



ISO 27001: Information Security Management System

Contents

Introduction	3
<hr/>	
Scope	4
<hr/>	
Policies & Declarations	5
<hr/>	
Asset management	7
<hr/>	
System approach	8
<hr/>	
Physical Security	9
<hr/>	
Operations Security	11
<hr/>	
Communications Security	13
<hr/>	
Incident management	14
<hr/>	
Business continuity	14
<hr/>	
Compliance	15

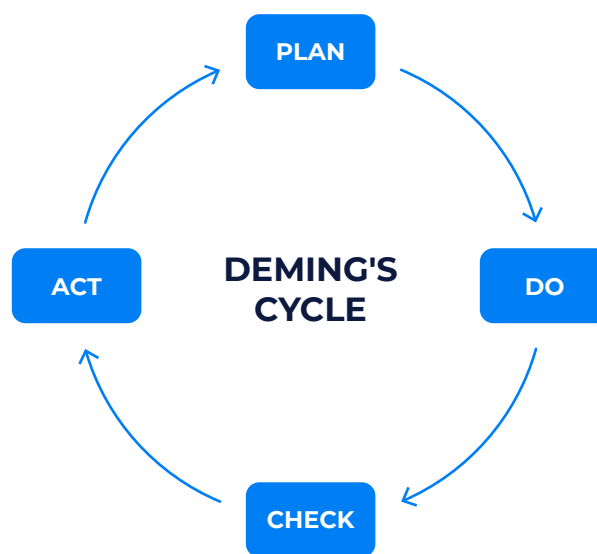
Introduction

SaM Solutions is an international software development services provider with more than 25 years of experience in the information technology market. The company's main areas of activity are custom software development in the U.S. and European markets, as well as consulting services in the development processes. Information security and confidentiality issues are one of the main priorities of the company, justifying the high level of trust of our customers, who include world leaders in various industries. To confirm compliance with the legal requirements of the European Union and customer requirements in the field of information security, the company's management has decided to implement **an Information Security Management System that meets the ISO 27001 standard**. SaM Solutions has successfully achieved the system certification from a prestigious international certification body.

The purpose of this overview is to make all interested parties aware of the general aspects of information security and personal data protection by SaM Solutions. All of these requirements and measures have been documented as the company's standards, policies, and guidelines, and have been communicated to all employees. For safety reasons, this document does not describe the specific procedures, activities, and methods to be performed.

Scope

SaM Solutions' **Information Security Management System** is built on the model of **Deming's Plan–Do–Check–Act Cycle**, which fully meets the requirements of ISO standards and allows for the development and effective operation of the system.



The scope of the system includes worldwide development centers and the headquarters in Germany, which makes it possible to meet the high requirements of information protection at all stages of software development:

- ***EN: Design, Development and Maintenance of Software. Project Management and Implementation***

The scope of the certification includes all the company's processes at all stages of operations, in particular, the project management process, including contract and delivery management.

Policies & Declarations

To define the strategic aspects of activities and the attitude towards security issues, relevant information security policies have been developed and public declarations have been made. All documents are publicly available on SaM Solutions' official website.

The Information Security Management System policy states the following:

The main goal that all the provisions of this Policy are intended to achieve is to protect information assets and data, including personal data of individuals from any damage caused by accidental or intentional interference with the company's information system or in the event of information security incidents.

In carrying out its activities in the field of certification "***Design, Development and Maintenance of Software Solutions. Project Management and Implementation***", SaM Solutions assumes the following obligations:

- To comply with national legislation and applicable international law, standards, and regulations in the field of information security.
- To prevent unauthorized or improper use of information resources and information systems.
- To use certified anti-virus software and avoid malware infections, and investigate all information security incidents.
- To use only licensed software in the company's information systems.
- To classify information, identify and evaluate assets, detect threats and vulnerabilities, manage risks, and classify informatization objects to ensure information system security and fault tolerance.

- To take effective measures to ensure the integrity, availability, confidentiality of information and data, up-to-dateness of hardware and software to maintain the necessary level of the information system security.
- To ensure uninterrupted operation of the information system, its fault tolerance, and rapid recovery in case of information security incidents.
- To ensure continuous improvement of the information security management system and compliance with certification requirements.
- To keep up-to-date and communicate the information security management system policy to counterparties, third parties, and employees.

To achieve the above obligations and ensure the effective functioning of the information security management system, SaM Solutions' management guarantees the provision of all necessary resources.

In addition to the Information **Security Management System policy**, SaM Solutions has adopted a number of other policies and made declarations in the field of information and personal data protection:

- 1. Policy on the Protection of Individuals** with regard to the Processing of Personal Data — describes the goals that SaM Solutions has set for the protection of personal data of individuals, as well as how these goals are achieved.
- 2. Declaration on the Processing of Personal Data** — describes the purposes, nature, and methods of collecting and processing of personal data of individuals by the company.
- 3. Third-Party Information Security Policy** — describes the relationships and requirements that SaM Solutions imposes on suppliers and subcontractors.

Detailed policies can be found on the SaM Solutions' website. The issued documents allow for a transparent delineation of the boundaries of interaction and the company's responsible approach to security issues.

Asset management

Asset management is one of the most important aspects of a systematic approach to security management. SaM Solutions regularly conducts inventory, accounting, and evaluation of assets. General management decisions to revise asset categories are made at least once a year. Assets are managed taking into account all requirements of the ISO series of standards. Employees who handle sensitive information are personally responsible, among other things, for ensuring its security. The categorization systems developed, and the methodologies used are not only based on the value of the assets but also take into account the security aspects of the assets regarding their hierarchical level.



BUSINESS LEVEL

- Relation between assets and their owners
- Impact on the business aspects of the company



APPLICATION LEVEL

- Dependence of assets on their purpose and use
- Grouping of assets by applicability and access categories



PHYSICAL LEVEL

- Relation between assets and their location
- Consideration of asset localization aspects

System approach

SaM Solutions system management decision-making process in the field of information security is based on a **risk-oriented approach**. The company uses modern methods and models of risk management at all stages, carrying out each of them in a planned manner:



- Risk identification and evaluation of the probability of its realization and the scale of the consequences, the determination of the maximum possible damage.
- Selection of methods and tools to manage the identified risk.
- Development of a risk strategy to reduce the probability of risk realization and minimize the possible negative consequences.
- Implementation of the risk strategy.
- Evaluation of the results achieved and adjustment of the risk strategy.

The Information Security Management System is regularly reviewed by management. Internal audits help to clarify compliance with established requirements, as well as to verify accepted evaluation criteria in systemic aspects. The company's top management is also involved in external audits, which ensures the involvement of management in all aspects of system management. Experience drawn from internal and external audits forms the basis of the continuous improvement model and forms the information security goals for the next reporting period.

Physical Security

The physical security required by ISO 27001 is ensured, taking into account current technical requirements. However, for individual projects and clients, SaM Solutions arranges additional protection measures based on contractual terms, which may include requirements for protection perimeters beyond those implemented and used routinely. The company's teams are experienced in executing projects with highly sensitive information in high-risk, high-protection environments.

The following documented physical security safeguards are implemented and used according to the requirements of ISO 27001:

Entry and Access Control

The company provides a high level of access control and records the admission of persons to its area and premises. For this purpose, a process of physical authentication and identification is ensured, and the admission levels are broken down into categories.

All perimeters of the enterprise are equipped with video surveillance system with the use of video archive and direct observation of camera information in real time.

Access to the perimeters is exercised using electronic cards, which ensure an authentication process with the delimitation of access rights.

All offices are locked with physical keys and keys are issued on a centralized basis with logging.

Office doors are equipped with automatic closing devices, taking into account fire safety requirements.

Officials handling confidential information keep it in locked cabinets and/or safes. Information handling policies were introduced, taking into account the use of shared devices (network printers, scanners, fax machines, etc.).

Removal Control

The control of removable media is governed by the relevant company's standards and includes:

- keeping records of bringing in/removing out equipment and other devices when entering or exiting buildings;
- storage of confidential information carriers separately and, if possible, with marking them in a special way;
- limiting the use of pluggable devices where appropriate.

Secure Areas

Secure areas are rooms with a special access mode, delimited by separate categories of admission. Secure areas include server rooms, rooms serving the building power supply, and other rooms classified based on risk analysis. The physical security of secure areas is ensured by appropriate measures:

- Secure areas are equipped with internal video surveillance systems.
- Access to secure areas is only possible with a key and an electronic access card with a properly programmed access category.
- The keys are issued to strictly identified employees of the company, who have the appropriate admission category.

Operations Security

The Information Security Management System documentation includes established **operations security** processes that ensure the following requirements are fully implemented:

- Only licensed software is used, all updates, patches, and new versions are installed on time.
- Antivirus software is used to detect and fight against malware and malicious code.
- Backup tools and systems are used to restore information in the event of a breach of its security properties.
- Events and actions are logged and accounted for using an automated system to monitor if the hardware and software are accessible and if there are any failures in their functioning.
- Periodic monitoring of logs and events is carried out manually on hardware selected based on the risk analysis and for specific software.
- Software is installed by authorized staff only on a centralized basis.
- A safety check is conducted on devices before putting them into the operating environment after purchasing, repairing, or otherwise being out of the company.

Access Controls

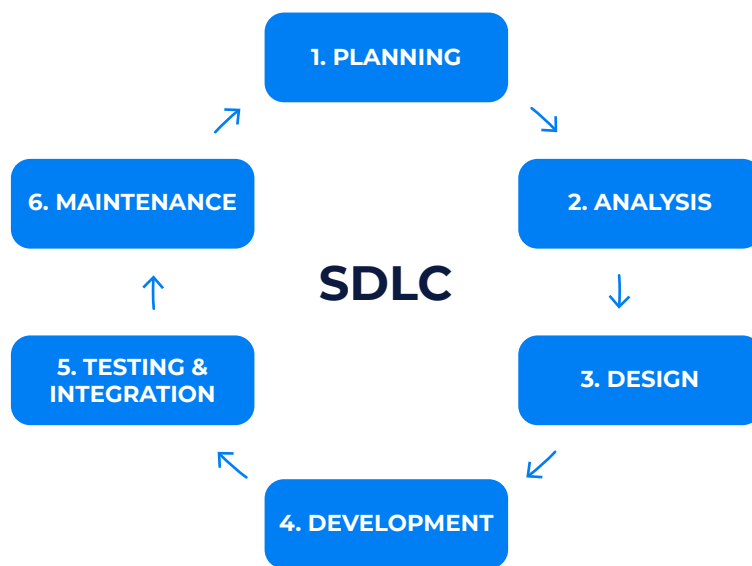
As part of the activities to ensure the operations security, special access control measures are applied to ensure that the level of security complies with ISO 27001. The main requirements to be fulfilled include:

- user rights and roles are differentiated both at the intranet level and in the various applications and systems used by the company, such as Jira, Confluence, Azure, and others;
- user actions for individual systems are logged and monitored;
- there are Active Directory security settings that ensure the necessary local device settings, such as locking accounts when an incorrect password is entered multiple times, locking the system when the user activity timeout expires, and others;

- centralized accounting records are maintained and blocked in case of dismissal of an employee and/or reassignment of rights in case of transfer of an employee to another division or another project.

A clean desktop policy has been introduced and applied.

System acquisition, development and maintenance



The Software Development Life Cycle is built and documented, which makes it possible to clearly define roles and responsibilities at all stages, ensuring the security of both the project environment and the information being processed.

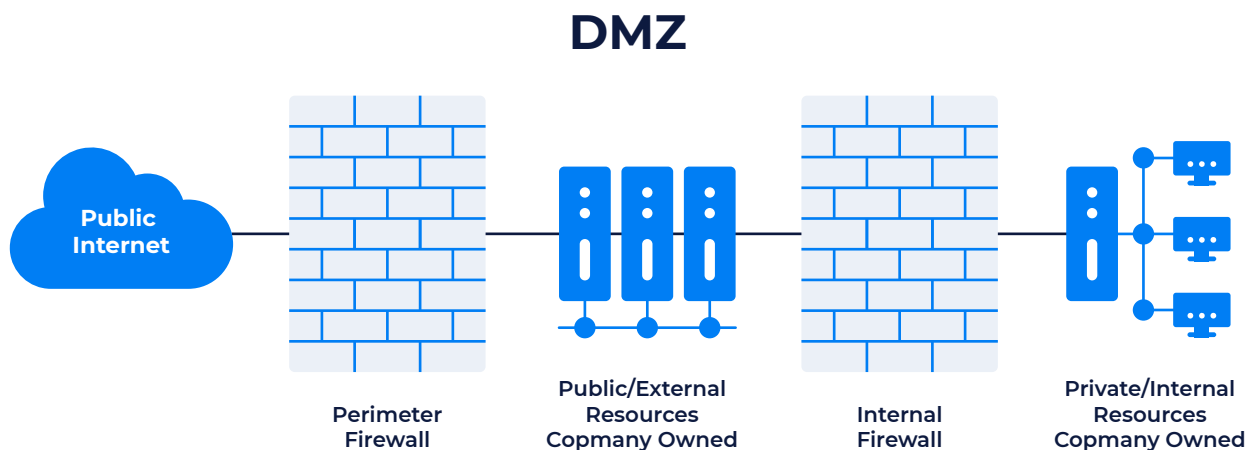
All significant changes to the project environment and production are made by staff authorized to do so; accordingly, changes to the environment as well as to the software packages are additionally controlled.

Development security is tested, as well as the level of compliance with security standards, and a set of security patterns and tools are determined by the customer.

Communications Security

As part of **communications security**, a diagram of networks and communications is developed and kept up to date. The segregation of systems and networks is applied, including the installation of firewalls between segments.

A **demilitarized zone (DMZ)** was created, to which projects and project segments with direct access to the Internet are moved. The DMZ is segmented and separated from other networks by firewalls, the production environment segments are separated from development and testing, which are also separated if possible.



Restrictions have been imposed on the use of communications between employees and for interaction with customers, which makes it possible to control the handling of confidential information. Within the company, certain messengers are used for communication, which are centrally managed by authorized staff.

The range of communications and properties are defined by a special code, which covers the foundations of corporate policy, communication style, and the nature and amount of information in negotiations or work activities

Incident management

SaM Solutions has documented **incident management** procedures, taking into account the classification of information security events. Measures and ways to respond to information security events have been developed, ranging from monitoring to investigations and emergency response measures. All information about information security incidents is stored and used to improve the information security management system in general and risk management in particular.

As a preventive response to information security events, regular scans of network and system vulnerabilities, as well as pen tests, are conducted.

Business continuity

A high level of responsibility to customers is one of the priorities of SaM Solutions' business. The company has developed a strategy of resilience to various crisis situations, according to which the entire infrastructure of the company can be fully restored within 24 hours of its complete destruction, for example, in the event of natural disasters or military operations.

To ensure fault tolerance and **business continuity**, modern technologies of virtualization, data backup, and other best practices in the field of information protection are used. Backups and fault tolerance of systems and networks are tested periodically.

Compliance

Ensuring compliance with high information security requirements is achieved through regular analysis and a systematic approach to security, response measures, development of corrective and preventive actions and goals, and management review. Compliance verification is carried out as part of an internal audit.

Every year, SaM Solutions undergoes external audits by an international certification body to confirm compliance with ISO 27001. In this way, the company ensures that there is third-party oversight of all declared security aspects and assumed compliance obligations.

Issued certificates with the current scope of certification are publicly available on the company's website [sam-solutions.com](https://www.sam-solutions.com).



SaM Solutions

Tel.: +49-8105-77890

www.sam-solutions.com

Data Protection Officer:

Alexandr Zorin

Chief Information Security Officer

E-mail: dpo@sam-solutions.com