TISAX®

INFORMATION SECURITY IN THE AUTOMOTIVE INDUSTRY

Based on the requirements of the "VDA Information Security Assessment" (VDA ISA), TISAX® is the audit procedure that you as a supplier or service provider in the automotive industry can use to prove the security of information entrusted to you. TISAX® stands for Trusted Information Security Assessment eXchange and is used to audit suppliers and service providers who work with their clients' sensitive information. The number of companies affected by this is larger than may be suspected.

In addition to the classic Tier 1 suppliers, TISAX® is also increasingly being required of suppliers on lower tiers, as well as service providers in e.g. data processing or advertising - in other words, by partner companies of the automotive industry in the broadest sense. If you are now faced with the task of meeting the automotive industry's requirements for information security management systems, then you need to make some decisions in advance of your TISAX® assessment.

Be well prepared when your assessment starts!

Seven essential considerations on the way to your assessment

Access to TISAX® is via a subscriber registration, which takes place online on the TISAX® portal. Registration is the prerequisite for being able to select a TISAX® accredited audit service provider. Registered participants will receive a list of accredited providers from which they can freely choose. An organization may also register several locations and have a group assessment carried out. After an assessment by DQS based on VDA-ISA, information can be provided or obtained in TISAX®.

1. Create a sound basis

Information security requirements and regulations are nothing new or unusual in contracts with your customers, even if you have not explicitly used the term before. You have had to deal with topics such as forwarding documents, dealing with patents and intellectual property, requirements for employees involved or the further use of acquired know-how. You are also familiar with certain exclusions from everyday practice - for example, that you have contractually agreed not to work with your customer's competitors in a particular field.

We would like to note here that most likely, your company has already made commitments to confidentiality and complies with these rules. With information security and TISAX®, you don't have to deal with even more rules. The rules are already there. What has undoubtedly changed - and undoubtedly grown! - is the importance of information and its need for protection. We still exchange information in print, verbally and digitally. In the course of digitalization, a new, critical aspect is speed: Today, we forward information with just a click (often carelessly) in a second, and we transmit information worth protecting via tablet and smartphone at almost any time and from any location. We answer complex technical question virtually in "real time" by sending a design drawing, or by giving project participants and suppliers access to data and information.

Why? Because it's easy to do, focused - and fast. With this in mind, and with some negative experiences that companies now carry in their luggage, it's not surprising when your customers refer to contractual agreements and ask the question, "How do you ensure that ...?" Companies in the automotive industry now refer to the TISAX® process*. This procedure has its origins in the "VDA ISA Standard on Information Security", which a company, regardless of its size, must face in order to be able to operate as a supplier or service provider in this industry. VDA ISA makes it mandatory to check measures for completeness and effectiveness. Carried out within the company, this analysis is an opportunity to become aware of the obligations entered into, and to include one's own information assets in the protection.

2. Get to know TISAX® - and ISO 27001

An information security management system (ISMS) is based on the international management standard ISO /IEC 27001 and is geared to the specific requirements of your organization for the necessary protection of (information) assets, i.e. information of value to your company. The ISMS is thus a system of procedures and rules of an organization, which serve to permanently manage and control information security. One or more protection goals are assigned to the "information of value" - for example, confidentiality, integrity and availability, but also privacy or resilience. These in turn are supported by measures to counteract any threats or risks appropriately and effectively. An ISMS in accordance with ISO 27001 is largely structurally consistent with existing management systems, such as a quality or environmental management system. Against the background of the High Level Structure, the common basic structure for management system standards, an ISMS can therefore be easily integrated. If a process-oriented workflow organization already exists, the requirements for protecting information can be easily identified and implemented on a process-specific basis. For this purpose, the ISMS provides a suitable model for the introduction, implementation, operation, monitoring, review, maintenance and improvement of the protection of information assets in order to achieve corporate goals on the basis of a risk assessment. Risks need to be dealt with against the background of the information assets. The catalog of measures must be designed to effectively address the identified risks.

As always in management systems, the appropriateness of the measures plays a decisive role. This is based on the (by no means only monetary) value of the information in conjunction with a residual risk to be accepted (also referred to as risk acceptance level). An ISMS is applicable to any organization of any size and regardless of industry. This is exactly where TISAX® comes in with its industry-specific framework for the automotive industry. Service providers and suppliers to the automotive industry must prove at three-year intervals that they comply with the high information security requirements of their customers. Until now, manufacturers primarily carried out these audits themselves. The basis for this was a questionnaire on information security (ISA - Information Security Assessment) developed by the German Association of the Automotive Industry (VDA). This refers to essential aspects of ISO 27001 and is extended by a maturity model. The current version of this catalog was and will continue to be the basis for TISAX® assessments in the future.

TISAX®: COMMON AUDITING AND EXCHANGE MECHANISM

The TISAX® process provides for cross-company recognition of information security assessments. This is intended to avoid recurring audits by different manufacturers - a major plus point of TISAX®. This is done on the basis of a common auditing and exchange mechanism. The results always remain under the control of the companies that are being audited. This means that this information is only exchanged after the results have been released in the TISAX® network, but naturally has the advantage of avoiding reassessments. All of the VDA's approximately 600 members honor the results of this assessment.

3. Clear up misconceptions

We often place information security on the same level as IT security. However, a closer look reveals the fallacy. While information security looks at the protection needs of information in a company as a whole, IT security refers to the purely technical security of information-processing systems, such as computers. Information security, on the other hand, is about the holistic view of important and relevant information within a company.

So before you assign responsibilities, clarify the question of what is of value to you and therefore worth protecting. Depending on the company and the industry, this question will have very different answers. For a software manufacturer, for example, this may be the source code of the software, which must not fall into the wrong hands under any circumstances. For other companies, it is information about the design of the product or even the technical specifications (until the release). For other companies, it may be about recipes, production processes or other know-how that is critical to the future viability of the company. In this context, you should also clarify to yourself all aspects involved in an innovation. This will also put you on the right track.

Within a company, it may also be department-specific information, such as a personnel file – which makes it clear once again that information security also has to take into account all relevant legal and regulatory requirements. In order to meet all these requirements, electronic data in particular is of ever-increasing importance and value in times of digitization and digital transformation. Much information (e.g., on new products and thus also on prototypes) is stored and distributed electronically. As a crucial component of the requirements for information security, IT security starts here and demands a state of the art to provide, for example, a secure IT infrastructure (from a firewall to the network to the end devices). This includes topics such as authentication of users via multiple factors (i.e., more than just an identifier and password), the correct use of encryption in storage and communication, or specifications for the use of end devices ("don't bring your own device," prohibited apps and programs) and the segmentation of networks. The technical and organizational requirements necessary for this are defined in the VDA-ISA question catalog, complete with exemplary key figures for measurement and verification.

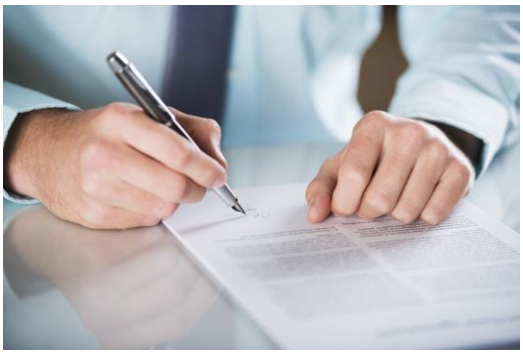
OUR RECOMMENDATION FOR A HOLISTIC VIEW

Anyone who regards information security as a purely IT task is falling short. Information security management is about a holistic view and the need for protection of all important and relevant information in a company, including of course the technical security of information-processing systems. Information security is a task for the entire company, not just the IT department. This encroaches on the comfort zones of everyone involved and must be viewed as a change process.

4 Clarify the role of Top Management – and all other roles, as well

At first glance, information security is a top management task. Hardly any top management will be able or willing to state that these facets of hazard assessment and defense are not original management tasks:

- Information security, including TISAX®, clearly pays off in terms of hazard prevention, i.e., averting, avoiding and mitigating risks.
- When determining suitable measures to ensure compliance with the specified protection goals, you may also have to accept certain risks. Such risk acceptance appears very understandable, for example, if the measure appears too costly in relation to the information value.
- Risks must also be weighed against your company's specific information values and their protection goals.



Then take a second look at the regulations and procedures already in place. These can be found in the documented information of management systems, in the implementation of legal requirements such as data protection (e.g., the handling of personal data), in the consideration of internal company requirements or the fulfillment of customer requirements. In all cases, it is possible, necessary and advisable to build on what already exists. Since these topics are more likely to be in the hands of management system, data protection and compliance officers or those responsible for projects and IT security, we are not looking at top management here.

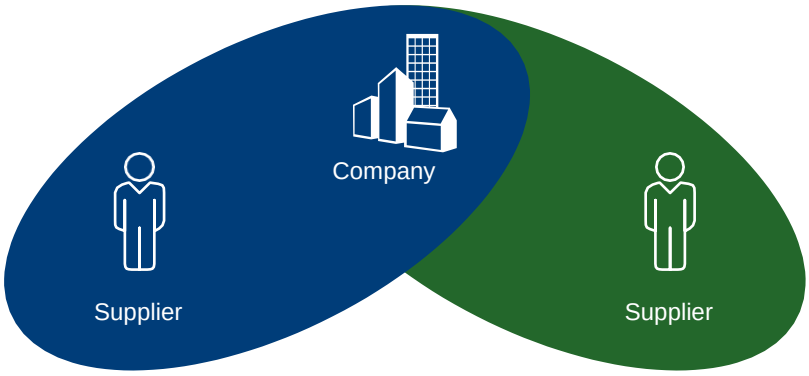
Operational implementation, on the other hand, is the responsibility of everyone in the company. Information security is often perceived as a restriction and experience shows that it encroaches on the comfort zones of everyone involved. The necessary change process require active support and guidance.

OUR RECOMMENDATION FOR IT SECURITY AWARENESS

Top management obviously sets the direction of information security. The design should build on the existing and actual implementation and should involve everyone in the company. In this context, creating an awareness of the compelling necessity of information security is of particular importance. Everyone should be aware of the risks to information assets, but also see the opportunities in the effective implementation of the measures adopted. That is the only way for an organization to be (adequately) prepared for an attack on information assets.

5 Get to know your suppliers

The system is tried and true: your customers expect quality from you and you expect the same from your suppliers. From the perspective of the TISAX® requirements, this also requires the inclusion of your suppliers in the protection of information assets. Here, too, it is worth taking a closer look at the protection goals, because this may enlarge the list of suppliers to be included.



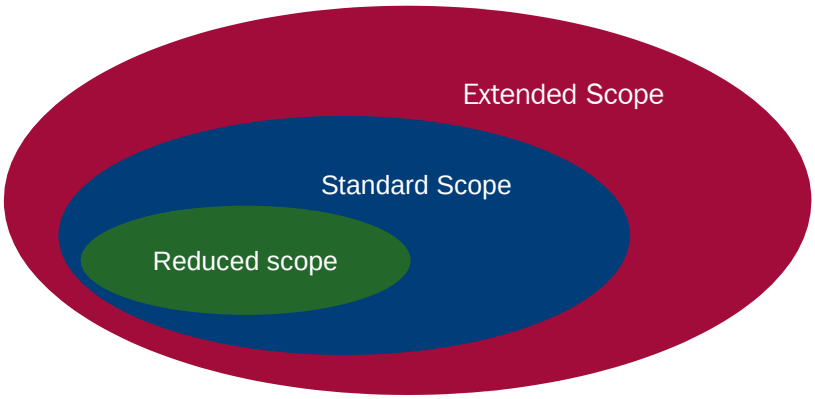
- A supplier who provides consumables or standard components rarely receives information worth protecting.
- Joint development, on the other hand, requires the exchange of information, so that confidentiality will be an absolute must. As a rule, NDAs (non-disclosure agreements) are used here.
- If you use an external data center, you will have to discuss data integrity and availability with them, as well as confidentiality. Framework or service level agreements (SLA) can regulate the scope and availability of services, or the response speed.
- Since access to the external data center must rely on the services of telecommunications providers, their availability will be the primary concern.
- If you have an external cleaning service provider, for example, you may only allow access to certain areas of the company, demand that paper waste be destroyed in a specified manner, or only allow a select group from this company access.

OUR RECOMMENDATION FOR SUPPLIER SECURITY

These examples make it clear that you need to differentiate and include suppliers according to their type of supply, and implement measures accordingly. While you may not need to change anything for supplier A, you may need to revise the contract with supplier B to include information security. You may want to require supplier C to initiate TISAX®, or include a focus on information security in your supplier audits. It is also extremely important to continuously review the classifications you have made, because nothing is as constant as change when it comes to risks and the value of information.

6 Define your TISAX® Audit Scope

Because many organizations are familiar with ISO or IATF certifications, they try to apply the familiar concept of scope to TISAX®. Unfortunately, this does not work and will lead to problems in the audit. When approaching TISAX®, there is no way around familiarizing yourself with the TISAX® participant manual and taking a closer look at the chapter of the TISAX® audit scope.



Scope Types: extended, standard, and reduced scope
Source: TISAX® Participant Handbook Version 2.3 (29 Jan 2021), Abschnitt 4.3.2 TISAX®-Assessment Scope

The major difference of the TISAX® audit scope is that it is predefined and directly formulated to include all areas of the company that come into contact with a customer's confidential information. The idea behind this is simple: All participants on the ENX platform benefit from the greatest possible standardization of the audit. This avoids any room for interpretation and all participants can almost blindly rely on a label with a standard scope. Although ENX still provides for both a reduced and an extended scope, it recommends the use of the standard scope precisely for the reasons mentioned – a recommendation followed by the absolute majority of registered organizations on the ENX platform. In the case of an existing ISO 27001 certification, the degree of coverage with the standard scope of TISAX® should be very high. If in the past attempts were made to limit the scope of ISO certifications as much as possible, the TISAX® audit standard scope will certainly be more comprehensive and more realistically cover your approach to information security.

OUR RECOMMENDATION FOR A PRECISE AUDIT SCOPE

TISAX® allows assessments based on an extended scope, a standard scope and a restricted scope. It is therefore essential to take a closer look at the TISAX® auditing scope chapter in the TISAX® Participant's Guide. Depending on the size of the company as well as the size and relevance of company sites in terms of protection goals, it is advisable to define precise and, if necessary, different TISAX® audit scopes. This has a direct influence on the scope of the entire audit.

7 Be clear about your certification level

The term “level” is often equated with the scope of the audit. However, the two are not the same. Rather, the individual assessment levels define the way in which the audit is carried out on the basis of the TISAX® audit objectives. For example, while the auditing effort between Level 2 and Level 3 is almost identical in the basic audit, Level 3 also includes an on-site audit, which does not exist in Level 2.
The TISAX® audit objectives depend on the defined need for protection to which the information requiring protection is subject. You should derive this need for protection from your customer’s specifications and then implement appropriate measures for the company-specific implementation of TISAX®.

TISAX® Assessments			
Protection level	**Basic**	**Optional**	
	Information security	Prototype protection	Data protection
Assessment Level 1 (normal)	Self-assessment	Self-assessment	Self-assessment
Assessment Level 2 (high)	Document review / remote	On site	Document review / remote
Assessment Level 3 (very high)	On site	On site	On site

Moduls and resulting authorizations in TISAX®– Version 5.0

It is not helpful if customers tell you that you should always check Level 3, i.e. the highest level, to be on the safe side. You should therefore independently include information from existing contracts and from the TISAX® participant manual. This can be used for a realistic classification, as the chapters of the TISAX® audit objectives, protection requirements and assessment levels do provide information on this. For example, information with a "high" (i.e., not "very high") need for protection may only be classified as "confidential" (i.e., not "secret"). In this case, assessment level 2 with "file review / remote" may be completely sufficient

OUR RECOMMENDATION FOR A SUITABLE CERTIFICATION LEVEL

Determine the protection needs of the information assets and the information classification derived from them against the background of your requirements and not with a focus on a potentially simpler audit procedure. In the end, it usually helps to simply talk to your audit service provider as early as possible. Together you can determine the perfect calculation for your audit scope

8 Conclusion

The VDA developed the TISAX® industry standard specifically for suppliers and service providers in the automotive supply chain. One major advantage is that all participants in the TISAX® network mutually recognize the audit results; this avoids time-consuming and costly multiple inspections. The basis for a TISAX® assessment is the VDA-ISA audit catalog, which in turn is based on the requirements of ISO 27001 but extends them to include industry-specific topics such as prototype protection and contract work. Only auditing service providers approved by TISAX®, such as DQS, are allowed to perform these assessments.

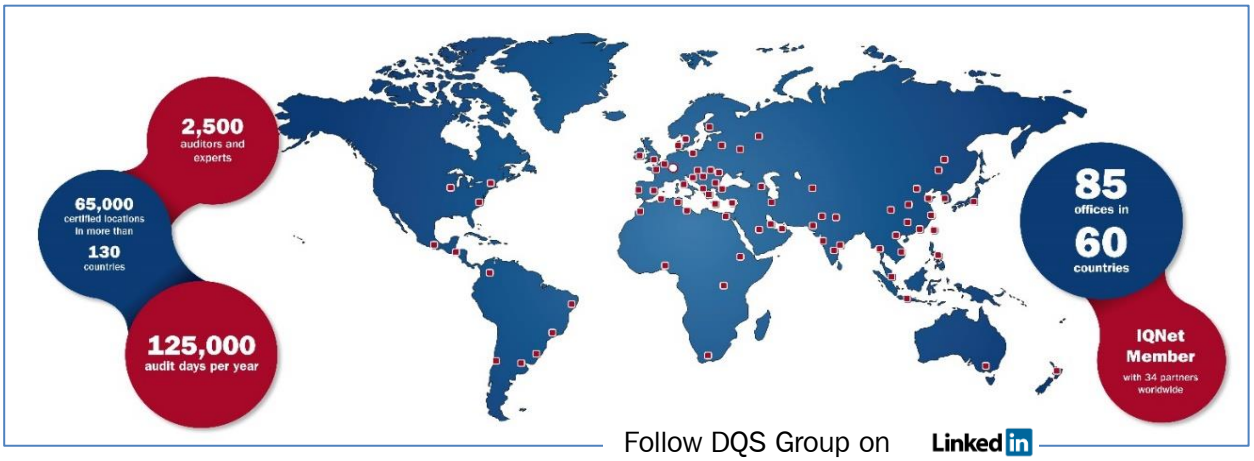
OUR OVERALL RECOMMENDATION

Do not underestimate the effort (both in terms of the required competence and in terms of time and money) in the implementation of the required measures. Based on an analysis of the status, the development of the appropriate measures should be assigned to a broad-based team. In the operational implementation, you will need to call upon the active contribution of everyone in the company. And even then, you may not achieve outstanding results in the first assessment. Continuous improvement, built upon a stable basis that meets the requirements, is a well-known tenet of management principles.

The original German text was authored by the following DQS auditors and experts for Information Security, Automotive, Management and IT: Mr. Andreas Altena, Dr. Holger Grieb, and Ms. Melanie Krauß

Are you ready for TISAX®? Then contact us!

DQS is one of the leading certification bodies for management systems worldwide. With 85 offices in 60 countries, and 2,500 auditors and experts worldwide, DQS is your trusted partner for sustainable success. DQS Holding, based in Frankfurt, provides the strategic leadership for all DQS offices worldwide. We strive for one common goal: to improve our customers' management systems and organizational health by offering value-adding assessment services.



Follow DQS Group on LinkedIn

DQS Holding GmbH
info@dqs-holding.com
www.dqs-holding.com

Certification expertise worldwide
Do you need specific information?
Please contact any DQS local office

wp TISAX_07-2021
published by IBD Corporate Marketing