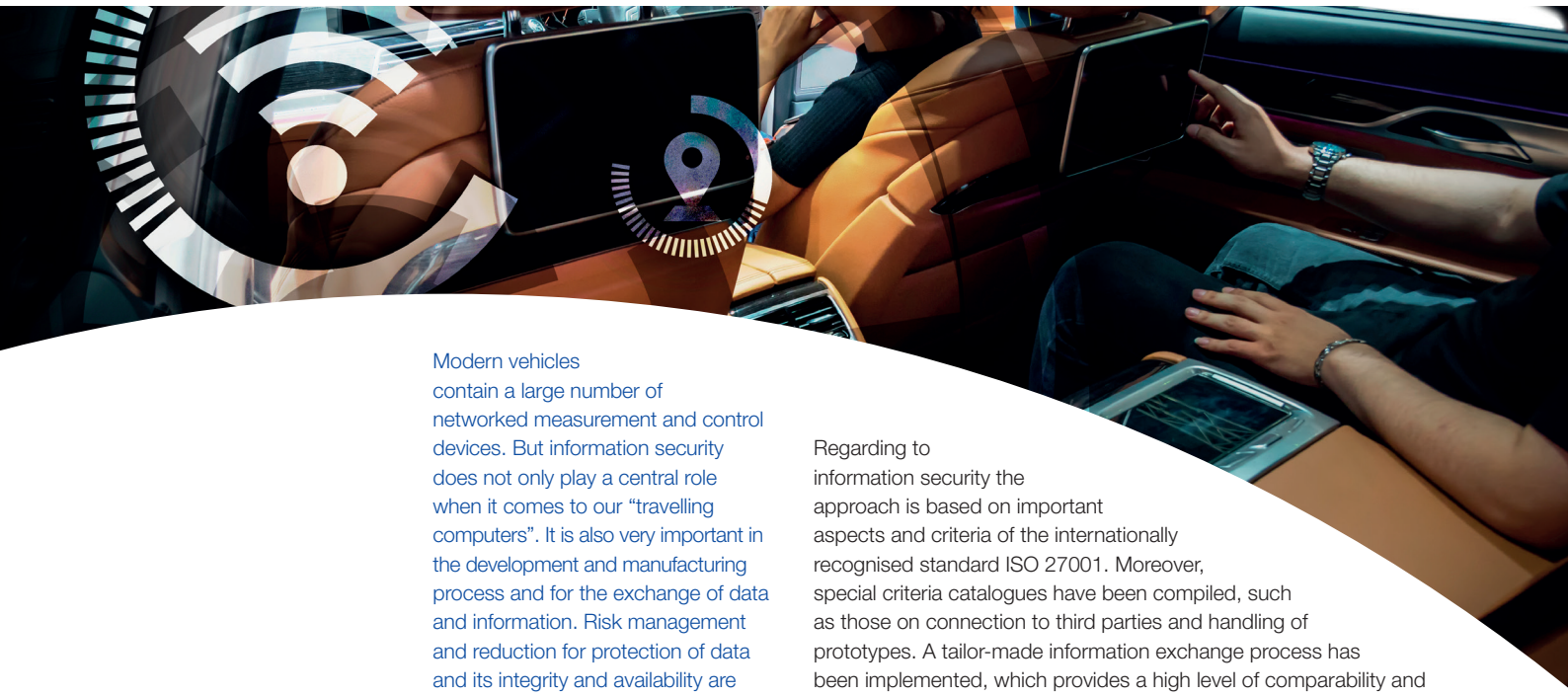
Assessments of information security management systems according to TISAX



Modern vehicles contain a large number of networked measurement and control devices. But information security does not only play a central role when it comes to our “travelling computers”. It is also very important in the development and manufacturing process and for the exchange of data and information. Risk management and reduction for protection of data and its integrity and availability are achieved by means of information security management systems (ISMS).

In the automotive area, the effectiveness of an ISMS can be established by means of assessments according to TISAX (Trusted Information Security Assessment Exchange), which are now explicitly required by many automotive manufacturers. The assessments are based on the VDA ISA requirement catalogue, developed by the German Association of the Automotive Industry VDA.

Regarding to information security the approach is based on important aspects and criteria of the internationally recognised standard ISO 27001. Moreover, special criteria catalogues have been compiled, such as those on connection to third parties and handling of prototypes. A tailor-made information exchange process has been implemented, which provides a high level of comparability and transparency and therefore strengthens the trust of customers demanding achievement of the TISAX label.

Two possible participation roles

There are two possible roles for participation within the data exchange model, which are available to participating companies depending on need:

- Passive participants (e.g. OEMs, automobile manufacturers): These require another company (e.g. supplier) to have an assessment carried out and then request access to the test results.
- Active participant or auditee (e.g. supplier): A company is required by another company (e.g. OEM or customer) to undergo an assessment according to the criteria catalogue or it undergoes the assessment on its own initiative. Following the assessment, the active participant allows selected companies (e.g. OEMs) to access its assessment results.

Companies gain access to the TISAX portal by registering as participants. Registration is also a prerequisite in order to commission an assessment by an accredited assessment organisation. Such organisations are known as XAPs.

TÜV®

TÜV NORD Singapore

Different protection and assessment levels and their test steps

There are different protection levels and corresponding assessment levels, which determine the assessment of a company:

Assessments with level 1 mostly play a role for internal purposes in the true sense of a self-assessment by the auditee himself.

In the case of a high protection level, an assessment is performed according to level 2 and involvement of an XAP is obligatory. The prerequisite here is that an assessment according to level 1, in other words the complete self-assessment, has been carried out. The assessment steps are as follows for the assessment according to level 2:

- Kick-off meeting
- Completeness and plausibility check of the self-assessment and of suitable evidences
- Telephone interview of the persons responsible for the ISMS based on the required documents (on-site inspection if required, e.g. if third parties and/or prototype protection are involved).

In the case of a very high protection level, an assessment is carried out according to level 3, and an XAP must be involved. Here, the test steps are similar to those of the level 2 assessment, with the addition that significant aspects are considered in an on-site inspection. Of course, a complete self-assessment must also be present:

- Kick-off meeting
- Completeness and plausibility check of the self-assessment and of suitable evidences
- Assessment of the effectiveness and maturity level of the ISMS by means of an on-site inspection with those involved (expert interviews on site, inspection of relevant areas of the organization).

After both the level 2 and level 3 assessments, the findings (e.g. the maturity levels) and the requirement for corrective actions are discussed and summarised in a preliminary report.

The following two assessment steps must then be carried out following the initial assessment described above in order to receive a TISAX label:

- Development of a plan for corrective actions by the auditee and review by the XAP. The plan is explained and summarised in a follow-up report which is generally in the form of an update of the preliminary report.
- Implementation of the corrective actions by the auditee and evaluation of the actions by the XAP. A report is also created here (generally a new update) which is then uploaded to the ENX platform as the final report. A maximum period of nine months is allowed from the first opening meeting up to this final stage, and if this is exceeded, the whole process must be started again from the beginning.

Each company can decide for itself who is allowed to view the results. The quality of the assessment process and the findings are reviewed by the ENX association, which then awards the TISAX label, valid for three years. After this time, the procedure as a whole has to be repeated.

Target groups for TISAX assessments

Assessments according to TISAX were developed for suppliers and service providers within the automotive sector who work with sensitive data. The TISAX labels are recognised by all VDA members including companies such as Audi, Volkswagen, BMW and many others. In some cases, assessment to TISAX is already mandatory for suppliers.

Benefits of the TISAX program

- All assessment criteria are relevant for the automotive sector
- High assessment quality and consistent results
- Standardised, strict assessment and reporting procedures
- Results are therefore both comparable and meaningful
- Duplicate and repeat assessments can be avoided
- Reduction of risks and establishment of a risk management system
- Broad acceptance and greater trust within the automotive sector
- Enhanced customer loyalty and promotion of new business
- Strong focus on the needs of customers

Our know-how for your success

For many years TÜV NORD CERT GmbH has been approved by the German accreditation body DAkkS for auditing and certification of information security management systems (ISMS) and on the basis of its proven expertise has also been granted approval by ENX as a TISAX Accredited Audit Provider (XAP) for the automotive sector.

Are you interested?
Please send us your response by e-mail.
We are looking forward to hearing from you.

☐ **Yes, I am interested in assessment of information security management systems according to TISAX.**

☐

Sender (Please use block capitals)

Company .....

Mr/Ms .....

Position .....

Address .....

Postcode/Town .....

Phone .....

Mobile .....

E-mail .....

TÜV NORD Singapore

25 International Business Park
#03-107 German Centre
Singapore 609916

Tel.: +65 6904 6700
ctang@tuv-nord.com

You can find further information and our subsidiaries at
www.tuv-nord.com