



Information Security Management System

S&T offers its customers a broad portfolio of consulting services designed for risk management within the field of information security.

The methodical establishment and maintenance of a secure corporate environment for information, transactions and the agreed availability of core processes is achieved by implementing an Information Security Management System (ISMS), which can be divided into the following phases:

- Organization of security with defined responsibilities
- Documentation and processes for:
 - Risk analysis for encountered / unencountered risks
 - Policies, standards and operational instructions
 - Realization by means of awareness training, process redesign and technology
 - Audits and reviews
 - Supplementary plans for business continuity and disaster recovery

The organizational environment

It is strongly recommended that the highest level of management commissions the document and assumes responsibility for the realization, since the comprehensive protection of information is classified as strategically important.

The management nominates the 'Chief Information Security Officer', who ensures the establishment and maintenance of the specified secure environment and who coordinates all the measures required for realizing the security policy.

The Security Policy

A central element in this procedural model is the formulation of a company-wide Security Policy, as this describes all strategic specifications and standards relevant to security. This policy is then used to clearly define responsibilities, staff behavior, processes and supporting technologies across a whole organization - the effectiveness can then be assessed via structured audits.

The Security Policy is thus the highest level of regulation, and is defined more precisely by means of standards and enhanced with definite operational instructions.

Organization of a Security Policy

A security policy is structured as follows:

- Organizational environment
- Data classification
- Policies for user groups and components
- Accompanying processes
- Further development and elucidation of the Security Policy

Classifications

A core aspect of the Security Policy is a multi-dimensional classification of data from which categorized protection requirements and measures can be derived and implemented.

The most common classification categories are data confidentiality, data restoration, system availability and the management of the stipulated retention periods for documents.

This classification and the linkage of classes to adequate protection measures with regard to processes, training and technologies, creates a secure environment for data, transactions and the availability of core business processes.

Processes

With 'Identity Management', the process required for the assignment, amendment, suspension and auditing of access rights per user group is described. With regards to the data restoration, it must be ensured that no extension of access rights takes place when backing up data.

Another important process is 'Incident Management', in which the lines of communication and the levels of escalation for system interruptions are defined – including fault notifications issued by users, partial system outages and even natural events.

Business Continuity and Disaster Recovery Plans

The fields of Business Continuity and Disaster Recovery Analysis involve the establishment of powerful emergency and crisis management solutions, which can maintain or rapidly re-establish important business processes in the case of long-lasting damage events.

The first step carried out by S&T consultants is to determine, together with the client, the business processes running in the business, and then analyze and assess these with regard to the core business of the company.

The next step involves identifying all the types of resources required for operating the core business



processes. In this context, their value within these processes is identified, along with possible dangers and weaknesses and the consequences of an unforeseen incident for the business.

The results of an analysis of the business consequences provide valuable information and, at the same time, create the basis for a Business Continuity Plan and a plan for prioritized rectification of the effects of business disasters.

The risk-based approach used by S&T for information security is compliant with commonly used information security standards and procedures.

Information Security Awareness & Education

People are the most critical part of an organization's security. More than 60% of security breaches are caused by people. Raising security awareness and providing security training significantly lower the number of information security incidents that occur.

Our training portfolio covers users as well as experts, in two phases:

Firstly, the S&T Information Security Consulting Team develops a corporate information security awareness program and performs the complete rollout. Web-based learning programs support the efficient and interactive distribution of content.

Secondly, focused workshops about security related subjects are held for the experts in the company's Information Security Team in order to keep them updated with leading strategies and associated methodologies.

Vulnerability & Penetration Testing

A penetration test actively evaluates the security measures that protect information assets. The most common procedure is to actively analyze the security measures related to design weaknesses, technical flaws and vulnerabilities.

[Read more: Penetrationtest](#)

Information System Auditing

Audits of Information Security Systems form an essential part of regular financial auditing. Financial and government organizations in many countries are required by national bodies to perform information systems audits and report the results to authorities.

S&T's experienced Certified Information Systems Auditors (CISA) and ISMS Auditors (ISO 27001) develop complete audit strategies and audit methodologies for their clients in order to assure compliance with the defined policies and standards.