PKWARE

PK Protect

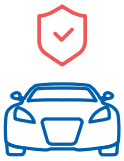
PK Protect

Solution Overview: TISAX Compliance

Setting the Information Security Standard in the Automotive Industry

Since 2003, the German Association of the Automotive Industry (Verband der Automobilindustrie, or VDA) has been working to create and maintain an industry standard for information security. Today, the VDA's Information Security Assessment (ISA) questionnaire is the established framework used by companies to assess their information-security maturity levels and build trust among manufacturers, suppliers, service providers, and consumers.

INFORMATION SECURITY



PROTOTYPE PROTECTION

PERSONAL DATA PROTECTION

The latest version of the VDA ISA consists of 67 controls, formulated as questions, designed to evaluate a company's organizational governance, risk management practices, and technical measures in three areas: information security, prototype protection, and personal data protection. It is updated periodically to account for evolving technologies and regulations, from cloud computing and the Internet of Things (IoT) to data privacy laws like the General Data Protection Regulation (GDPR).

The Trusted Information Security Exchange

To ensure cross-company standardization, quality, and recognition of assessments—and to avoid multiple audits of individual companies—the VDA set up the Trusted Information Security Assessment Exchange (TISAX) and consigned its operation to a neutral third party, the ENX Association. Organizations can register online as participants, find audit providers accredited by ENX to perform an assessment, and exchange official results with other participants. Each assessment is valid for three years.

To date, more than 2,800 companies from around the globe have registered with TISAX and performed more than 2,600 assessments.

> "In the past two years,more than 25,000 improvements in information security have been achieved in the participating companies."
>
> VDA Annual Report 2020

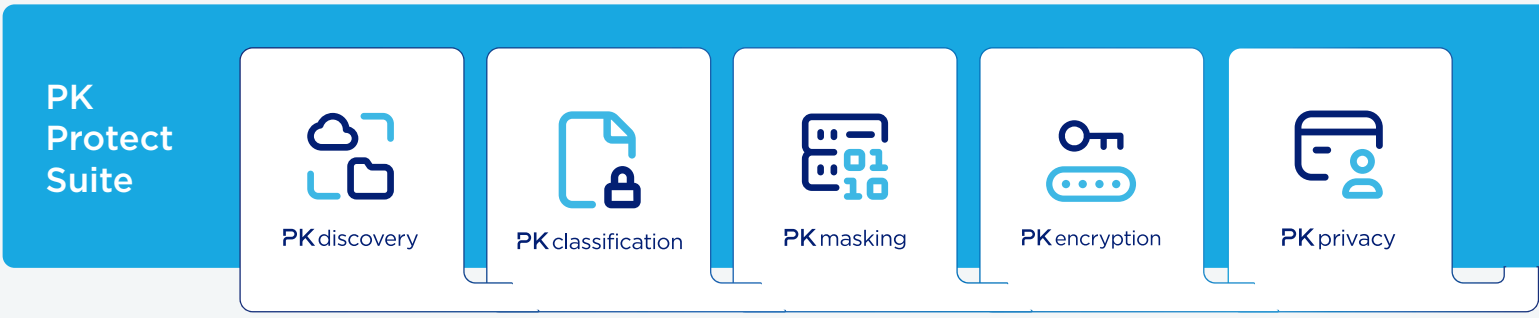
Does My Company Need to Comply with TISAX?

Information security is critical given that some of the most complex supply chains in the world now produce what are basically computers on wheels. Highly sensitive data and personal information is constantly shared among automotive companies, as well as public authorities and other companies working to improve traffic safety and product efficiency.

While TISAX is not a law, it is the automotive industry standard for information security and, in effect, a prerequisite for close cooperation between manufacturers and their suppliers or service providers.

PKWARE's Approach to TISAX Compliance

PKWARE strives to simplify compliance by enabling a wide range of data protection capabilities in a single solution—one that is designed to integrate easily into your IT ecosystem and existing information security processes. Our automated solution allows you to find and protect sensitive data wherever it lives and moves.



What Does PKWARE's Technology Do?

PK Protect is a comprehensive suite of data discovery and protection solutions designed to prevent personal and sensitive data from being lost, stolen, or inappropriately exposed wherever it is stored, used or share.

The PK Protect suite includes the following solutions:

- **PK Discovery:** Locate and identify sensitive data across your organization
- **PK Classification:** Categorize and tag data based on your business needs
- **PK Masking:** Desensitize data for maximum usability by business teams
- **PK Encryption:** Restrict access to sensitive data to authorized users only
- **PK Privacy:** Automated compliance for policies, laws, and personal obligations

Which TISAX Requirements Does PKWARE Support?

An organization's maturity level (or score) will depend on how—and how well—people and technology work together in a process to meet those requirements. The VDA ISA has several requirements around level of protection and uses a six-level maturity model with scoring from 0-5. The target maturity level is 3.

The following charts show where PKWARE adds value. For applicable control questions, PKWARE will typically address some but not all of the requirements. For example, control 1.3.1 requires that "information assets of critical value to the organization are identified and recorded" and that "a person responsible for these information assets is assigned." PKWARE can identify and report any sensitive data it discovers, but it needs to be "told" who the data owner should be.

For more details about each requirement, download the latest VDA ISA catalog, and contact us to learn how PKWARE can help you comply.

Click here to download the latest VDA ISA catalog (XLSX)

PKWARE Can Help with These Information Security Controls (22/40)

1.2.1	To what extent is information security managed within the organization?
1.2.3	To what extent are information security requirements taken into account in projects?
1.3.1	To what extent are information assets identified and recorded?
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?
1.4.1	To what extent are information security risks managed?
1.5.1	To what extent is compliance with information security ensured in procedures and processes?
1.6.1	To what extent are information security events processed?
2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?
4.1.1	To what extent is the use of identification means managed?
4.1.2	To what extent is the user access to network services, IT systems and IT applications secured?
4.2.1	To what extent are access rights assigned and managed?
5.1.1	To what extent is the use of cryptographic procedures managed?
5.1.2	To what extent is information protected during transport?
5.2.1	To what extent are changes managed?
5.2.2	To what extent are development and testing environments separated from operational environments?
5.2.4	To what extent are event logs recorded and analyzed?
5.2.5	To what extent are vulnerabilities identified and addressed?
5.2.6	To what extent are IT systems technically checked (system audit)?
5.3.4	To what extent is information protected in shared external IT services?
6.1.1	To what extent is information security ensured among suppliers and cooperation partners?
7.1.1	To what extent is compliance with regulatory and contractual provisions ensured?
7.1.2	To what extent is the protection of personal data taken into account when implementing information security?

PKWARE Can Help with These Data Protection Controls (3/4)

9.2	To what extent are organizational measures taken in order to ensure that personally identifiable data is processed in conformance with legislation?
9.3	To what extent is it ensured that the internal processes or workflows are carried out according to the currently valid data protection regulations and that these are regularly subjected to a quality check?
9.4	To what extent are the relevant processing procedures documented with regard to their admissibility according to data protection law?

What About Prototype Protection?

The Prototype Protection section of the VDA ISA contains 22 controls, most of which cover physical and environmental security and organizational requirements.

Because prototypes are subject to project-related (1.2.3) and regulatory (7.1.1) information security requirements, the electronic information created, shared, and stored about prototypes—e.g., schematics, images, and recordings—automatically demands high or very high protection needs.

PKWARE can help keep this information secure.

Reduce the Risks and Costs of TISAX Compliance with PKWARE

From the moment sensitive data is created, PKWARE can track and protect it as it is used and shared. PKWARE solutions are proven to reduce the risks and costs of compliance with TISAX as well as other governmental regulations enacted to ensure data security and privacy. Whether you want to start with endpoints, limited TISAX requirements or go all in, PKWARE can support.

Ready To See It Live? Contact Us!

pkware.com/demo

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

Follow Us

/company/PKWARE

facebook.com/PKWARE

@PKWARE