Information security requirements for suppliers and service providers (Status: March 2023)

Table of contents

1 Purpose

Information- and IT-Security is an essential part of business processes and supply chains for us and our customers. OEMs (original equipment manufacturers) work with a wide range of companies throughout the value chain to develop and manufacture products. In the process, confidential information, such as the design of a prototype, is passed on to suppliers/service providers, among other things. Production processes are also highly IT-supported and the OEM relies on the protection of IT-Systems against failures, such as an attack by an extortion Trojan. Consequently, Information and IT-Systems must be adequately protected so that the exchange of data and the availability of IT-Systems along the supply chain is not compromised. Due to this, OEMs require us and our suppliers/service providers to have a functioning Information Security Management System (ISMS) in place, in order to adequately protect their information and to avoid interruption of production processes.

2 Protection requirement level & Obligation to produce proof

The implementation of Information- and IT-Security requirements depends on the information we exchange along the value chain. We have divided this information exchange into the information classification levels harmonized by the German Association of the Automotive Industry (VDA) (public, internal, confidential and strictly confidential). Depending on this, the requirements for protection are determined and, in turn, we derive the certificates to be submitted. The information as to which level of protection the supplier/service provider must fulfill is communicated to the supplier/service provider separately.

12 months after receipt of this information in the form of a request from the Brose Group (e.g. by e-Mail), the suppliers/service providers have the opportunity to submit the relevant certificates at partner-informationsecurity@brose.com. Evidence of TISAX certification must be shared via the ENX portal with the Brose Participant ID P1X21X. After expiration of the deadline, Brose reserves the right to consider the lack of certificates in the supplier evaluation.

Confidentiality level of the information	**Protection requirement level**	**Required certificate* (minimum requirement)**
Public	No protection requirement	N/A
Internal	Normal protection requirement	Filling in the VDA ISA self-assessment with management signature
Confidential	High protection requirement	Options: • TISAX according VDA ISA based on Assessment Level 2 • TPISR • SOC 2 Typ 2 Report (depending on the scope)
Strictly confidential	Very high protection requirements	Options: • TISAX according VDA ISA based on Assessment Level 3 • ISO/IEC 27001 (depending on the scope)
Strictly confidential + Prototypes	Very high protection requirements	TISAX according to VDA ISA based on Assessment Level 3+

*Of course, the requirements for a higher level of protection can also be demonstrated.

3 Definitions

TISAX according to VDA ISA
TISAX stands for Trusted Information Security Assessment Exchange and is a standard for information security defined by the German Association of the Automotive Industry (VDA), whose requirements are anchored in a questionnaire (VDA ISA). The requirements are based on the international industry standard ISO/IEC 27001 and have been adapted to the automotive world. This covers the topics of information security, proto-type and data protection. The ENX Association acts as a governance organization in this system - approving test service providers and monitoring the quality of the tests. The prerequisite for this is registration with ENX. (ref.: TISAX)

TPISR
The Automotive Industry Action Group (AIAG), which primarily includes major U.S. companies in the automotive industry, has published a cybersecurity standard for suppliers. TPISR, which stands for Third-Party Information Security Requirements, defines minimum IT security requirements for companies that receive, store and process proprietary information from automotive companies. TPISR thus fulfills a similar role for U.S. companies as TISAX does in the German auto industry, although the quality is significantly lower due to the lack of independent verification of the information. (ref.: TPISR)

SOC 2 Type 2 Report
The Service Organization Control (SOC) Reports are comprehensive frameworks provided by the American Institute of Certified Public Accountants (AICPA) as a standard for auditing service providers or service organizations according to defined rules. These reports focus on internal controls relating to security, availability, integrity and confidentiality (data protection). The Type II report also tests the effectiveness of the implemented controls over a defined period of time.

ISO/IEC 27001
The international standard ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continuously improving a documented information security management system, taking into account the context of an organization. In addition, the standard includes requirements for assessing and addressing information security risks according to the individual needs of the organization. All types of organizations (e.g., commercial enterprises, government organizations, non-profit organizations) are considered.

4 Contact

If you have any questions, please contact us by e-mail: partner-informationsecurity@brose.com