INFORMATION SECURITY POLICY

thinkproject

ISMS

Management system: ISMS
Product: ALL
Document ID: ISMS_00001
Version: 1.8
Classification: Open

Created by	Andreas Blücher	16.04.2020
Approved by	Tom Harman	21.04.2020
Date of original issue	29.04.2020	

Please do not print copies of this document.

CONTENT TABLE

1 PURPOSE

thinkproject is a collective of market-leading products and professionals with the goal to develop and deliver best-in-class solutions to support, connect and advance the construction industry and the people in it.

This includes information and data processing on behalf of our customers. **Therefore, customer information must be protected in terms of confidentiality, integrity and availability.** This Information Security Policy describes how to achieve this goal. Information Security is established by means of an Information Security Management System (ISMS) according to ISO 27001. This is an industrial standard for information security. The ISMS provides policies, processes and concepts to achieve information security.

Within the thinkproject group all important processes around information security are provided centrally. These centralised processes ensure group wide standards for information security. Each subsidiary works to the same level of information security with these centralised processes. There are centralised processes for asset management, risk management and information security incidents.

In addition to centralised processes there are local processes for specific techniques or tools that are used in the subsidiaries.

1.1 Release

thinkproject's CEO has released this 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.

1.2 Controls and sanctions

The Information Security Policy is obligatory for all those who, within its scope, work either for or with the thinkproject 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 thinkproject companies are 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.

1.3 Point of contact

Inquiries, suggestions and criticism are always welcome. Please direct any of these, as well as any complaints, to the thinkproject Information Security Officer.

Munich, February 2020

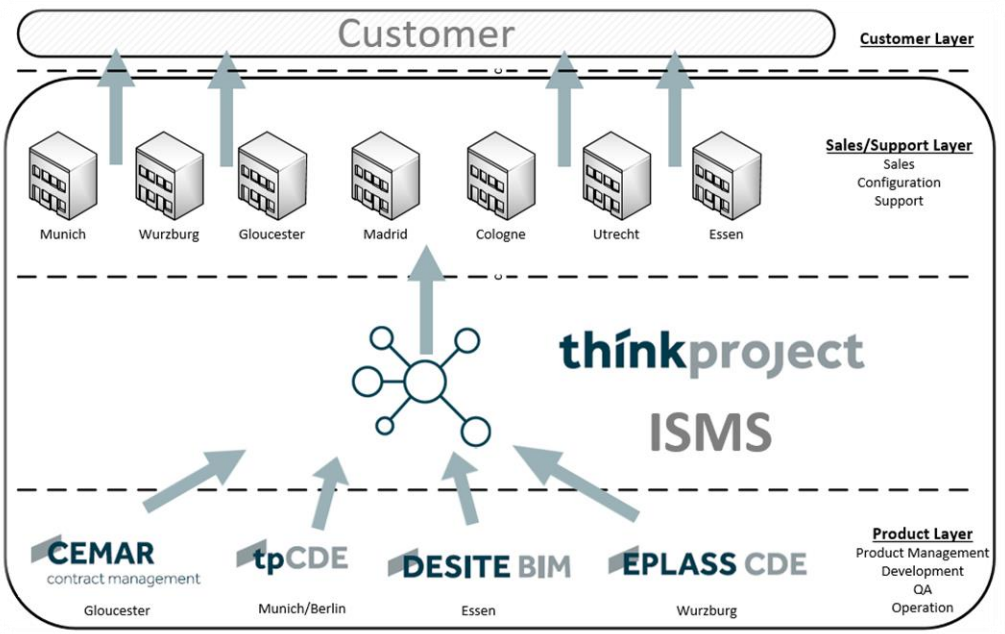
Gareth Burton, CEO

2 SCOPE

The scope of an ISMS describes what has to be considered from the perspective of information security and what will not be considered. The scope of thinkproject's ISMS covers the:

Locations

- Munich
- Gloucester
- Wurzburg
- Berlin
- Cologne
- Madrid
- Essen
- Utrecht



Products

- thinkproject CDE
- EPLASS CDE
- CEMAR
- DESITE

Services

- Product management
- Software development incl. Testing
- Operation of the software incl. Hosting
- Sales
- Configuration of the software
- Customer support
- Internal office IT
- User Management
- Administration

The services include cross sales and cross support activities.

Although there are products and locations in thinkproject group that are not within the scope they should apply the ISMS standards whenever possible. This might be necessary to achieve a level of information security that might be required by GDPR.

3 DEFINITIONS AND ABBREVIATIONS

3.1 Information Security

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

3.2 ISMS

An Information Security Management System (ISMS) is understood to be the component of a group 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 group.

The thinkproject group runs an ISMS according to ISO 27001.

4 OBJECTIVES AND PRINCIPALS

4.1 Objectives

The thinkproject 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 provider
- 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

4.2 Principles

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

4.2.1 Adequacy

Measures are taken in order to come to a higher level of information security. These measures involve costs. The principle of adequacy ensures that there is a reasonable ratio between increase in costs and increase in the level of information security.

4.2.2 Resources

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

4.2.3 Involvement of employees

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

4.2.4 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. Information is classified according to the protection categories confidentiality, integrity and availability.

5 RESPONSIBILITIES

The following roles/responsibilities ensure the proper running of our Information Security Management System:

5.1 Personal responsibility

Within the scope of fulfilling their duties, each employee is responsible for the information, processes and workflows entrusted to them. It is up to every employee to keep the level of information security high. A chain is as strong as its weakest link. The company's internal security organisation is clearly structured in order to support this.

5.2 ISMS Board

The ISMS Board manages all centralised ISMS processes like asset, risk and control management. The board is responsible for strategic orientation and the improvement of the ISMS. The ISMS Board meets regularly and reports to the CxO team.

5.3 Process Owner

Every process that is relevant to information security has a process owner. They are responsible for defining the process and applying it. Process descriptions ensure that every employee is on the same page.

5.4 Asset Owner

From information security point of view an asset is anything that is related to information or processing of information. This could be a computer, a database, a storage system, a piece of software for example. Assets play an important role in information security. That is why every asset is assigned to an owner who is responsible for that asset. Assets are maintained in an asset register.

5.5 Risk Owner

Assets are threatened by risks. Measures shall be taken in order to reduce the risks impact or probability of occurrence. Every risk is assigned to a risk owner. In most cases the risk owner is the same person as the owner of the threatened asset.

5.6 Top Management

The top management provides all required resources to run the ISMS effectively. It is important that the top management has committed itself to the ISMS. In the management review the Group Information Security Officer reports on the current state of the ISMS.

5.7 Group Information Security Officer

Together with the ISMS Board the Group Information Security Officer runs all centralised processes for the ISMS.

- Management Review
- Moderates ISMS Board
- SoA Management
- Defines Standards
- Manages external and internal audit programs

The Group Information Security Officer is responsible for ensuring the group wide ISMS is ready for certification. This includes ensuring that all products and locations satisfy the relevant controls of ISO 27001.

5.8 Local Information Security Officer

Every location within the scope appoints a person that is responsible for local implementation of the ISMS. This includes the tasks:

- Taking part on ISMS Board regularly
- Managing local assets in centralised asset register
- Identifying local risks
- Preparing the location for internal and external audits
- Taking part at ISMS Board meetings
- Conducting awareness training
- Monitoring local processes

5.9 Data Protection Officer

Every location within the scope appoints a person that is responsible for data protection on site. This includes

- Ensuring processes and products are compliant with GDPR and country specific regulations
- Maintaining local records of processing activities (Art. 30 GDPR)
- Interactions with data protection authorities
- Interactions with customers in questions of data protection

Small subsidiaries are permitted to hire external data protection officers.

6 INFORMATION SECURITY PROCESS AND RISK MANAGEMENT

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

Differing protection levels are defined within each protection category.

6.1 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.

Table 1: Protection level for confidentiality

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.

A measure to achieve higher confidentiality could be for example encryption.

6.2 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.

Table 2: Protection level for integrity

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.

6.3 Availability

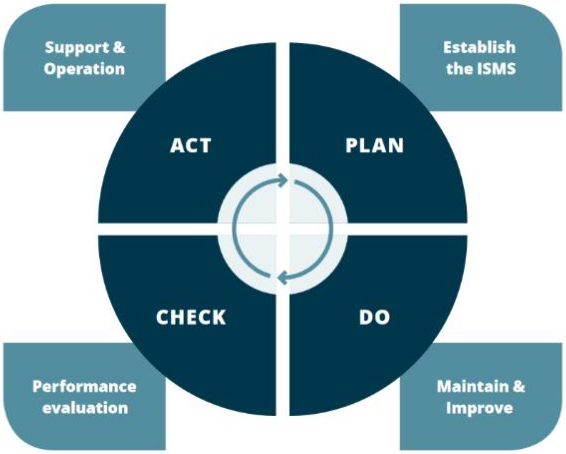
Availability is a measure of the period of time during which a piece of information (a system) is available for business processes. This protection category is defined as a tolerable period of down time for each designated time frame.

Table 3: Protection level for availability

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.

6.4 PDCA Model

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).



6.5 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).

6.6 Supporting and operating the ISMS (Do)

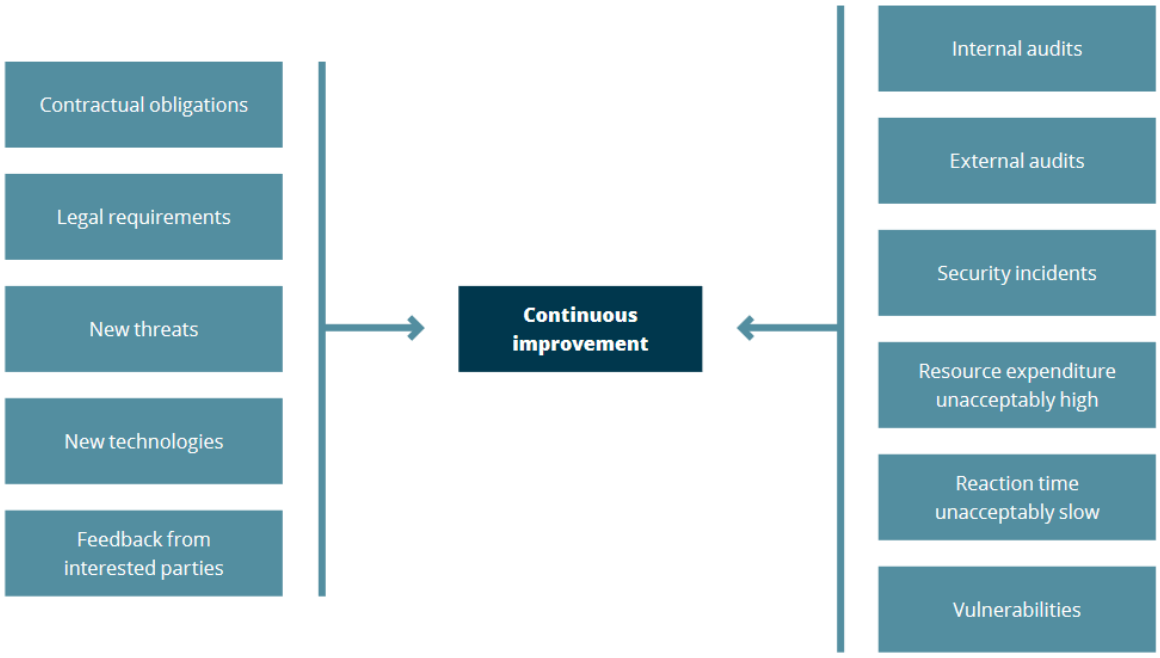
The organisational and technical regulations and measures that are specified in the planning phase are then to be implemented and documented. Results arising outside of operations are documented as logs or other records and are made available for analyses, error corrections and improvements.

6.7 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.

6.8 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.

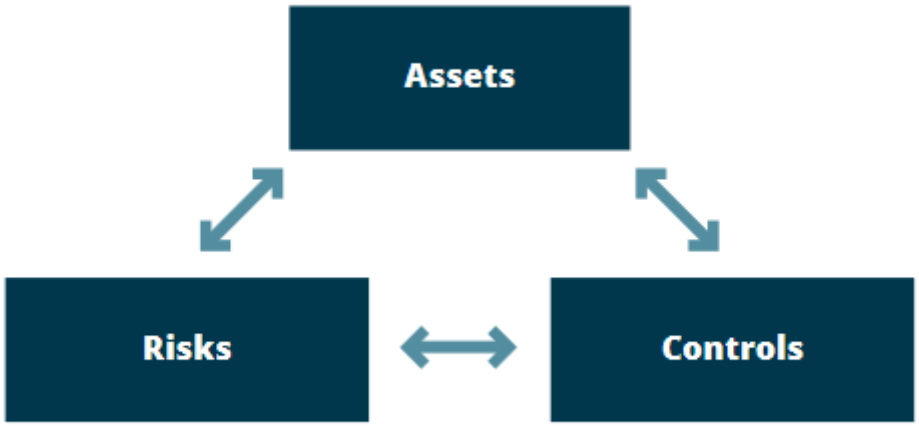


Causes triggering continuous improvement

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

6.9 Risk assessment

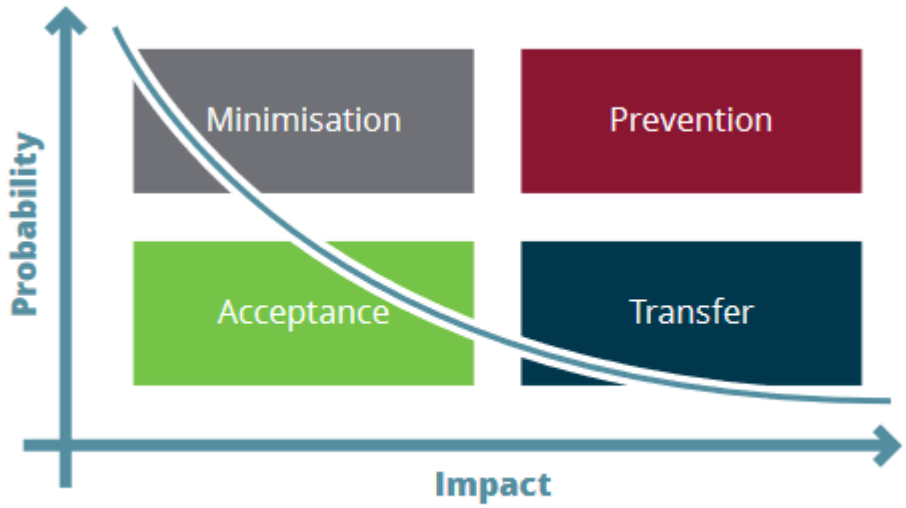
Risk analyses are a significant element of the ISMS. They are used to identify and assess risks. Through the use of preventative actions, they are also used to prevent, minimise or transfer negative events to third parties. Furthermore, the are used to communicate about situations of risks, for example, 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

Assets are threatened by risks. Measures and controls are taken to mitigate risks occurrence.

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

Risks are calculated as the product of impact and probability. The above shown graph shows a line on constant risk. In addition, four steps of risk handling are shown. Please refer to thinkproject risk process for detailed information.

7 SECURITY REGULATIONS AND STANDARDS

In addition to our ISMS which is based on ISO27001 data protection law (GDPR) has to be taken in account when considering information security. Data protection focusses more on confidentiality and integrity than on availability. From viewpoint of a software company the principals “Privacy by Design” and “Privacy by Default” play an important role.

8 DOCUMENT CONTROL

Version	Date	Author	Approved by	Details of changes made
1.0	14.02.2020	AB	Peter Mezger	Initial version
1.2	19.02.2020	TH	Petter Mezger	Feedback Tom, ready to distribute to ISMS Board
1.4	17.03.2020	AB	Peter Mezger	Feedback ISMS Board, new template
1.6	18.03.2020	AB	Jules van der Weide	Added location Utrecht in chapter 2
1.8	29.04.2020	RG	Gareth Burton	Release by CEO and CFO