



Directives



Certification



Security

Certification of management systems for
integrated and defense-in-depth information security

Information Security Management Systems (ISMS)

According to ISO 27001/BSI IT-Grundschutz/B3S (KRITIS)/TISAX®*

More information security in your company with an ISMS

Whether critical infrastructure or not, business and operational data are sensitive business assets and contribute significantly to the operation and efficiency of a company. To ensure the protection of your sensitive business and operational data (trade secrets), risks should be assessed and vulnerabilities identified. Possible measures to reduce risks and increase information security can then be selected, implemented and controlled according to your company requirements.

Norms and standards such as ISO/IEC 27001, Federal Office for Information Security (BSI) IT-Grundschutz, industry-specific security standards (B3S) or TISAX® for the automotive industry, describe general as well as specific requirements which are imposed on an Information Security Management System (ISMS). In addition, the standards contain specific measures for the implementation in your company. Your company's own requirements and basic prerequisites should be taken into account when choosing the standard for implementing the ISMS, since each standard offers specific advantages.

A Management System for Information Security (ISMS) – define the security profile

A management system for information security is a framework in which processes, measures and regulations are created in order to ensure the sustainable protection of business and operational information. The integration into the organizational structure and the allocation of clear responsibilities will significantly improve information security.

Nowadays companies are increasingly resorting to certifications in order to be able to officially prove their professional handling with critical business information. Documented processes and data processing procedures form the basis for an internationally acknowledged certification according to information security standards (e.g. ISO/IEC 27001).

A certification not only demonstrates your professional handling of sensitive business and operational information, but also creates additional trust and transparency towards partners and clients. In more and more industries, standards such as ISO/IEC 27001 (TISAX® for example in the automotive industry) are already a prerequisite for business relationships. These standards are also increasingly becoming a basis for fulfilling legal requirements. These include the General Data Protection Regulation (GDPR) as well as the Directive (EU) 2016/943 or the Law for the Protection of Trade Secrets (Gesetz zum Schutz von Geschäftsgeheimnissen, GeschGehG).

Why Warth & Klein Grant Thornton?

As a BSI approved incident response partner and official certification body pursuant to BSIG, you will benefit from our professional consultation on all information security processes. With our experienced team, consisting of

- ISO/IEC 27001 Lead Auditors with audit competence for § 8a (3) BSIG,
- BSI qualified service providers for Cyber Incident Response/ APT Response according to § 3 BSIG,
- CISSP and ITIL V3 experts,
- Data protection officers (DSB) and
- Penetration testers

we offer you extensive possibilities to implement your ISMS in a needs-oriented and cost-effective manner and guide you through the certification process.



The ISMS certification as a competitive advantage

We support you in the drafting of all necessary documents and descriptions of procedures. Moreover we assist you in the preparation for obtaining the planned **certificate**, the **KRITIS (industry of critical infrastructure) verifications** required by the BSI or the **TISAX® labels** as needed. We guide your company purposefully through the entire certification process and ensure that all necessary measures for a permanent certification are implemented.

As an approved certification body, we are also able to carry out KRITIS audits according to § 8a (3) BSIG for companies managing critical infrastructure.

Our approach in detail:

- We advise you on the selection of the standard that is best suited for your company and on the implementation of the ISMS.
- Using our proven IT risk assessment and project management we support you in the cost-efficient implementation of your ISMS project.
- We carry out a risk treatment and gap analysis for your entire IT infrastructure including critical systems, and determine the prioritization and the degree of implementation with you.
- Based on our long-standing experience we recommend Best Practice Approaches as well as assessment according to the protection required and effort of your critical systems and processes.

- We support you in the creation of all documents and regulations.
- We advise and support you at all levels in the development of a customized security awareness campaign (awareness program) for your employees.
- We accompany you during the final certification process.
- In order to guarantee the continuous improvement of your information security, we advise you continuously in all questions around the standards of information security, ISMS, IT security components and of course the recertification.

Your added value

We pursue a total cost-optimized approach and advise you with the aim of making optimum use of resources so that your project always remains transparent and calculable for you.

Our approach has proved successful in numerous national and international cyber security projects in various industries during our many years of activities. You benefit from an optimized and interface-reduced workflow throughout the entire ISMS certification cycle.

Transparent and proactive communication as well as consistent project management will give you the assurance of receiving professional advice on information security at all times.

Your Contacts



Helmut Brechtken
Partner
T +49 211 9524 8576
E helmut.brechtken@wkgt.com



Martin Bodenstein
Senior Manager
T +49 89 36849 4226
E martin.bodenstein@wkgt.com

International Competence

Even if you have international questions, you do not have to do without our high quality standards. For cross-border tasks, we work together with the powerful Grant Thornton International network. Over 56,000 employees in around 140 countries guarantee you world-class services at a consistently high level – for each of your challenges and with the right local experts.

* TISAX® is a registered trademark of the European Network Exchange (ENX) Association. Warth & Klein Grant Thornton AG and the European Network Exchange (ENX) Association have no specific business relationship with each other and have no legal relationship.

© 2020 Warth & Klein Grant Thornton AG All rights reserved.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or missions. As of 7/2020.

