INFORMATION SECURITY MANAGEMENT - ISMS

INFORMATIONSECURITYHASBECOMEAKEYTASKINEVERYORGANIZATION DUE TO THE CONTINUAL GROWTH IN THE STRATEGIC SIGNIFICANCE OF INFORMATION SYSTEMS.

ISMS - (Information Security Management System) represents an essential approach to establishing an environment in the organization that can provide sufficient protection of information from threats. ISMS deployment includes the design and implementation of processes leading to information security management, implementation of necessary measures, checks of their effectiveness, and continual maintenance and improvement.

[WHY ISMS SHOULD BE INTRODUCED]

ISMS deployment is advisable in situations where it is necessary to protect the data of customers and citizens, improve information security in a company, or ensure operational continuity in the event of a security incident. Another reason for ISMS deployment could be a decision to spend money more efficiently and direct investment into areas with significant risks. Last but not least, information security management is an obligatory activity for organizations that must comply with legal or regulatory requirements.

Subsequent certification of the Information Security Management System can demonstrate the trustworthiness of a company to customers, help achieve a competitive advantage, and fulfil conditions for participation in tenders.

[APPROACH AND EXPERIENCE]

We can design not only processes for all the above-mentioned stages, but also risk analysis, draft security policies and other security documentation, assessments, and the design and implementation of security measures. Our offer includes security audits and emergency planning. We approach each customer individually and apply best practices to ISMS deployment.

FEATURES AND BENEFITS

- Establishment of an environment providing information security and privacy protection
- Reduction of risks related to unavailability, leaks or loss of information
- Optimization of costs for information security assurance appropriate to asset value
- Avoiding costs of security incidents consequences
- Increase in employee awareness and responsibility
- Demonstration of an effort in the area of information protection to customers, partners, the authorities and the public
- Competitive advantage
- Enhanced company image

Our consultants are qualified experts with internationally recognized certificates (CISM - Certified Information Security Manager), and they are authorized to handle information from Confidential to Top Secret levels. They have long-term experience with projects implemented for various private and government customers.

[STANDARDS USED]

We apply the following standards when preparing an ISMS design:

- ČSN ISO / IEC 27001, which specifies requirements for the correct design, deployment, monitoring, maintenance and improvement of an Information Security Management System within a company.
- ČSN ISO / IEC 27002, which provides a detailed summary of specific security measures, the implementation of which a company must take into account when building an ISMS (Act No 181/2014 on cyber security and the linked standardization Directive No 316/2014 on cyber security).

[PDCA MODEL]

We provide professional consultancy services for the complete sequence of steps required by information security management. We follow the above-specified ISO 27001 standard for ISMS implementation according to ČSN ISO IEC 27001.

„Plan" stage

Planning is the foundation of an ISMS building process. This stage includes determining the scope of the security management system, the definition of the security policy, the proposed risk management, including risk assessment, and a selection of measures aimed at risk reduction.

„Work" stage

The „Work" stage includes the deployment and use of security measures, processes and procedures including monitoring of their efficiency. It also includes the establishment of a continuity plan and response procedures to security incidents.

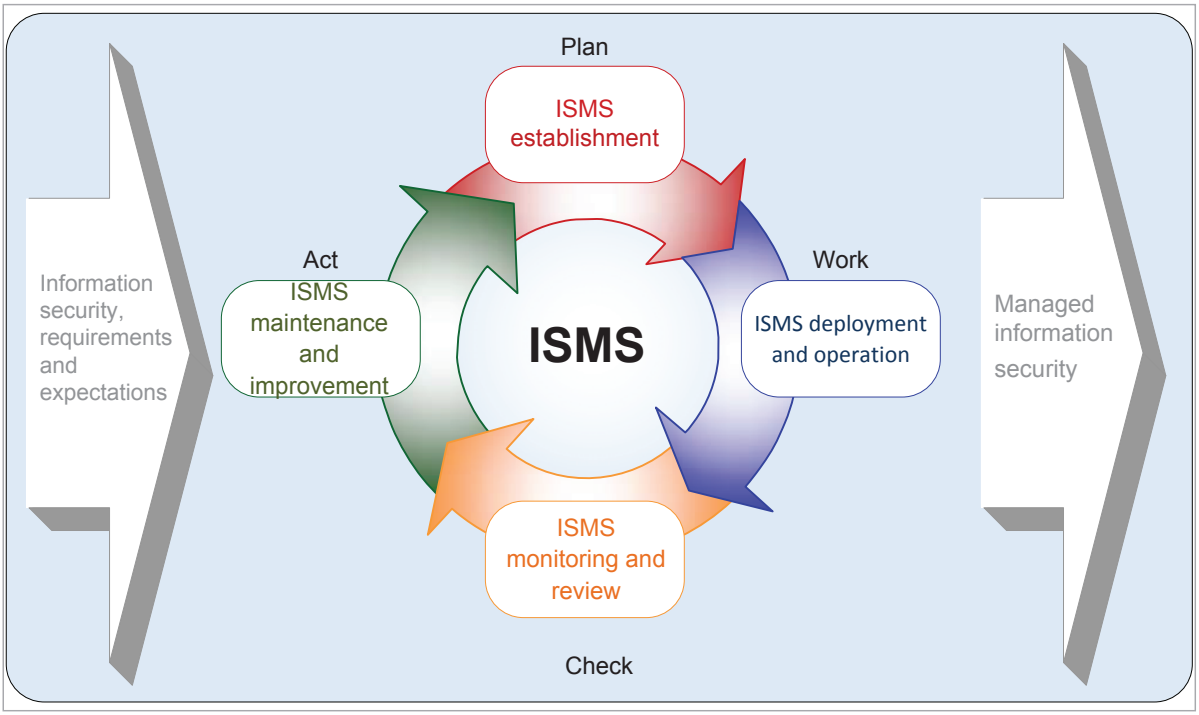
„Check" stage

The functionality and effectiveness of the processes and measures are assessed in this stage. Internal audits are performed, risks are reconsidered, and the Information Security Management System is reviewed.

„Act" stage

Corrective and preventive measures are adopted according to the results of the previous stage.

■ PDCA model chart



COMMERCIAL CONTACT

ICZ a.s. Na hrebenech II 1718/10
140 00 Prague 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz