thinkproject!

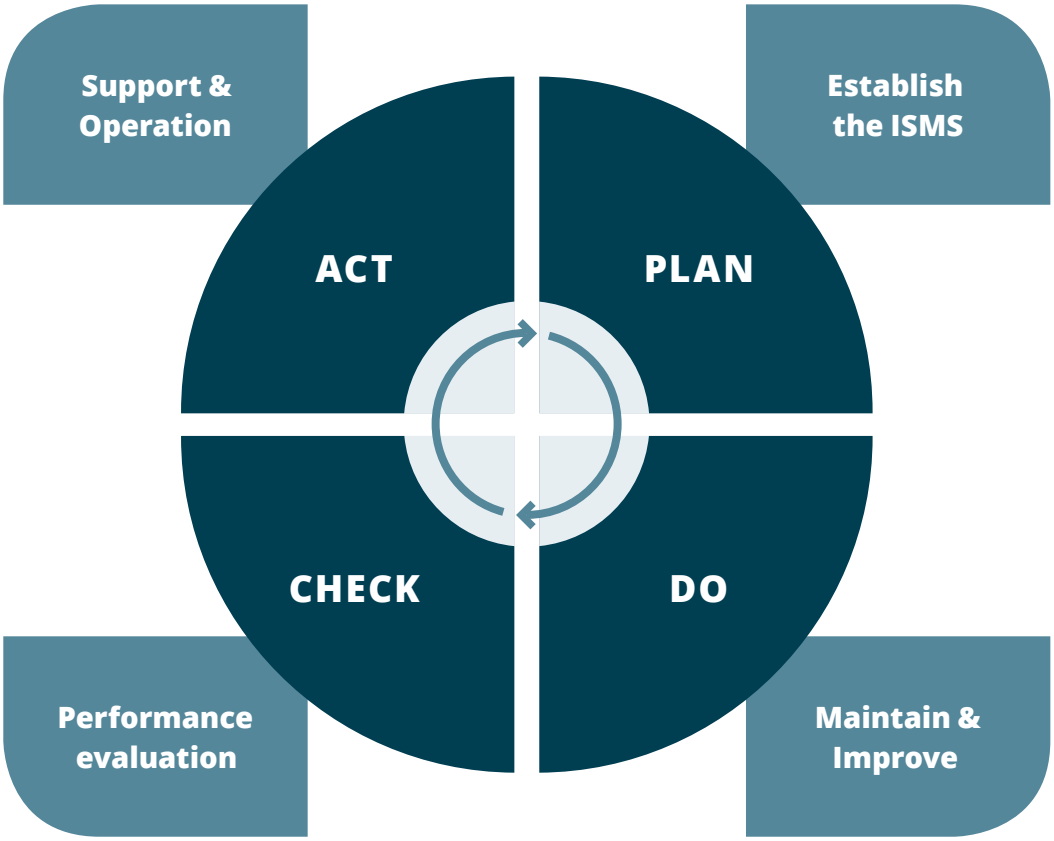
INFORMATION SECURITY POLICY

think project! Information Security Management System (ISMS)

Version 2.7 // 01.12.2016

thinkproject!

INFORMATION SECURITY PROCESS (PDCA)



This document is only valid in its online form. Versions that have been printed out or otherwise saved are not subject to the change service.

Classification: Restricted

thinkproject!

TABLE OF CONTENTS

1 OVERVIEW AND BINDING DECLARATION

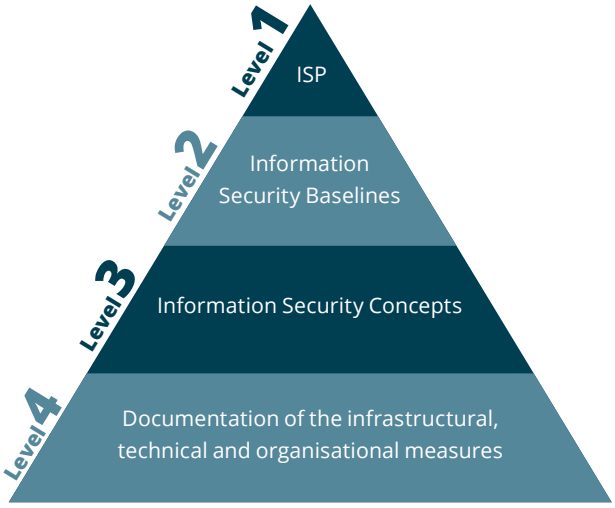
1.1 THE IMPORTANCE OF INFORMATION SECURITY

Information security is of the utmost importance to the think project! companies as well as to its customers. This is founded upon a high dependence on efficient and available information processing, and through the demands that result in connection with corporate governance, risk management and data protection laws. Information security is therefore an integral component of the think project! company strategy.

The think project! companies, its employees and external service providers are all highly obligated to take control of risks toward information processing and to reduce them to an acceptable level. These risks include, for example, data leakage, data manipulation, technical disruptions or sabotage. In order to fulfil this obligation, an Information Security Management System (ISMS) has been implemented that will be regulated across the companies and coordinated centrally. As the superior policy, the existing document – the Information Security Policy – shall ensure that appropriate and effective security controls will be taken. These controls shall correspond to the respective purpose of data protection.

1.2 ISMS DOCUMENT STRUCTURE

The Information Security Policy (ISP) constitutes the highest level of the documentation of the ISMS.



The document structure of the ISMS

Each and every employee of the think project! companies is to uphold the Information Security Policy and all standards and guidelines derived from it. This shall protect the information of both the think project! companies and its customers, as well as guaranteeing availability of this information.

1.3 RELEASE

Top Management has released the existing Information Security Policy after carrying out an examination of it. All employees are instructed to apply these regulations. All employees are also instructed to conduct themselves responsibly and to take heed of information security effectively and within the law.

1.4 CONTROLS AND SANCTIONS

The Information Security Policy is obligatory for all those who, within its scope, work either for or with the think project! companies. This includes employees, consultants, service providers and suppliers. Compliance with the ISMS will be examined regularly and on a case-related basis.

Each employee of the think project! companies is to observe the Information Security Policy and all standards and guidelines derived from it. Violations of its directives will be pursued and disciplinary measures will be taken.

1.5 POINT OF CONTACT

Inquiries, suggestions and criticisms are always welcome. Please direct any of these, as well as any complaints, to the think project! Information Security Officer.

Munich, December 2016

Thomas Bachmaier
CEO

2 DEFINITIONS

2.1 INFORMATION SECURITY

Information security covers the properties of information processing systems and organisational units that ensure the confidentiality, availability and integrity of information. Information security serves in protecting against hazards and threats, preventing damage, and minimising risks.

2.2 ISMS

An Information Security Management System (ISMS) is understood to be the component of a company-wide management system which covers the establishment, implementation, execution, evaluation, maintenance and improvement of information security based on a business risk approach. The ISMS covers the structures, guidelines, planning activities, responsibilities, practices, methods, processes and resources of the companies.

2.3 ASSET OWNER

For every business process and application that processes information, a representative is designated as process representative or asset owner who is responsible for all queries concerning information processing and information security within the scope of these business processes. The owner ensures that the security measures relevant to the business processes meet the security needs.

3 OBJECTIVES AND PRINCIPLES OF INFORMATION SECURITY

3.1 OBJECTIVES

The think project! companies' information security objectives are:

- The fulfilment of customer requirements towards confidentiality, integrity and availability
- Reliable support for business processes through the use of information technology and through guaranteeing the continuity of workflows within the organisation
- The realisation of more secure and trustworthy communications with customers, authorities and external service providers
- The preservation of the value invested in technology, information, work processes and knowledge
- Securing the high value of information
- The fulfilment of requirements resulting from legal guidelines
- The guaranteeing of the right to informational self-determination of those parties affected by the processing of personal information (data protection)
- The reduction of costs resulting from incidents

3.2 PRINCIPLES

During the creation of information security baselines and concepts, the following principles are to be considered:

3.2.1 Adequacy

The objectives of security controls and the required costs are proportional to one another. Apart from adhering to the legally prescribed security requirements, security controls also undergo an adequacy examination in relation to the purposes of protection.

3.2.2 Resources

Sufficient financial, human and time resources are made available in order to reach and maintain an appropriate level of security.

3.2.3 Involvement of employees

Information security concerns all employees. Each individual must help to prevent damage through responsible conduct and security-awareness.

3.2.4 Information classification

All information that is processed within the scope of business processes is classified according to its protective requirements. This is a prerequisite for the risk assessment and for the implementation of appropriate security controls.

4 RESPONSIBILITIES

4.1 PERSONAL RESPONSIBILITY

Within the scope of fulfilling their duties, each employee is responsible for the information, processes and workflows entrusted to them. The company's internal security organisation is clearly structured in order to support this.

4.2 ASSET OWNER

The asset owner:

- Ascertains the business relevance of their information and determines its protective requirements.
- Ensures the implementation of security and control measures towards the administration and protection of their information.

The asset owner defines methods of accessing information, as well as the type and extent of authorisation required for the respective access methods. In doing so, storage regulations, as well as legal requirements in connection with the information, will be taken into account.

4.3 PROCESS OWNER

The process owner is responsible for defining the strategic objectives of the process and for providing all required resources. They are also responsible for executing the process in compliance with all laws and regulations.

4.4 TOP MANAGEMENT

The top management provide the human, organisational and financial resources required for the ISMS to operate effectively and to be improved. They are also responsible for evaluating the information security standard achieved in terms of its effectiveness and adequacy.

4.5 INFORMATION SECURITY OFFICER

The Information Security Officer (ISO) is assigned as a direct staff member of the top management. The ISO is responsible for the maintenance of the ISMS and is therefore accountable for ensuring that the information security processes are practised within the companies. The ISO advises all departments within the companies. The ISO also reports regularly, as well as on an ad hoc basis, to the top management concerning the performance of security controls and regarding any security incidents.

4.6 DATA SECURITY OFFICER

The Data Security Officer (DSO) works towards compliance with the Federal Data Protection Act (Germany) and other regulations concerning data protection. The DSO monitors the compliant implementation of data processing procedures and advises departments on all queries relating to data protection.

4.7 PROCUREMENT

The procurement of IT components and services is executed and coordinated by the Systems Engineering department. As needed, IT suppliers and external service providers are contractually required to comply with the Federal Data Protection Act (Germany) and with other security-related regulations.

4.8 COST CONTROL

Controlling pays particular attention to the cost-benefit analysis of security-related projects and their operating costs.

5 ASSETS AND PROTECTION LEVELS

Protective requirements are based on the information that is to be protected. The protective requirement is then transferred onto the processes, IT applications, databases, servers, personal computers, networks, rooms etc. and also onto buildings and grounds as necessary.

The protective requirement is substantiated through the following protection categories:

- Confidentiality
- Integrity
- Availability
- Authenticity
- Liability

Differing protection levels are defined within each protection category.

5.1 CONFIDENTIALITY

Confidentiality is the characteristic of a piece of information that is intended for only a limited group of recipients (persons, units, processes).

The information is protected from unauthorised viewing and is not to be revealed without the permission of the information owner.

Protection Level	Description
Open	No prescribed confidentiality.
Restricted	A breach of confidentiality is assessed as a normal risk when there exists little to no expected impact.
Confidential	A breach of confidentiality is assessed as a serious risk when a significant impact can result. An adverse effect on personal integrity cannot be ruled out.
Sensitive	A breach of confidentiality is assessed as an extremely serious risk when it could mean societal or economic ruin. An adverse effect on personal integrity is possible and it could place life and limb in danger.

5.2 INTEGRITY

Integrity designates the propriety (intactness) and completeness of information and the correct functionality of systems. Information is to be protected against falsification and loss.

Protection Level	Description
Normal	A loss of integrity is assessed as a normal risk when there exists little to no expected impact.
Enhanced	A loss of integrity is assessed as a serious risk when a significant impact can result. An adverse effect on personal integrity cannot be ruled out.
High	A loss of integrity is assessed as an extremely serious risk when it could mean societal or economic ruin. An adverse effect on personal integrity is possible and it could place life and limb in danger.

5.3 AVAILABILITY

Availability is a measure of the period of time during which a piece of information (a system) is available for business processes. This protection category is defined as a tolerable period of down time for each designated time frame.

Protection Level	Description
Normal	System failures and losses of information availability are assessed as normal risks when there exists little to no expected impact.
Enhanced	System failures and losses of information availability are assessed as serious risks when a significant impact can result, or when the company's public standing or customer relations can be damaged.
High	System failures and losses of information availability are assessed as extremely serious risks when they could mean societal or economic ruin, or when they can cause lasting damage to the company's public standing or permanently cease relations with key accounts.

Where required for individual cases, the following will be consulted as additional protection categories:

5.4 AUTHENTICITY

Authenticity is the characteristic of clearly allocating a message or transaction based on the genuineness, verifiability and trustworthiness of a unique sender and/or receiver.

5.5 LIABILITY

Liability (non-repudiation) means that it is not possible to make an undue dispute concerning actions performed, nor may an undue dispute exist concerning the authorisation of a transaction.

6 THE INFORMATION SECURITY PROCESS AND RISK MANAGEMENT

The company-wide information security process ensures that the objectives and quality of the ISMS are guaranteed through a model containing the Plan, Do, Check and Act phases (PDCA Model according to ISO 9001).

6.1 PLANNING THE ISMS (PLAN)

The ISMS is planned as a PDCA Model under the auspices of the Information Security Officer. Information and security items are identified and documented based on a determination of sensitivity. Security concepts and directives are created at the foundation of the Information Security Policy (including, for example, the data protection concept, the virus protection concept, the emergency precautions concept, and regulations pertaining to the usage of IT systems).

6.2 SUPPORTING AND OPERATING THE ISMS (DO)

The organisational and technical regulations and measures that are specified in the planning phase are then to be implemented and documented. Results arising outside of operations are documented as logs or other records and are made available for analyses, error corrections and improvements.

6.3 MONITORING THE ISMS (CHECK)

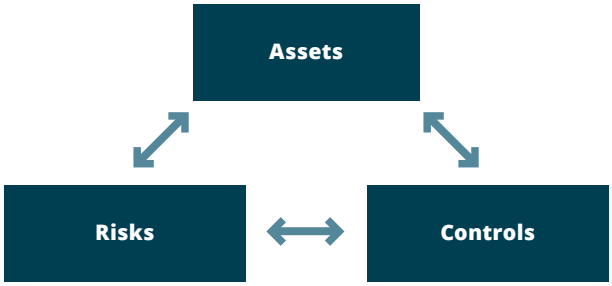
All employees are obligated to report security incidents to their superiors or directly to the Information Security Officer. This can include, for example, virus alerts, established unauthorised access attempts, the loss of mobile digital storage devices, inadequate availability of information, or the incorrect representation of information. The Information Security Officer classifies the reported incidents and implements further controls. The effectiveness of the ISMS is checked annually by the Information Security Officer through internal audits. Additionally, an annual audit will be carried out by an externally contracted certification body.

6.4 IMPROVING THE ISMS (ACT)

Those nonconformities and recommendations ascertained through internal and external audits will be constantly and promptly checked and implemented through appropriate measures. The effectiveness and quality of the ISMS will be evaluated using key performance indicators.

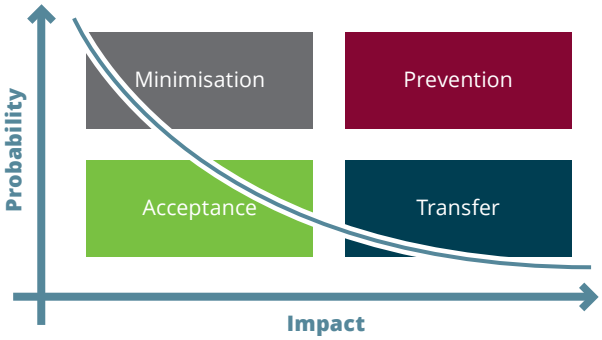
6.5 RISK ASSESSMENT

Risk analyses are a significant element of the ISMS. They are used to identify and assess risks. Through the use of preventative actions, they are also used to prevent, minimise or transfer negative events to third parties. Furthermore, they are used to communicate about situations of risks, for example, in order to promote the perception of a risk. Based on the identified assets possessing an allocated protection requirement, scenarios are considered in which vulnerabilities towards potential threats will arise. After assessing the probability of a threat's occurrence and the resulting level of impact, respective controls are to be determined in a technical and organisational manner. These are then to be evaluated according to their implementation costs, the time necessary to implement them, and their effectiveness.



Risk Management

In justified cases, instead of preventing, minimising or transferring the risk, it may be decided to actively carry the risk – as long as this will not breach any laws, regulations or contracts. Such risk acceptances are reserved as a decision of the top management.



Handling of risks

7 SECURITY REGULATIONS AND STANDARDS

7.1 LAWS, CODES AND STANDARDS

Compliance with laws, codes, standards, regulations and contracts is of the highest priority, including, for example:

- KonTraG (Company Control and Transparency Law, Germany)
- FDPA (Federal Data Protection Act, Germany)
- TKG (Telecommunications Act, Germany)
- TMG (Telemedia Act, Germany)
- ISO/IEC 27001

The currency of the prevailing laws, codes, standards and regulations will be regularly checked. Changes will be assessed and flow into the continual improvement of the ISMS.

7.2 GROUNDS, BUILDINGS AND FACILITIES

Grounds, buildings and facilities that are used by employees or which serve in housing IT components represent externally protected areas. Access to all grounds, buildings and rooms is securely regulated and controlled (identification, burglary protection, etc.). Grounds, buildings and facilities through which visitors and suppliers pass, or which are made available to business partners, are to be delimited through technical and organisational controls from those areas used exclusively by the company's own employees. Hazard alert and alarm systems are to be installed in important areas.

7.3 SERVER ROOMS/SPECIAL FUNCTIONAL AREAS

Access to computing centres and to other rooms/building sections/ areas housing central IT components as well as to functional areas such as the human resources department or the administrative accounting department is only permitted for those personnel authorised for said areas. Such access is to be controlled and protected through particularly effective measures.

7.4 INFORMATION RISK MANAGEMENT

Information Risk Management is a fundamental component of a functional ISMS. Every department within the think project! companies evaluates their risks and regularly checks the relevant controls according to their effectiveness and currency. These are then adapted to new requirements, be they technical or otherwise.

7.5 NEED-TO-KNOW

Access to operating systems, software applications, databases/files, configuration data, etc. occurs only through specially authorised persons according to the need-to-know principle. The methods for the system administration and usage of IT components are specified according to necessity and target audiences.

7.6 UNINTERRUPTIBLE OPERATIONS

During power outages, an uninterruptible power supply ensures adequate coverage necessary to operate the most important servers, network components and communication facilities.

7.7 ENVIRONMENTAL CONDITIONS

Where necessary, IT rooms shall possess climate control in order to regulate humidity and temperature. Sensitive components (discs, hard drives, printers, scanners, etc.) should be protected from contamination (dust, pollution) and strong magnetic fields.

7.8 DIGITAL STORAGE DEVICES

Digital storage devices (discs, magnetic tapes, removable discs, etc.) used for backups and archives should be stored in fireproof safes or rooms. These should also be duplicated and stored separately as required.

7.9 CABLING SECURITY

The cabling of active and passive network components, as well as of data and voice terminals, is completed in a tamper-proof manner and in line with the relevant regulations according to EMC/EMP. All important connections are securely laid out. All cabling is fully documented and is also available as a printed hardcopy. Any area that houses cabling components is particularly secured and only accessible to specially authorised personnel.

7.10 WAN/LAN/WLAN

The network and its components are laid out in a manner providing for redundancy of important sections. The network and its components are also installed in secured rooms.

7.11 ACCESS BY EXTERNAL PARTIES

Access by external parties to the network/IT systems for the purpose of remote maintenance access is secured to a higher degree. The same applies to access made via the extranet. Access to the internet services offered is secured through corresponding state-of-the-art technical measures that prevent manipulation of these services and which make any influence over internal IT systems impossible.

7.12 INTERNET SERVICES

The usage of internet services (web, email, instant messaging, etc.) takes place according to operational necessity. Criminal, radical, racist and pornographic content is neither allowed to be called up, nor may it be saved.

7.13 SOCIAL NETWORKS/VIDEO PORTALS

Social networks are to be used exclusively according to the company-wide policies. This means using them in a moderated manner for marketing purposes and for communication with users and between users.

7.14 CLOUD SERVICES

A variety of versions of cloud services are used. When selecting and monitoring a cloud service provider, the data protection provisions are to be adhered to.

7.15 BRING YOUR OWN DEVICE

Employees are provided with those devices necessary to fulfil their tasks. The usage of privately procured devices for the personal organisation of work takes place exclusively according to company-wide policies.

7.16 PC WORKPLACES

Employees will be provided with suitable electronic devices as required. Selection, procurement and configuration occurs centrally according to the company-wide policies and the corresponding functional requirements. Usage that deviates from this is fundamentally prohibited and can only be approved by the top management in exceptional cases. Data on mobile devices and mobile hard drives with a classification of "confidential" or higher is encrypted using state-of-the-art technology. Security-related updates are implemented as necessary. Security settings may not be deactivated or altered by users.

7.17 WORKGROUP PRINTERS

Documents printed from printers and fax machines are to be removed from the machines by the person authorised to do so, and this is to occur immediately after printing.

7.18 VIRUS PROTECTION AND PROTECTION FROM INTRUSIONS

Systems and networks are protected by appropriate technical and organisational controls such that any computer virus attack or intrusion into these systems will be prevented by state-of-the-art technology.

7.19 CONFIGURATION

Configurations may only be carried out by the person responsible for them. There are also measures in place to prevent configurations from being made by persons unauthorised to do so.

7.20 MEDIA DISPOSAL

The disposal of IT components and the destruction of storage media (paper etc.) occurs exclusively through the positions responsible for the components and data according to the regulations contained within DIN 66399.

7.21 ENCRYPTION

When saving and transferring information that is subject to the protection levels of confidentiality and integrity, it will be secured through appropriate encryption methods.

7.22 DATA BACKUP/RESTORE

Data backups will take place regularly. The storage of digital storage devices involved in these backups takes place in facilities with enhanced security. The restore capability will be reviewed at regularly intervals.

7.23 OUTSOURCING

The outsourcing of IT tasks and the supply of IT components is – as far as security-related departments are concerned – planned and controlled with particular care. The corresponding contracts and agreements consider, among other things:

- The fulfilment of legal requirements
- Guidelines for the control and quality of outsourcing partners
- The implementation of control measures
- Emergency planning in the case of the loss of a partner

7.24 EMERGENCY PLANNING

Emergency plans are created for all operations-related departments. These emergency plans are regularly reviewed, adapted and implemented with respect to their objectives and their effectiveness in terms of changes to the surrounding environment and changing internal factors.

7.25 BUSINESS CONTINUITY

It is a mandatory requirement that an efficient business continuity management system (BCMS) is developed for the systematic preparation toward events of loss that endanger important business processes.

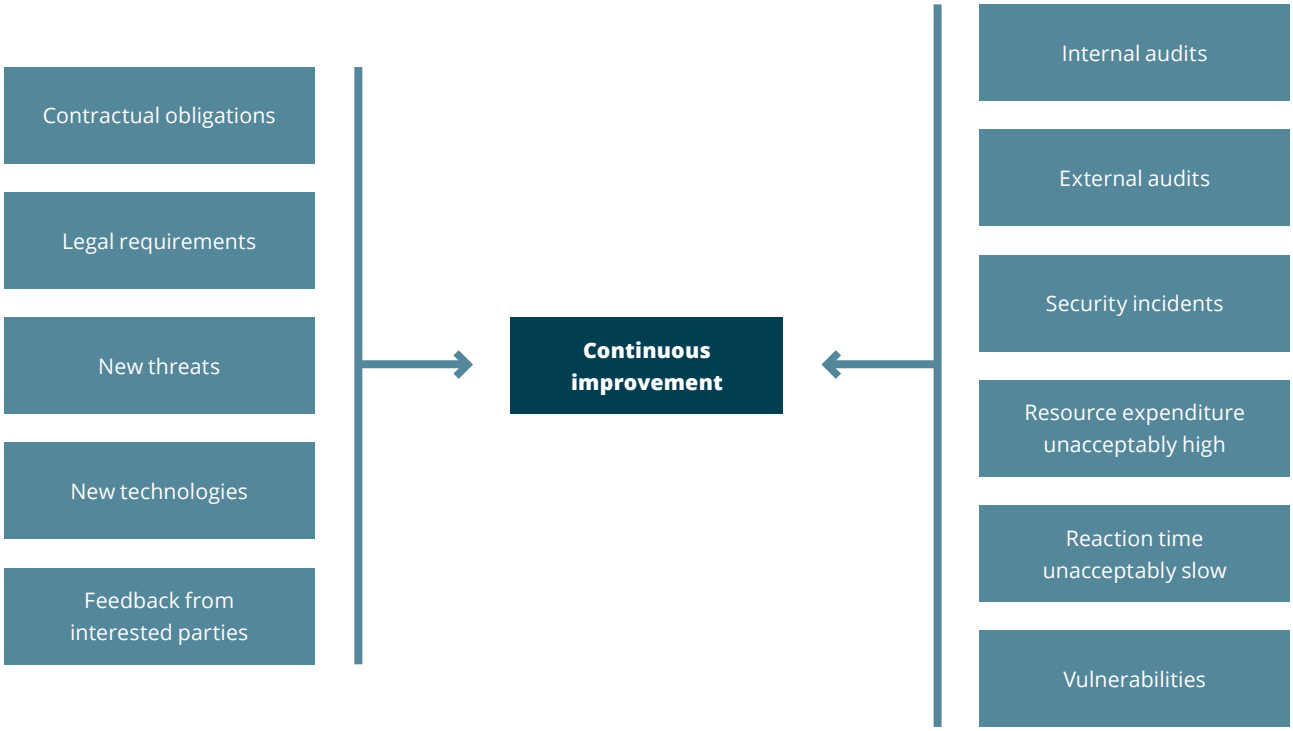
This concerns not only IT and system outages, but also:

- Loss of buildings
- Loss of personnel
- Loss of partners/suppliers

The lifecycle model for the continuation of business activities during times of crises, or at least during difficult conditions, is ensured through a scaled concept of measures.

8 CONTINUOUS IMPROVEMENT

The effectiveness of the ISMS will be continually improved. Corrective and preventive actions are derived from various sources and aspects.



Causes triggering continuous improvement

The focus of continuous improvement is on preventive actions and on controls that possess the greatest effect at the lowest possible usage of resources.

thinkproject!

50 countries

10,000 projects

› 150,000 users

About think project!

The global construction industry faces many challenges, such as pressure to deliver projects in time and on budget, as well as the increasing data volumes generated by an ever increasing number of parties involved on construction and engineering projects.

As a result, there is an emerging need for digital construction solutions such as think project! that facilitate cross-enterprise collaboration and overall information management.

think project! addresses today's digitalisation challenges in construction and engineering by providing state-of-the-art software solutions as well as industry expert consulting and services.

think project! – your partner for digital transformation

Representatives worldwide
www.thinkproject.com/contact-us