DataGuard

TISAX®

Checklist

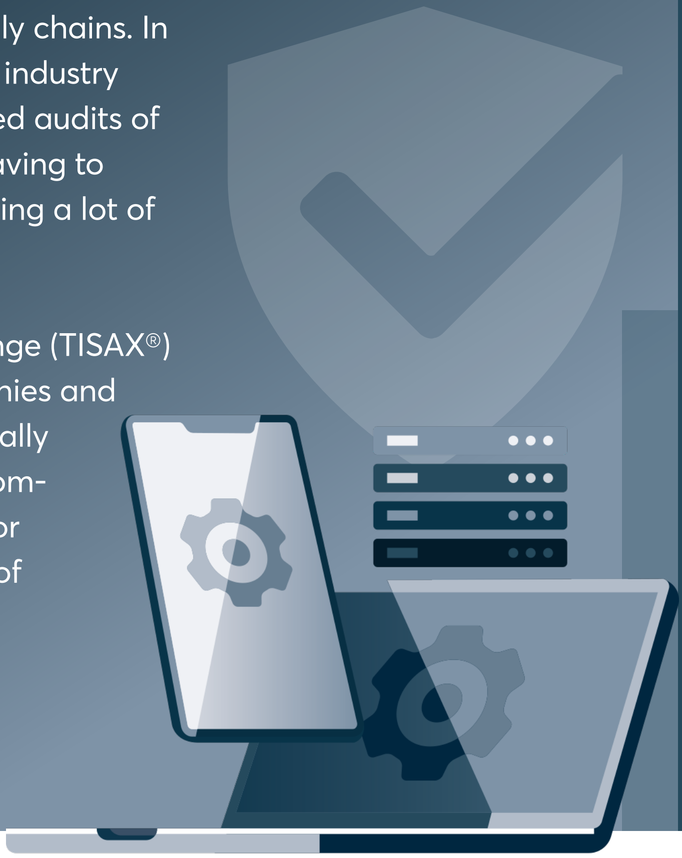
dataguard.co.uk

DATAGUARD TISAX® CHECKLIST

Why TISAX® ?

Automotive OEMs (Original Equipment Manufacturers) and their suppliers form one of the world's most complex supply chains. In the past, the stringent requirements prevalent in this industry meant that many individual manufacturers conducted audits of their suppliers independently. This led to suppliers having to complete multiple audits by multiple customers, costing a lot of effort, time, and money.

The Trusted Information Security Assessment Exchange (TISAX®) was developed to prevent multiple audits for companies and drive efficiency in the industry. By creating one mutually accepted standard, TISAX® can be applied across companies and even other industries, without the need for additional audits. Thanks to TISAX®, a uniform level of information security is now visible and understood.



TISAX® is a registered trademark of the ENX Association.

WHO FROM YOUR ORGANISATION NEEDS TO BE INVOLVED?

While this topic is often pushed to the IT team, TISAX® affects all business processes. For example, external auditors will examine what security measures you have in place when offboarding and onboarding new employees. The tasks involved (handover of keys or key cards, signing contracts and agreements, the creation of new email accounts) will usually be split across multiple departments. As such, all departments that play a role in the landscape of your core processes will be involved in some way: HR, Legal, IT, Office Managers, Leadership and more.

HOW LONG
SHOULD I PREPARE FOR THE ASSESSMENT?

The implementation of a strong Information Security Management System (ISMS) takes six months to complete on average. You can be slightly faster, especially with the help of an expert who specialises in preparing for TISAX ® assessments.

The duration of the assessment by the external auditor depends on the size of your company and the amount of travel required between your locations. Around 2-3 days on site to complete the assessment can be expected for an SMB-size company with around 50 employees.

WHAT HAPPENS
DURING THE ASSESSMENT?

This assessment can only be performed by certification companies accredited for TISAX® by the ENX Association, which runs the TISAX® scheme. The auditor will look under the hood of your ISMS to assess your processes. For example, they will take a close look at your approach to data privacy and how personal and confidential data is processed in your organisation. Auditors will also examine your premises and what protective measures you have in place (for example, in the delivery and dispatch areas, or in the IT rooms).

The process is made up three assessments:

- Initial assessment
- Corrective action plan assessment
- Follow-up assessment

The second and third assessment can often take place several times. This will occur until your organisation has closed all the gaps - all within a maximum period of nine months. If nine months is exceeded, you must complete the initial assessment again.

WHAT RESULT
SHOULD I AM FOR?

- **Conform:** This means you have fulfilled all requirements. This should be your primary aim.
- **Minor non-conform:** This means you have at least one minor non-conformity. With this result, you can get temporary TISAX® labels until the issues are resolved.
- **Major non-conform:** This means you have at least one major non-conformity. With this result, you will not receive any labels until the issues are resolved.

The result is valid for a period of three years, after which your business must repeat the assessment again.

SECTION 1: YOUR ISMS

□ **DEFINE AND DOCUMENT THE SCOPE OF YOUR ISMS**
Scope defines your limits/boundaries for which your ISMS implementation will be applicable. Your scope should cover all your organisation's systems, processes, physical locations, services, products and departments that need to be protected.

□ **CREATE A LIST OF ALL THE INFORMATION YOU ARE PROTECTING**
Examples include information stored in cloud services (Office, G-Suite), or inside tools like Salesforce, Pipedrive, Workday, Cognos and Slack. It also includes prototyping tools like Figma and Miro, or any other cloud-based tool or platform that your team uses. It should also include information on servers, information that resides with subcontractors/suppliers, information received from customers, etc.

□ **DEFINE AND DOCUMENT YOUR INFORMATION SECURITY OBJECTIVES**
This should cover all the ways you intend to ensure confidentiality, integrity, and availability of company information.

□ **DEFINE PRINCIPLES FOR THE SECURE OPERATION OF YOUR SYSTEMS**
Your principles should ensure that your information is protected against unauthorised disclosure, unauthorised or accidental modifications (e.g. deletion or editing the data). All information should be easily accessible for authorised users.

SECTION 2: YOUR TEAM

□ **DEFINE ROLES AND RESPONSIBILITIES**
Nominate the responsible members of your team who will help prepare for the assessment. As noted previously, this should include a cross-section of staff, not just IT.

□ **DEFINE AND IMPLEMENT A METHOD FOR TRAINING YOUR EMPLOYEES**
Regular trainings should take place to ensure that all staff are up-to-date on information security topics and how this affects their daily work.

□ **CREATE A GUIDELINE FOR ACCESS CONTROLS**
You need to define rules and guidelines for how access to your information is given, controlled and monitored.

SECTION 3: RISK ASSESSMENT AND TREATMENT

□ **DEFINE A RISK ASSESSMENT METHODOLOGY**
This should cover both natural and physical risks, legal and contractual risks, compliance risks and financial risks.

□ **CREATE A RISK TREATMENT PLAN AND DOCUMENT THE RESULTS**
Your plan should cover what possible risks can occur and how they will be responded to. For example, what would happen if your servers crash, or if an important cloud service became unavailable.

□ **CREATE A RISK ASSESSMENT REPORT**
This report is a detailed summary of any potential threats to your organisation. For each risk you should determine the probability of occurrence, the resulting impact, and the security controls required to prevent it.

SECTION 4: CUSTOMERS, SUPPLIERS AND PARTNERS

□ **CREATE A GUIDELINE FOR COMPLIANCE WITH SUPPLIERS**
This document is critical to clarify your company's requirements, expectations, and penalties regarding matters relating to business operation (e.g. service standards, deliveries, product conditions). Include clauses for your areas of greatest concern (e.g. how information about confidential prototypes is shared and processed).

□ **DOCUMENT HOW YOU PROTECT THE DATA OF YOUR CUSTOMERS**
Are you processing the personal or sensitive data of your customers? If so, auditors will check that you have the necessary measures in place to protect this data.

□ **ENSURE ALL LEGAL AND CONTRACTUAL REQUIREMENTS ARE RECORDED AND FULFILLED**
Define a clear method for documenting requirements for each business relationship.

SECTION 5: TESTING AND EVALUATION

□ **DEVISE A METHOD FOR MONITORING AND MEASURING YOUR ISMS**
The best way to determine this is to evaluate how detailed your ISMS is and how smoothly it is running. For example, your progress on risk identification, evaluation and treatment, the status of your documentation, regular management reviews and analysis, etc. An auditor will look to see if the ISMS is working in practice.

□ **EVALUATE THE RESULTS OF YOUR MONITORING AND MEASURING PROCESS**
What incidents have occurred, and how many? What incidents have been prevented? Has each staff member been trained effectively? Is each objective you set out at the beginning being met?

□ **DOCUMENT THE CORRECTIVE MEASURES YOU HAVE TAKEN BASED ON YOUR FINDINGS**
This could be anything that you do to avoid or neutralise threats. For example, setting up a new fence or relocating your servers.

□ **COMPLETE A TISAX® SELF-ASSESSMENT**
To be ready for a TISAX® Assessment, you must ensure that your ISMS is stable and effective. To find out whether it matches the expected level, you should conduct a self-assessment based on the ISA.

DataGuard is a Compliance software company focused on Data Privacy and Information Security. As a European leader in the Compliance SaaS category, we enable over thousands of SMB and Corporate customers to automate and operationalise Privacy, InfoSec, and Compliance ("PIC") with ease. Our end-to-end SaaS solution drastically reduces the time and money companies spend to comply with privacy legislation such as GDPR, manage consents and preferences, and obtain infosec certifications such as ISO 27001. This enables our customers to focus on their core business, create value through trust and compliance, whilst mitigating risks and preventing breaches. We have offices globally in Munich, Berlin, London, and Vienna.

Let's talk about your challenges and define first steps on your compliance journey:

Contact us

You might also like:

→ **TISAX® Assessment Implementation Roadmap**

→ **The standard for Information Security**

→ **Information Security for Beginners**