FAQ – FREQUENTLY ASKED QUESTIONS

TISAX®

Digitalization of the automotive industry is making information security increasingly important. These frequently asked questions are designed to explain how the TISAX® platform provides automotive manufacturers and suppliers around the world ways to improve the transparency and security of information while minimizing the number of compliance audits.

1. What Is TISAX®?

TISAX® stands for Trusted Information Security Assessment Exchange. It is a global platform, established in early 2017, where organizations in the automotive industry – manufacturers, suppliers and service providers – can demonstrate to potential partners throughout the supply chain their compliance with information security standards.

2. What Standard Is the Basis of TISAX® Compliance?

TISAX® is derived from the ISO/IEC 27001 and adapted to the requirements of the automotive industry. Compliance with information security requirements is the principal concern, but additional modules are offered to address topics such as prototype protection, data protection and third-party connections.

3. What Advantages Does TISAX® Offer?

Beyond the obvious benefits of better security and transparency, the primary advantage of TISAX® is that it saves time and money, since participants avoid having to undergo multiple compliance audits. The platform's standardized, uniform assessment process proves organizations' conformity with information security standards, and the quality and objectivity of the TISAX® audits are recognized by automotive manufacturers and suppliers around the world. In fact, OEMs (Original Equipment Manufacturers) increasingly demand a valid TISAX® label as a prerequisite for partner companies. With TISAX®, organizations gain a competitive edge, creating new business opportunities and winning more contracts.

In addition, TISAX® participants decide for themselves which third parties may access their results and can use the platform to select suitable suppliers and service providers.

4. How Does TISAX® Address Differing Information Security Requirements Among Organizations?

TISAX® provides assessments of the implementation by means of a maturity model. It defines the maturity of an organization while assessing five different levels in relation to information security, prototype protection, third party connections and data protection. The model starts with level 0 describing a situation where nothing is in place yet and ends in level 5 where all the mentioned parts runs smoothly.

5. How Often Do Organizations Have to Renew Their Certification?

Organizations using TISAX® only have to provide proof of information security every 3 years.

6. How Do I Know What Kind of TISAX® Assessment Is Required?

The OEMs defining the level which they want to have.

7. How Can I Best Prepare for a TISAX® Assessment?

Our consultants can determine your company's status quo with a pre-assessment (GAP analysis) that imitates an actual TISAX® assessment. The pre-assessment indicates where your organization currently stands regarding information security and provides a foretaste of what awaits you in the official assessment.

During the pre-assessment, our experts typically uncover major and minor findings, which we then use to create a corrective action plan aimed at closing those gaps. Throughout implementation of the plan, our consultants are at your side with advice and assistance.

9. What Does My Organization Need for a Successful TISAX® Assessment?

Prerequisites for TISAX® approval include: a company-wide **Information Security Management** System (ISMS); technical, organizational and structural security measures; employee awareness.

10. What Kind of Support Does DEKRA Offer for TISAX® Assessments?

Since our **TISAX®** consulting services are fully customized; clients decide what kind of support they require and how much.

Our fast track assessment is comprised of three phases: initiation, implementation and coaching assessment. In the initiation phase, we conduct a GAP analysis workshop that provides documentation of the company's initial status. During implementation, we determine the project's scope and contents, including the various project stages. This is followed by coaching for those in leadership positions, the training of an information security officer and the creation of a stable ISMS. The coaching assessment phase supports you through the implementation of ISMS measures, an audit defense and regularly scheduled follow-up audits and certifications.

Our experts are also available for project management support, suitable for companies who require less oversight and assistance preparing for and completing their TISAX® audit. We have the answers to your questions regarding TISAX® requirements and how they apply to your organization.

11. Where Can I Get More Detailed Answers to My TISAX®-Related Questions?

In our introductory workshops we answer questions such as "How can I establish an ISMS according to TISAX® requirements while conserving company resources?" or "What are the steps, in order, of creating a TISAX® approved ISMS?" Other topics include **risk management** and ways to implement and demonstrate security measures. Participants learn practical approaches to TISAX® certification and create work packets that can be used to support implementation in their companies.

12. Does My Organization Need an Information Security Officer?

Our authorized ISO 27001 auditors can help you answer this question. We are also capable of providing an expert to act as an external information security officer for your company. In this case, you benefit from our substantial experience and efficiency.

13. Why Is DEKRA the Right Partner for TISAX® Consulting?

Our consultants are themselves authorized ISMS auditors and can therefore accurately estimate your company's level of preparedness for an official TISAX® assessment. We are skilled and knowledgeable when it comes to ISMS planning and implementation as a result of our many years of experience and an intimate knowledge of the automotive industry.

DEKRA Cyber Security

When people use technology, safety and security are two of the key challenges. In times of the Internet of Things, something can only be safe if it's also secure. Thus cyber security has become indispensable, irrespective of the market and the company size. With our DEKRA 360° CyberSafety Services we offer you a comprehensive portfolio for the protection and security of your data, your network and products as well as your IT infrastructures and processes.

From competent support to detailed risk and vulnerability analysis: As an experienced provider of integrated solutions, we support you in the prevention, detection and management of IT & OT security risks and incidents. Rely on our many years of experience and increase the overall IT security in your company with us - because we are your global partner for a safe and secure world.

Would you like more information?

Contact us

DEKRA