordance with TISAX.

TÜV Rheinland is one of the few testing services providers authorized to test and certify organizations in the automotive industry worldwide according to TISAX.

YOUR ADVANTAGES AT A GLANCE

- The assessment produces important value-added for information security in tested organizations (potential improvements are identified).
- Renewal of existing supplier relationships is made easier.
- TISAX assessments are recognized beyond the individual customer.
- Multiple tests are therefore increasingly a thing of the past.

PROCEDURE FOR A TISAX ASSESSMENT:

1 DEFINITION	Definition of the assessment level by the OEM, e.g. also with prototype protection, etc.
2 REGISTRATION	Registration of the organization in ENX where the organization receives the scope ID (preparation of self-information).
3 INITIAL ASSESSMENT	**Inspection:**documents and processes, either a telephone interview at assessment level 2 or an on-site assessment at assessment level 3, prototypes or third-party connection
4 PRESENTATION OF THE FINDINGS	Discussion concerning the findings, presentation and verification of the corrective action plan by the auditee and completion of the initial assessment through preparation of a report
5 RECTIFICATION OF FINDINGS	Customer rectifies findings according to the corrective action plan – in accordance with the valid periods
6 FOLLOW-UP ASSESSMENT	**Inspection:** Further examination and evaluation of documents and processes with findings. Preparation of the follow-up assessment report. Issue of a TISAX label if all non-conformities have been eliminated.

TÜV Rheinland
ICT & Business Solutions
Am Grauen Stein
51105 Köln
Tel. +49 221 56783 501
tisax@de.tuv.com

www.tuv.com/tisax

TÜVRheinland®
Genau. Richtig.

12.2017