MEETING TISAX SECURITY STANDARDS WITH PKWARE

European automotive companies use the Trusted Information Security Assessment Exchange (TISAX) to enforce a common set of information security requirements for manufacturers, suppliers, and service providers.

Like many other security mandates, TISAX is only a few years old, and many organizations are still searching for the right approach to it. TISAX has many sections, and some of the most challenging requirements for organizations to meet are those regarding data security.

This paper explores the specific requirements that auto industry suppliers and service providers must meet. It will also discuss some of the best practices in data security to make workflows more efficient and to make both meeting compliance and staying compliant easier.

WHAT IS TISAX AND WHY DOES IT MATTER?

The Trusted Information Security Assessment Exchange (TISAX) is a framework for data security verification within the European automotive industry.

TISAX was introduced in 2017 and has become the standard process for demonstrating that organizations have implemented appropriate data security. TISAX is coordinated by ENX, the European automotive industry association.

Through TISAX, companies undergo third-party assessments of their data security systems and processes and share their assessment results with customers and partners. TISAX assessments are based on requirements defined in the VDA ISA (Verband der Automobilindustrie Information Security Assessment), which itself is based on ISO 27001 standards.

The VDA ISA assessment covers 18 core areas of information security, with additional sections that address third-party data sharing and protection for prototypes.

In each section, the assessment contains questions related to high-level corporate governance and risk management topics, as well as technical details related to process and technology implementations.

After completing an assessment, companies can use the TISAX system to share their assessment results with their partners, customers, or prospective customers.

As more manufacturers begin using TISAX, companies that are unable to demonstrate their compliance with the assessment standards will find it difficult or impossible to compete in the European automotive market.

TISAX HAS BECOME THE STANDARD PROCESS FOR ASSESSING AND VERIFYING DATA SECURITY WITHIN THE EUROPEAN AUTOMOTIVE INDUSTRY.

BEST PRACTICES: ADDRESSING DATA SECURITY CHALLENGES

Meeting the data security requirements of TISAX can be painful and time-consuming. Data security mandates like TISAX are complex and multifaceted, requiring the coordination of efforts of multiple departments within an organization, along with multiple vendors, partners, and advisors. Even requirements for a single section of the guidelines can involve coordination between large groups of stakeholders and solutions from several different vendors.

One way to streamline the process is to implement solutions that have one or both of the following characteristics:

1. **The solution can address multiple requirements.**

   This could be a solution that has the ability to, for instance, both classify files and encrypt data persistently.

2. **The solution can keep the company compliant going forward with minimal manual intervention.**

   This could be, for example, the ability to automate data security. Solutions are available in which a) admins create security policies, b) the system automatically goes finds sensitive data as defined in the policy, c) applies remediation (such as classification and persistent encryption) to those data files as per the policies, and d), the system automatically scans and remediates files as they are created and changed.

Addressing multiple data security requirements and automating the discovery and remediation of sensitive data would reduce workloads on IT and compliance resources, as well as reduce the number of solutions (and the initial investment) a company needs to use to meet its obligations.

TISAX DATA SECURITY REQUIREMENTS

For each aspect of information security covered in an organization's TISAX assessment, the organization is assigned a "maturity level" that indicates how fully the organization has met TISAX standards.

The VDA ISA assessment lists procedures and technologies that must be implemented in order to meet the standards, along with optional methods that organizations can implement at their discretion. The assessment also contains many specific requirements for high-value data, described as data with "high protection needs" or "very high protection needs."

This whitepaper discusses TISAX standards, technological considerations, and best practices related to the following areas of information security:

- Cryptography
- Data classification
- Sensitive data on mobile storage devices
- Controlling access to sensitive information
- Event logging
- Electronic exchange of information
- Confidentiality and protection of personally identifiable data

CRYPTOGRAPHY

Encryption is the strongest form of data protection, making it impossible (assuming the encryption was done properly) for anyone to read sensitive data without the correct decryption key.

TISAX standards (in Section 10.1 of the assessment) call for sensitive data be protected with encryption both at rest and in transit. Encryption isn't just a checkbox here, however. The role of both key management and strong encryption algorithms must also pass muster.

Approaches to encryption

Some technologies (such as encrypted hard drives or file server encryption) focus on encrypting data at rest. As long as the files are in a "secure location," they're protected. But copy the file onto Dropbox, a cloud instance, or a mobile storage device (or anywhere but that secure location), and the file loses its protection.

Data-in-transit encryption, on the other hand, focuses on creating encrypted tunnels, such as those made by VPNs or WAN encryptors. The issue with this, however, is that the onus is often on the user to start the tunnel and choose to send the sensitive data through it.

Marking the checkbox in this case might be easy to do with a VPN, but doesn't make it easy for users (or enforceable by organizations) to actually keep the data safe.

Best practice: persistent encryption...

Persistent encryption technology provides the provides the benefits of both data-at-rest and data-in-transit encryption, with additional security.

Unlike other forms of encryption, persistent encryption is applied to data itself, rather than to a storage location or transmission system. Information protected by persistent encryption remains secure throughout the entire data lifecycle, whether files are saved on servers, endpoint devices, removable storage, or in the cloud.

Because persistent encryption keeps the protection attached to the data, the files are not only protected wherever they go (Dropbox, USB drive, etc.) but also are protected when they are in transit, from Point A to Point B.

...with enterprise-class key management

Generally considered the most challenging aspect of enterprise-wide encryption, key management involves a variety of functions, including key generation, key storage, key exchange, and key rotation.

To ensure effective protection and ease of use, organizations should consider encryption vendors that support a variety of encryption key formats, offer the ability to manage of millions of keys and certificates, and support integrations with hardware security modules and related infrastructure.

FORMS OF ENCRYPTION

Encryption can be implemented many different ways, some of which leave data vulnerable to inappropriate access as it moves from user to user and device to device.

Network encryption protects data as it travels across a network. Data is encrypted while in motion from its origin to its destination, but remains in the clear on either side of the transmission, unless another form of encryption is used.

Transparent encryption protects data at rest. When transparent encryption is applied, the protection is removed before data is accessed. This makes the encryption process "transparent" to end users, but also means data exists in the clear any time it is moved or copied from the protected location.

Persistent encryption travels with data as it is shared, copied, and moved from one system or user to another.

CONTROLLING ACCESS TO SENSITIVE INFORMATION

Section 9 of the VDA ISA security assessment deals with access control. In its subsections, it defines standards for policies and procedures related to user registration, permission management, data access, and other aspects of access management.

As with other areas of TISAX compliance, many of Section 9's requirements overlap with each other and with other sections of the assessment. And as with other TISAX standards, some approaches can better help organizations meet these requirements and demonstrate compliance to assessors, customers, and partners.

Subsection 9.1 asks "To what extent are policies and procedures regarding the access to IT systems in place?" In addition to standards for creating and documenting policies, 9.1 also dictates a few specific approaches for controlling access to sensitive information. Data requiring "high protection" should to be protected by passwords at a minimum, while data requiring "very high protection" must be protected with measures that include multi-factor authentication.

Subsection 9.5 goes into more detail on limiting access to sensitive information. Most of the subsection focuses on internal processes for granting and reviewing access permissions. It also contains one specific requirement for data requiring very high protection—it must be secured using "Encrypted data storage in order to prevent access and viewing by unauthorized persons/roles (e.g. administrators) at least on file level.".

Best practice: associate encryption keys with user identities

Certain vendors have an approach to policy management and encryption key management that allows organizations to maintain strict control over the protection applied to sensitive data and the access different users and groups have to that data.

One approach is providing organizations the option of associating encryption keys, classification schemes, and other security features to user identities (contained in Active Directory, for example). This means that administrators can create granular policies that allow each user or group to access only the data they are authorized to use. Integration with Active Directory—and the enforcement of information access because of it—is an especially effective way to reduce the organization's exposure to risks from insider threats.

A real-world example: if an employee has access to an encryption key but leaves the company, the employee record can be removed from Active Directory and that person will no longer have access to the key, or any files encrypted with the key, even if the employee copies them before leaving the company.

Best practice: Automated encryption with support for MFA

To ensure compliance with standards for "very high protection," organizations should implement a solution that applies strong encryption and supports multi-factor authentication (MFA) as well.

These technologies, especially when using a key management approach that associates user identity with decryption keys, provide an exceptional level of organizational control over highly sensitive information.

In this case, a user who attempts to access a file that requires MFA would be prompted the user to enter a token code (or other MFA credential), and validate the code through an integration with the organization's MFA technology. If (and only if) the user has entered a valid MFA code will the file be decrypted.

DATA CLASSIFICATION

If you're a supplier or service provider, you likely work on sensitive projects with your partners, requiring a daily exchange of sensitive information. Your partners need to know that you're handling their sensitive information with care, protecting it from theft, loss, and manipulation.

Many information security regulations recommend the use of classification to ensure that sensitive information is being appropriately protected and handled, and TISAX standards are no different.

Question 8.2 in the VDA ISA asks "To what extent is information classified according to its protection needs and are there regulations in place regarding labelling, handling, transport, storage, retention, deletion and disposal?" Specific requirements include the use of a consistent, policy-based classification scheme and the classification of data based on criteria such as value, confidentiality, and legal requirements.

Differing approaches to data classification

Many vendors offer data classification as part of their security platforms. Many times, the technology requires users to classify documents manually. This can be an effective approach for files created or modified going forward.

However, this approach is ineffective for the thousands (or millions) of files generated before the classification project was implemented. Older files represent a huge amount of sensitive data that must be classified, often far too much to be handled manually.

Best practice: automated classification

Other vendors combine automated data discovery with batch classification tools. In this scenario, data discovery tools are automatically set to search for specific terms or file characteristics. Once certain criteria are met, the appropriate classification is applied to the file. This takes the burden off employees to make decisions on how files should be classified, while ensuring that your classification rules are applied consistently across your entire organization. This is precisely what the TISAX security assessment requires.

Automated classification does have a drawback, in that inaccuracies in the search criteria can lead to misclassification of a small percentage of files.

In these cases, implementing the ability for human override of classification can solve this issue. Many organizations prefer the misclassification of a small percentage of their files over giving their users the onerous task of manual classification of years' worth of old files.

BENEFITS OF CLASSIFICATION

Data classification delivers a wide range of benefits, making an organization's sensitive data more secure and easier to manage.

Improve effectiveness of other solutions
In addition to adding human-readable file labels, classification applies metadata tags that can direct the actions of downstream security and data management technology, such as cloud access security broker (CASB) solutions and reporting tools.

Build a culture of security
Human error is to blame for a large percentage of security breaches. Heavy workloads, new technology, and insufficient training can lead employees to violate data security policies unintentionally. The inclusion of end users in the classification process helps to build a culture of security awareness across the organization.

Facilitate safer collaboration
Data classification provides a means of building security into the corporate culture in a way that encourages, rather than inhibits, productivity and collaboration. A single set of classification policies, applied consistently across the entire organization, removes obstacles that might otherwise prevent employees from sharing important information with colleagues and partners.

SENSITIVE DATA ON MOBILE STORAGE DEVICES

The use of mobile storage devices, such as USB thumb drives, poses a significant risk to data exposure, as demonstrated by the 2018 Heathrow Airport breach. It's not surprising that automotive companies are concerned about the use of mobile storage devices by their suppliers and service providers.

To meet TISAX standards (specifically section 8.3), automotive companies must define the measures they take to make sure sensitive information on mobile storage devices doesn't fall into the wrong hands—especially if a device is lost or stolen.

Differing approaches to encryption on mobile storage

Many organizations have encryption solutions in place. Sometimes organizations implement disk-based encryption (such as solutions that encrypt laptop hard drives or network storage drives). Other solutions include "data-at-rest" encryption, which encrypt files that are stored in secure folders or other secure locations.

These solutions are easy to implement, but suffer security drawbacks. Disk-based encryption is only effective when the drive is shut down (or in some cases asleep). Files aren't protected when the drive or laptop is on. Data-at-rest solutions protect files in those secure locations.

With both these solutions, if users copy the files onto a mobile storage device (or copy it to Dropbox, or an Azure instance, or anywhere but that secure location), the file loses its protection. An organization's employees might be walking around with dozens of unprotected files in their pocket—and this is not compliant with TISAX.

Best practice: persistent encryption

There is another approach: persistent encryption remains with files even when transferred between devices or other media, keeping the files inaccessible to unauthorized users. PKWARE's data security platform can automatically apply persistent strong encryption to files based on classification labels or other parameters (defined by policies). As part of the automated security workflow, the security policies are applied to the files before they ever hit the mobile storage device.

EVENT LOGGING

Section 12.5 of the VDA ISA assessment requires that companies have the means to record events and protect them against modification so that in the event of a security incident, companies are able to determine the cause and take the appropriate actions to remediate and protect against future incidents.

Many vendors have reporting tools within their data security solutions that allow security teams and audit personnel to monitor activity. An organization should make sure protections are in place to protect the logs from being altered. Capabilities such as reporting data by time and event type, and the ability to search for specific terms within event logs should be part of a considered solution.

Best practice: integration with existing business intelligence tools

If an organization chooses a solution with multiple capabilities, such as data discovery, classification, and protection activity, its activity logs should be easy to import into an intelligence tool such as Splunk (or whatever your organization has standardized on) in order to maximize visibility and usefulness.

ELECTRONIC EXCHANGE OF INFORMATION

Huge amounts of sensitive information are exchanged and transferred daily between partners in the automotive industry. To ensure its protection, Section 13.4 of the VDA ISA assessment requires companies to define which service can be used for which type of data and which protective measures are to be taken when using the services.

Best practice: automation and persistent encryption

Instead of creating paper policies, training employees, and ensuring that every employee has access to every service that should be used to transfer or exchange information, companies are encouraged to use a solution with data security automation, which combines the discovery, classification, and rules enforcement based on your organization's policies.

Some vendors provide dozens of policies based on common regulations and standards throughout the world that can be used as templates to build an organization's rules.

While several remediation options could be permitted, a solution that features persistent encryption (as a best practice to meet other requirements) will meet this requirement, preventing unauthorized access no matter where or how the files are transferred or exchanged. Be sure that any solution chosen allows data to be exchanged securely no matter what service is used, including via cloud, FTP, Outlook and other methods.

CONFIDENTIALITY AND PROTECTION OF PERSONALLY IDENTIFIABLE DATA

Like GDPR, TISAX standards require the protection of personally identifiable information (PII).

Section 18.2 of the assessment states that files containing PII must be classified to indicate the sensitivity of their contents, and that the files must be protected.

Best practice: integrated classification and protection

Automation and integration are the keys to protecting personal information. A solution that features automatic remediation after a discovery tool finds sensitive data (as defined by your organization's policies) is the best way to ensure that nothing slips through the cracks.

Organizations should look for solutions that can automatically detect files containing PII, apply the appropriate classification tags, and then protect the files according to policy.

This approach allows organizations to be confident that any systems with sensitive data or PII will meet TISAX requirements—not just in a fixed point in time, but in real time going forward.

Best practice: encrypting PII

TISAX standards do not dictate how files containing PII must be protected. However, persistent strong encryption is the most effective form of protection, and should be applied to consumer data, HR records, and other forms of sensitive data.

Encryption also reduces the risk of violations under other security mandates, including GDPR. In fact, GDPR contains provisions that exempt organization from data breach reporting and other requirements, if they protect personal data with persistent strong encryption.

CONCLUSION

TISAX compliance is a critical consideration for companies in the European automotive market, and requires a significant investment of time and resources.

However, meeting TISAX standards doesn't have to be complicated, disruptive, or prohibitively expensive. Companies in the automotive industry can streamline their compliance efforts—and improve the results of their TISAX assessments—by choosing security solutions that address a wide variety of TISAX standards.

Automated security workflows are recommended to combine data discovery with data classification, encryption, key management, and event logging through a single data security platform.

No single vendor can address every aspect of TISAX, but by choosing the right partners and the right approach to compliance, your organization can meet its compliance goals and improve its competitive position in the European automotive market..

PKWARE: AUTOMATED DATA SECURITY

Organizations around the world use PKWARE's data security platform to meet a variety of their compliance needs, including TISAX standards. PKWARE addresses specific requirements for data classification, data protection, encryption key management, and activity logging—from a single solution.

But perhaps the best capability of the PKWARE solution is the ability to automate data security, helping to assure your company that it will constantly be within TISAX guidelines, even if new files, new systems, and new users come online.

PKWARE's solution allows your organization to combine data discovery scanning and persistent encryption in a single workflow, so whenever an employee creates a file that has sensitive data in it (as defined by your policies), persistent strong encryption (and many other remediation options) can be applied automatically—and immediately. Security workflows can be set up in many different ways, but this automated data security workflow is unique to PKWARE's solution.

With PKWARE's automatic policy enforcement and persistent strong encryption, you can be confident that any systems with sensitive data you have will meet TISAX standards for data protection.

PKWARE®

www.PKWARE.com

PKWARE solutions help organizations eliminate security gaps, manage sensitive data, and meet their data compliance goals.

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

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249