Trusted Information Security Assessment Exchange (TISAX)
Information security in the automotive industry

Information security is 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 vehicles, which have long been computers on four wheels. As a service provider or supplier to the automotive industry, a company must prove to customers, at regular intervals, whether it complies with standardised and specific requirements relating to information security.

What is TISAX and why go for it?

Trusted Information Security Assessment Exchange (TISAX) is a common assessment and exchange mechanism in the automotive industry and beyond. It is an inter-company test and exchange mechanism based on the VDA Information Security Assessment (ISA).

TISAX has been developed under the guidance of the VDA to ensure a unified level of information security. TISAX brings standardisation, quality assurance and mutual recognition of audits.

TISAX provides for information security assessments by audit providers in accordance with VDA standards and helps avoid redundant audits.

Forerunners of TISAX

The German Association of the Automotive Industry (VDA) has developed a catalogue of questions for Information security, based on the ISO/IEC 27001 standard. The VDA published the questionnaire for checking Information Security Assessment and Information Security Management (Version 4.1.0) in December 2018.

ENX is a non-profit organisation that was built in the year 2000. It is an association of European automotive manufacturers and suppliers. ENX is used for the exchange of information as it enables all partners to exchange data between companies and across borders in a uniform, harmonised way.

TISAX is a part of the ENX platform and establishes a common assessment and exchange mechanism in the automotive industry. The ENX Association acts as a governance organisation of TISAX. It accredits the audit providers and monitors the quality of implementation and assessment results.

Scope of TISAX assessments

<table>
<thead>
<tr>
<th>Information security management system (ISMS)</th>
<th>Data protection</th>
<th>Prototype protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is the basic module for determining the maturity of information security processes and their management. This module is always necessary.</td>
<td>This module is required when the supplier processes the personal data of customers.</td>
<td>This module is required when the supplier works with strictly confidential information about prototypes. The focus is on the implementation of physical measures.</td>
</tr>
<tr>
<td>Number of controls: 52</td>
<td>Number of controls: 4</td>
<td>Number of controls: 22</td>
</tr>
</tbody>
</table>

Connection with third party

This module is required when the supplier is connected to an IT network or a similar technical exchange of confidential data where the manufacturer is established.

Number of controls: 4
Approach for TISAX assessments

PwC (Auditor)

- Accreditation
- Audit application
- Report provision
- Report request
- Audit and report

ENX

Participant (e.g. OEM)

Link to the report

TISAX (trusted anchor)

Release of the report

Auditee (participant in the supply chain)

Benefits of TISAX

- Trusted partners for OEM
  - Creates trust for your manufacturer, thereby helping you with contracts with various automotive manufacturers.
- Uniform standard
  - Provides a harmonised standard for information security within the automotive industry.
- Maturity assessment
  - Helps assess the maturity of the information security controls in an organisation.
- Recognition
  - Strengthens the existing alliance and promotes new business relations.
- Awareness
  - Improves employees’ awareness pertaining to information security.
- Lower cost
  - Helps reduce costs and efforts with the manufacturer and suppliers related to multiple information security assessments.

How PwC can help

- Conduct initial assessments
- Identify gaps
- Support in remediating gaps
- Support in certification
- Revalidate assessments

Why PwC?

We deliver great value because we invest in sector solutions and work with our clients to build their skills to achieve greater benefits. We believe we will deliver high value-added support to you through:

- Diverse and experienced team
  - We have an experienced team and an approach that will address your key challenges and bring out valuable insights. A Cyber Risk team that brings together 600+ IT and Cyber Risk management professionals.
  - We employ adaptive methodologies
    - Our methodologies are robust yet flexible and we tailor them to the client environment. The key components in our methodologies include our well-tested framework and strong database of risks and reference documents.
  - We use the right set of technologies
    - We have deep and broad experience of information security assessment, with the independence and ability to bring in a fresh perspective with respect to your organisation’s operation model.
- Knowledge sharing and transfer
  - We are committed to working collaboratively with you and helping you identify your roadmap. As part of the engagement delivery, we, along with our centre of excellence team in Germany, will help you to secure the security gaps we identify during information security assessments.
- Client confidence
  - We form close, long-term relationships with our clients. Our clients re-use our services and would recommend us to others. We are looking forward to a long-term relationship with you.
About PwC

At PwC, our purpose is to build trust in society and solve important problems. We’re a network of firms in 158 countries with over 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India’s service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2019 PwC. All rights reserved

Accredited ISO 27001 certification body
The PwC Certification Services GmbH (former PERSICON) is accredited by the “Deutschen Akkreditierungsstelle” (DAkkS) as an accredited test institute for “Information Security Management Systems” (ISMS) subject to ISO 27001. PwC is therefore entitled to issue certificates according to ISO 27001.

Expert inspection body for data protection
The PwC Certification Services GmbH (former PERSICON) is an acknowledged inspection body for data protection.

Contacts

P. Unnikrishnan
Partner
Cyber Security Services
Email: unnikrishnan.padinjyaroot@pwc.com
Mobile: +91 9845118097

Rachit Chhokera
Associate Director
Cyber Security Services
Email: rachit.chhokera@pwc.com
Mobile: +91 9820988266

Shivakumar Jayashankar
Associate Director
Cyber Security Services
Email: shivakumar.jayashankar@pwc.com
Mobile: +91 9840131120

With PwC, our purpose is to build trust in society and solve important problems.