Information Security Management System (ISMS)

What is an ISMS, and why should you have one?

An information security management system is an integrated collection of methods, rules, and regulations within a company for continuous control and improvement of information security.

The primary goal of an ISMS is to identify risks related to the information it processes and manage those risks in a targeted manner.

Establishing an ISMS has numerous benefits:

- Compliance with regulatory and contractual requirements
- Proof of information security for third parties
- Identification, evaluation, and handling of existing risks
- Improved cost-effectiveness through planning of risk-based measures

Focus on information

The key focus of an ISMS is the information, plus all the resources required for it, that is essential to the company and the achievement of its goals. In many cases that means IT, since IT is generally the primary support process. However, other areas such as documented information, personnel, and building security also need to be taken into account.

Based on your company's goals and value creation, your company's essential information and values are identified and evaluated with respect to your confidentiality, availability, and integrity requirements.

Risk-based approach and recognized standards

Existing risks are identified, evaluated, and handled in the context of their relation to the selected values. Risk management creates a valid and, above all, transparent and reproducible foundation for drawing up and implementing suitable measures. In addition, you have the option of targeted risk acceptance, risk avoidance, or risk transfer.

As part of our risk management process, the actions to be taken are generally derived from recognized standards. In particular, they are based on the ISO/IEC 27002:2013 standards, the IT-Grundschutz standards for basic protection established by Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI), or common industry standards. These standards supplement risk management processes and serve as a solid foundation for achieving your desired level of information security.

The key to success

An integrated approach is the key to success for an ISMS since it focuses on protecting essential information across every link in the value chain. To achieve the desired level of security, an ISMS interacts heavily with existing organizations and their processes. In addition to IT, an ISMS mainly addresses issues such as the following:

- Corporate organization
- Personnel security
- Physical security

- Access control
- Incident management
- Business continuity planning

Continuous improvement process

Setting up and running an ISMS is not just a one-time process. Instead, it is a process that is continuously repeated. It involves performing all regular activities such as risk management, internal audits, and management reviews. Moreover, the ISMS processes, rules, and results undergo continual critical evaluation and, if need be, are adapted to produce needed improvement.

Appropriate and cost-effective

Thanks to the structured coordination in an ISMS, complex and generally expensive measures in particular are not implemented in an isolated manner. Instead, they are carried out in an appropriate context of existing risks and economic feasibility. This creates synergies and helps to sustainably lower the costs of planning, execution, and ongoing operation.

In practice, it has been shown that centralized solutions can generally be operated with fewer resources, greater security, and higher reliability than competing and, in many cases, overlapping custom solutions.

Integrated management systems operation

An ISMS does not have to be developed and implemented as an isolated system. Instead, it can be integrated or based on existing management systems (e.g. QMS, BCMS). This approach leverages synergies, avoids redundancies, and sustainably increases acceptance among your employees.

Proof of certification

An ISMS that conforms to national or international standards (e.g. ISO/IEC 27001:2013 and the IT-Grundschutz standards) can be certified by an accredited organization.

A certificate enables you to provide third parties such as government authorities, auditors, customers, and partners with proof of information security.

TÜV Rheinland Services

- Gap analyses to determine current situation
- Analysis of existing ISMS
- Planning and implementation of ISMS
- Continuous operation of ISMS (external CISO)
- Performance of risk assessments
- Design and conducting of awareness campaigns
- Coaching of information security managers

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne, Germany
Phone +49 221 806-0
Fax +49 221 806-2295
service@i-sec.tuv.com