Warth & Klein Grant Thornton

Directives

Certification

Security

Certification of management systems for information security in the KRITIS environment

Information Security Management Systems

According to ISO 27001 and B3S pursuant to BSIG

More information security in your company with an ISMS

For companies managing critical infrastructure (KRITIS), sensitive corporate assets such as business and operating information are not only crucial for profitability but also essential for the operation of critical business processes. To ensure the protection of your critical business and operational information (trade secrets), risks should be assessed and vulnerabilities identified. The possible measures to reduce risks and increase information security can then be selected, implemented and controlled specifically in line with your company requirements.

According to § 8a BSIG, critical IT systems, components and processes must be protected against disruptions to availability, integrity, authenticity and confidentiality by appropriate state-of-the-art precautions. Industry-specific security standards (B3S) and standards such as ISO/IEC 27001 are used to implement this requirement. These frameworks describe general and specific requirements for an Information Security Management System (ISMS). They also contain concrete measures for implementation in your company. Your company's specific requirements and prerequisites should be taken into account when implementing the ISMS.

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. KRITIS companies are increasingly resorting to a certification of ISMS in order to be able to officially prove their professional handling with critical business information to business partners and public authorities. 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 for instance the General Data Protection Regulation (GDPR) 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 and long term experience 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 or BSI-KRITIS audit process.

The ISMS as basis for every KRITIS infrastructure

We support you in the drafting of all necessary documents and descriptions of procedures. Moreover we assist you in the preparation for obtaining the **KRITIS verifications** required by the BSI or the planned **certificate.** We guide your company purposefully through the entire audit/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 a KRITIS audit according to § 8a (3) BSIG in your company and to create all necessary KRITIS verifications.

Our approach in detail:

- We advise you on the selection / analysis of B3S and on the implementation of the according 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 needed 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 external audit.
- 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 and IT security components.

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.

Warth & Klein Grant Thornton

wkgt.com