Hochschule
Augsburg University of
Applied Sciences

Fakultät für
Elektrotechnik

## Master Thesis

Master Degree Course
Industrial Security

Matthias Mödinger

# Metrics and Key Performance Indicators for Information Security Reports of Universities

Author of the Master Thesis
Matthias Mödinger
Büschelstr. 24
86465 Welden
Phone +49 174 9775668
m-moedinger@t-online.de

First Examiner: Prof. Dr. Clemens Espe
Second Examiner: Prof. Dr. Björn S. Häckel
Supervisor: Christian S. Fötinger, MSc.
Application Date: September 28, 2018

Hochschule für
angewandte Wissenschaften –
Fachhochschule Augsburg
University of Applied Sciences

An der Fachhochschule 1
D-86161 Augsburg

Telefon +49 821 55 86-0
Fax +49 821 55 86-3222
www.hs-augsburg.de
info@hs-augsburg.de

# Abstract

Not only governments, enterprises, and organizations are currently faced with the huge and difficult challenge to protect their enormous quantities of personal and sensitive data, but also universities have to face this challenge to ensure the academic freedom of science, research, and teaching as enshrined in the German constitution. A guarantee of complete and consistent information security does not exist. Security threats, malicious attacks, and the misuse of information are constantly increasing. Due to this progression, a total of twelve Bavarian state universities and universities of applied sciences have taken important steps to implement an information security management system (ISMS) in order to control, monitor, maintain, and improve their information security continuously. The work with its three elaborated research questions on the improvement and implementation, measurement, and reporting of information security offers all universities a valuable benefit and support for their ISMS build-up phase.

Initially, the universities' information security controls and processes were examined in a comparative analysis by means of internal audits and a defined maturity model with appropriate maturity levels. Proposals for action according to the ISO/IEC 27000-series were worked out. On the basis of this investigation, the universities will be able to implement their missing ISMS requirements and information security controls, profit by the comparability created among themselves, and improve their information security situation in the end.

To ensure information security on a long-term basis, the information security controls and processes need to be monitored and measured—because what cannot be measured, cannot be managed. For this reason, an information security measurement system with own metrics (fifteen performance and nine effectiveness indicators) was created according to the bottom-up approach. A value benefit analysis was modelled and carried out to derive a handful of key performance indicators (KPIs). By the prepared measurement procedures, the universities will be able to measure the performance and effectiveness of their information security controls and processes. Thus, the universities can constantly monitor their information security.

Ultimately, the important decision-makers like the university management and the competent authorities need to be informed about the current information security situation in order to be in the position to draw the right conclusions in controlling and steering the information security processes and, if necessary, to take appropriate actions. Therefore, the applicability of an information security report was scrutinized and a report structure with its components was determined by a requirements elicitation according to the ISO/IEC 27000-series. Finally, an information security report template was drafted. This establishes the basis for a uniform way of reporting and communicating within and between the universities.

# Table of Contents

Page No.

Page No.

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| Avg. | Average / Average Maturity Level (audit results) |
| BayDSG | Bayerisches Datenschutzgesetz |
| BayEGovG | Bayerisches E-Government-Gesetz |
| BCM | Business Continuity Management |
| BIA | Business Impact Analysis |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CERT | Computer Emergency Response Team |
| CIA | Confidentiality—Integrity—Availability (security goals) |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CSIRT | Computer Security Incident Response Team |
| DFN | Deutsches Forschungsnetz |
| DIN | Deutsches Institut für Normung |
| EI | Effectiveness Indicator |
| HSA | Hochschule Augsburg |
| IEC | International Electrotechnical Commission |
| InfoSec | Information Security |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| KPI | Key Performance Indicator |
| PDCA | Plan—Do—Check—Act (cycle) |
| PI | Performance Indicator |
| SoA | Statement of Applicability |

# 1. Introduction

## 1.1. Information Security

Over the past few years, the term information security has been put more and more into focus—not only for governments and enterprises, but also for smaller organizations as well as every individual. In order to understand the meaning and growing importance of information security, it is useful to take a closer look at its related terminologies and security goals at first.

The term is a composition of the two words ‘information’ and ‘security’. Generally, security is defined as “the quality or state of being secure” (Merriam-Webster, 2018). This definition goes along with everyone’s wish for protection of critical and valuable information assets against security threats, malicious attacks, errors, and all potential hazards. “Security is a broad term that serves as an umbrella for many topics including but not limited to computer security, internet security, communication security, network security, application security, data security, and information security.” (Alsmadi et. al., 2018, p. 1) The last-named topic is significant because information is an important asset that “is essential to an organization’s business and, consequently, needs to be suitable protected” (ISO/IEC, 2018a, p. 12). The forms in which information can be stored and occurred are wide-ranging. **Table 1** gives an overview of the classification of information.

**Table 1:** Classification of Information

| Classification | | Examples |
|---|---|---|
| information format | physical information | contract on paper, handwritten note |
| | electronical information | e-mail, website |
| information state | information creation | writing a message |
| | information processing | printing, faxing |
| | information storage | safe, hard drive, cloud |
| | information transition | public or private network |
| | information destruction | document shredder |
| information location | information in motion | laptop computer, postal dispatch |
| | information at rest | desktop computer, archived information |
| information sensitivity | confidential information | medical record, corporate secret |
| | private information | payroll, marital status |
| | public information | press release, public directory |

(Adapted from: Alsmadi et. al., 2018, p. 2 ff.)

Thus, it appears that the format, state, and location of information can change quickly. Therefore, confidential and private information in particular are constantly exposed to a variety of threats. “Information security, sometimes referred to as InfoSec, is defined as processes, methodologies, standards, mechanisms, and tools which are designed and implemented for the purposes of protecting information from unauthorized access, use, modification or destruction, in order to ensure confidentiality, integrity, and availability of information.” (Alsmadi et. al., 2018, p. 1) In addition to the most important CIA triad (confidentiality, integrity, availability), further security goals need to be considered. **Figure 1** shows all relevant information security goals.

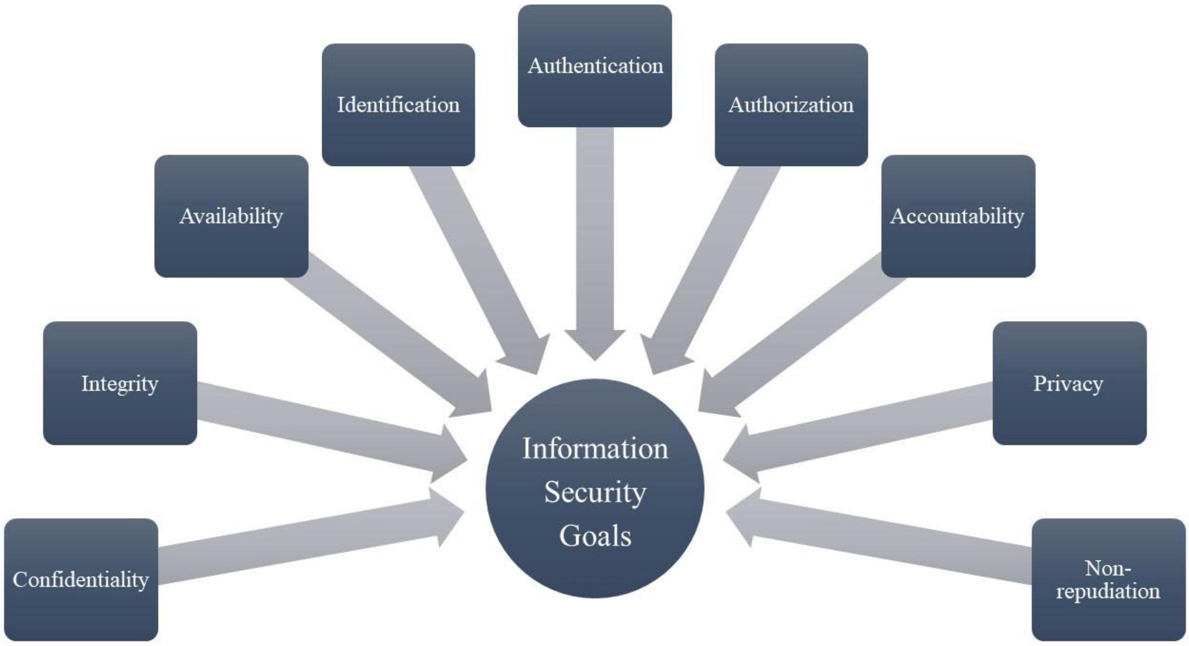


**Figure 1:** Information Security Goals

(Adapted from: Alsmadi et. al., 2018, p. 7)

- **Confidentiality** keeps information hidden and secured from unauthorized access.
- **Integrity** ensures that information has not been altered or corrupted.
- **Availability** makes sure that legitimate information access cannot be hindered.
- **Identification** proves that a person has the legitim access to information.
- **Authentication** examines the authenticity of the alleged identity.
- **Authorization** grants access permissions to information.
- **Accountability** ensures that actions are clearly traceable.
- **Privacy** restricts access to specific information.
- **Non-repudiation** prevents denying previous commitments or actions.

Information security and its presented security goals are "achieved through the implementation of an applicable set of controls [(in German: 'Maßnahmen')], selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software[,] and hardware to protect the identified information assets" (ISO/IEC, 2018a, p. 12). (cf. Alsmadi et. al., 2018, pp. 1–7)

## 1.2. Information Security Management System (ISMS)

The realization of information security is not completed at a specific date, it is a cyclic and continuous process. Therefore, the implementation of an information security management system, abbreviated as ISMS, is a solution for many organizations to assess their own risks and to reduce or best to avoid damages permanently. According to ISO (ISO, 2018), 39 501 ISMSs have been certified worldwide—1 339 of them in Germany (status: December 31, 2017).
"An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining[,] and improving an organization's information security to achieve business objectives." (ISO/IEC, 2018a, p. 11 f.) The continuous improvement process becomes clear with the aid of the PDCA (plan, do, check, act) cycle, which originates from the field of economics and is also known as the Deming circle or Shewhart cycle. The iterative four-step process is illustrated in **Figure 2**.

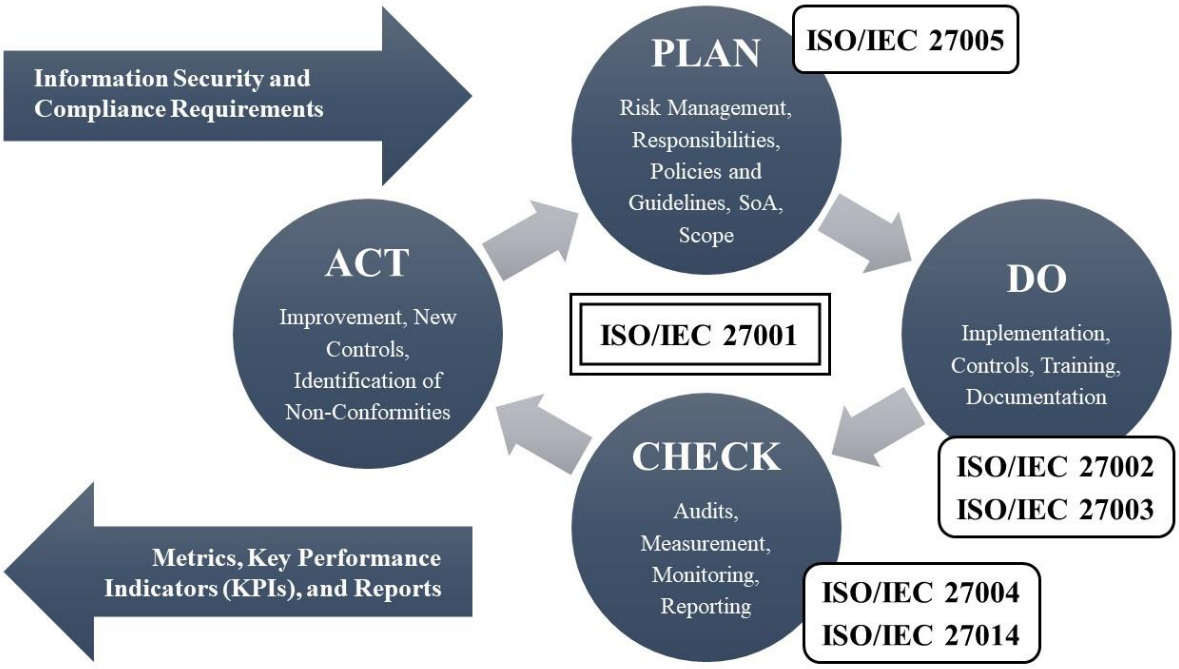

Information Security and Compliance Requirements
PLAN
Risk Management, Responsibilities, Policies and Guidelines, SoA, Scope
ISO/IEC 27005
DO
Implementation, Controls, Training, Documentation
ISO/IEC 27002
ISO/IEC 27003
CHECK
Audits, Measurement, Monitoring, Reporting
ISO/IEC 27004
ISO/IEC 27014
ACT
Improvement, New Controls, Identification of Non-Conformities
ISO/IEC 27001
Metrics, Key Performance Indicators (KPIs), and Reports

**Figure 2:** PDCA Cycle Applied to Information Security Management Systems

(Adapted from: Helmke & Uebel, 2013, p. 205 f.)

The procedure is closely linked to the standards of the ISO/IEC 27000-series, which are scrutinized in the second chapter: **2. ISMS Family of Standards (ISO/IEC 27000-series)**.

1) In the first phase, the planning phase, the ISMS is established.

   Information worth protecting is identified. The scope and coverage are determined, and the management's responsibility is agreed in writing. The Statement of Applicability (SoA), an information security policy, an information security guideline, and topic-specific policies and guidelines are drafted pursuant to the compliance requirements. Additionally, according to the standard ISO/IEC 27005 (*Information security risk management*), an information security risk management process is performed.

2) In the second phase, the doing phase, the ISMS is implemented.

   With the aid of the standards ISO/IEC 27002 (*Code of practice for information security controls*) and ISO/IEC 27003 (*Guidance*), the adopted information security policy, controls, and processes are put into practice. The employees are integrated and trained in the matter of their responsibilities, rights, and obligations. A corresponding documentation is required "as a proof of the implementation of the controls (e.g., preventive, detective[,] and corrective actions)" (Boehmer, 2008, p. 225).

3) In the third phase, the checking phase, the ISMS is reviewed and monitored.

   The information security performance and the effectiveness of the ISMS are monitored, measured, analyzed, and evaluated. For this purpose, an appropriate measurement framework with metrics needs to be developed. Internal audits are carried out to derive improvement potential, to evaluate security incidents, and to assess the current information security situation. By means of those audits and the determination of maturity levels within an appropriate maturity model, it is checked whether the standard ISO/IEC 27001 (*Requirements*) is complied with. Subsequently, an ISMS certification can be carried out by an accredited certification body according to the requirements of ISO/IEC 27001. All relevant results are reported and submitted to interested parties and the important decision-makers, such as the top management. The standards ISO/IEC 27004 (*Monitoring, measurement, analysis and evaluation*) and ISO/IEC 27014 (*Governance of information security*) are helpful for this phase.

4) In the fourth phase, the acting phase, the ISMS is improved continuously.

   Based on the results of the audits, corrective and preventive controls are implemented and non-conformities are identified.

The implementation of an ISMS is a strategic management decision that depends on the organization's security requirements, objectives, organizational procedures, size, structure, and business branch. An ISO/IEC 27001 ISMS certification provides considerable advantages, such as cost savings due to the avoidance of security incidents, better comparability of information security services, the fulfillment of legal requirements, and a positive marketing effect. "It should be kept in mind that no set of controls can achieve complete information security. Additional management actions should be implemented to monitor, evaluate[,] and improve the efficiency and effectiveness of information security controls to support the organization's aims." (ISO/IEC, 2018a, p. 16) In most cases, an ISMS is associated with organizations of the economic sector, but it also plays a significant role in the scientific and education sector. Institutions like universities own huge quantities of sensitive data, for example research results and personal information, that need to be adequately protected.
(cf. Helmke & Uebel, 2013, p. 204 ff.)

## 1.3. Objective and Organization of the Research

The IT service center of Augsburg University of Applied Sciences (in German: Hochschule Augsburg, abbreviated as HSA) including the 'Stabstelle Informationssicherheit bayerischer Hochschulen und Universitäten' develops, networks, supports, and provides advise in all aspects of information security in collaboration with the 'Stabstelle IT-Recht staatlicher bayerischer Hochschulen und Universitäten'. The BayEGovG (Bayerisches E-Government-Gesetz) stipulates that Bavarian universities and universities of applied sciences have to implement and operate an ISMS. The development of an ISMS at the HSA is currently under construction. To support the procedure, three research questions, which are outlined on the next page, were worked out by communicating with the responsible persons of the IT service center. Their elaboration builds the focus of the work.

In the following course of the master thesis, 'university' is used as an umbrella term that includes universities as well as universities of applied sciences. The top management of the universities, consisting of 'Präsidium und erweiterte Hochschulleitung', is referred to as 'university management'.

### Research Question 1

**Are similar information security controls implemented at various Bavarian universities and in what way could the information security situation of these universities be improved?**

The information security controls at various Bavarian universities need to be analyzed and compared with each other. “Controls include any process [...], policy [...], device, practice, or other actions which modify risk.” (ISO/IEC, 2018a, p. 3) The investigation includes twelve Bavarian state universities (nine universities of applied sciences and three universities). By means of internal audits carried out by these universities according to the standards ISO/IEC 27001 and ISO/IEC 27002, the current information security situation needs to be evaluated in conformity with the ISMS requirements, control objectives, and the defined maturity levels. The results of the comparative analysis should show similarities or differences of the implemented information security controls but also create better comparability between the universities. Proposals for action (in German: ‘Handlungsvorschläge’) need to be worked out in order to support the universities in implementing their missing ISMS requirements and information security controls, and to improve their information security situation finally.

### Research Question 2

**How can the compared information security controls of the first research question be measured?**

By means of the standard ISO/IEC 27004, appropriate measurement types, processes, and indicators need to be considered in detail, compared, and finally applied. Consequently, a measurement system with own metrics and key performance indicators (KPIs) needs to be developed. This approach is aimed to create a tailored measurement framework that the universities can use to measure the performance and effectiveness of their information security controls and processes.

## Research Question 3

**Is the preparation of a uniform information security report for universities feasible and what might a template for such a report look like?**

Each university has to report regularly on the current information security situation. This raises the question of it would be feasible to create a uniform information security report template in order to support and facilitate the reporting processes at the universities. For this purpose, it is necessary to carry out a requirements elicitation to examine which structure and components a report should contain. In addition, questions on the applicability of an information security report need to be discussed, as the ones in the following:

- Who should be the recipients of the report?
- Which period of time should be gathered by the report and how often should it be submitted?
- Is the report template suitable for universities of various sizes (universities/universities of applied sciences)?
- Would an overall information security report of all universities be feasible?

The aim is to create a uniform template of an information security report that can be used by several universities. As a result, a uniform way of reporting and communicating should be created within and between the universities.

**The master thesis is written in American English (AE/AmE) and structured as follows:**
In chapter 2, the ISO/IEC 27000-series is discussed to understand its structure and content-related aspects, which are essential for the further course of the work. This series of standards is the most important source of supply. In chapter 3, chapter 4, and chapter 5, the three research questions are worked out successively. The results are presented at the end of the respective chapter. Additionally, chapter 6 summarizes all results and their connection. Finally, chapter 7 concludes the work and provides suggestions for a continuation of the research.

# 2. ISMS Family of Standards (ISO/IEC 27000-series)

The ISMS family of standards, also known as the ISO/IEC 27000-series or abbreviated as ISO27k, "comprises mutually supporting information security standards that together provide a globally recognized framework for best practice information security management" (IT Governance, 2018). The standards of the series are drafted, further developed, routinely reviewed, and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in collaboration with their national standards bodies, for example, the German Institute for Standardization (DIN). According to ISO/IEC, the ISMS family of standards consists of nineteen interrelated standards that are categorized in a standard describing an overview and terminology, standards specifying requirements, standards describing general guidelines, and standards describing sector-specific guidelines, as indicated in **Figure 3**. In addition, thirteen control-specific guidelines standards extend the series. Further standards, like in the fields of cybersecurity and electronic discovery, are currently under development (status as of August 2018). "Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets, including financial information, intellectual property, and employee details, or information entrusted to them by costumers or third parties." (ISO/IEC, 2018a, p. v)
(cf. IT Governance, 2018)

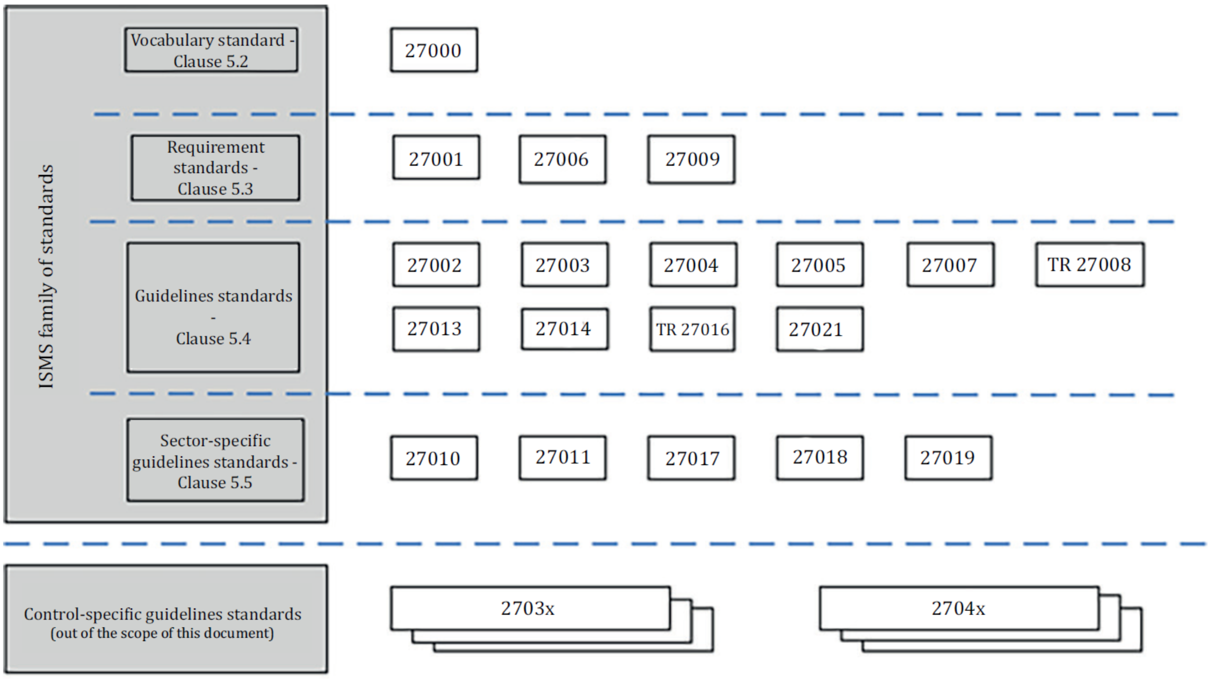

ISMS family of standards
Vocabulary standard - Clause 5.2
27000
Requirement standards - Clause 5.3
27001
27006
27009
Guidelines standards - Clause 5.4
27002
27003
27004
27005
27007
TR 27008
27013
27014
TR 27016
27021
Sector-specific guidelines standards - Clause 5.5
27010
27011
27017
27018
27019
Control-specific guidelines standards (out of the scope of this document)
2703x
2704x

**Figure 3:** ISMS Family of Standards Relationships

(Source: ISO/IEC, 2018a, p. 19)

The standards of the ISO/IEC 27000-series that are relevant and used for the work are listed below and considered more closely. (cf. ISO/IEC, 2018a, pp. 18–25) Current versions were provided by the IT service center of Augsburg University of Applied Sciences.

**ISO/IEC 27000:2018-02**

*(Overview and vocabulary)*

**Relevant to:** All Research Questions

This thirty-four-page standard provides 77 terms and definitions used throughout the ISMS family of standards. Furthermore, an introduction to information security management systems and an overview of the ISO/IEC 27000-series create basic knowledge and complete the standard.

**DIN EN ISO/IEC 27001:2017-06**

*(Requirements)*

**Relevant to:** All Research Questions

This thirty-two-page standard “provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS” (ISO/IEC, 2018a, p. 20). The requirements are specified in clauses 4 to 10 (*4 Context of the organization*, *5 Leadership*, *6 Planning*, *7 Support*, *8 Operation*, *9 Performance evaluation*, *10 Improvement*) and are “intended to be applicable to all organizations, regardless of type, size[,] or nature” (ISO/IEC, 2017a, p. 6). Therefore, the requirements are worded in general terms and are not too technical. If an organization wants to be certified according to ISO/IEC 27001 and claims conformity to this standard, all requirements of clauses 4 to 10 have to be fulfilled. At the end of the document, in Annex A, control objectives and controls are listed. They are used in context with the requirement clause ‘*6.1.3 Information security risk treatment*’. The excerpt below indicates that the controls of Annex A only serve as standard of comparison. Their implementation is not mandatory.

> “ **6.1.3 Information security risk treatment**
>
> The organization shall define and apply an information security risk treatment process to:
>
> a) select appropriate information security risk treatment options, taking account of the risk assessment results;
>
> b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
>
> NOTE Organizations can design controls as required, or identify them from any source.

> c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;
>
> NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.
>
> NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed. ”

(DIN EN ISO/IEC, 2017a, p. 9)

Annex A provides fourteen superordinate security control clauses (*A.5 Information security policies*, *A.6 Organization of information security*, *A.7 Human resource security*, *A.8 Asset management*, *A.9 Asset control*, *A.10 Cryptography*, *A.11 Physical and environmental security*, *A.12 Operations security*, *A.13 Communications security*, *A.14 System acquisition, development and maintenance*, *A.15 Supplier relationships*, *A.16 Information security incident management*, *A.17 Information security aspects of business continuity management*, *A.18 Compliance*). Each security control clause contains one or more main security categories as well as each main security category contains one control objective and one or more controls. In sum, the fourteen security control clauses are subdivided into 35 main security categories which contain 114 controls in total.

**DIN EN ISO/IEC 27002:2017-06**

*(Code of practice for information security controls)*

**Relevant to:** All Research Questions

This ninety-three-page standard is intended to provide support for the preceding standard DIN EN ISO/IEC 27001:2017-06 and is “designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls” (DIN EN ISO/IEC, 2017b, p. 8). Each of the 114 controls of Annex A (*A.5.1.1* to *A.18.2.3*, ISO/IEC 27001) is extended by a specific implementation guidance, which “provides more detailed information to support the implementation of the control and meeting the control objective” (DIN EN ISO/IEC, 2017b, p. 11). Additionally, other information, such as legal considerations and references to other standards, provides useful hints. “The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options[,] and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations.” (DIN EN ISO/IEC, 2017b, p. 9).

### **ISO/IEC 27003:2017-03**

*(Guidance)*

**Relevant to:** All Research Questions

This fifty-two-page standard “provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations (‘should’), possibilities (‘can’)[,] and permissions (‘may’) in relation to them” (ISO/IEC, 2017, p. v). Each requirement of the clauses 4 to 10 (*4.1* to *10.2*, ISO/IEC 27001) is described in more detail by the sections ‘Required activity’, ‘Explanation’, ‘Guidance’, and ‘Other information’. “Organizations implementing an ISMS are under no obligation to observe the guidance in this document.” (ISO/IEC, 2017, p. v)

### **ISO/IEC 27004:2016-12-15**

*(Monitoring, measurement, analysis and evaluation)*

**Relevant to:** Research Question 2

This sixty-eight-page standard “provides guidelines intended to assist organizations to evaluate the information security performance and the effectiveness of the ISMS” (ISO/IEC, 2018a, p. 21) and to fulfil the requirements of ISO/IEC 27001 clause ‘*9.1 Monitoring, measurement, analysis and evaluation’*. **Figure 4** shows the relation between ISO/IEC 27001 and ISO/IEC 27004.

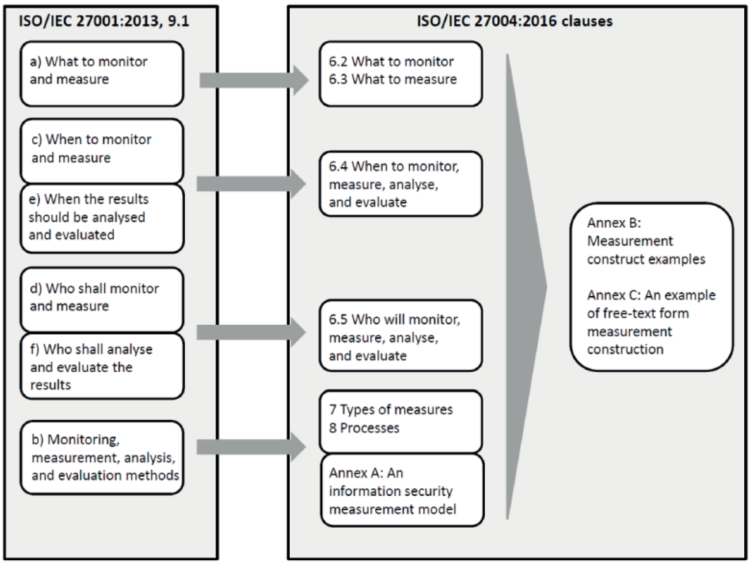

ISO/IEC 27001:2013, 9.1
a) What to monitor and measure
c) When to monitor and measure
e) When the results should be analysed and evaluated
d) Who shall monitor and measure
f) Who shall analyse and evaluate the results
b) Monitoring, measurement, analysis, and evaluation methods
ISO/IEC 27004:2016 clauses
6.2 What to monitor
6.3 What to measure
6.4 When to monitor, measure, analyse, and evaluate
6.5 Who will monitor, measure, analyse, and evaluate
7 Types of measures
8 Processes
Annex A: An information security measurement model
Annex B: Measurement construct examples
Annex C: An example of free-text form measurement construction

**Figure 4:** Relation between the Standards ISO/IEC 27001 and ISO/IEC 27004

(Source: ISO/IEC, 2016, p. 2)

**<u>ISO/IEC 27005:2018-07</u>**

*(Information security risk management)*

**Relevant to:** All Research Questions

This sixty-page standard "provides guidelines for the information security risk management [...][,] supports the general concepts specified in ISO/IEC 27001[,] and is designed to assist the satisfactory implementation of information security based on a risk management approach" (ISO/IEC, 2018b, p. 1). The activities of the information security risk management process, which is shown in **Figure 5**, **Annex**, **p. 99**, are explained in detail. These include the context establishment, the information security risk assessment, the information security risk treatment, the information security risk acceptance, the information security risk monitoring and review, and the information security risk communication and consultation. The annexes of the standard provide examples, methods, and additional information on the above-mentioned topics.

**<u>ISO/IEC 27014:2013-05-15</u>**

*(Governance of information security)*

**Relevant to:** Research Question 3

This twenty-page recommendation standard "provides guidance on concepts and principles for the governance of information security, by which organi[z]ations can evaluate, direct, monitor[,] and communicate the information security related activities within the organi[z]ation" (ISO/IEC, 2013, p. 1). In addition, Annex A and B contain examples of an information security status.

# 3. Comparative Analysis of the Information Security Controls at Bavarian Universities

The analysis is based on summarized data that were collected by internal audits carried out by twelve Bavarian state universities (nine universities of applied sciences and three universities) according to the standards ISO/IEC 27001 and ISO/IEC 27002. Each university was evaluated individually. The universities' IT service centers were in charge of the data acquisition. The audit results were provided by the IT service center of Augsburg University of Applied Sciences and are treated anonymously. They cannot be attributed to the respective university. The internal information serves as an important source for this research question, but in order to protect its confidentiality, the titles and page references are not quoted directly. The audits were conducted by interviews and, to some extent, by on-site inspections at the universities in the period from March to December, 2017. Commissioners of the audits were heads of IT service centers, Chief Information Officers (CIOs), and information security officers. The aim was a status survey to inform about to what extent the ISO/IEC 27001 and ISO/IEC 27002 control objectives are fulfilled in the administrative area and the central services at the Bavarian state universities and to what extent an ISMS is realized and operated.

## 3.1. Approach

To achieve the desired results, which are supposed to create better comparability between the universities and provide proposals for action to improve the universities' information security, the analysis is performed as follows:

1) **Valuation basis:** Consideration of the selected maturity model and its maturity levels
2) **Data collection:** Representation of the audit results
    - Results to the ISMS requirements specified in clauses 4 to 10 of ISO/IEC 27001
    - Results to the controls specified in Annex A of ISO/IEC 27001 (or ISO/IEC 27002)
3) **Data evaluation and analysis:** Evaluation of the audit results and comparative analysis with proposals for action
4) **Findings:** Results and discussion

By means of the data evaluation and analysis, it is possible to determine those kinds of processes and areas of the universities in which information security has been implemented insufficiently and the target maturity level has not been achieved. The guidance notes and recommendations of the standard guidelines ISO/IEC 27002 and ISO/IEC 27003 as well as additional literature are used to work out in what way existing information security controls can be improved and missing controls and ISMS requirements implemented to increase the maturity levels and enhance the information security in consequence.

## 3.2. Maturity Model and its Maturity Levels

Maturity models are efficient tools for the evaluation of an organization’s performance capability. Originally, they became popular in the field of software development due to the widespread use of the Capability Maturity Model (CMM) which was released in 1991 and replaced by the newer Capability Maturity Model Integration (CMMI) in 2002. These models define skill levels and maturity levels based on a specific ranking. The levels determine what needs to be achieved in certain areas—not how it is achieved. In the field of information security, maturity assessments serve in particular as an impulse for the continuous improvement process of an organization’s information security and as a support of the internal learning process.
(cf. Grönert et. al., 2014, p. 1517; cf. Jacobs Stephan, 2013)
The following maturity levels, which are shown in **Table 2**, were used for the audit surveys. As a result, each university carried out the ISMS inventory on the same valuation basis.

**Table 2:** Maturity Levels

| Maturity Level | Level Description |
|---|---|
| **0** | Non-existence of discernible policies, processes, controls, etc. |
| **1** | Development was started and requires significant effort to fulfill the requirements. |
| **2** | Development is in progress but not finished yet. |
| **3** | Development is more or less complete, although details are missing or not implemented yet; used and supported by the management actively. |
| **4** | Development is finalized; process or control has been implemented and started recently. |
| **5** | The requirement is completely fulfilled, works as expected, is monitored and improved actively. There are sufficient evidences for the auditors. |

(Adapted from: Augsburg University of Applied Sciences)

The twelve universities were evaluated with the presented maturity levels according to the 27 ISMS requirements specified in clauses 4 to 10 of ISO/IEC 27001 and the 114 controls specified in Annex A of ISO/IEC 27001 (or in ISO/IEC 27002). An average maturity level was calculated from the twelve survey results for each requirement and control. The maturity level 3 (Development is more or less complete, although details are missing or not implemented yet; used and supported by the management actively) is assumed as the next target level. An average level of at least 3 is desirable. Accordingly, for the evaluation, average levels from 3.0 to 5.0 are rated positively, whereas average levels from 0.0 to 2.9 are rated negatively.

## 3.3. Audit Results

As calculated below, the data collection captures 1 692 audit results. From these results, one average result for each requirement and control (141 in total) was determined additionally.

$$(27\ ISMS\ requirements + 114\ controls) \times 12\ universities = 1\,692\ audit\ results$$

The audit results are listed tabularly. In the table header, the twelve universities are indicated anonymously as ‘U1’ to ‘U12’. Some requirements and controls could not be assessed by the audit commissioners. They were marked with ‘—’ and excluded in the average calculation. The average levels (‘Avg.’) are rounded to one decimal place.

- The audit results to the ISMS requirements specified in clauses 4 to 10 of ISO/IEC 27001 are tabulated in **Table 3**, **Annex**, **p. 91**.
- The audit results to the controls specified in Annex A of ISO/IEC 27001 (or ISO/IEC 27002) are tabulated in **Table 4**, **Annex**, **p. 93**.

By examining the tables, it can already be stated that almost every technical control has been implemented at the Bavarian universities, however, no university has been implemented all controls completely.

## 3.4. Evaluation of the Audit Results

Initially, the audit results are graphically processed with the aid of multiple charts to show clearly the affected processes and areas of the universities in which information security is implemented insufficiently. For this purpose, each average maturity level determined for the 27 ISMS requirements and 114 controls is displayed as a separate bar in the following bar charts. It should be noted that the graphics only show simple mean values of the twelve universities. Therefore, the average maturity level might be bad, although a single university was evaluated well. Then, the other universities must have been evaluated badly. However, due to these differences, it becomes possible to perform a comparative analysis.

**Figure 6** shows the graphic evaluation of the audit results to the ISMS requirements specified in clauses 4 to 10 of ISO/IEC 27001. It pertains to **Table 3**, **Annex**, **p. 91**. Each bar represents one ISMS requirement from clause *4.1* to clause *10.2* (left to right). The target average maturity level of 3 is indicated by the green horizontal line. The bars, or the requirements, that exceed this line are considered as positive and fulfilled—the ones below as negative and not fulfilled.

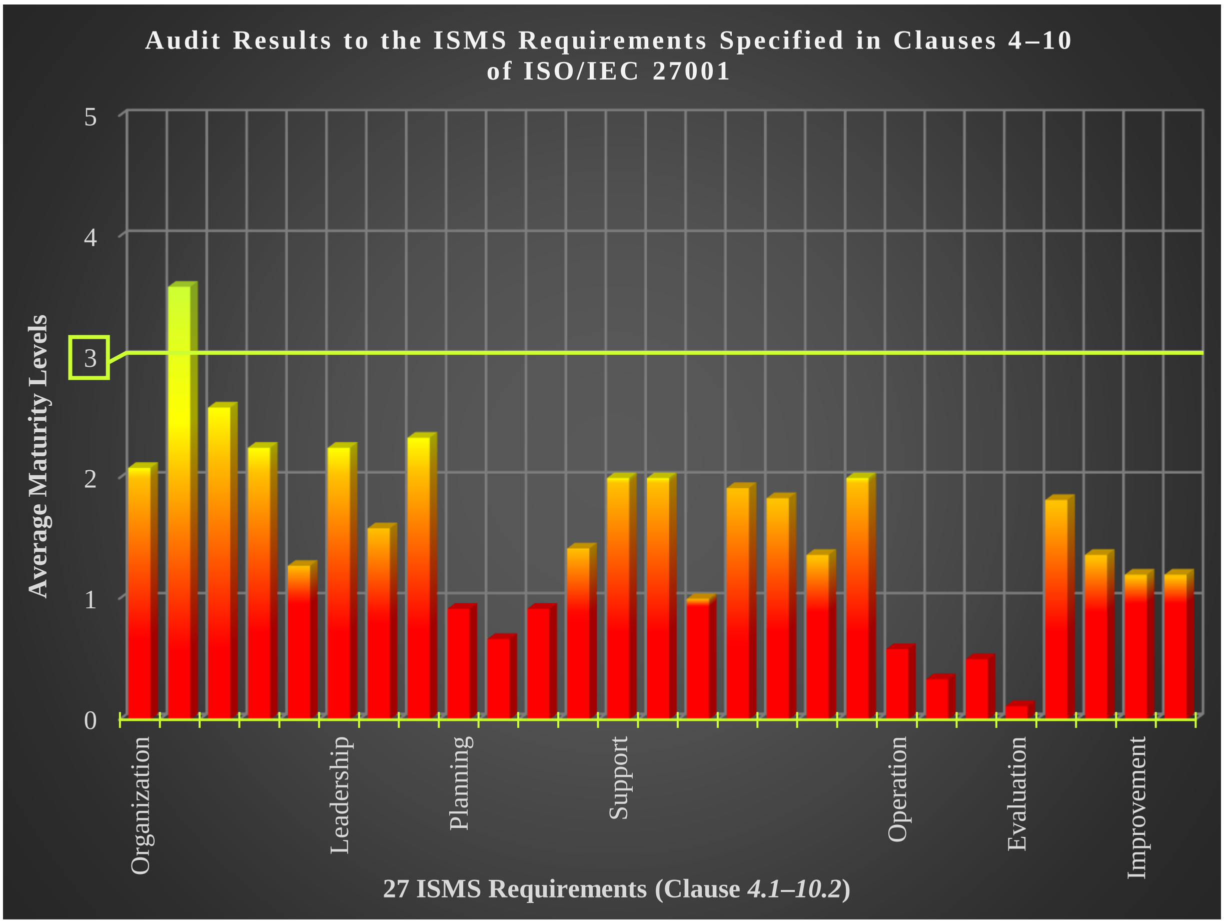


**Figure 6:** Bar Chart on the Audit Results to the ISMS Requirements

(Adapted from: Augsburg University of Applied Sciences)

As it can be seen in **Figure 6**, only one organization requirement (*Identify the involved environment including applicable laws, regulations, contracts, etc*.) out of 27 ISMS requirements was evaluated positively with an average maturity level over 3. All other requirements fall under the desired maturity level. In particular, the risk management requirements specified in the clauses '*6 Planning*' and '*8 Operation*' are almost non-existent. They were evaluated with the lowest maturity level. The requirement '*Monitor, measure, analyze, and evaluate the ISMS and the controls*' was rated with 0.1, which is the worst average maturity level of all requirements. For a better illustration and understanding of the overall information security situation at the Bavarian universities, **Figure 7** visualizes the percentage fulfillment of the ISMS requirements' maturity levels.

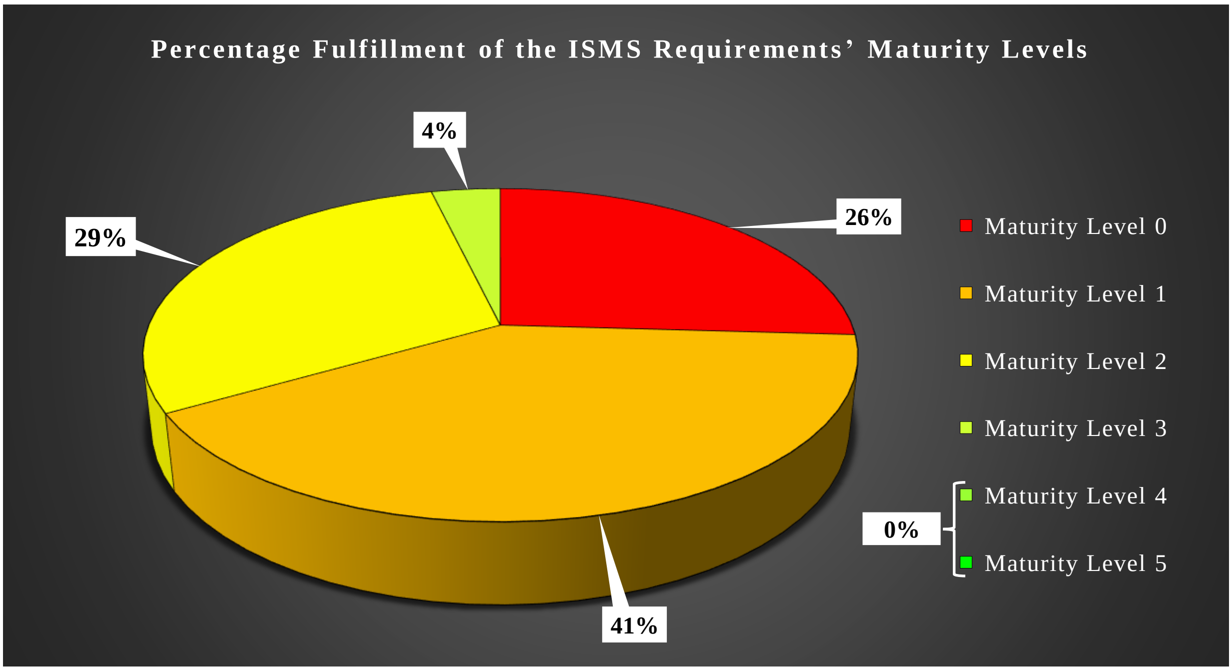


**Figure 7:** Pie Chart on the Percentage Fulfillment of the ISMS Requirements' Maturity Levels

(Source: Own illustration)

The pie chart shows that the implementation of the majority of the ISMS requirements (74%) at the universities has started, is in progress, or is more or less complete. But 96% of the requirements are below the target maturity level of 3. An average maturity level of 4 or 5 is not reached at all. These results demonstrate clearly that the twelve Bavarian universities have taken the first steps to meet the ISMS requirements.

In the following, the audit results to the 114 controls are considered. **Figure 8** shows the graphic evaluation of the audit results to the controls specified in Annex A of ISO/IEC 27001 (or ISO/IEC 27002). It pertains to **Table 4**, **Annex**, **p. 93**.

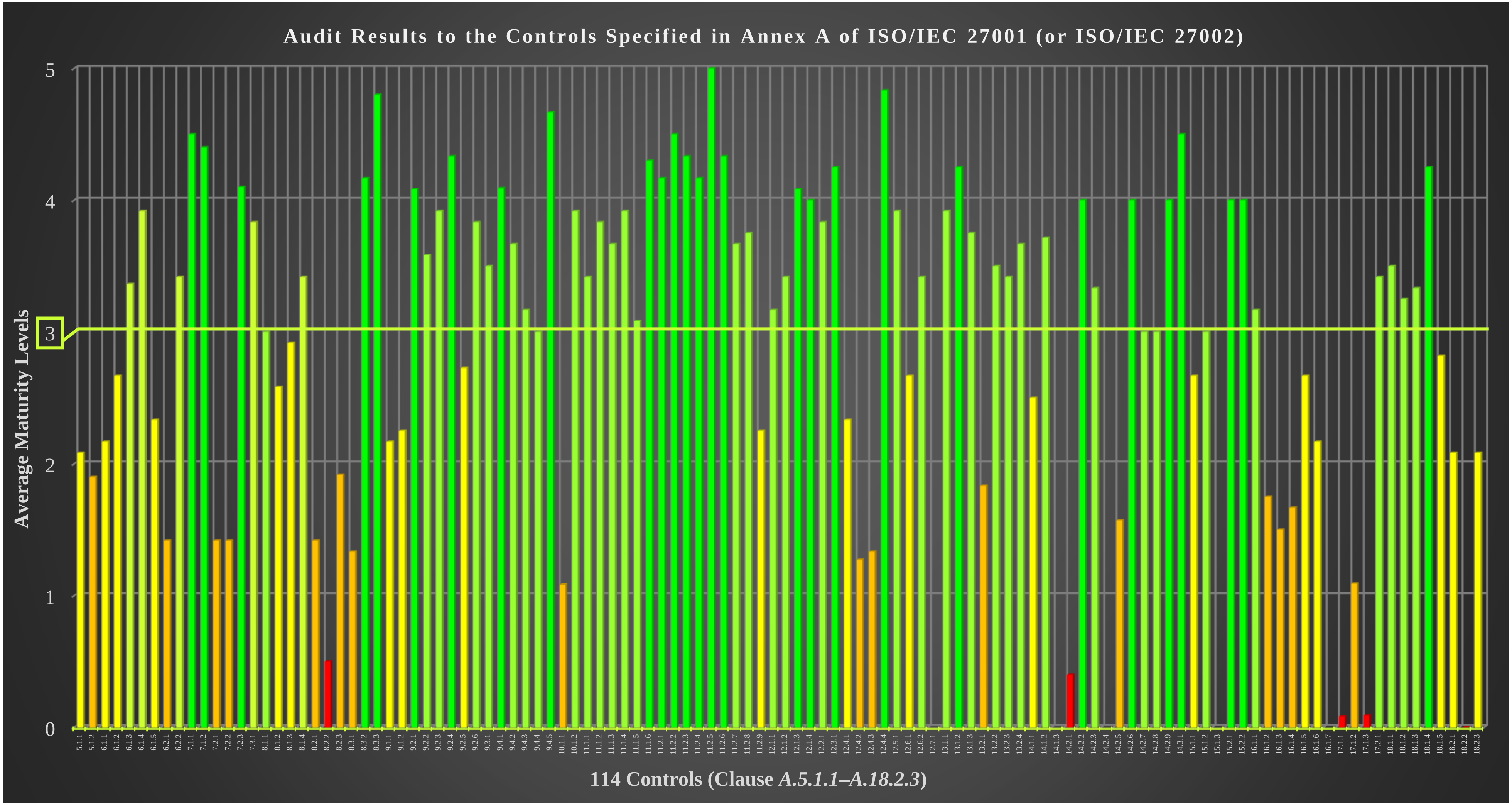


**Figure 8:** Bar Chart on the Audit Results to the Controls

(Adapted from: Augsburg University of Applied Sciences)

As it can be seen in **Figure 8**, 70 out of 114 controls were rated positively with an average maturity level over 3. The controls from the superordinate security control clause '*A.11 Physical and environmental security*' were evaluated and implemented best. From this clause, only one out of fifteen controls was rated negatively. **Figure 9** visualizes the percentage fulfillment of the controls' maturity levels.

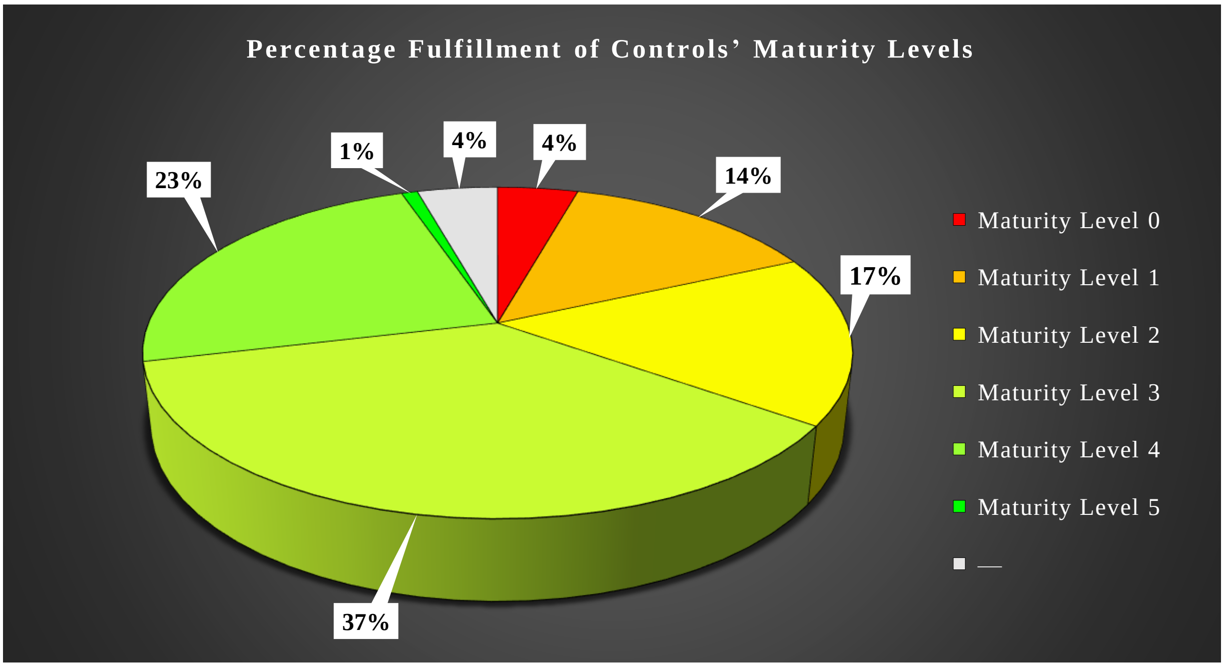


**Figure 9:** Pie Chart on the Percentage Fulfillment of the Controls' Maturity Levels

(Source: Own illustration)

The pie chart shows that 61% of the controls have reached or exceeded the target maturity level and were evaluated positively. Compared to the ISMS requirements, the percentage of controls fulfilled is about fifteen times higher. Thus, it appears that the universities are already well aware of the control and mitigation of risks associated with the information assets that universities are trying to protect. Nevertheless, the implementation of 35% of the controls is still not completed. In addition, 4% of the controls were not evaluated. It is necessary to look at them more closely in the following analysis to see why they have not been assessed.

In summary, the twelve Bavarian universities have not yet reached the target maturity level on average in 96% of the ISMS requirements and 35% of the controls according to the ISO/IEC 27000-series.

Therefore, a comparative analysis with proposals for action needs to be carried out in the next section to determine how to increase the maturity levels and improve the information security at all universities—because an ISMS requirement or control that one university has well implemented can help another university that has not realized it yet.

## 3.5. Comparative Analysis and Proposals for Action

The ISO/IEC 27002 and ISO/IEC 27003 guideline standards and, if necessary, supplementary literature are used to analyze how the general ISMS requirements and controls can be transferred to the universities. In order to provide assistance to universities that have not met certain ISMS requirements or controls yet, proposals for action are worked out. It starts with the security control clauses, followed by the ISMS requirement clauses. In the process, proposals for action are drawn up for each individual requirement and control for which at least one university was evaluated negatively (maturity level below 3). The compared situations at the universities were adopted from the summary of the audit result of December, 2017. As it can be seen in **Figure 10**, the aim of the analysis is the improvement of the information security at the Bavarian universities. Thereto, the elaborated proposals for action need to come into effect.

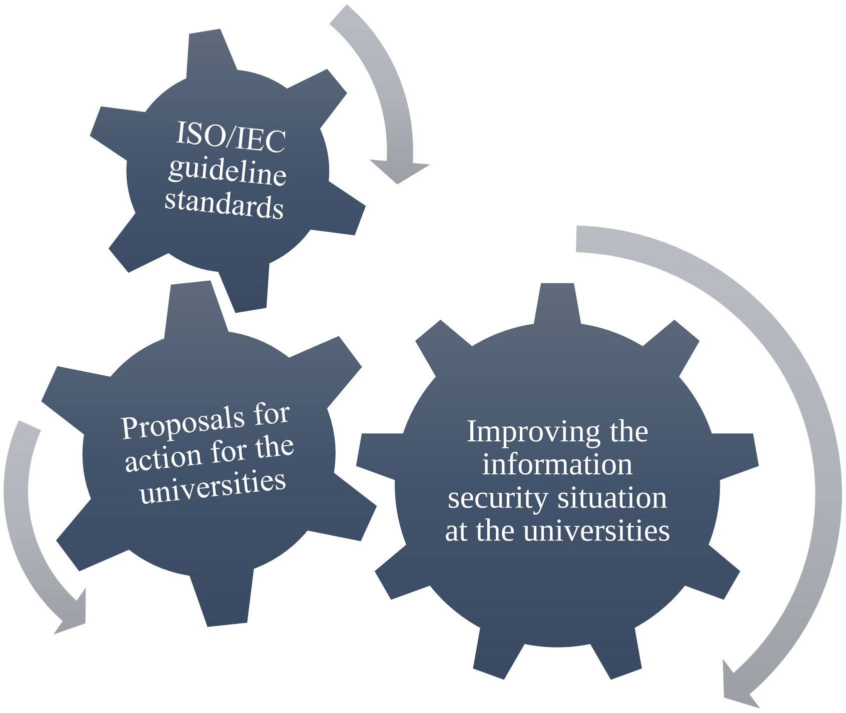

ISO/IEC guideline standards
Proposals for action for the universities
Improving the information security situation at the universities

**Figure 10:** Intended Functioning of the Analysis

(Source: Own illustration)

## CONTROLS (ISO/IEC 27001, Annex A)

### A.5 Information Security Policies (Avg. Maturity Level: 2.0)

Compared situation at the universities:

Nearly half of the surveyed universities are about to adopt a sample information security guideline variant or have already adopted one. Only at three universities, such a document was already existing and revised in 2017.

Proposals for action:

☑ Define and document an information security policy internally at the highest level, which is approved by the university management. The policy sets out the university’s approach to manage its information security.

☑ Draw up an information security guideline and publish it, for example, on the official university website. The guideline is supplemented with topic-specific policies or guidelines that are considered to be relevant to the university management, e.g., a clear desk policy.

☑ For each policy and guideline, determine a responsible person who has been approved by the management as responsible for its development review and evaluation.

ℹ A sample policy (‘Richtlinie’) for universities can be downloaded under the following link:

https://www.hs-augsburg.de/Binaries/Binary25088/Sicherheits-Organisation-template-20171231.docx?mode=download

ℹ A sample guideline (‘Leitlinie’) for universities can be downloaded under the following link:

https://www.hs-augsburg.de/Binaries/Binary25087/SicherheitsLL-template-ISO27K-20170331.docx?mode=download

### A.6 Organization of Information Security (Avg. Maturity Level: 2.8)

Compared situation at the universities:

In most cases, the internal organization is regulated formally. Tasks for IT security and IT service center operation are not separated. Often, an overarching committee eliminates this conflict of interest. Contacts with interest groups (authorities, working groups, and independent communities) are maintained. IT security in projects is available, especially in projects with personal data. Risk assessment is not carried out schematically.

In many cases, the implementation of IT security in projects is not mandatory from the outset. There are hardly any regulations handling the use of mobile devices. Telework is largely well regulated and agreements exist.

Proposals for action:

☑ Define and allocate all information security responsibilities in accordance with the information security policy, guideline, and topic-specific policies and guidelines. Responsible persons may delegate security tasks to others. But they remain accountable and should ensure that all delegated tasks have been performed correctly.

☑ Identify and define assets and information security processes. Assign an entity that is responsible for each asset or information security process and document the details of all responsibilities. Define and document authorization levels. Identify and document also the coordination and oversight of information security aspects of supplier relationships.

☑ Segregate conflicting duties and areas of responsibility. Examine whether it would be better to separate tasks from IT security and IT service center operation. To distribute the responsibilities even more strongly and uniformly, the 'RACI system' can be used to differentiate between responsible, accountable, consulted, and informed responsibilities. (cf. Kersten et. al., 2016, p. 107)

☑ Maintain appropriate contacts with relevant authorities, special interest groups, and other specialist security forums and professional associations.

ℹ Relevant authority:

"Art. 9 Landesamt für Sicherheit in der Informationstechnik

Es besteht ein Landesamt für Sicherheit in der Informationstechnik (Landesamt). Es ist dem Staatsministerium der Finanzen, für Landesentwicklung und Heimat unmittelbar nachgeordnet." (BayEGovG, 2015)

ℹ Special interest groups (examples):

- Deutsches Forschungsnetz (DFN)
  https://www.dfn.de/
- Stabstelle Informationssicherheit bayerischer Hochschulen und Universitäten
  https://www.hs-augsburg.de/Rechenzentrum/Stabstelle-Informationssicherheit.html

☑ Integrate information security into the universities' project management methods. An appropriate person of responsibility has to be assigned for each project. "This could be, for example, the project leader, a special security coordinator within the project team, or a person outside the project team." (Kersten et. al., 2016, p. 108)

☑ Implement a policy and supporting security controls to manage the risks introduced by mobile devices. These controls have to include, for instance, requirements for the official use of private mobile devices, the obligation to report suspected misuse and loss of a device, or rules for backup, restore, and virus protection.

☑ Implement a policy and supporting security controls to manage the risks introduced by teleworking. In addition, conclude individual agreements with the employees on teleworking. "They shall regulate the object of work, the working time, the classification of data, the use of the organization's specific IT applications, the revocation of authorizations, the return of equipment at the end of telework, checking and monitoring the security of the teleworking place, and insurance matters." (Kersten et. al., 2016, p. 110)

## A.7 Human Resource Security (Avg. Maturity Level: 3.3)

Compared situation at the universities:

According to the public administration, the recruitment and resignation processes are regulated. Information security obligations or personal responsibilities, primarily of executives, are weak points in general. Information security training is rarely offered and is not mandatory for all university members.

Proposals for action:

☑ Ensure that all employees and students agree to the terms and conditions concerning information security. Determine their and the universities' responsibilities in contractual agreements, for example, in an obligatory way with the students' matriculation. This also includes the information security responsibilities and duties that remain valid after de-registration, termination, or change of employment.

☑ The university management shall inform employees and students of their information security roles and responsibilities before gaining access to confidential information or information systems, e.g., through guidelines and created information security awareness. In addition, the management need to set a good example to motivate the employees.

☑ Provide information security education and training. Establish an information security awareness program. This could be done, for example, by organizing an ‘information security day’ once a semester but also by offering a computer-based training (CBT) or a web-based training (WBT) like a mandatory ‘Moodle self-training’ with a final knowledge test for all employees. Newsletters, regular meetings, and frontal training courses are also helpful.

## A.8 Asset Management (Avg. Maturity Level: 2.6)

Compared situation at the universities:

In the majority of cases, the procedure inventory (in German: ‘Verfahrensverzeichnis’) is the only inventory of IT procedures. They are formally documented for personal data. Currently, there is not much tool support existing and no formal asset classification (exception in the authority network) is available. Information is not marked (individual exceptions for personnel files in paper form). Dealing with (information) assets is usually regulated by a user regulation. Access, transport, and destruction of information is well regulated and controlled.

Proposals for action:

☑ Identify assets, including their characteristics, that are relevant in the information lifecycle. A characteristic of an asset could be its need for security, its criticality, and if necessary, also its material value. For physical assets like hardware, it could be its installation location. For data, software, etc., it could be its storage location. For networks, it could be its individual network links. Draw up and maintain an asset inventory, such as a database, spreadsheet, webpage, etc. As already addressed in **Table 1** on **p. 1**, the lifecycle of information includes the information state of creation, processing, storage, transition, and destruction. Therefore, a change management would be useful to monitor the fast change processes and to update the asset inventory.

☑ On management approval, determine an owner, a responsible person, or an entity for each asset maintained in the inventory. The owner is also an asset characteristic.

☑ Inform employees and students who use or have access to university assets about the information security requirements and their associated assets, for example, by clear instructions for the usage. This also includes the full return of assets after completion of the work or studies at the university.

☑ Classify information by a consistent classification scheme with protection levels. These levels should be assessed by analyzing the security goals of the information. The goals, such as the CIA triad, were already discussed in the introduction: **1.1 Information Security**. An example would be the classification of applications and data according to the protection requirements of the 'BSI – IT-Grundschutz'. Draw up a classification policy.

ℹ The BSI standards support the ISO/IEC 27000-series. They are freely accessible under the following link:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

ℹ A sample classification policy for universities can be downloaded under the following link:

https://www.hs-augsburg.de/Binaries/Binary25111/Richtlinie-Klassifizierung-template-20180131.docx?mode=download

☑ Label classified information and its related assets in physical and electronic formats and draw up procedures for handling, processing, storing, and communicating information consistent with its classification. For printouts, the class can be used as a header line in any page or be indicated by a stamp. For data in form of files, the class belongs to the meta data. If such a scheme is to be introduced, the number of classes or classifications should not be too large, since this would make it more difficult to distinguish the levels or classes consistently. This would also lead to a more difficult the access control (*control clause A.9*).

☑ Implement and document procedures for the management of removable media in accordance with the classification scheme. This includes, e.g., making contents of any re-usable media that are to be removed unrecoverable, storing of all media in a safe and secure environment, and copying especially important data to separate data carriers.

## A.9 Access Control (Avg. Maturity Level: 3.5)

Compared situation at the universities:

Access to applications is well regulated and, with a few exceptions, controlled via a central identity management (IdM). Access control policies do not exist. Many aspects are regulated informally or in minutes of meetings. The IdM solutions are very different and well solved.

Individual improvements could be addressed during the audits. The allocation process is often automatized. Only in the case of two universities, there is an irregular request by the specialist departments to check the validity of the rights or accounts. At nearly half of the institutions, the high level of automation or temporary accounts support the correctness of the database. Privileged accesses by functional accounts are regulated well. Apart from two exceptions, passwords are not changed regularly and are often a few years old. Only one university uses higher access protection for identification. Even the most sensitive information is only protected by passwords. The network segmentation is documented, and the transitions are regulated. Firewalls or next-generation firewalls (NGFW) are often used.

Proposals for action:

☑ Establish, document, and review an access control policy based on the business and information security requirements. The policy should determine how the authorization assignment has to be carried out in practice. This includes the application, allocation, modification, and remove of authorizations. By the comparison of the users (employees, professors, and students) and the assets, the authorizations are assigned. "In principle, it should be considered whether to pursue an open strategy ('everything is permitted that is not explicitly prohibited') or whether to proceed restrictively ('everything is prohibited that is not explicitly permitted')." (Kersten et. al., 2016, p. 124)

☑ Draw up a policy that concerns the use of networks and network services. The policy should include the networks and network services that are allowed to be accessed, the authorization procedures, and the management controls and procedures to protect the access. The means used to access, the user authentication requirements, as well as the monitoring of the use of network services in accordance with the access control policy are also part of the policy.

☑ The access rights of the users need to be reviewed by the asset owners at regular intervals. This could be done at the beginning of each semester. Remove the access rights of persons after they have finished their work or studies.

☑ Regulate and document rights to execute utility programs on university-owned computers. It should only be possible to use or install utility programs or tools that are actually required for the application purpose. The access to source code has to be strictly regulated to prevent manipulation. "A particularly interesting target for attacks is the changes to software libraries, because they usually affect a wide variety of programs and applications." (Kersten et. al., 2016, p. 136)

☑ Perform a rights verification in critical sensitive areas of the administration (students' grades, budget), in the active directory, and in the university online portal.

ℹ To regulate the secure use of passwords, the BSI provides detailed information:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html

## A.10 Cryptography (Avg. Maturity Level: 2.5)

Compared situation at the universities:

There is no policy for using encryption technology. Connections are only established via insecure protocols in exceptional cases. Certificates from the DFN or the government network are used. These certificates are partly used for encrypted mail dispatch.

Proposals for action:

☑ Develop and implement a policy on the usage of cryptographic controls for the protection of information. In addition to this policy, it would be useful to develop a cryptographic concept and to identify a responsible body, role, or person who is particularly well versed with the subject. Among other things, it must be taken into account in which cases cryptography is useful (compared to the effort), where cryptography should be applied, and which procedures to follow.

☑ Develop and implement a policy on the usage, protection, and lifetime of cryptographic keys through their whole lifecycle. It would also be useful to merge this policy with the policy on the use of cryptographic controls. This topic requires specialist knowledge, possibly with external support, since the topic is only discussed superficially in the ISO/IEC standards.

## A.11 Physical and Environmental Security (Avg. Maturity Level: 3.9)

Compared situation at the universities:

The access protection and the building protection are regulated in individual departments. The access to the IT service center is protected. There are records for maintenance condition to buildings, but not to the technical rooms or to the IT service center.

The infrastructure supply (electricity, air conditioning, telecommunications) is not always secured redundantly or without interruption. Burglar alarm systems are rarely installed. Uniform standards for the IT service centers and a general description of the security controls per security zone are missing. At two universities, the IT service centers are directly accessible from public areas and only secured by a lock. In general, the physical security is well established under the special circumstances of public institutions.

Proposals for action:

☑ Classify the different types of premises, such as offices, laboratories, printing and copying rooms, utility rooms, public spaces, or lecture rooms. Develop specific physical protection controls for each class. Assign access authorizations according to the least privilege principle. If students or employees want to access certain rooms, they have to lodge an application, for example, for the activation of their campus card for these rooms.

ℹ A sample application form can be found under the following link: https://www.hs-augsburg.de/Binaries/Binary24545/Antragsformular.pdf

☑ Maintain lists of the output or return of devices, data media, and documents. These lists can also be kept in connection with the inventory list. At least, carry out random checks to monitor compliance with the regulations.

☑ Verify all items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten in advance to disposal or re-use. Delete, overwrite, or destroy the information otherwise (e.g., shredding the storage media by a certified disposal company). Encrypting a storage medium also makes the disposal easier, since unauthorized persons cannot use the encrypted data without the key.

☑ Adopt a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities. “The activating of a password-protected screen saver would be the minimum requirement—or even the switching off of the computers and/or the locking of rooms. Separate printer rooms (departmental or floor printers) and copy stations involve the problem that printed or copied documents often remain unattended in the devices for long periods of time. This problem actually calls for the ‘clear printer policy’.” (Kersten et. al., 2016, p. 149) Another solution would be printers with PIN codes or printers that only print when the campus card is inserted or held in front of them.

## A.12 Operations Security (Avg. Maturity Level: 3.3)

Compared situation at the universities:

The documentation is incumbent upon the responsible administrators. Operating procedures are rarely documented formally in operating manuals. Improvements are carried out as quickly as possible according to the administrators. The administrators' knowledge is decisive for the IT security of the IT systems. For significant changes, procedures and consequences are discussed in meetings (formal/schematic risk assessment is missing) and recorded in protocols. During tests, system functions are checked according to the administrators and changes are released. Change management, capacity management, and the separation of system environments are regulated. Only specifications and formal descriptions are missing. Uncertain log data, which is not determined on the basis of a risk assessment, is available. Due to the manageable size of the teams at the universities, existing protocols are not stored in a tamper-proof manner and are not sufficient to guarantee complete accountability of the administrators. Often, the ability for improvement depends just on individuals. Only a quarter of the investigated universities use vulnerability scans to detect errors. A regular or structured process is not implemented anywhere. In most cases, the vulnerabilities are tracked via a ticket system, such as OTRS (Open Technology Real Services, originally: Open-Source Ticket Request System) or Zabbix. The respective administrators are responsible for the system. The services on the systems are limited to a minimum. Improvements are developed independently.

Proposals for action:

☑ Document operating procedures as computer start-up/close-down procedures, backups, equipment maintenances, and media handlings. Make the documentations available to all users, e.g., by publishing them on the university website or in printed form.

☑ Produce, keep safe, and regularly review event logs that record user activities, exceptions, faults, and information security events. Also record unsuccessful logs and access attempts. “Records shall contain the data that is relevant and necessary for the intended evaluation and analysis. For example, in order to trace user activities back to individuals, the user ID, the date and time of an activity, the location of the activity [...], and the type of the activity have to be recorded.” (Kersten et. al., 2016, p. 157) Provide sufficient personnel for manual evaluation, even if some log records can be evaluated automatically.

Choose time intervals for the evaluations in such a way that the damage caused by undiscovered incidents only leads to tolerable losses.

☑ Protect logging facilities and log information against tampering and unauthorized access. They shall not be restricted selectively, temporarily disabled, or interrupted without detection. Implement and carry out technical controls (e.g., electronic signature of data records) as well as organizational controls (e.g., the dual control principle).

☑ Log, protect, and review system administrator and system operator activities regularly. For this purpose, an intrusion detection system (IDS) or intrusion prevention system (IPS) could be implemented that is managed outside of the control of system and network administrators.

ℹ An IDS and IPS provider market overview can be found under the following link: http://2014.kes.info/archiv/online/08-2-058.htm

☑ Obtain information about technical vulnerabilities of systems being used in due time, evaluate the university's hazard, and take appropriate measures to address the associated risks. The asset inventory of '*control clause A.8*' should be used in order to not oversee any systems. Specific information that is needed to support technical vulnerability management includes the software vendor, version numbers, the current state of deployment, and the person(s) within the university who are responsible for the software. Define and establish the roles and responsibilities which are associated with technical vulnerability management, including monitoring and risk assessment of vulnerabilities, patching, asset tracking, and coordination responsibilities. Identify information resources and define a timeline to react to notifications of potentially relevant technical vulnerabilities. Use own know-how as well as know-how of third parties, for example, know-how of experienced consultants, the respective system manufacturer, CERTs (Computer Emergency Response Teams), or other relevant authorities and associations. If software vulnerabilities occur, patches or new releases should be applied, or configuration settings need to be changed.

ℹ Concrete contact addresses and areas of responsibility of German computer emergency response teams and providers can be found under the publicly accessible directory of the 'Trusted Introducer Service':
https://www.trusted-introducer.org/directory/teams.html#url=c%3DDE%26q%3D

ℹ Among them, the ‘Bayern-CERT’ and ‘DFN-CERT’ are listed:
https://www.lsi.bayern.de/staatsverwaltung/index.html
https://www.dfn-cert.de

☑ The control ‘*A.12.7.1 Information systems audit control*’ has not been evaluated because no official audits by accredited certification bodies are planned at the universities yet.

## A.13 Communications Security (Avg. Maturity Level: 3.5)

Compared situation at the universities:

Network concepts exist and are managed centrally. Only one third of the universities has defined a formal policy for the transfer of information that refers mainly to the network design. For the transmission of confidential information via e-mail, certificates of the DFN or the Bavarian administration are mostly used.

Proposals for action:

☑ Implement a formal transfer policy as well as procedures and controls to protect the transfer of information through the use of all types of communication facilities. Information transfer includes many different types of communication, such as e-mail, telephone, fax, video transmission, or software transmission via the internet. It needs to be developed:

- procedures to prevent the transmitted information of being intercepted, copied, altered, redirected, or destroyed;
- detection procedures for the protection against any transmission of malicious software, for example, via the e-mail attachment;
- procedures to raise awareness of employees and students in dealing with proper information transmission, e.g., warnings of chain letters that must not be opened and forwarded;
- and procedures to use encryption technologies (see *control clause A.10*).

Also consider the other adopted policies, such as the access control policy (*control clause A.9*) and the specifications of information classifications (*control clause A.8*), because they already define information and data groups of different sensitivity, access rules, and authorizations. These rules shall also apply accordingly to the information transfer.

- ☑ Establish agreements on the secure transfer of business information between the university and external parties. These include, among other things, the management responsibilities for controlling and notifying transmission, dispatch, and receipt as well as procedures to ensure traceability and non-repudiation. The agreements should take the form of an official contract in electronic or paper form.

### A.14 System Acquisition, Development and Maintenance (Avg. Maturity Level: 3.1)

Compared situation at the universities:

Systems are set up in a standardized way and there is hardly any support of formalized criteria or guidelines for secure configuration. Concrete security requirements are not defined, not even in cooperation with third parties (‘Onlineverwaltungsserver HIS Online-Portal’ or ‘PRIMUSS’). Changes are carried out and tested independently and documented generally. There are not many in-house developments of software (campus management systems). No regulations or training courses for secure software development are known.

Proposals for action:

- ☑ Apply the InfoSec requirements also to new information systems and existing information systems that are being improved. Take all security requirements and properties into account, right from the planning and specification stages since it is difficult to implement necessary security afterwards (time delays, high costs, and reduced security). Create a security concept for new information systems and existing information systems that are being improved. The concept should include the purpose of use, the presentation of the operational environment, a risk assessment, a weak point analysis, the derivation of security controls for risk reduction, and the determination of remaining risks. (cf. Kersten et. al., 2016, p. 172)
- ☑ The control ‘*A.14.1.3 Protecting application services transactions*’ has not been evaluated because no relevant transactions of application services exist at the universities.
- ☑ The controls of the main security categories ‘*A.14.2 Security in development and support processes*’ and ‘*A.14.3 Test data*’ were evaluated only rarely or not at all because the universities as research institutions mostly only develop software and systems in research projects. Nevertheless, proposals for the few negatively evaluated controls are presented hereafter.

☑ Draw up a policy for secure development if new software and systems are developed at the university. This policy should include the security of the development environment, the security of the software development lifecycle, the security requirements in the design phase, security reviews, secure repositories, required application security knowledge, and secure programming techniques.

☑ Establish, document, maintain, and apply principles for engineering secure systems. Examples of such principles are the isolation and separation of security functions from the insecure rest of the system, keeping the size of software small (no large, unmanageable software), code transparency, and the separation of sensitive and non-sensitive data. "Such principles should be documented in a developer's guide and applied to every project. These principles have to be reviewed from time to time to ensure that they are still up to date—so, that their application is still state-of-the-art." (Kersten et. al., 2016, p. 180)

### A.15 Supplier Relationships (Avg. Maturity Level: 3.4)

Compared situation at the universities:

Additionally purchased services are regulated by the DFN or in framework agreements (order data processing agreements).

Proposals for action:

Since the universities as state institutions maintain a manageable number of supplier relationships and regulations with the DFN already exist, the controls of this superordinate security control clause were almost not evaluated (6 out of 60 possible results). However, in order to meet the control objectives and to ensure information security in supplier relationships further on, it is useful to classify and list all suppliers with their respective fields of activity, to conclude clearly defined contracts with them, and to draw up a policy for protecting information assets from suppliers. This policy should include all relevant information security requirements in terms of reducing the risks associated with suppliers' access to the university's assets, such as processes for monitoring compliance with the specified agreements, awareness training for dealing with suppliers, and procedures for supplier changes.

### A.16 Information Security Incident Management (Avg. Maturity Level: 2.2)

Compared situation at the universities:

Security incidents are not defined explicitly and are treated situationally. Usually, there is an e-mail address available for the incident capture and best practices that help with recovery and correction. 70% of the universities use a ticket system to track incidents. The documentation is also carried out by the ticket system. Occasionally, there is an incident management report on the status of incidents which is sent to the university management. Cooperation with authorities is regulated. If there is time, findings from incidents are reported back and flow into the administrators' daily work.

Proposals for action:

Initially, it is helpful to consider the terminology of various types of security events with regard to the information security incident management. **Figure 11** shows the relation between different security events and their increasing impact on the information security goals.

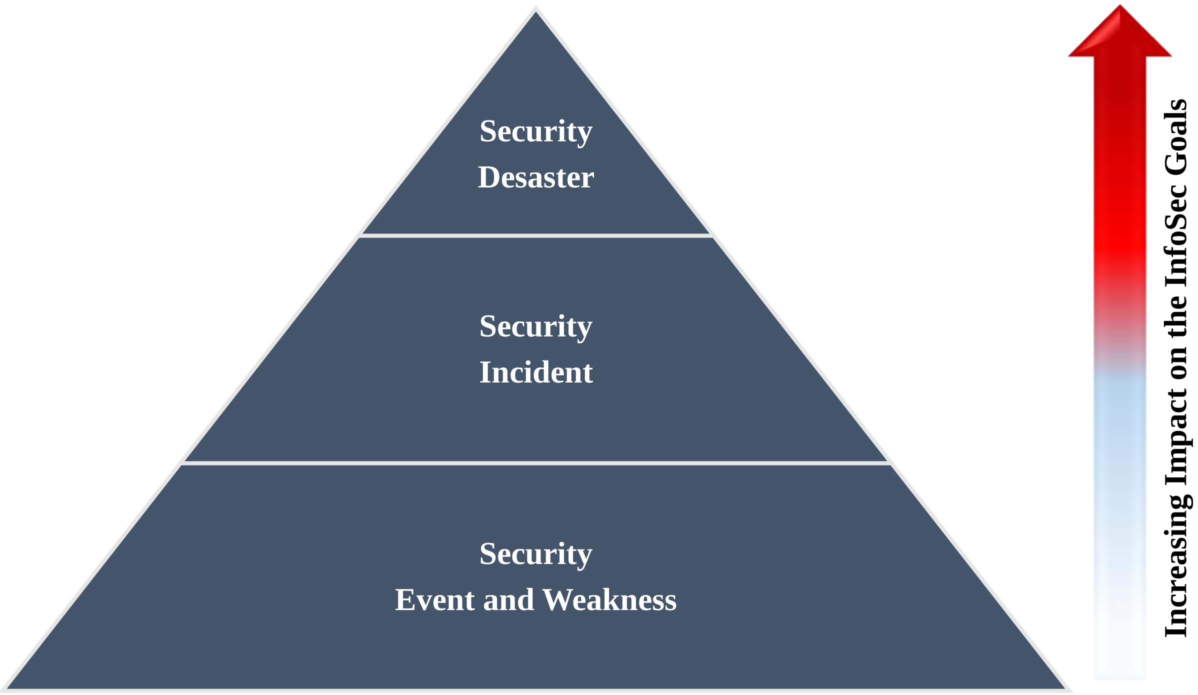


**Figure 11:** Security Events in Relation to their Impact on the Information Security Goals

(Source: Own illustration)

If security events and weaknesses occur, it is assumed that they impair the information security. But it is not yet clear whether they could result in damage to the organization or not. They have the lowest potential for damage and require further assessment.

In contrast, a security incident is an event that is highly likely to be detrimental to the security goals of the organization or has already caused corresponding damage. An assessment has already been carried out.

The worst conceivable event is a security disaster. It has serious or even catastrophic impacts, such as a complete system shutdown. This distinction of terms is important in the further course of the work.

☑ Establish management responsibilities and procedures to ensure a quick, effective, documented, and consistent response to information security incidents. These include:

- procedures for planning and preparing response to incidents;
- procedures for monitoring, detection, analyzing, and reporting;
- procedures for logging incident management activities;
- procedures for handling of forensic evidence;
- procedures for assessment and decision making;
- and response procedures.

An issue tracking system, also called incident ticket system (ITS), facilitates the procedures for tracking and documenting incidents.

ℹ The following link provides a good comparison of issue tracking systems (ITS): http://www.comparisonofissuetrackingsystems.com

☑ Make all employees aware of their responsibility to report information security events and weaknesses as quickly as possible. Provide contact persons and contact addresses easy to find, for example, on the university website. How to report properly can be taught in training courses. These could be offered every semester. Situations that need to be considered for information security event reporting include ineffective security controls, breaches of information integrity, confidentiality or availability expectations, human errors, non-compliances with policies or guidelines, breaches of physical security arrangements, uncontrolled system changes, malfunctions of software or hardware, and access violations.

☑ Define a classification scheme with levels of criticality for security events that is used for the assessment of and the decision on information security events and weaknesses. The criticality levels "serve to prioritize the processing steps: The higher the criticality, the more urgent it is to deal with the case—an important rule if, for example, several notifications arrive practically simultaneously" (Kersten et. al., 2016, p. 192). The risk classification has to be documented.

☑ Learn from information security incidents and evaluate them to reduce future risks to the university. With regard to the amount of damage, also "record data on the effort, duration, costs of processing, and possible consequential damage for each incident" (Kersten et. al., 2016, p. 193). Create a regular report on the status of incidents, for example every semester, and submit it to the university management.

☑ The control '*A.16.1.7 Collection of evidence*' has not been evaluated. For the purpose of disciplinary and judicial proceedings, the universities should develop and follow internal procedures for handling evidence. During the identification, collection, acquisition, and preservation of evidence, "care must be taken to ensure that any left traces that may provide information about the causes, authors, and the course of events are not destroyed or falsified by the processing of the incident or other causes" (Kersten et. al., 2016, p. 194).

ℹ A number of ISO/IEC standards provide detailed guidance on information security incident management. The standards and their applicability to the examination process classes and examination activities are shown in **Figure 12**, **Annex**, **p. 100**.

### A.17 Information Security Aspects of Business Continuity Management (Avg. Maturity Level: 1.2)

Compared situation at the universities:

There is no regulated business continuity management (BCM) process (emergency management) implemented and a business impact analysis (BIA) for IT emergencies is missing. Essentially, in an emergency, the systems are attempted to be completely restored. A limitation of information security aspects is not given because critical systems are designed redundantly. These redundancies are not based on requirements from the departments (due to an IT impact analysis) but according to the specifications and budget of the IT service center managers.

Proposals for action:

☑ Determine the requirements and the continuity of information security management in adverse situations, e.g., during a crisis or disaster. If requirements have not yet been implemented in any BCM process or disaster recovery management process, it should be assumed that information security requirements remain the same in adverse situations compared to normal operational conditions. In addition, clarify whether other (e.g., higher) requirements for the maintenance of information security and the information security management are required in adverse situations than in normal operational conditions. For this purpose, compile possible adverse situations for the university, like the failure of important IT support (e.g., cloud service, service provider) or of important IT applications (e.g., management server of the students' grades). Identify the need for confidentiality, integrity, availability, and other security goals in these situations in order to maintain information security and the functioning of the information security management.

☑ Develop an adequate management structure for the preparation, mitigation, and response to disruptive events. Incident response personnel with the necessary responsibility, authority, and competence should also be determined. Develop and approve documented plans and response and recovery procedures that describe in detail how the university is going to manage a specific disruptive event. Provide regular training and education to teach and practice the use of these plans. In order to limit the effort, perform a BIA to identify and analyze critical university processes that can cause high damage.

☑ Verify the established and implemented information security continuity controls at regular intervals and after changes of the requirements for information security. This ensures that the information security continuity controls are valid and effective during adverse situations. A regular review could take place every semester.

ℹ The standards ISO/IEC 27031, ISO/IEC 22313, and ISO/IEC 22301 provide detailed guidance on business continuity management systems.

## A.18 Compliance (Avg. Maturity Level: 2.7)

Compared situation at the universities:

The regulations of the applicable legislation, especially of the BayDSG (Bayerisches Datenschutzgesetz) and the protection of the intellectual property rights, are generally well regulated. An independent verification of information security is carried out by the 'zentrale Stabstelle Informationssicherheit'. Due to the lack of policies, compliance with this verification cannot currently be checked. At the twelve evaluated universities, only three technical security tests have been carried out in recent years to verify and identify vulnerabilities. Only two universities examine their systems tool-based on a regular basis.

Proposals for action:

☑ Collect, document, and update all relevant legislative, regulatory, and contractual requirements as well as the specific controls and individual responsibilities to meet these requirements regularly. The requirements include but are not limited to laws (e.g., BayEGovG), data protection regulations (e.g., BayDSG), crypto regulations, and software copyright and license regulations.

☑ To protect intellectual property rights, indicate any existing license rights for each asset in the asset inventory and refer them to the applicable policies or guidelines. Raise awareness and train employees and students on copyright protection and the university's existing policies.

☑ Protect records from loss, destruction, falsification, unauthorized access, and publication in accordance with the legislative, contractual, and business requirements. Create a list and categorize records into record types, e.g., database records or audit logs. Also list details of the retention periods, the type of allowable storage media (e.g., paper or optical), and the cryptographic keys and programs if applicable. Publish guidelines for the retention, storage, handling, and disposal of records and information.

☑ Note that the legal and regulatory situation for cryptographic controls varies from state to state. This is important for the import, export, and use of cryptographic functions and encryption technologies. Create a table with the legal requirements and apply them accordingly. In addition, legal advice could be sought.

☑ The university management should arrange for an independent review of the university's approach to handling information security periodically or after significant changes.

An independent review may be carried out by internal auditors of the university who are not involved in the test object; by commissioned external auditors, individuals, or an entire team. “The classic rule is that audits concerning compliance with ISO 27001 should be carried out (at least) once a year.” (Kersten et. al., 2016, p. 207)

☑ The responsible persons have to check compliance with security policies and guidelines and other security requirements in their area of responsibility on a regular basis. “The type of inspection is left to each responsible person. These can be on-site inspections at critical points, technical audits, evaluation of records that have been kept by special monitoring tools, checking configuration files, etc.” (Kersten et. al., 2016, p. 207) The responsible persons have to archive and record the results.

☑ Apply automated tools to review compliance with technical specifications. The results have to be interpreted by technical experts. Manual checks can also be performed. Plan and document tests that could affect the system security, such as penetration testing and vulnerability assessments.

☑ The compliance results should be submitted in an information security report to the university management.

ℹ The standards ISO/IEC 27007 and ISO/IEC TR 27008 provide specific guidance for carrying out the independent review and the technical compliance review.

(cf. Kersten et. al., 2016, pp. 99–208)

## ISMS REQUIREMENTS (ISO/IEC 27001)

### 4 Context of the Organization (Avg. Maturity Level: 2.4)

Compared situation at the universities:

Clear information security objectives or critical areas in the environment have been hardly defined by the university management. Only the regulatory requirements and needs are known. An intact standard-compliant ISMS is not operated at any university.

Proposals for action:

☑ Determine all issues that affect the purpose, task, or activity of the university and may have an impact on its security.

Review the external and internal environment to identify relevant external and internal issues. Compose all relevant information (documents, notes, protocols in written or electronic form).

☑ Establish the scope of the ISMS with its boundaries and applicability. The scope can include one or more specific processes, functions, services, sections and locations, an entire legal entity, and an entire administrative entity. “There should be no attempt to marginalize the scope of application as small as possible—an approach that is often chosen in order to achieve a certification quickly.” (Kersten et. al., 2016, p. 19) The scope has to be defined in writing.

☑ Establish, implement, maintain, and improve the ISMS continually by means of the PDCA cycle (see **Figure 2** and its procedure on **p. 2**). The PDCA approach is no longer mandatory according to the newest version of the ISO/IEC 27001 standard but still highly recommended.

## 5 Leadership (Avg. Maturity Level: 2.1)

Compared situation at the universities:

Only a few university managements have already dealt with the topic of information security in such a way to establish a goal-oriented organization that takes on the tasks of strengthening information security. At some universities, security policies are in the drafting stage or not treated any further by the management. Only at one university, a policy was developed as a 'matter of the boss' and clear specifications were defined for further development. Policies are limited to user orders, teleworking, and, occasionally, network security. General IT service center documentation is available in a more or less structured form. However, it does not have a policy character. Many parts of this documentation could be used as a template for the ISMS. Organizationally, roles and committees have been defined everywhere. Occasionally, these are already well established. The scarcity of resources (persons and time) is generally considered (especially at the universities of applied sciences) to be the largest problem. Therefore, the area of IT security (technical controls) is pronounced best in the It service centers. Comprehensive organizations that cover administration, research, teaching, and support to the supreme managements are the exception.

Proposals for action:

☑ As top management, the university management has to demonstrate leadership with respect to the ISMS. Its tasks include setting up and operating an appropriate ISMS with sufficient resources, establishing and enforcing an information security policy, and motivating and supporting all involved persons to contribute to security; improving the ISMS continuously, discharging existing responsibilities properly, and integrating information security into all business processes. Most of the tasks can be delegated to responsible persons and bodies. However, the management's obligatory tasks are to put an information security policy into effect, to initiate all tasks, to motivate and support, and to control the results.

☑ As already discussed in '*control clause A.5*', the university management has to define and document an information security policy. The policy has to be made familiar to the target group, for example, by training courses. The target group includes those affected by the security controls, e.g., the university's employees.

☑ The university management has to ensure that the roles, responsibilities, and authorities that are relevant to information security are assigned and communicated. These include security officers and representatives, asset managers, process owners, IT emergency managers, backup managers, and compliance managers; an ISO 27001 compliance and monitoring officer and a person who is responsible for preparing reports on the performance and effectiveness of the ISMS and submitting them to the top management. All roles and responsibilities have to be made familiar within the organization.

## 6 Planning (Avg. Maturity Level: 1.0)

Compared situation at the universities:

The general handling of information risks is partly documented in procedural directories and is thus limited to the implementation of the BayDSG. Formal, schematic, and comprehensible evaluations and proactive treatment plans are scarce or non-existent. The dealing with risks is informally and ad hoc. Controls are defined and implemented situationally. There are hardly any concrete information security requirements from the departments for the service centers. The most frequently pursued security objectives are the availability and confidentiality of personal data.

Concrete information security objectives with responsibilities, metrics and indicators, or the evaluation of what has been achieved are not documented. At this point, there might be the danger that there is too much done (for availability) in some places than it is actually needed.

Proposals for action:

☑ Determine risks and opportunities in order that the ISMS achieves its objectives, avoids undesirable effects on operations, and is improved continuously. Record ISMS conditions and expectations, e.g., in tabular form, and compare them with corresponding controls. Update the table regularly and check its compliance and effectiveness. Determine possible risks (risk assessment), define and implement suitable controls (risk treatment), and check their effectiveness (risk evaluation). For this purpose, the information assets need to be captured and kept up to date (see *control clause A.8 Asset management*). The ISMS can be improved continuously according to the PDCA model. "It hast to be planned, prepared, communicated, and put into practice." (Kersten et. al., 2016, p. 23) Document the planning. Create an ISMS guideline or ISMS description.

☑ The risk assessment shall include a comparison between the selected controls and the controls listed in Annex A, so that important aspects and controls are not overseen. In practice, create a table that includes the existing or planned measures for each control. "Decisions on what is or is not implemented, or whether individual controls are not applicable, have to be substantiated accordingly. Strictly speaking, this procedure has to be applied to each asset or group of similar assets." (Kersten et. al., 2016, p. 26) This results in the Statement of Applicability (SoA), a comprehensive table of controls, options, and actions.

ℹ ISO/IEC 27005 (information security risk management) contains specific guidelines and detailed information for the entire information security risk management process.
The risk management process is shown in **Figure 5**, **Annex**, **p. 99**.

☑ Assign roles and hierarchy levels to achieve specific security objectives and communicate them. "It is important to assign each role or level to the implementation in a precise and formal way by specifying the objectives and control, the resources available, the deadlines, etc. The relevant (written) instruction has to be kept, and used again in the subsequent review or evaluation of the results." (Kersten et. al., 2016, p. 23)

## 7 Support (Avg. Maturity Level: 1.7)

Compared situation at the universities:

Currently, the information security officers can only perform their tasks to 10–20%. Awareness programs covering the entire university have not been launched, however, information events are offered in isolated cases. For the university employees, there is no obligation in any university to participate in such training courses. Information security specific documents as policies or user rules have been created in some cases and structured approaches are used occasionally.

Proposals for action:

☑ The university management has to provide the necessary resources for the life cycle (PDCA cycle) of the ISMS. These include personnel, processes, expertise, organizational tools, training, testing, infrastructural and technical resources, as well as review procedures. In addition, resources have to be considered that are necessary for the implementation of the controls which are documented in the SoA and not yet implemented.

☑ Appropriate competences (knowledge, experience, and practice) have to be identified and documented. They have to be made available, checked, and if not available, built up through training and counselling. The university management has to delegate the tasks of information security to at least two full-time information security officers (one person for administration and one person for research and teaching) and need to be informed about the current situation in order to be able to bear their responsibility.

☑ Impart university policies and guidelines, but also disciplinary and warning procedures in cases of non-compliance to all university members. This can be realized by means of briefings, awareness programs, events, or computer or web-based training. Set up an information platform with important security information, reports on incidents, upcoming audits, events, programs, and training and education offers.

☑ Define communication relationships, e.g., between the security management and the university management. Create a table to determine who communicates with whom, on what topics, on what occasions, and in what form. According to Kersten et. al (Kersten et. al, 2016, p. 29), typical communication forms are:

- unilateral, targeted dissemination of information (e.g., report from the security management to the university management);

- broad dissemination of information (e.g., publishing security information on the university website);
- participation and co-signature procedures (e.g., adoption of a policy or guideline);
- and gathering information (e.g., requesting CERT information).

☑ Capture all documented information (reports, data, concepts, protocols, proofs, lists, policies and guidelines) as part of the ISMS and make them available for evaluations. Label the documents precisely (author, date, version, reason for change, etc.) and select a suitable format (text, graphics, audio, video, etc.) and medium (paper or other data carriers) for information storage. Ensure the availability of the documents, the suitability for its intended recipients, protection against unauthorized access and loss, and the control of changes by appropriate controls and processes (e.g., by target-oriented document presentation, encryption, access protection, backup and archive procedures, creation of version history, and review procedures).

## 8 Operation (Avg. Maturity Level: 0.5)

Compared situation at the universities:

There are no specifications for assessing or controlling risks. Risks in IT are treated informally (best practice) and controls are implemented. Other risks are limited to individual cases (e.g., amok run or bomb threat).

Proposals for action:

Fulfill all relevant (legal and contractual) requirements by planned measures. Perform (e.g., once a semester and after significant changes) a regular risk assessment with risk identification, analysis, and evaluation; and a risk treatment with possible actions, measures and acceptance of the remaining risks subsequently. Implement all risk-reducing actions and measures of the risk treatment. Plan, document, and archive all steps carefully including deadlines, personnel, finances, resources, difficulties, and problems.

ℹ ISO/IEC 27005 (information security risk management) contains specific guidelines and detailed information for the entire information security risk management process.
The risk management process is shown in **Figure 5**, **Annex**, **p. 99**.

## 9 Performance Evaluation (Avg. Maturity Level: 1.1)

Compared situation at the universities:

Due to the lack of an ISMS, a performance evaluation is not possible. The individual audit reports of the audits carried out are often the first reports to the university managements on the state of information security.

Proposals for action:

☑ Determine which university areas or indicators need to be monitored and measured in order that the information security performance and the effectiveness of the ISMS can be analyzed and evaluated. Assign roles and responsibilities that are able to perform the monitoring, measurement, analysis, and evaluation processes and operate appropriate measuring equipment and methods. Document and archive all activities and results. Define how often and at what time measurements and their evaluation need to be carried out.

☑ Perform independent internal audits by external auditors or internal auditors who are not involved in the test object. Set up an audit management program or table that includes the various audits with their test object, frequency, personnel, reporting, and documentation. Generate an audit schedule and an audit report for each audit.

☑ The university management has to regularly review the ISMS at scheduled intervals. This also includes the assessment of received reports, e.g., on measurement and risk assessment results, and deciding on possible actions and necessary changes.

ℹ **Research question 2** and **research question 3** of this master thesis focus on the ISMS requirement ‘*9. Performance evaluation’*. For this purpose, the standards ISO/IEC 27004 and ISO/IEC 27014 are consulted additionally.

(cf. Kersten et. al., 2016, pp. 17–37)

## 10 Improvement (Avg. Maturity Level: 1.2)

Compared situation at the universities:

Due to the lack of an ISMS and of suitable specifications or policies, improvement processes are not formally planned.

Proposals for action:

Regarding to the current status of the ISMS, proposals for action on the improvement are not functional. First, the previous ISMS requirements and controls have to be pursued and fulfilled.

## 3.6. Results and Discussion

The evaluation of the audit results and the comparative analysis have shown that the twelve Bavarian universities are currently in the planning and doing phase of an ISMS. Many similar information security controls and processes have already been realized at the Bavarian universities, but in contrast to larger organizations that provide far more personnel, money, and working time to pursue the goal of implementing an ISMS, the universities' ISMS implementation only depends on a manageable number of persons, who work on improving information security in addition to data center operations. As a result, the security of IT and data center operations have already been well-implemented, however, systematic and organizational requirements, such as policies and guidelines, risk management, and business continuity management, are almost non-existent.

The elaborated proposals for action are intended to facilitate and support the universities' ISMS build-up phase. They serve as a guidance to review which ISMS requirements and information security controls and processes have not yet been implemented and in what way they can be realized. Due to the fact that the requirements and controls of the certification standard ISO/IEC 27001 are very general and offer a large scope of interpretation, it was necessary to work with further guidelines and recommendations. The explanations in the ISO/IEC guideline standards and in books are very extensive. They had to be applied to the universities' unfulfilled ISMS requirements and controls, and were formulated in key points. By the proposals for action, the universities will be able to implement their missing ISMS requirements and information security processes and profit by the comparability created among themselves. It may also be necessary to formulate own controls if certain control objectives and requirements are not reflected at a university.

Inferentially, the universities need to establish more personnel and new competences in order to be able to fulfil the many ISMS requirements, information security tasks, and proposals for action for the ISMS implementation. It would be useful to set up a Bavarian university ISMS network, that involves at least one representative of each participating university.

By the intensifying communication among each other, the implementation of an ISMS could be facilitated and improved. This would lead to less time exposure and costs as well as to a reduction of the total effort, and, above all and most importantly, to the improvement of the information security situation at all universities.

# 4. Development of an Information Security Measurement System for Universities with Metrics and Key Performance Indicators (KPIs)

As outlined in the first research question, the ISMS requirement '*9. Performance evaluation'* stipulates the evaluation of the information security performance and the effectiveness of the ISMS. As a reminder of the audit results, the requirement clause '*9.1 Monitoring, measurement, analysis and evaluation'* was the worst evaluated requirement with an average maturity level of 0.1. The fulfilment of this requirement clause offers significant benefits. These include an increased accountability for information security, an improved information security performance, improved ISMS processes, the evidence of meeting requirements, and the support of risk-informed decision-making. ISO/IEC 27004 (*Monitoring, measurement, analysis and evaluation*) provides guidelines that help to fulfill the requirements of ISO/IEC 27001, *clause 9.1*. The mapping of ISO/IEC 27001 to ISO/IEC 27004 has already been shown in **Figure 4** on **p. 11**. **Figure 13** illustrates the monitoring, measurement, analysis, and evaluation processes.

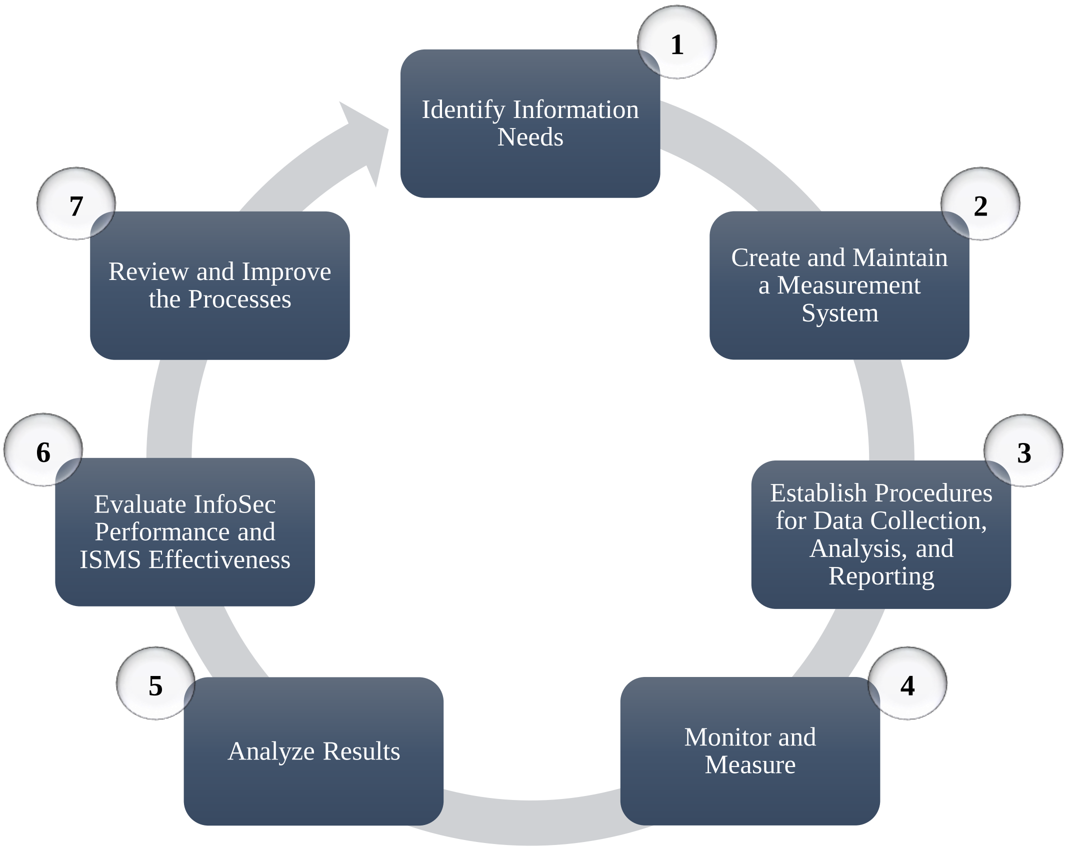

1
Identify Information Needs
2
Create and Maintain a Measurement System
3
Establish Procedures for Data Collection, Analysis, and Reporting
4
Monitor and Measure
5
Analyze Results
6
Evaluate InfoSec Performance and ISMS Effectiveness
7
Review and Improve the Processes

**Figure 13:** Monitoring, Measurement, Analysis, and Evaluation Processes

(Adapted from: ISO/IEC, 2016, p. 10)

The first step ('Identify information needs') of the cycle was covered as good as possible by the first research question. The universities' existing ISMS controls and processes were examined and listed. However, due to the current initial status of the ISMSs and the lack of controls and processes, such as the risk management process, it was not possible to prioritize them and, if necessary, to sort out some irrelevant processes for the measurement. Consequently, all measurable ISMS procedures with relevance to the universities are used for the measurement system.

The second step ('Create and maintain a measurement system') is dealt with in this chapter (second research question). A measurement system or framework is developed that the universities can use to measure the performance of their information security controls and processes. "The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements." (Chew et. al., 2008, p. 9) First, fundamentals and the usage of metrics and key performance indicators are considered. Afterwards, the approach is described and a measurement system with key performance indicators is developed that is tailored to the universities. In the last section of this chapter, the results, the further procedures and process steps (3–7) of the cycle in **Figure 13**, **p. 48**, as well as open questions are discussed.

## 4.1. Fundamentals

### 4.1.1. Scope of the Information Security Measurement System

In order to develop an information security measurement system for universities, the first question that arises is what should be measured. According to ISO/IEC (ISO/IEC, 2016, p. 5 & p. 12), "measurement can be applied to any ISMS processes, activities, controls[,] and groups of controls" and "should respond to the information need". Therefore, the information security measurement system to be developed will be geared to the measurable ISMS requirements and controls of ISO/IEC 27001, including Annex A (first research question). "Organizations should create measures once and thereafter review and systematically update these measures at planned intervals or when the ISMS's environment undergoes substantial changes." (ISO/IEC, 2016, p. 11) Thus, it is important to note that "only processes that can be consistent and repeatable should be considered for measurement" (Chew et. al., 2008, p. 10).

### 4.1.2. Types of Measures

A measure (as noun in German: ‘Messgröße’) is a “variable to which a value is assigned as the result of measurement” (ISO/IEC, 2018, p. 6). ISO/IEC 27004 defines two types of measures: performance and effectiveness measures. Whereas performance measures directly show the progress in implementing an information security process or control, effectiveness measures indicate whether a process or control operates as intended. EIs are used to derive an effect that the realization of an information security process and control has on the organization’s security objectives. “After most performance measures reach and remain at 100%, the organization should begin to focus its measurement efforts on effectiveness measures.” (ISO/IEC, 2016, p. 8) Both measures “are used to facilitate decision making, improve performance, and increase accountability through the collection, analysis, and reporting of relevant performance-related data [...]” (Chew et. al., 2008, p.viii). Usually, they are expressed in quantifiable values, so-called metrics, for example, in percent values or pure numbers.

### 4.1.3. Metrics and Key Performance Indicators

In order to avoid confusion, the terms measure, metric, and key performance indicator are differentiated as follows. Initially, “a measure is a fundamental or unit-specific term—a metric can literally be derived from one or more measures.[...] A metric is a quantifiable measure that is used to track and assess the status of a specific process.” (Taylor, 2017) Accordingly, quantifiable performance and effectiveness measures (metrics) are determined within the measurement system. In the following course of the work, these metrics are indicated as performance indicators (PIs) and effectiveness indicators (EIs).

From the PIs and EIs, “according to the significance and importance of the indicators to the organization’s purposes, key performance indicators (KPI—sometimes also referred to as ‘key success indicators’) can be identified” (ISO/IEC, 2016, p. 17). KPIs are a handful of performance and effectiveness indicators that are most meaningful for organizations. These key indicators are intended to show at a glance what the current information security situation is like and how the ISMS is performing. The characteristics of a KPI are best described by the ‘SMART’ acronym, which can be seen in **Figure 14** on the next page.

According to the acronym, a KPI has to be specific, which means that it has to be clear about what is exactly measured. Therefore, different users draw the same conclusions from one KPI. Furthermore, a KPI is measurable in order to compare the actual result with the target result.

The target result has to be achievable and important for the organization. So, a KPI is always result-oriented and should give a deep insight into relevant areas. Lastly, a key indicator is only of significance if the temporal dimension in which it is implemented is known.
(cf. Hassler, 2012; cf. Lead Light, 2018)

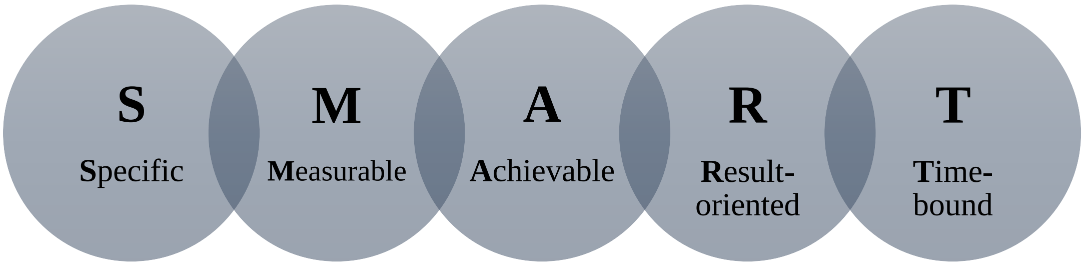


**Figure 14:** Characteristics of a Key Performance Indicator ('SMART' Acronym)

(Source: Own illustration)

## 4.2. Approach

To work on the second research question, the bottom-up approach is used as method. In doing so, performance and effectiveness indicators are defined in an information security measurement system first, from which certain KPIs are derived afterwards. This procedure has the advantage that after the implementation of the measurement system, "the individual relevant metrics can be selected pragmatically and quickly and, thus, the focus is put directly to the most important thing[s]" (Hassler, 2012, p. 295). The basic principle is illustrated in **Figure 15**.

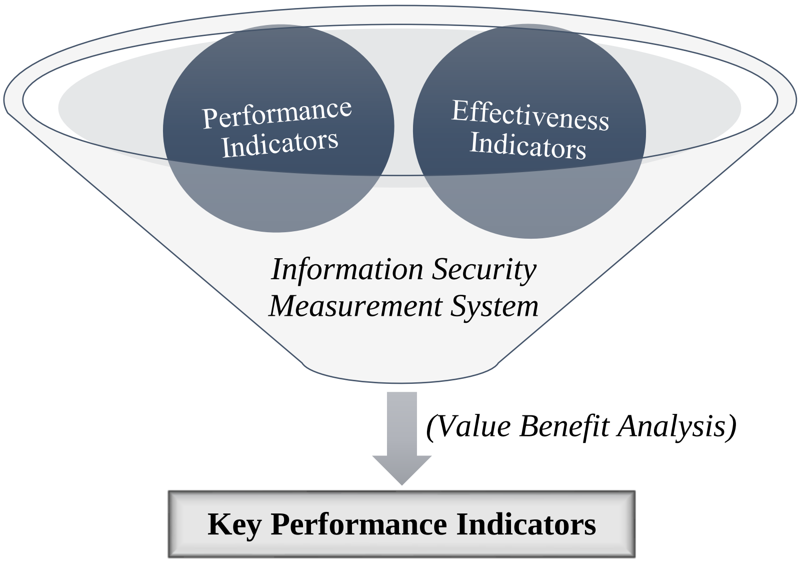


**Figure 15:** Information Security Measurement System Concept

(Source: Own illustration)

The information security measurement system consists of suitable performance and effectiveness indicators that are tailored to the universities. Inter alia, it is provided for what purpose, how often, and by whom these are measured and reported, and which information is needed. For this purpose, the adapted measurement template, which is depicted in **Table 5**, is used for each measurement. The general measurement construct examples of the standard ISO/IEC 27004 serve as the measurement basis and are applied to the universities. (cf. ISO/IEC, 2016, pp. 20–55) They are already specially adapted to the ISMS requirements and controls of ISO/IEC 27001, including Annex A, and are very useful as guidance.

**Table 5:** Measurement Template

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | Specific identifier. |
| Information need | Overarching need for understanding to which the measure contributes. |
| Measure | Measurement statement. |
| Measure Type | Performance indicator (PI) or effectiveness indicator (EI). |
| Formula/scoring | How the measure should be evaluated, calculated, or scored. |
| Target | Desired result of the measurement. (Target result) |
| Implementation evidence | Evidence that validates that the measurement is performed; helps to identify possible causes of poor results and provides input for the formula/scoring. |
| Frequency | How frequently the data should be collected and reported. |
| Responsible parties | The persons responsible for gathering and processing the measurement. |
| Data source | Potential data sources can be databases, reports, tracking tools, other parts of the university, external organizations, or specific individual roles. |
| Reporting format | How the measure should be collected and reported, e.g., as text, numerically, graphically (pie chart, line chart, bar chart, etc.). |
| ISO/IEC 27001 allocation | Relation to the ISMS requirements and controls of ISO/IEC 27001, including Annex A. |

(Adapted from: ISO/IEC, 2016, p. 13)

As a result or output of the measurement system, corresponding key performance indicators are determined from the PIs and EIs, which briefly and precisely reflect the progress and degree of fulfillment of certain important information security areas of the universities. The prioritization of the metrics by importance and, consequently, the selection of the right KPIs need to be carried out according to the university's own information security objectives and requirements. In order to facilitate the decision-making and provide guidance for the universities, it is attempted to determine the KPIs by means of a value benefit analysis with weighted evaluation criteria.

## 4.3. Information Security Measurement System for Universities

The information security measurement system for universities is built up from 23 measurement procedures that serve as a strong basis for measuring information security performance and effectiveness. Henceforth, they can be supplemented by measurements depending on the individual university’s needs. Measurement methods that do not meet the requirements can also be modified or removed.

As a result of the measurement procedures, metrics (performance and effectiveness indicators) are generated. As shown in **Figure 16**, they are not measured once and the process is completed, but they need to be monitored continuously and compared with the target measurement results. If an indicator shows undesirable results, the causes must be investigated, and actions taken if required. If necessary, the metric need to be adjusted and changed. This process for the ongoing use of metrics goes hand in hand with the steps *‘Analyze results’* and *‘Review and improve the processes’* of the monitoring, measurement, analysis, and evaluation cycle which is illustrated in **Figure 13**, **p. 48**.

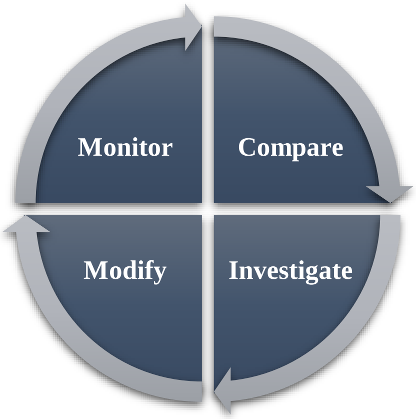


**Figure 16:** Procedure for the Ongoing Use of Metrics

(Adapted from: Hassler, 2012, p. 287)

Each measurement procedure is described in tabular form according to the measurement template of **Table 5**, **p. 52**. To provide a better overview and readability, the tables in this section have been broadened compared to the standard page width. **Table 6** shows the structure of the measurement system.

**Table 6:** Information Security Measurement System Structure

| Table | Measurement | Measure Type (Metric) | Unit | ISO/IEC 27001 Allocation | |
|---|---|---|---|---|---|
| | | | | Requirements | Controls (Annex A) |
| **7** | Resource Utilization | EI | Pure number | 5.1, 7.1 | |
| **8** | University Management Commitment | PI and EI | Pure number | 5.1, 9.3 | |
| **9** | ISMS and Information Security Awareness Training | PI | % | 7.2 | A.7.2.1, A.7.2.2 |
| **10** | ISMS and Information Security Awareness Training Effectiveness | EI | % | 7.2 | A.7.2.1, A.7.2.2 |
| **11** | Policies Review | PI | % | 7.5.2 | A.5.1.2 |
| **12** | Risk Potential | EI | Pure number | 8.2, 8.3 | |
| **13** | Audit Program | PI | % | 9.2 | A.18.2.1 |
| **14** | Improvement Actions | EI | % | 10 | |
| **15** | Security Incident Costs | PI | € | 10 | |
| **16** | Learning from Security Incidents | EI | Pure number | 10 | A.16.1.6 |
| **17** | Review of User Access Rights | PI | % | | A.9.2.5 |
| **18** | Physical Entry Controls | PI | % | | A.11.1.2 |
| **19** | Physical Entry Controls Effectiveness | EI | Pure number | | A.11.1.2 |
| **20** | Maintenance of Information Systems | PI | Days | | A.11.2.4 |
| **21** | Change Management | PI | Pure number | | A.12.1.2 |
| **22** | Malware Protection | PI | Pure number | | A.12.2.1 |
| **23** | Log Files Review | PI | % | | A.12.4.1 |
| **24** | Vulnerability of Information Systems | PI | % | | A.12.6.1, A.18.2.3 |
| **25** | Security Incident Management Effectiveness | EI | Pure number | | A.16 |
| **26** | Security Incident Trend | EI | Pure number | | A.16.1 |
| **27** | Security Events and Weaknesses Reporting and Assessment | PI | Pure number | | A.16.1.2, A.16.1.3, A.16.1.4 |
| **28** | Availability of IT Services | PI | Pure number | | A.17.2.1 |
| **29** | ISMS Review Process | PI | Pure number | | A.18.2.1 |

(Source: Own illustration)

As it can be seen in **Table 6**, the measurement procedures are sorted in an ascending order according to the clauses of the ISO/IEC 27001 requirements and controls. Fifteen performance indicators (PIs) and nine effectiveness indicators (EIs) result from the measurement system. Almost all of them are expressed in units of percentage or pure numbers. Only the ‘security incident costs’ measurement is expressed in ‘€’ and the ‘maintenance of information systems’ measurement in ‘days’. Often, the traffic light colors green, yellow, and red are used as scale for the target classification of percentage measurements. They make it easier to assess and later, during visualization, to present more clearly the extent to which interventions need to be taken (red), the indicator needs to be monitored (yellow), or the measurement result is within the optimal target range (green).

The responsible parties or persons indicated in the measurements (information security officer, the information security manager, CSIRT, CISO, CIO, etc.) are designed for the ideal case that these parties are all existent, occupied, and working together. However, since this is not the case at most universities and only a few people are responsible for information security, as the first research question has shown, this area of responsibility can or rather need to be varied by each university itself so that all measurement responsibilities are assigned.

The individual measurement procedures are depicted in the following **Tables 7–29**:

**Table 7:** Measurement: Resource Utilization

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\boldsymbol{Resource\ Utilization}}$ |
| Information need | Quantify the resources that are being used and allocated to information security in regard to the university budget |
| Measure | Itemization of the resources allocated to information security (internal personnel, contracted personnel, hardware, software, services) within semester/annual budget compared to the resources used |
| Measure Type | Effectiveness indicator |
| Formula/scoring | $EI = \frac{Allocated\ resources\ to\ information\ security}{Used\ resources\ (of\ the\ allocated\ resources\ to\ InfoSec)\ within\ a\ budgeted\ period\ of\ time\ (semester/annual\ budget)}$ |
| Target | $EI = 1$ |
| Implementation evidence | Information security resource monitoring |
| Frequency | Every semester/annually (every two semesters) |
| Responsible parties | ▪ Information owner and collector: information security manager (information security officer)<br>▪ Measurement client: university management |
| Data source | Information security budget; information security effective expenditure; InfoSec resources usage reports |
| Reporting format | Radar diagram with a resource category for each axis and the double indication of allocated and used resources |
| ISO/IEC 27001 allocation | Clauses *5.1 Leadership and commitment* and *7.1 Resources* |

**Table 8:** Measurement: University Management Commitment

| Information Descriptor | Meaning or Purpose |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\textbf{University Management Commitment}}$ ; $\boldsymbol{EI}_{\textbf{University Management Commitment}}$ |
| Information need | Assess the university management commitment and the information security review activities regarding the university management review activities |
| Measure | a) University management InfoSec review meetings completed to date<br>b) Average participation rates in university management InfoSec review meetings to date |
| Measure Type | a) Performance indicator<br>b) Effectiveness indicator |
| Formula/scoring | a) $PI = \frac{InfoSec\ University\ management\ review\ meetings\ performed}{InfoSec\ University\ management\ review\ meetings\ scheduled}$<br>*b)* $EI = Compute\ mean\ and\ standard\ deviation\ of\ all\ participation\ rates\ to\ InfoSec\ university\ management\ review\ meetings$ |
| Target | a) $0.7 \leq PI \leq 1.1$ (to conclude the achievement of the control objective)<br>$PI > 0.5$ (even if it fails, PI should be still over 0.5 to conclude the least achievement)<br>b) Computed confidence limits based on the standard deviation indicate the likelihood that an actual result close to the average participation rate will be achieved. Very wide confidence limits suggest a potentially large departure and the need for contingency planning to deal with this outcome. |
| Implementation evidence | ▪ Count the university management InfoSec review meetings scheduled to date<br>▪ Per university management InfoSec review meetings to date, count the managers planned to attend and add a new entry with a default value for unplanned meetings performed in an ad hoc manner<br>▪ Count the planned university management InfoSec review meetings held to date<br>▪ Count the unplanned university management InfoSec review meetings held to date<br>▪ Count the rescheduled university management InfoSec review meetings held to date<br>▪ For all university management InfoSec review meetings that were held, count the number of managers who attended |
| Frequency | ▪ Collection: monthly<br>▪ Analysis and reporting: every semester<br>▪ Measurement revision: review and update every two years |
| Responsible parties | ▪ Information owner and collector: quality system manager (information security manager; information security officer)<br>▪ Measurement client: managers responsible for the ISMS |
| Data source | Information security university management review plan/schedule; university management review minutes/records |
| Reporting format | Line charts depicting the indicators over several data collection and reporting periods with the statement of the measurement results. The number of data collection and reporting periods should be defined by the university |
| ISO/IEC 27001 allocation | Clauses *5.1 Leadership and commitment* and *9.3 Management review* |

**Table 9:** Measurement: ISMS and Information Security Awareness Training

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{ISMS\ and\ Information\ Security\ Awareness\ Training}}$ |
| Information need | Evaluate compliance with the requirement of ISMS and information security awareness training |
| Measure | Percentage of personnel who received ISMS and information security awareness training |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ employees\ who\ received\ ISMS\ and\ information\ security\ awareness\ training}{Number\ of\ employees\ who\ have\ to\ receive\ ISMS\ and\ information\ security\ awareness\ training} \times 100$ |
| Target | Green: $PI \geq 90\%$, Yellow: $89\% \geq PI \leq 59\%$, Red: $PI \leq 60\%$<br>▪ Green: no action is required<br>▪ Yellow: indicator should be watched closely for possible deterioration to red<br>▪ Red: intervention is required, causation analysis has to be conducted to determine the reasons for non-compliance and poor performance |
| Implementation evidence | Participation lists of all awareness trainings; count of participants and compulsory participations; registries of all ISMS and information security awareness trainings |
| Frequency | Measurement revision and period of measurement: annually (every two semesters) |
| Responsible parties | ▪ Information owner and collector: information security officer (training manager)<br>▪ Measurement client: managers responsible for the ISMS; information security manager |
| Data source | Employee database; training records; participation list of awareness trainings |
| Reporting format | Bar chart with bars color-coded based on the targets. Brief summary of the meaning of the measure and possible university management actions should be attached to the bar chart |
| ISO/IEC 27001 allocation | Clauses *7.2 Competence*, *A.7.2.1 Management responsibilities*, and *A.7.2.2 Information security awareness, education, and training* |

**Table 10:** Measurement: ISMS and Information Security Awareness Training Effectiveness

| **Information descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\boldsymbol{ISMS\ and\ Information\ Security\ Awareness\ Training\ Effectiveness}}$ |
| Information need | Measure whether the participated employees have understood the content of the ISMS and information security awareness training |
| Measure | Percentage of participated employees passing a knowledge test after ISMS and information security awareness training |
| Measure Type | Effectiveness indicator |
| Formula/scoring | Let all employees, who took part in the training, fill out a knowledge test.<br>$EI = Percentage\ of\ training\ participants\ passed\ the\ test$ |
| Target | Green: $EI \geq 90\%\ of\ people\ passed\ the\ test$, Yellow: $89\% \geq PI \leq 59\%\ of\ people\ passed\ the\ test$, Red: $PI \leq 60\%\ of\ people\ passed\ the\ test$<br>▪ Green: no action is required<br>▪ Yellow: indicator should be watched closely for possible deterioration to red<br>▪ Red: intervention is required, causation analysis has to be conducted to determine the reasons for non-compliance and poor effectiveness |
| Implementation evidence | ISMS and information security awareness training documents/information provided to employees; list of employees who took part in the training; knowledge tests |

*(continued)*

| | |
|---|---|
| Frequency | ▪ Collection: one day after or last day of information security awareness training<br>▪ Reporting: for each collection |
| Responsible parties | ▪ Information owner and collector: information security officer (training manager)<br>▪ Measurement client: managers responsible for the ISMS; information security manager |
| Data source | Employee database; information security awareness training information; knowledge test results |
| Reporting format | Pie chart representing percentage of employees who passed the test. Line chart that shows the results' development in case of an additional training course that has been organized for a specific topic |
| ISO/IEC 27001 allocation | Clauses *7.2 Competence*, *A.7.2.1 Management responsibilities*, and *A.7.2.2 Information security awareness, education, and training* |

**Table 11:** Measurement: Policies Review

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\textbf{\textit{Policies Review}}}$ |
| Information need | Evaluate whether the policies for information security are reviewed at planned intervals or after significant changes |
| Measure | Percentage of information security policies reviewed |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ InfoSec\ policies\ that\ were\ reviewed\ at\ planned\ intervals\ or\ after\ significant\ changes}{Number\ of\ information\ security\ policies\ in\ place} \times 100$ |
| Target | Green: $PI \geq 80\%$, Yellow: $79\% \geq PI \leq 39\%$, Red: $PI \leq 40\%$<br>▪ Green: no action is required<br>▪ Yellow: indicator should be watched closely for possible deterioration to red<br>▪ Red: intervention is required, causation analysis has to be conducted to determine the reasons for non-compliance and poor performance |
| Implementation evidence | Policy history mentioning review of policy; policy list indicating date of last review |
| Frequency | ▪ Collection: annually (every two semesters) or after significant changes<br>▪ Reporting: for each collection |
| Responsible parties | ▪ Information owner: policy owner who has approved management responsibility for the development, review, and evaluation of the policy<br>▪ Information collector: internal auditor<br>▪ Measurement client: CISO (CIO) |
| Data source | Review plan of policies; history section of a security policy; list of documents |
| Reporting format | Pie chart showing the current review situation and line chart showing the development of compliance |
| ISO/IEC 27001 allocation | Clauses *7.5.2 Creating and updating of documented information* and *A.5.1.2 Review of the policies for information security* |

**Table 12:** Measurement: Risk Potential

| Information Descriptor | Meaning or Purpose |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\boldsymbol{Risk\ Potential}}$ |
| Information need | Assess the hazard of the university to information security risks |
| Measure | a) High and medium risks beyond the acceptable threshold<br>b) Timely review of high and medium risks |
| Measure Type | Effectiveness indicator |
| Formula/scoring | The acceptable threshold for high and medium risks should be defined and the responsible persons/parties alerted if the threshold is breached<br>$EI = Number\ of\ risks\ without\ status\ update$ |
| Target | $EI = 0$ |
| Implementation evidence | Updated risk register |
| Frequency | Collection and reporting: every semester |
| Responsible parties | Information owner and collector: security staff |
| Data source | Information risk register |
| Reporting format | Trend chart depicting high and medium risks; Trend chart showing accepted high and medium risks |
| ISO/IEC 27001 allocation | Clauses *8.2 Information security risk assessment* and *8.3 Information security risk treatment* |

**Table 13:** Measurement: Audit Program

| Information Descriptor | Meaning or Purpose |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{Audit\ program}}$ |
| Information need | Completeness of the audit program |
| Measure | Total number of audits performed compared to the total number of audits planned |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Total\ number\ of\ audits\ performed}{Total\ number\ of\ audits\ planned} \times 100$ |
| Target | $PI \geq 95\%$ |
| Implementation evidence | Monitoring of audit program and related reports |
| Frequency | Annually (every two semesters) |
| Responsible parties | ▪ Information owner and collector: audit manager<br>▪ Measurement client: university management |
| Data source | Audit program and audit reports |
| Reporting format | Trend graph showing the ratio of completed audits to audits planned for each year |
| ISO/IEC 27001 allocation | Clauses *9.2 Internal audit* and *A.18.2.1 Independent review of information security* |

**Table 14:** Measurement: Improvement Actions

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\textit{\textbf{Improvement Actions}}}$ |
| Information need | Verify the status of information security improvement actions and their management according to planned actions |
| Measure | Comparison of percentage of information security improvement actions on time, costs, and quality (i.e., requirements) with all planned actions. The actions should be the ones planned (i.e., opened, stand-by, and in progress) in the beginning of the timeframe. A weighting of each action, taking into account its criticality (e.g., actions that address high risks), can improve and specify the measurement. |
| Measure Type | Effectiveness indicator |
| Formula/scoring | $EI = \frac{Improvement\ actions\ on\ time,\ costs,\ and\ quality}{Number\ of\ planned\ improvement\ actions} \times 100$ |
| Target | $EI \ \geq 90\%$ |
| Implementation evidence | Status monitoring of each action |
| Frequency | Every semester |
| Responsible parties | ▪ Information owner and collector: project management office<br>▪ Measurement client: information security manager (information security officer) |
| Data source | Relevant project plans |
| Reporting format | List of all information security improvement actions and their status (actual time, costs, and quality forecast versus planned) with the percentage of actions on time, costs and, quality |
| ISO/IEC 27001 allocation | Clause *10 Improvement* |

**Table 15:** Measurement: Security Incident Costs

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\textit{\textbf{Security Incident Costs}}}$ |
| Information need | Calculation of the costs resulting from a lack of information security |
| Measure | Sum of the costs for each information security incident occurred in the sampling period |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \sum Costs\ of\ each\ information\ security\ incident$ |
| Target | $PI < Acceptable\ threshold\ defined\ by\ the\ university$ |
| Implementation evidence | Systematic gathering of costs for each information security incident |
| Frequency | Every semester |
| Responsible parties | ▪ Information owner: computer security incident response team (CSIRT)<br>▪ Information collector: information security manager/officer<br>▪ Measurement client: university management |
| Data source | Incident reports |
| Reporting format | Bar chart showing the costs of information security incidents for this and previous sampling periods in comparison with the acceptable thresholds |
| ISO/IEC 27001 allocation | Clause *10 Improvement* |

**Table 16:** Measurement: Learning from Security Incidents

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\boldsymbol{Learning\ from\ Security\ Incidents}}$ |
| Information need | Verify whether security incidents trigger actions for improvement of the current information security situation |
| Measure | Number of security incidents that trigger information security improvement actions |
| Measure Type | Effectiveness indicator |
| Formula/scoring | $EI = \frac{\sum Security\ incidents\ that\ trigger\ actions\ for\ improvement}{\sum Security\ incidents}$ |
| Target | $EI > Threshold\ defined\ by\ the\ university$ |
| Implementation evidence | Action plans with link to the security incidents |
| Frequency | Collection and reporting: every semester |
| Responsible parties | ▪ Information owner: Computer security incident response team (CSIRT)<br>▪ Information collector and measurement client: information security manager (InfoSec officer) |
| Data source | Incident reports |
| Reporting format | Bar chart showing the calculated effectiveness indicator for this and previous sampling periods |
| ISO/IEC 27001 allocation | Clauses *10 Improvement* and *A.16.1.6 Learning from information security incidents* |

**Table 17:** Measurement: Review of User Access Rights

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{Review\ of\ User\ Access\ Rights}}$ |
| Information need | Measurement on how many systematic user access rights reviews are performed on critical systems of the university (e.g., management server of the students' grades) |
| Measure | Percentage of critical systems that are regularly reviewed for user access rights |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ information\ systems\ classified\ as\ critical\ where\ periodic\ access\ rights\ reviews\ are\ performed}{Total\ number\ of\ information\ systems\ classified\ as\ critical} \times 100$ |
| Target | Green: $PI \geq 90\%$, Yellow: $89\% \geq PI \leq 69\%$, Red: $PI \leq 70\%$<br>▪ Green: no action is required<br>▪ Yellow: indicator should be watched closely for possible deterioration to red<br>▪ Red: intervention is required, causation analysis has to be conducted to determine the reasons for non-compliance and poor performance |
| Implementation evidence | Proofs of reviews (e.g., ticket system) |
| Frequency | ▪ Collection: after any changes in work relationships, such as recruitment or termination of work<br>▪ Reporting: every semester |
| Responsible parties | ▪ Information owner: risk owner<br>▪ Information collector: CISO (CIO)<br>▪ Measurement client: information security manager (information security officer) |
| Data source | Asset inventory; system used to track whether reviews were performed (e.g., ticket system) |
| Reporting format | Pie chart that presents the current situation and line chart that shows the development of compliance |
| ISO/IEC 27001 allocation | Clause *A.9.2.5 Review of user access rights* |

**Table 18:** Measurement: Physical Entry Controls

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{Physical\ Entry\ Controls}}$ |
| Information need | To show the existence, extent, and quality of the system used for access control |
| Measure | Strength of physical entry control system |
| Measure Type | Performance indicator |
| Formula/scoring | $PI\ =\ Scale\ from\ 0 - 100\%$<br>0%: There is **no access control system**<br>20%: There is an access system where **PIN code** (one factor system) is used for entry control<br>40%: There is an access control card system (**campus card system**) where passing the campus card (one factor system) is used for entry control<br>60%: There is a **campus card system** where passing card **and PIN code** is used for entry control<br>80%: There is a **campus card system** where passing card and **PIN code** is used for entry control and **log functionality** is activated<br>100%: There is a **campus card system** where passing card is used for entry control, PIN code is replaced by **biometric authentication** (fingerprint, voice recognition, retina scan, etc.), and **log functionality** is activated |
| Target | $PI \geq 40\%$ (satisfactory) |
| Implementation evidence | Control the type of entry control system and inspect the following aspects:<br>▪ Access control card system evidence<br>▪ PIN code usage<br>▪ Log functionality<br>▪ Biometric authentication |
| Frequency | ▪ Collection, analysis, and reporting: annually (every two semesters)<br>▪ Measurement revision: after twelve months<br>▪ Period of measurement: applicable twelve months |
| Responsible parties | ▪ Information owner: facility manager<br>▪ Information collector: internal auditor/external auditor<br>▪ Measurement client: university management |
| Data source | Identity management record |
| Reporting format | Pie chart representing the strength of physical entry control system |
| ISO/IEC 27001 allocation | Clause *A.11.1.2 Physical entry controls* |

**Table 19:** Measurement: Physical Entry Controls Effectiveness

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\boldsymbol{Physical\ Entry\ Controls\ Effectiveness}}$ |
| Information need | 1. Ensure an environment of comprehensive security and accountability for personnel, facilities, and products<br>2. Integrate physical and information security protection mechanisms to ensure appropriate protection of the university's information resources |

*(continued)*

| | |
|---|---|
| Measure | Number of unauthorized entries into facilities containing information systems (subset of physical security incidents) |
| Measure Type | Effectiveness indicator |
| Formula/scoring | $EI = Current\ number\ of\ physical\ security\ incidents\ allowing\ unauthorized\ entry\ into\ facilitites\ containing\ information\ systems$ |
| Target | $EI = 0$ |
| Implementation evidence | Systematic analysis of physical security incident reports and access control logs |
| Frequency | Data gathering and reporting: every semester |
| Responsible parties | ▪ Information owner: physical security officer (information security officer)<br>▪ Information collector: computer security incident response team (CSIRT)<br>▪ Measurement client: CIO; CISO |
| Data source | Physical security incidents reports; physical access control logs |
| Reporting format | Plot showing the trend of unauthorized entry into facilities containing information systems for the last sampling periods |
| ISO/IEC 27001 allocation | Clause *A.11.1.2 Physical entry controls* |

**Table 20:** Measurement: Maintenance of Information Systems

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\ \boldsymbol{Maintenance\ of\ Information\ Systems}}$ |
| Information need | Evaluate timeliness of maintenance activities in relation to the schedule |
| Measure | Maintenance delay per completed maintenance event |
| Measure Type | Performance indicator |
| Formula/scoring | $PI\ [in\ days;\ for\ each\ completed\ event] = Date\ of\ scheduled\ maintenance - Date\ of\ actual\ maintenance$ |
| Target | 1. University-specific (e.g., if the average delay is consistently over three days, the causes need to be examined)<br>2. Trend should be stable or close to $PI = 0$ days<br>3. Trend should be stable or upwards |
| Implementation evidence | Dates of scheduled maintenance; dates of completed maintenance; total number of planned maintenance events; total number of completed maintenance events |
| Frequency | ▪ Collection: every semester<br>▪ Reporting: annually (every two semesters) |
| Responsible parties | ▪ Information owner: security administrator<br>▪ Information collector: security staff<br>▪ Measurement client: information security manager (information security officer) |
| Data source | Plan/schedule of system maintenances; records of system maintenances |
| Reporting format | Line chart that depicts the average deviation of maintenance delay, superimposed with lines produced during previous reporting periods and the numbers of systems within the scope |
| ISO/IEC 27001 allocation | Clause *A.11.2.4 Equipment maintenance* |

**Table 21:** Measurement: Change Management

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{Change\ Management}}$ |
| Information need | Evaluate whether the best practices of change management and the hardening policies are respected |
| Measure | Percentage of new installed systems that meet change management best practices and hardening policies |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ new\ installed\ systems\ for\ which\ the\ proofs\ of\ respecting\ the\ change\ management\ best\ practices\ are\ furnished}{Number\ of\ new\ installed\ system}$ |
| Target | $PI = 1$ (All systems have to follow the change management guidelines) |
| Implementation evidence | Ticket system; e-mails; reports; checklist used for configuration |
| Frequency | ▪ Collection: every semester<br>▪ Reporting: annually (every two semesters) to university management; every semester to information security manager (information security officer) |
| Responsible parties | ▪ Information owner and collector: risk owner<br>▪ Measurement client: information security manager (information security officer) |
| Data source | Ticket system; e-mails; reports; checklist used for configuration; configuration review tool report |
| Reporting format | Pie chart showing the current situation and line chart showing the development of compliance |
| ISO/IEC 27001 allocation | Clause *A.12.1.2 Change management* |

**Table 22:** Measurement: Malware Protection

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{Malware\ Protection}}$ |
| Information need | Number of malware affected systems which do not have an updated anti-malware solution |
| Measure | Number of malware affected systems connected to the university's network with obsolete (e.g., more than one week old) anti-malware signatures |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ malware\ affected\ systems\ (connected\ to\ the\ univerity's\ network)\ with\ an\ obsolete\ antivirus}{Number\ of\ all\ systems\ (connected\ to\ the\ univerity's\ network)}$ |
| Target | $PI = 0$ |
| Implementation evidence | Monitoring of antivirus activities in each malware affected system |
| Frequency | Daily |
| Responsible parties | ▪ Information owner and collector: IT operations<br>▪ Measurement client: CISO |
| Data source | Monitoring tools; anti-malware console |
| Reporting format | List with the numbers per system classes (workstations, servers, operating systems) |
| ISO/IEC 27001 allocation | Clause *A.12.2.1 Controls against malware* |

**Table 23:** Measurement: Log Files Review

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\textbf{\textit{Log Files Review}}}$ |
| Information need | Assess the compliance status of the regular review of critical system log files |
| Measure | Percentage of audit log files reviewed per time period |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ \log files\ reviewed\ within\ specified\ time\ period}{Total\ number\ of\ \log files} \times 100$ |
| Target | $PI\ \geq 20\%$ ($PI\ < 20\%$: causes of underperformance should be examined) |
| Implementation evidence | Add up the total number of log files listed in the review log list |
| Frequency | ▪ Collection and analysis: monthly (depending on critically, possibly daily or real-time tracking)<br>▪ Reporting: every semester<br>▪ Measurement revision: every two years<br>▪ Period of measurement: applicable: two years |
| Responsible parties | ▪ Information owner: information security manager (information security officer)<br>▪ Information collector: security staff<br>▪ Measurement client: managers responsible for the ISMS; security manager |
| Data source | System; individual log files; evidence of the log review |
| Reporting format | Line chart that depicts the trend with a summary of the findings and the proposed management actions |
| ISO/IEC 27001 allocation | Clause *A.12.4.1 Event logging* |

**Table 24:** Measurement: Vulnerability of Information Systems

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\textbf{\textit{Vulnerability of Information Systems}}}$ |
| Information need | Evaluate whether information systems handling sensitive data are vulnerable to malicious attacks |
| Measure | Percentage of critical information systems that have been verified by vulnerability analysis or penetration testing since their last major release |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ critical\ information\ systems\ that\ have\ undergone\ a\ vulnerability\ analysis\ since\ their\ last\ major\ release}{Total\ number\ of\ critical\ information\ systems} \times 100$ |
| Target | Green: $PI = 100\%$, Yellow: $99\% \geq PI \geq\ 75\%$ (satisfactory), Red: $PI < 75\%$ |
| Implementation evidence | Reports of vulnerability assessments and penetration tests performed on information systems compared to number of information systems classified as critical in the asset inventory |
| Frequency | ▪ Collection: annually<br>▪ Reporting: for each collection |
| Responsible parties | ▪ Information owner: risk owner<br>▪ Information collector: experts with the know-how to execute vulnerability analysis or penetration tests |
| Data source | Asset inventory; penetration test reports |
| Reporting format | Pie chart representing the current situation and line chart showing the development of compliance |
| ISO/IEC 27001 allocation | Clauses *A.12.6.1 Management of technical vulnerabilities* and *A.18.2.3 Technical compliance review* |

**Table 25:** Measurement: Security Incident Management Effectiveness

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\boldsymbol{Security\ Incident\ Management\ Effectiveness}}$ |
| Information need | Assess the effectiveness of information security incident management |
| Measure | Incidents that have been not resolved in target timeframe |
| Measure Type | Effectiveness indicator |
| Formula/scoring | a) Define security incident categories and their target time frames in which the security incidents should be resolved<br>b) Define acceptable indicator thresholds for security incidents that exceed the category target time frame<br>c) Compare the number of incidents whose resolution time exceeds the category target time frames with the indicator thresholds |
| Target | $EI = Number\ of\ incidents\ whose\ resolution\ time\ exceeds\ the\ category\ target\ time\ frames\ is\ within\ the\ defined\ indicator\ thresholds$ |
| Implementation evidence | Target indicators and incidents whose resolution time exceeds the category target time frames get reported monthly |
| Frequency | ▪ Collection, analysis, reporting, and period of measurement: monthly<br>▪ Measurement revision: every semester |
| Responsible parties | ▪ Information owner: managers responsible for the ISMS<br>▪ Information collector: Incident management manager<br>▪ Measurement client: university management; managers responsible for the ISMS; security management; incident management |
| Data source | ISMS; individual incidents; incident reports; incident management tool |
| Reporting format | Table and trend charts showing the monthly target indicator thresholds and the number of incidents whose resolution time exceeds the category target time frames |
| ISO/IEC 27001 allocation | Clause *A.16 Information security incident management* |

**Table 26:** Measurement: Security Incident Trend

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{EI}_{\boldsymbol{Security\ Incident\ Trend}}$ |
| Information need | 1. Trend of information security incidents<br>2. Trend of categories of information security incidents |
| Measure | 1. Number of information security incidents in a defined timeframe (e.g., one month)<br>2. Number of information security incidents of a specific category in a defined timeframe (e.g., one month) |
| Measure Type | Effectiveness measure |
| Formula/scoring | $EI = \frac{Average\ number\ of\ information\ security\ incidents\ (of\ a\ specific\ category)\ of\ the\ last\ two\ timeframes}{Average\ number\ of\ information\ security\ incidents\ (of\ a\ specific\ category)\ of\ the\ last\ six\ timeframes}$<br>Define threshold values for the trend indicators, for example:<br>▪ Green: $EI < 1$<br>▪ Yellow: $1 \leq EI \leq 1.3$<br>▪ Red: $EI > 1.3$<br>1. Perform analysis for all incidents<br>2. Perform analysis for each specific category |

*(continued)*

| | |
|---|---|
| Target | $EI < 1$ (Green) |
| Implementation evidence | Number of information security incidents is reported monthly |
| Frequency | Monthly |
| Responsible parties | Information owner and collector: computer security incident response team (CSIRT)<br>Measurement client: CIO; CISO |
| Data source | Information security incident reports |
| Reporting format | Table representing the calculated effectiveness indicators and the defined threshold values; trend diagram |
| ISO/IEC 27001 allocation | Clause *A.16.1 Management of information security incidents and improvements* |

**Table 27:** Measurement: Security Events and Weaknesses Reporting and Assessment

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{Security\ Events\ and\ Weaknesses\ Reporting\ and\ Assessment}}$ |
| Information need | Measure whether security events and weaknesses are reported and formally treated |
| Measure | Sum of security events and weaknesses reported to the computer security incident response team (CSIRT) in relation to their assessment whether they are classified as information security incidents |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{\sum Number\ of\ security\ events\ and\ weaknesses\ reported\ to\ the\ CSIRT}{\sum Number\ of\ reported\ security\ events\ and\ weaknesses\ that\ are\ treated}$ |
| Target | $PI = 1$ |
| Implementation evidence | Ticket system used for the assessment of security events and weaknesses |
| Frequency | Collection and reporting: annually (every two semesters) |
| Responsible parties | ▪ Information owner: computer security incident response team (CSIRT)<br>▪ Information collector: information security manager (information security officer)<br>▪ Measurement client: information security manager (information security officer); university management |
| Data source | Reports of security events, weaknesses, and incidents; ticket system |
| Reporting format | Trend line showing the development of reported and treated security events and weaknesses over the last periods |
| ISO/IEC 27001 allocation | Clause *A.16.1.2 Reporting information security events*, *A.16.1.3 Reporting information security weaknesses* and *A.16.1.4 Assessment of and decision on information security events* |

**Table 28:** Measurement: Availability of IT Services

| **Information descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{Availability\ of\ IT\ Services}}$ |
| Information need | Evaluate the total availability of IT services in comparison with the defined maximum downtime |
| Measure | For each IT service, the end-to-end availability is compared with the maximum availability (i.e., excluding the previously defined downtime windows) |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{\sum Total\ availability\ of\ each\ IT\ service}{\sum Maximum\ availability\ excluding\ downtime\ windows\ of\ each\ IT\ service}$ |

*(continued)*

| | |
|---|---|
| Target | $PI = 1$ |
| Implementation evidence | Monitoring of end-to-end availability of each IT service |
| Frequency | Monthly |
| Responsible parties | ▪ Information owner: IT operations<br>▪ Information collector: IT quality<br>▪ Measurement client: CIO |
| Data source | Monitoring tools |
| Reporting format | For each IT service, two lines in the chart:<br>▪ line linking the actual availability (percentage) of each sampled period<br>▪ line (for comparison purposes) showing the availability target |
| ISO/IEC 27001 allocation | Clauses *A.17.2.1 Availability of information processing facilities* |

**Table 29:** Measurement: ISMS Review Process

| **Information Descriptor** | **Meaning or Purpose** |
|---|---|
| Measure ID | $\boldsymbol{PI}_{\boldsymbol{ISMS\ Review\ Process}}$ |
| Information need | Assess the degree of accomplishment of independent reviews of information security |
| Measure | Progress ratio of accomplished independent reviews |
| Measure Type | Performance indicator |
| Formula/scoring | $PI = \frac{Number\ of\ conducted\ independent\ reviews}{Total\ number\ of\ planned\ independent\ reviews}$ |
| Target | $0.8 \leq PI \leq 1.1$ (to conclude the achievement of the control objective; no action required)<br>$PI > 0.6$ (PI should be at least over 0.6 if the indicator fails to meet the primary condition) |
| Implementation evidence | Number of conducted independent reviews; total number of planned independent reviews |
| Frequency | ▪ Collection, analysis, and reporting: every semester<br>▪ Measurement revision: reviewing and updating every two years<br>▪ Period of measurement: applicable: two years |
| Responsible parties | ▪ Information owner: managers responsible for the ISMS<br>▪ Information collector: internal auditor; quality manager<br>▪ Measurement client: managers responsible for the ISMS; quality system manager |
| Data source | Reports of reviews; plans of reviews |
| Reporting format | Bar chart depicting compliance over several reporting periods in relation to the defined target thresholds |
| ISO/IEC 27001 allocation | Clause *A.18.2.1 Independent review of information security* |

## 4.4. Determination of Key Performance Indicators for Universities by means of a Value Benefit Analysis

After 24 performance and effectiveness indicators have been determined, now it is necessary to identify a handful of key performance indicators from those ones, which “are the main steering tool in measuring information security” (Humpert-Vrielink & Vrielink, 2012, p. 49). Of course, all 24 indicators could be considered as KPIs and so the issue would be settled but such a large number of KPIs would make them seem indifferent and would not lead to targeted and meaningful indicators. Based on a few key metrics, it has to be immediately apparent how the university is performing in terms of information security. It is important to note that there are no universal KPIs. They have to be individually tailored to the university's own information security objectives and requirements. Consequently, all measurement indicators need to be prioritized by the universities themselves and the highest weighted ones lead to the key performance indicators.

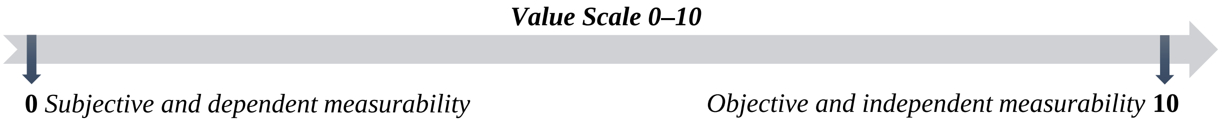
In order to facilitate the decision-making and the determination of the KPIs, a well-known analysis method of decision theory, the value benefit analysis, can be very useful. (cf. Herbig, 2016) This section discusses in what way such an analysis could be carried out in practice in this specific case. However, it should be mentioned at this point that the results and criteria of the value benefit analysis are not binding and generally valid. Rather, it should show how the determination of the KPIs can be implemented by this method and provide assistance.

### 4.4.1. Weighted Assessment Criteria

First of all, the weighted assessment criteria need to be defined. They form the assessment basis for the goals and the quality of the measurements. The sum of all percentage-weighted criteria has to be result in 100%. The criteria will be evaluated for each measurement of the measurement system individually by values of a scale from 0 to 10. The value 10 is the maximum (the criterion is fully met) and the value 0 is the minimum (the criterion is by no means met). Five evaluation criteria were selected and weighted for the model, which will be discussed in more detail hereafter.

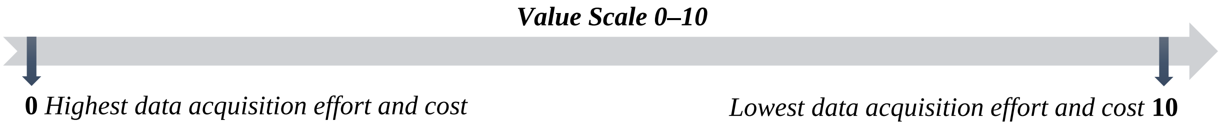
**Criterion 1:** Objective and Independent Measurability (Weighting: 10%)

The first criterion questions the independence and objectivity of the measurements. If a measurement only refers to other measurement results and is dependent on them, it can lead to errors and inaccuracies that have arisen from these previous measurements. Furthermore, subjective influencing factors, such as personal misjudgments and human errors, can influence the result. This can affect the informative value and quality of the KPI in a negative way. Therefore, the criterion of objectivity and independence of a measurement has to be considered and it is weighted by 10%.


*Value Scale 0–10*
**0** *Subjective and dependent measurability*
*Objective and independent measurability* **10**

**Criterion 2:** Data Acquisition Effort and Cost (Weighting: 10%)

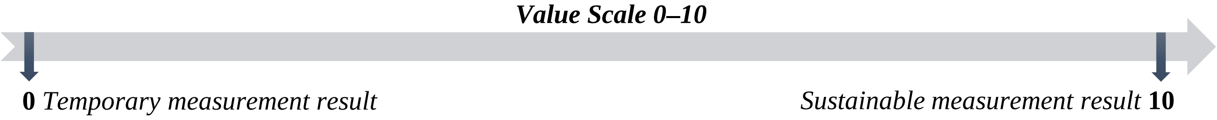
High effort and high costs for the collection and provision of data or information that are required for the measurement always involve a risk. It is counterproductive if many resources concerning a lot of personnel, time, and high costs are spent on a measurement and then the benefit or efficiency of the measurement turns out to be very low. Therefore, this criterion needs to be considered for the determination of the KPIs (weighted by 10%.) and always needs to be balanced in relation to the significance of the respective measurement (criterion 5).


*Value Scale 0–10*
**0** *Highest data acquisition effort and cost*
*Lowest data acquisition effort and cost* **10**

**Criterion 3:** Sustainable Measurement Result (Weighting: 20%)

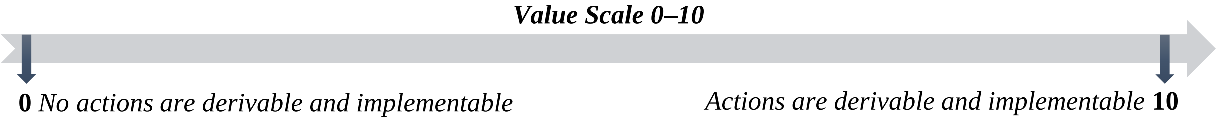
A measurement result with short-term significance that can vary from one moment to the next is not meaningful and corresponds to no KPI. Otherwise, a sustainable measurement result provides a stable reference value that can be used for subsequent measurements.

This is important for the achievement of long-term goals and continuous improvement processes and, therefore, it is weighted by 20%.


*Value Scale 0–10*
**0** *Temporary measurement result*
*Sustainable measurement result* **10**

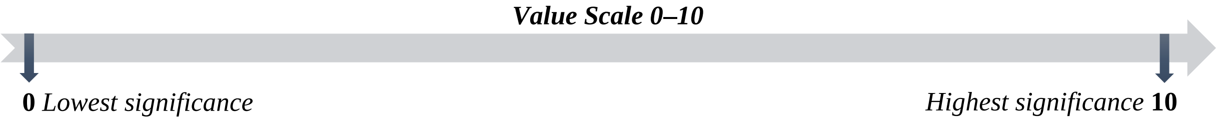
### **Criterion 4:** Actions for Improvement are Derivable and Implementable (Weighting: 30%)

As **Figure 13**, **p. 48** has shown, the monitoring, measurement, analysis, and evaluation processes have to be continuously reviewed, updated, and improved to achieve the desired objectives. Suitable and targeted conclusions must be drawn from KPIs in order to optimize measurement results and improve these processes. This is one of the most important criteria and it was weighted by 30%.


*Value Scale 0–10*
**0** *No actions are derivable and implementable*
*Actions are derivable and implementable* **10**

### **Criterion 5:** Measurement Significance for the University's Information Security Objectives (Weighting: 30%)

Information security measurements can provide valuable results in many areas, but KPIs in particular should reflect the specific objectives of the university that stand for information security and ISMS success. These objectives are usually defined by the university management and the responsible persons of the ISMS/InfoSec. Accordingly, the significance of a KPI for the university's information security objectives in relation to effort and cost is one of the most important criteria and it is rated by 30%.



### 4.4.2. Evaluation and Results of the Value Benefit Analysis

The value benefit analysis was performed in Microsoft Excel. Its evaluation is shown in **Figure 17** on the next page.

For criterion 5 (‘measurement significance for the university’s information security objectives’), the following university’s information security objectives are assumed, on the basis of which the measurements are evaluated for this criterion: high information security, low risk potential, high availability of information-relevant systems, low cost, and high know-how in the field of information security.

Each individual rating (0–10) in the white cells was multiplied by the associated weighting criteria in percentage, which results in the score shown in yellow. For each of the 24 measurements, five scores were calculated that were subsequently added and displayed as sum. Therefore, the range of a score sum reaches from 0.0 (minimum) to 10.0 (maximum).

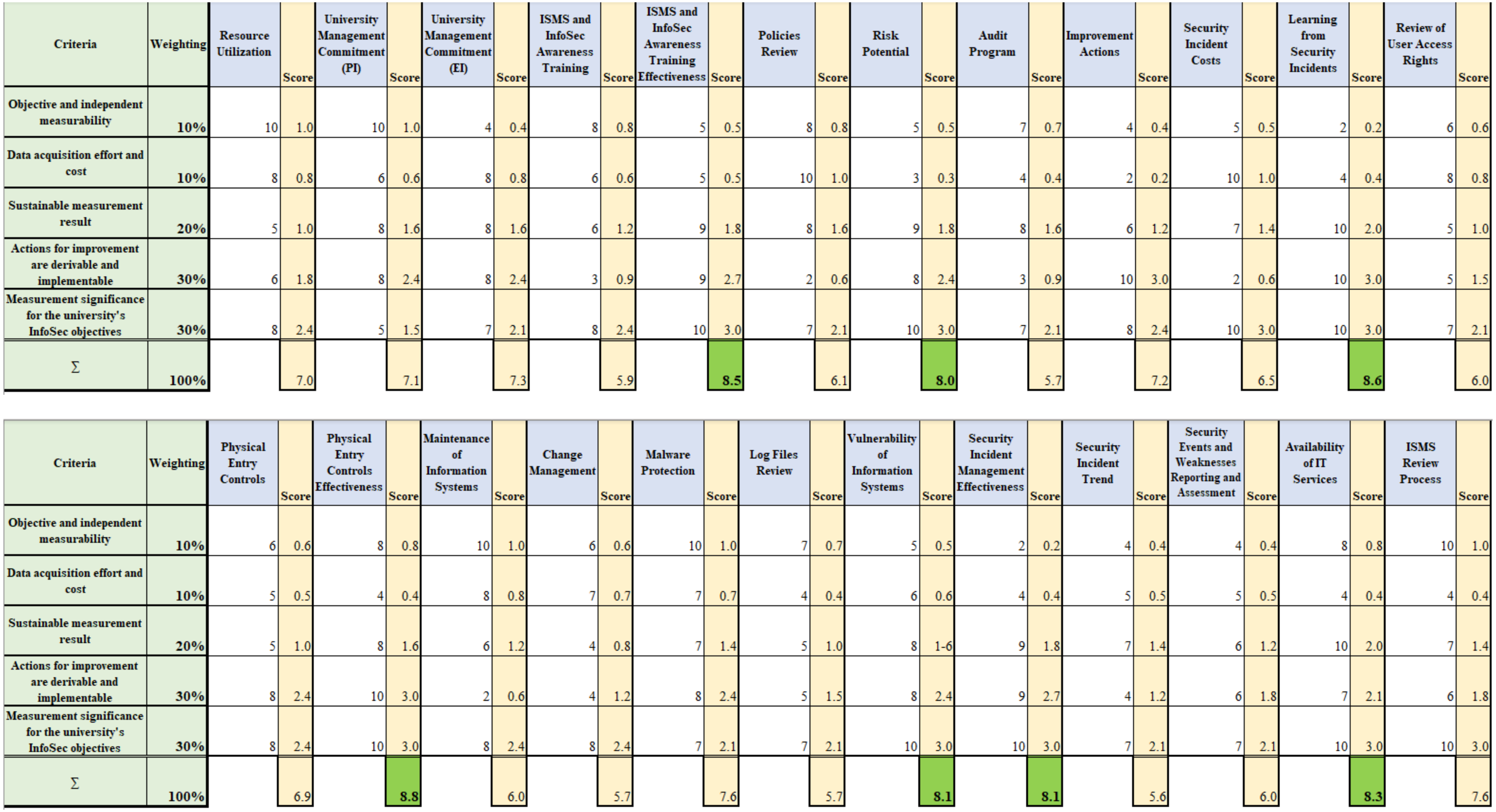
The KPI range was set from 8.0 to 10.0. As a logical consequence, the measurements with a total score of at least 8.0 (green marked) determine a key performance indicator. The following KPIs were calculated and result from this model:

**Table 30:** Key Performance Indicators for Universities

| Total Score | Key Performance Indicator | Table | Page |
|---|---|---|---|
| 8.6 | $EI_{Learning\ from\ Security\ Incidents}$ | 16 | 61 |
| 8.5 | $EI_{ISMS\ and\ Information\ Security\ Awareness\ Training\ Effectiveness}$ | 10 | 57 |
| 8.3 | $PI_{Availability\ of\ IT\ Services}$ | 28 | 67 |
| 8.2 | $EI_{Physical\ Entry\ Controls\ Effectiveness}$ | 19 | 62 |
| 8.1 | $PI_{Vulnerability\ of\ Information\ Systems}$ | 24 | 65 |
| 8.1 | $EI_{Security\ Incident\ Management\ Effectiveness}$ | 25 | 66 |
| 8.0 | $EI_{Risk\ Potential}$ | 12 | 59 |

(Source: Own illustration)

The result shows that seven key metrics were determined from the 24 metrics of the measurement system. This approach delivers good results that are aligned with the exemplarily set up university's information security objectives. Of course, the interpretation of the KPI range, the definition of the criteria, and the evaluation itself are influenced by subjective factors, however, in the end, the university's own ‘subjective’ goals and wishes need to be fulfilled and measured.



| Criteria | Weighting | Resource Utilization | Score | University Management Commitment (PI) | Score | University Management Commitment (EI) | Score | ISMS and InfoSec Awareness Training | Score | ISMS and InfoSec Awareness Training Effectiveness | Score | Policies Review | Score | Risk Potential | Score | Audit Program | Score | Improvement Actions | Score | Security Incident Costs | Score | Learning from Security Incidents | Score | Review of User Access Rights | Score |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Objective and independent measurability | 10% | 10 | 1.0 | 10 | 1.0 | 4 | 0.4 | 8 | 0.8 | 5 | 0.5 | 8 | 0.8 | 5 | 0.5 | 7 | 0.7 | 4 | 0.4 | 5 | 0.5 | 2 | 0.2 | 6 | 0.6 |
| Data acquisition effort and cost | 10% | 8 | 0.8 | 6 | 0.6 | 8 | 0.8 | 6 | 0.6 | 5 | 0.5 | 10 | 1.0 | 3 | 0.3 | 4 | 0.4 | 2 | 0.2 | 10 | 1.0 | 4 | 0.4 | 8 | 0.8 |
| Sustainable measurement result | 20% | 5 | 1.0 | 8 | 1.6 | 8 | 1.6 | 6 | 1.2 | 9 | 1.8 | 8 | 1.6 | 9 | 1.8 | 8 | 1.6 | 6 | 1.2 | 7 | 1.4 | 10 | 2.0 | 5 | 1.0 |
| Actions for improvement are derivable and implementable | 30% | 6 | 1.8 | 8 | 2.4 | 8 | 2.4 | 3 | 0.9 | 9 | 2.7 | 2 | 0.6 | 8 | 2.4 | 3 | 0.9 | 10 | 3.0 | 2 | 0.6 | 10 | 3.0 | 5 | 1.5 |
| Measurement significance for the university's InfoSec objectives | 30% | 8 | 2.4 | 5 | 1.5 | 7 | 2.1 | 8 | 2.4 | 10 | 3.0 | 7 | 2.1 | 10 | 3.0 | 7 | 2.1 | 8 | 2.4 | 10 | 3.0 | 10 | 3.0 | 7 | 2.1 |
| Σ | 100% | | 7.0 | | 7.1 | | 7.3 | | 5.9 | | 8.5 | | 6.1 | | 8.0 | | 5.7 | | 7.2 | | 6.5 | | 8.6 | | 6.0 |

| Criteria | Weighting | Physical Entry Controls | Score | Physical Entry Controls Effectiveness | Score | Maintenance of Information Systems | Score | Change Management | Score | Malware Protection | Score | Log Files Review | Score | Vulnerability of Information Systems | Score | Security Incident Management Effectiveness | Score | Security Incident Trend | Score | Security Events and Weaknesses Reporting and Assessment | Score | Availability of IT Services | Score | ISMS Review Process | Score |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Objective and independent measurability | 10% | 6 | 0.6 | 8 | 0.8 | 10 | 1.0 | 6 | 0.6 | 10 | 1.0 | 7 | 0.7 | 5 | 0.5 | 2 | 0.2 | 4 | 0.4 | 4 | 0.4 | 8 | 0.8 | 10 | 1.0 |
| Data acquisition effort and cost | 10% | 5 | 0.5 | 4 | 0.4 | 8 | 0.8 | 7 | 0.7 | 7 | 0.7 | 4 | 0.4 | 6 | 0.6 | 4 | 0.4 | 5 | 0.5 | 5 | 0.5 | 4 | 0.4 | 4 | 0.4 |
| Sustainable measurement result | 20% | 5 | 1.0 | 8 | 1.6 | 6 | 1.2 | 4 | 0.8 | 7 | 1.4 | 5 | 1.0 | 8 | 1-6 | 9 | 1.8 | 7 | 1.4 | 6 | 1.2 | 10 | 2.0 | 7 | 1.4 |
| Actions for improvement are derivable and implementable | 30% | 8 | 2.4 | 10 | 3.0 | 2 | 0.6 | 4 | 1.2 | 8 | 2.4 | 5 | 1.5 | 8 | 2.4 | 9 | 2.7 | 4 | 1.2 | 6 | 1.8 | 7 | 2.1 | 6 | 1.8 |
| Measurement significance for the university's InfoSec objectives | 30% | 8 | 2.4 | 10 | 3.0 | 8 | 2.4 | 8 | 2.4 | 7 | 2.1 | 7 | 2.1 | 10 | 3.0 | 10 | 3.0 | 7 | 2.1 | 7 | 2.1 | 10 | 3.0 | 10 | 3.0 |
| Σ | 100% | | 6.9 | | 8.8 | | 6.0 | | 5.7 | | 7.6 | | 5.7 | | 8.1 | | 8.1 | | 5.6 | | 6.0 | | 8.3 | | 7.6 |

**Figure 17:** Evaluation of the Value Benefit Analysis with Microsoft Excel

(Source: Own illustration)

## 4.5. Results and Discussion

The development of an information security measurement system for universities was realized according to the bottom-up approach. In other words, a handful of key metrics were determined by a large number of metrics.

First, 23 measurement procedures were modeled in tabular form, yielding fifteen performance indicators (PIs) and nine effectiveness indicators (EIs). As a logical consequence of the first research question, these procedures are specifically adapted to the ISO/IEC 27001 requirements and controls. The measurement system can be used by universities to measure the performance and effectiveness of their information security processes and controls. Of course, it is possible to add, modify, and remove measurement procedures that do not meet the university's own information security conceptions and requirements, but this step always needs to be questioned in the view of the ISMS requirements of ISO/IEC that are mandatory for an ISMS certification. If this aspect is taken into account, the system can be individually adapted and applied.

In the next step, key performance indicators were derived from the 24 indicators. For the universities, the KPIs should be the most important indicators that show at a glance what the current information security situation is like and how the ISMS is performing. Since the KPIs always need to be geared specifically to the university's objectives and no universally applicable KPIs exist, a prioritizing of the 24 indicators and the subsequent selection of the KPIs by the universities themselves would be most effective. To support the KPI determination process, a value benefit analysis was modelled. For this purpose, five weighted evaluation criteria were drawn up and a KPI range was selected. The self-conducted analysis resulted in seven KPIs, which are shown in **Table 30**, and serves as guidance for the universities in determining their individual KPIs.

In order to continue the monitoring, measurement, analysis, and evaluation cycle (**Figure 13, p. 48**) and to put the measurement system into practice, "interested parties who should be participating in the security measurement process should be made aware of measurement activities and the rationale behind it [...] and [...] data collection and analysis tools should be identified and, if needed, modified, to effectively and efficiently gather measures" (ISO/IEC, 2016, p. 14). Furthermore, the measurement results and information that is needed for the measurement must be stored securely, so that they can only be made available to those who are responsible. All metrics, in particular the KPIs, must be monitored and reported purposefully. KPIs are best monitored and reported in dashboards and scorecards.

There is already a lot of valuable literature on these techniques, among others (Hassler, 2012, pp. 374–385), (Kütz, 2009, pp. 120–130), (Lea & Fui-Hoon Nah, 2013, pp. 116–123), and (Junus, 2008, pp. 333–366).
After all relevant procedures and measurement thresholds have been defined, the indicators must be measured and monitored over the specific periods of time. Subsequently, the measurement results and KPIs should be analyzed and interpreted in relation to the specified university's information security objectives. "Guidance for statistical analysis can be found in ISO/TR 10017." (ISO/IEC, 2016, p. 15) The analysis results should provide insights into the university's information security performance and ISMS effectiveness and "should identify gaps between the expected and actual measurement results of an implemented ISMS, controls[,] or groups of controls" (ISO/IEC, 2016, p. 15). On the basis of these identified gaps, suitable conclusions and actions can be initiated to improve the information security situation. Overall, a continuous measurement and monitoring process is created by maintaining, reviewing, and improving all procedures before of a new measurement starts. As an evidence of the university's information security monitoring and measurement, all processes have to be documented and recorded securely for the communication to self-selected interested parties.

In sum, as a crucial element in the initial phase of the continuous cycle of the monitoring, measuring, analysis, and evaluation processes, the presented information security measurement system forms the basis of a successful measurement for the universities according to the ISO/IEC 27000-series.

# 5. Creation of a Uniform Information Security Report Template for Universities

As outlined in the first research question, the ISMS requirement '*9. Performance Evaluation*', more precisely its subclause '*9.3 Management review*', stipulates that the ISMS has to be regularly reviewed by the top management (the university management). "The purpose of [a] management review is to ensure the continuing suitability, adequacy[,] and effectiveness of the ISMS." (ISO/IEC, 2017, p. 36) In order to make a review possible, the persons who are responsible for information security need to report to the university management at planned intervals. But as the audit results showed, the current situation at the universities is that the individual audit reports of the audits carried out are often the first reports to the university management on the state of information security.

In order to support the reporting processes at the universities, it is examined whether a template for an information security report is useful and can be developed. In this way, a uniform reporting and communication within and between the universities should be created. First, a requirements elicitation needs to be carried out to determine the report structure and its components. For this purpose, the requirements and recommendations for reporting of the ISO/IEC 27000-series are analyzed. Afterwards, questions on the applicability of an information security report for universities need to be clarified. On the results of the investigations, an information security report template is designed finally.

## 5.1. Requirements Elicitation (Report Structure and Components)

Before determining the concrete structure and components of the report, it is helpful to consider the basics of creating an information security report first. According to Hassler (cf. Hassler, 2012, p. 384 f.), it is important that the report is clear and well-structured. The structure should change only insignificantly over time. This helps the recipient and reader to understand and interpret the report quickly. In addition, it is useful to report numerical results, such as measurement results, in relation to the results of previous reporting periods, for example, as percentage changes. This provides an important interpretation aid to the reader for classifying and interpreting the results correctly. It should be borne in mind that the readership is usually not made up of technical experts alone. Accordingly, the report content should be as comprehensible and concise as possible by focusing on the key points.

The interpretation of results, metrics, and key performance indicators can be simplified by specifying the defined target and threshold values, such as visually by the traffic light colors that were often used as a scale for the target classification of percentage measurements. By visually depicting facts as charts and graphs instead of pure tables of numbers, the contents can be captured more easily and quickly. For this purpose, a suitable reporting format was indicated for each measurement procedure in the second research question. For the KPIs, it is also helpful to provide a brief interpretation aid in the form of a few meaningful indicator descriptions that can also contain countermeasures in the event of critical changes concerning the value.

Since the evaluation of the twelve Bavarian universities (first research question) and the development of a measurement system (second research question) are based on the ISO/IEC 27000-series, consequently, the requirements for an information security report are also determined from the ISMS family of standards in order to guarantee standard conformity. In the following, reporting requirements and recommendations are investigated.

### Requirements and Recommendations of ISO/IEC 27003 (ISO/IEC 27001)

The guidance of the ISMS requirement clause '*9.3 Management review*' suggests electronic and verbal communication in addition to the evaluation of reports for prescribed regular management reviews. "These activities could vary from daily, weekly, or monthly organizational unit meetings to simple discussions of reports. Top management is ultimately responsible for management review, with inputs from all levels of the organization." (ISO/IEC, 2017, p. 36) These inputs to the university management must provide evidence of the performance of the ISMS. "Key inputs are the results of the information security measurements as described in [the requirement clause] 9.1 ['*Monitoring, measurement, analysis, and evaluation*' (second research question)] and the results of the internal audits described in [the requirement clause] 9.2 ['*Internal audit*' (first research question)] and risk assessment results and risk treatment plan status." (ISO/IEC, 2017, p. 36) Nonconformities, corrective actions, as well as the fulfilment of information security objectives also need to be included, since they are essential security-related issues for the university management. These topics need to be reflected in the information security report that is intended to be an important source of information for each management review.

## Requirements and Recommendations of ISO/IEC 27005

According to ISO/IEC 27005 clause ‘*11 Information security risk communication and consultation*’, “[i]nformation about risk should be exchanged and/or shared between the decision-makers and other stakeholders.[...] [The] [c]ommunication is bi-directional.” (ISO/IEC, 2018b, p. 20) For this reason, the university management, as the decision-maker, has to report or receive reports of risks from internal stakeholders, e.g. the security personnel, external stakeholders, competent authorities, or the ministry (‘Landesamt für Sicherheit in der Informationstechnik’). In accordance with the risk management process (**Figure 5**, **Annex**, **p. 99**), “risk communication should be carried out in order to [...] provide assurance of the outcome of the organization’s risk management, [to] share the results from the risk assessment and present the risk treatment plan, [and finally to] support decision making [and] improve awareness” (ISO/IEC, 2018b, p. 21). Consequently, the risk assessment results and risk treatment plan status need to be included in the information security report.

## Requirements and Recommendations of ISO/IEC 27014

The standard ISO/IEC 27014 provides recommendations on how information security-relevant activities can be controlled and communicated within an organization. “[A]n effective governance of information security ensures that the governing body receives relevant reporting [...] about information security-related activities. This enables pertinent and timely decisions about information security issues in support of the strategic objectives of the organi[z]ation” (ISO/IEC, 2013, p. iv) The ‘governing body’ is understood as part of the top management that is responsible for the organization’s performance and conformity and, in this context, can also be considered as part of the university management or as the university management itself. “One of the methods to [‘]communicate[’] is [an] information security status which explains information security activities and issues [...].” (ISO/IEC, 2013, p. 6) A very good example of a detailed information security status, which is incorporated into the information security report template, is depicted in ISO/IEC 27014, Annex B.

## 5.2. Applicability Aspects of an Information Security Report for Universities

Before an information security report template can be created and a report can be written, the following key questions on the applicability of the report need to be considered and clarified:

❓ **Who should be the recipients of the report?**

Since an information security report contains confidential and critical information about an organization's security, its content should only be intended for the organization’s decision-makers (top management) and confidential partners or persons. In the university sector, the university management acts as decision-maker and is therefore one of the main recipients of the report. All important decisions concerning the security of the university are approved by the head of the university. Confidential partners or persons include, for example, the ‘Stabstelle Informationssicherheit bayerischer Hochschulen und Universitäten’, IT working groups, security personnel or students that conduct research in this area. As the higher-level decision-makers, the relevant authorities or the ministry (‘Landesamt für Sicherheit in der Informationstechnik’) should also be involved and informed if required.

❓ **Which period of time should be gathered by the report and how often should it be submitted?**

At this point, a distinction must be made between a regular information security report dealt with in this research question and an occasion-related information security report. The last-mentioned report is written irregularly, for example due to unexpected security problems or risks. This reporting is particularly necessary if the problems that arise cannot be solved by the security personnel themselves, e.g., because material resources are required outside the approved budget and they can only be provided by the management. In contrast, the regular information security report supports the management review as required by ISO/IEC 27001. “All aspects of the ISMS should be reviewed by management at planned intervals, at least yearly, by setting up suitable schedules and agenda items in management meetings. New or less mature ISMSs should be reviewed more frequently by management to drive increased effectiveness.” (ISO/IEC, 2017, p. 36) Therefore, a typical annual reporting cycle would be appropriate.

But due to the facts that the semester cycles at universities are half-yearly, the winter semester does not end simultaneously with the end of the year, and the current ISMS is in the building phase, is advisable to prepare and submit an information security report at the end of every semester covering the reporting period of the respective semester.

❓ **Is the report template suitable for universities of various sizes (universities/universities of applied sciences)?**

Since the information security report template is specified according to the requirements and recommendations of the ISO/IEC 27000-series that refers to all types and sizes of organization, the report template is suitable for both universities and universities of applied sciences. It should only be noted that a semester at universities begins a few weeks later than at universities of applied sciences. This aspect should be taken into account and coordinated in an overall report.

❓ **Would an overall information security report of all universities be feasible?**

An overall information security report of all participating universities would be feasible if each university is willing to submit their information security reports to a specific body or person who prepares the overall report carefully and reliably by a certain deadline. Through the use of the uniform information security report template, the results and report contents can be easily put together and combined. Thus, the overall information security situation at Bavarian universities could be reported to the competent authorities or the ministry in one report. This step would facilitate communication and bureaucracy burdens between universities and the concerned authorities vastly.

## 5.3. Information Security Report Template for Universities

The information security report template was created with Microsoft Word in English and German. Input fields were generated with the developer tools to improve the usability. They are displayed as light grey surrounding fields as soon as the cursor is on the input fields. To state the correct content in the correct report place, keywords in curly brackets '{}' describe what to enter. The notes in the brackets can be overwritten or deleted.

- The information security report template in English is depicted in **Figure 18**, **Annex**, **p. 101**.
- The information security report template in German is depicted in **Figure 19**, **Annex**, **p. 104**.

In addition, the templates are submitted as Microsoft Word documents with the prepared input fields to this master thesis separately.

## 5.4. Results and Discussion

As stipulated in the ISO/IEC 27001 requirement clause '*9.3 Management review*', the top management (the university management) has to review its ISMS at planned intervals. For this purpose, the management need to be regularly informed about the current information security status by informative reports. Since the evaluation of the audit results in the first research question has shown that an organized reporting was hardly implemented at the twelve evaluated Bavarian universities, the aim of this investigation was to examine whether the preparation of a uniform information security report for universities would be feasible in order to facilitate and support the universities' reporting processes.

Due to the fact that the establishment of an ISMS at the universities is based on the ISO/IEC 27000-series, a requirements elicitation of the report structure and components was carried out according to this series of standards to guarantee standard conformity. The audit results, the measurement results and KPIs, the risk assessment results, the risk treatment plan, and further information security related aspects must be included in the report. After the applicability of an information security report has been scrutinized, it was clear that the preparation of a uniform information security report for universities is feasible and even highly advisable. All components and the exact report structure are shown in the drafted information security report template in English in **Figure 18**, **Annex**, **p. 101** and in German in **Figure 19**, **Annex**, **p. 104**.

The information security report template can be used by both universities and universities of applied sciences and is primarily addressed to the respective university management as the main recipient. Due to the facts that the semester cycles at universities are half-yearly, the winter semester does not end simultaneously with the end of the year, and the current ISMS is in the building phase, it is advisable to prepare and submit an information security report at the end of every semester covering the reporting period of the respective semester. An overall information security report on the information security situation at all Bavarian universities could be reported to the competent authorities or the ministry in one report if each university is willing to submit their information security report to a specific body or person who prepares the overall report carefully and reliably by a certain deadline. This step would facilitate the communication and bureaucracy burdens between the universities and the relevant authorities vastly.

By the drafted information security report template, all universities benefit from a uniform report framework that simplifies their own information security reporting processes and at the same time creates a uniform way of reporting and communication between all universities.

# 6. Summary of All Results and their Connection

As mentioned at the beginning of the work, the realization of information security is not completed at a specific date, it is a cyclic and continuous process. The three research questions that were discussed in this master thesis are all part of the PDCA cycle and therefore build on each other. **Figure 20** shows the research questions' connection and the main tasks that were performed for each research question.

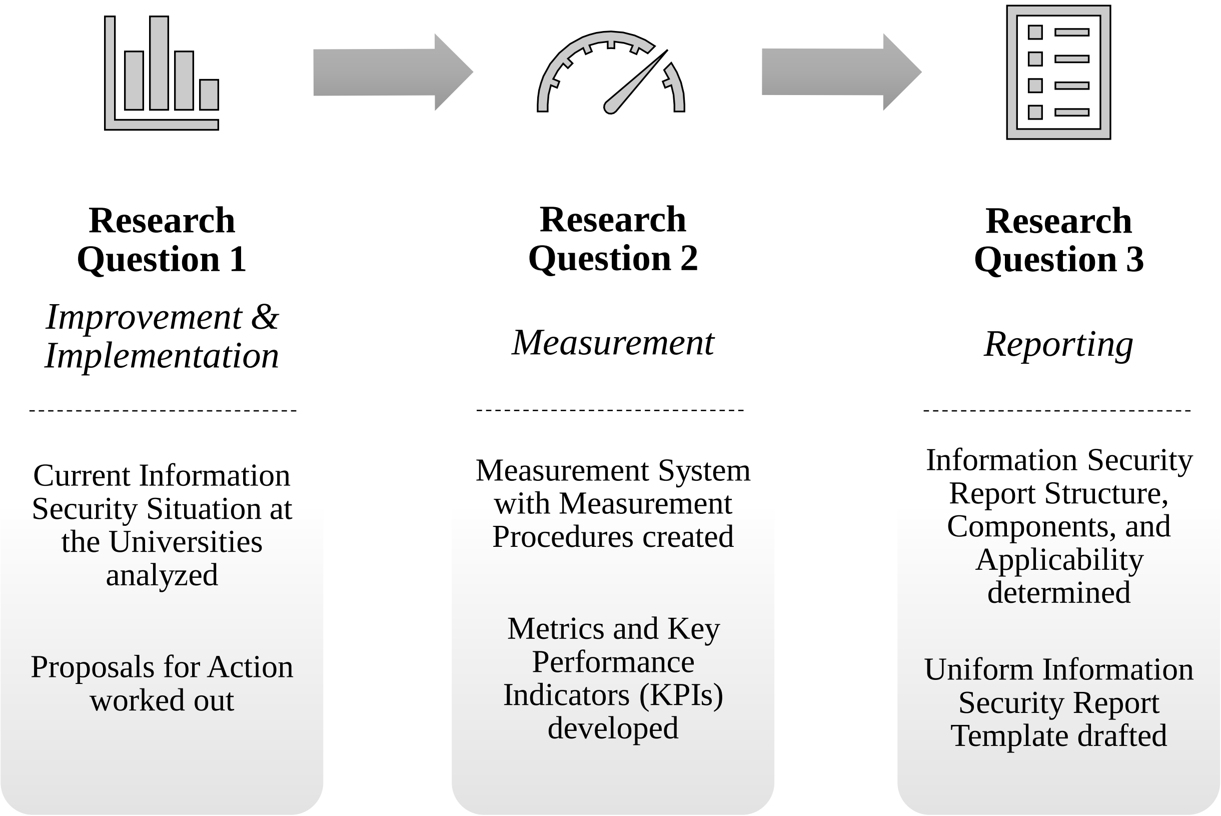

Research Question 1
Improvement & Implementation
Current Information Security Situation at the Universities analyzed
Proposals for Action worked out
Research Question 2
Measurement
Measurement System with Measurement Procedures created
Metrics and Key Performance Indicators (KPIs) developed
Research Question 3
Reporting
Information Security Report Structure, Components, and Applicability determined
Uniform Information Security Report Template drafted

**Figure 20:** Connection of the Research Questions

(Source: Own illustration)

The first research question focused on the improvement of the information security controls and processes as well as on the implementation of missing ISMS requirements and information security controls at the twelve Bavarian state universities. Subsequently, these controls and processes need to be measured in order to be managed. The second research question dealt with this topic. Finally, the current information security situation (first research question) and the measurement results (second research question) need to be reported to the decision-makers in order to draw the right conclusions in controlling and steering the information security processes and, if necessary, take appropriate actions. This process step led to the third research question.

In the following, the research questions are taken up again and answered briefly and succinctly. All results are summarized.

## Research Question 1

**Are similar information security controls implemented at various Bavarian universities and in what way could the information security situation of these universities be improved?**

The evaluation of the audit results and the comparative analysis have shown that all investigated universities have taken the first steps towards the implementation of an ISMS by the realization of many similar information security controls and processes. Almost every technical control specified in the standard ISO/IEC 27001 (or ISO/IEC 27002) has been implemented at the Bavarian universities. However, most of the obligatory ISMS requirements have not yet been fulfilled and no university has implemented all controls completely. In order to benefit from these differences in implementation and to improve the information security situation at all universities, proposals for action were drawn up. They serve as a guidance to review which ISMS requirements and information security controls and processes have not yet been implemented and in what way they can be realized. In order to fulfil the many ISMS requirements, information security tasks, and proposals for action, the universities need to establish more personnel and new competences. It would be useful to set up a Bavarian university ISMS network, that involves at least one representative of each participating university. By the intensifying communication among each other, the implementation of an ISMS could be facilitated and improved. This would lead to less time exposure and costs as well as to a reduction of the total effort, and, above all and most importantly, to the improvement of the information security situation at all universities.

## Research Question 2

**How can the compared information security controls of the first research question be measured?**

In order to measure the information security controls and processes, an information security measurement system with own metrics and key performance indicators (KPIs) was created according to the bottom-up approach. A handful of key metrics were determined by a large number of metrics. 23 measurement procedures were modeled in tabular form, yielding fifteen performance indicators and nine effectiveness indicators. Since the KPIs must always be specifically geared to the university's objectives and no universally applicable KPIs exist, a prioritizing of the 24 indicators and the subsequent selection of the KPIs by the universities themselves would be most effective. To support the KPI determination process, a value benefit analysis was modelled. For this purpose, five weighted evaluation criteria were drawn up and a KPI range was selected. The self-conducted analysis resulted in seven KPIs. By the prepared measurement procedures, the universities will be able to measure the performance and effectiveness of their information security controls and processes.

## Research Question 3

**Is the preparation of a uniform information security report for universities feasible and what might a template for such a report look like?**

After the applicability of an information security report has been scrutinized and a report structure with its components could be determined by a requirements elicitation according to the ISO/IEC 27000-series, it was clear that the preparation of a uniform information security report for universities is feasible and even highly advisable. In consequence, an information security report template with input fields was designed by Microsoft Word in English and German. It can be used by both universities and universities of applied sciences and is primarily addressed to the respective university management as the main recipient. Due to the facts that the semester cycles at universities are half-yearly, the winter semester does not end simultaneously with the end of the year, and the current ISMS is in the building phase, it is advisable to prepare and submit an information security report at the end of every semester covering the reporting period of the respective semester.

An overall information security report on the information security situation at all Bavarian universities could be reported to the competent authorities or the ministry in one report if each university is willing to submit their information security report to a specific body or person who prepares the overall report carefully and reliably by a certain deadline. This step would facilitate the communication and bureaucracy burdens between the universities and the relevant authorities vastly. By the drafted information security report template, all universities benefit from a uniform report framework that simplifies their own information security reporting processes and at the same time creates a uniform way of reporting and communication between all universities.

# 7. Conclusion

The comparison of the twelve Bavarian state universities and universities of applied sciences at the beginning of the work has shown that all universities have overcome the first obstacles towards the implementation of an information security management system by the realization of many similar information security controls and processes. Nevertheless, there is still a lot of work to be done in order to fulfill all requirements of the ISO/IEC 27001 certification standard. In order to facilitate this work, the master thesis provides valuable results on the improvement and implementation, measurement, and reporting of information security.

The proposals for action that were worked out should help the universities to implement their missing ISMS requirements and information security controls, to profit by the comparability created among themselves, and to improve their information security situation in the end. They should be given to all universities as a guidance.

By the created information security measurement system with its 23 measurement procedures, the universities will be able to measure the performance and effectiveness of their information security controls and processes successfully. For the continuation of the research, the measurement system should be put into practice by measuring and monitoring their indicators and KPIs continuously. The monitoring, measurement, analysis, and evaluation cycle should be maintained in the future.

The drafted information security report template provides all universities a report framework, which facilitates their own reporting processes on information security and at the same time creates a uniform way of reporting and communication between all universities. After all, an active communication between the universities should not be neglected but intensified in the future.

As the work has demonstrated, the implementation of the ISMS requirements and the information security controls according to the ISMS family of standards, the measurement of these processes, as well as the reporting on the current information security situation are not easy tasks for universities. A multitude of existing procedures must be scrutinized and analyzed. Personnel, money, and know-how must be made available. But it is worth the effort because the ensuring of information security is indispensable. The challenges and threats to information security will continue to increase in the future, however, the Bavarian universities are undoubtedly on the right track and well prepared to protect their information in this future.

# List of Cited Literature

**Alsmadi, Izzat; Burdwell, Robert; Aleroud, Ahmed; Wahbeh, Abdallah; Al-Qudah, Mahmood; Al-Omari, Ahmad (2018):** Practical Information Security. A Competency-Based Education Course. Springer International Publishing AG, n.p.p., 2018.

**BayEGovG (2015):** Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG). (GVBl. S. 458) BayRS 206-1-F (Art. 1–19). München, December 15, 2015.

**Boehmer, Wolfgang (2008):** Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001. Second International Conference on Emerging Security Information, Systems and Technologies, pp. 224–231, Cap Esterel, France, IEEE, August 25–31, 2008.

**Chew, Elizabeth; Swanson, Marianne; Stine, Kevin; Bartol, Nadya; Brown, Anthony; Robinson, Will (2008):** Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Revision 1, Gaithersburg, July 2008.

**DIN EN ISO/IEC (2016):** DIN EN ISO/IEC 27042. Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence (ISO/IEC 27042:2015); German version EN ISO/IEC 27042:2016. DIN Deutsches Institut für Normung e. V., Beuth Verlag, Berlin, December 2016.

**DIN EN ISO/IEC (2017a):** DIN EN ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015); English version EN ISO/IEC 27001:2017, English translation of DIN EN ISO/IEC 27001:2017-06. DIN Deutsches Institut für Normung e. V., Beuth Verlag, Berlin, June 2017.

**DIN EN ISO/IEC (2017b):** DIN EN ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015); English version EN ISO/IEC 27002:2017, English translation of DIN EN ISO/IEC 27002:2017-06. DIN Deutsches Institut für Normung e. V., Beuth Verlag, Berlin, June 2017.

**Grönert, Tobias; Pöppelbuß, Jens; Breiter, Andreas (2014):** Reifegradbestimmung der IT-Governance: Eine Fallstudie zur Anwendbarkeit des COBIT 5 PAM in der öffentlichen Verwaltung. Informatik 2014, pp. 1513–1525, Gesellschaft für Informatik e.V., Bonn, 2014.

**Hassler, Marko (2012):** Web Analytics. Metriken auswerten, Besucherverhalten verstehen, Website optimieren. Mitp, Heidelberg, München, Landsberg, Frechen, Hamburg, 2012.

**Helmke, Stefan; Uebel, Matthias (2013):** Managementorientiertes IT-Controlling und IT-Governance. Springer Gabler, Wiesbaden, 2013.

**Herbig, Norbert (2016):** Nutzwertanalyse. Eine Methode zur Bewertung von Lösungsalternativen und zur Entscheidungsfindung. BoD – Books on Demand, Norderstedt, 2016.

**Humpert-Vrielink Frederik; Vrielink Nina (2012):** A Modern Approach in Information Security Measurement. Securing Electronic Business Processes, pp. 48–53, Springer Fachmedien, Wiesbaden, 2012.

**ISO (2018):** ISO Survey 2017. International Organization for Standardization (ISO), August 2018. Accessed January 15, 2019 from https://www.iso.org/the-iso-survey.html.

**ISO/IEC (2018a):** International Standard ISO/IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO/IEC, Switzerland, Fifth edition, February 2018.

**ISO/IEC (2018b):** International Standard ISO/IEC 27005. Information technology — Security techniques — Information security risk management. ISO/IEC, Switzerland, Third edition, July 2018.

**ISO/IEC (2017):** International Standard ISO/IEC 27003. Information technology — Security techniques — Information security management systems — Guidance. ISO/IEC, Switzerland, Second edition, March 2017.

**ISO/IEC (2016):** International Standard ISO/IEC 27004. Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation. ISO/IEC, Switzerland, Second edition, December 15, 2016.

**ISO/IEC (2013):** International Standard ISO/IEC 27014. Information technology — Security techniques — Governance of information security. ISO/IEC, Switzerland, First edition, May 15, 2013.

**IT Governance (2018):** The ISO/IEC 27000 Family of Information Security Standards. Accessed November 8, 2018 from https://www.itgovernance.co.uk/iso27000-family.

**Jacobs, Stephan (2013):** CMMI (Capability Maturity Model Integration). Accessed December 3, 2018 from http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/is-management/Systementwicklung/reifegradmodelle/cmmi/index.html.

**Janus, Philo (2008):** Pro PerformancePoint Server 2007. Building Business Intelligence Solutions. Apress, n.p.p., 2008.

**Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen; Schröder, Klaus-Werner (2016):** IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Springer Vieweg, Wiesbaden, 2016.

**Kütz, Martin (2009):** Kennzahlen in der IT. Werkzeuge für Controlling und Management. 3., überarbeitete und erweiterte Auflage. dpunkt.verlag GmbH, Heidelberg, 2009.

**Lea, Bih-Ru; Fui-Hoon Nah, Fiona (2013):** Usability of Performance Dashboards, Usefulness of Operational and Tactical Support, and Quality of Strategic Support: A Research Framework. Human Interface and the Management of Information. Information and Interaction for Health, Safety, Mobility and Complex Environments (Part 2), pp. 116–123, Springer, Berlin, Heidelberg, 2013.

**Lead Light (2018):** The KPI S-M-A-R-T Rule. Lead Light Technologies Corporation. Accessed December 20, 2018 from http://www.lltcorp.com/content/kpi-s-m-r-t-rule.

**Merriam-Webster (2018):** Definition of "Security". Merriam-Webster Online. Accessed September 4, 2018 from https://www.merriam-webster.com/dictionary/security.

**Taylor, Jonathan (2017): '**What is a KPI, Metric or Measure?'. Klipfolio Inc. February 22, 2017. Accessed December 7, 2018 from https://www.klipfolio.com/blog/kpi-metric-measure.

# Annex

**Table 3:** Audit Results to the ISMS Requirements Specified in Clauses 4 to 10 of ISO/IEC 27001

| Clause | ISMS Requirement | Avg. | U1 | U2 | U3 | U4 | U5 | U6 | U7 | U8 | U9 | U10 | U11 | U12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4<br>*Context of the organization* | Determine the university's ISMS objectives and the issues that affect the effectiveness | **2.1** | 3 | 4 | 3 | 1 | 2 | 1 | 1 | 0 | 1 | 3 | 1 | 5 |
| | Identify the involved environment including applicable laws, regulations, contracts, etc. | **3.6** | 4 | 4 | 3 | 3 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 |
| | Determine the information security requirements and the obligations of the involved environment | **2.6** | 3 | 4 | 3 | 1 | 2 | 2 | 2 | 3 | 2 | 4 | 1 | 4 |
| | Determine and document the scope of the ISMS | **2.3** | 3 | 4 | 3 | 1 | 4 | 2 | 1 | 0 | 0 | 3 | 1 | 5 |
| | Establish, implement, maintain, and continually improve an ISMS in accordance with the standard | **1.3** | 1 | 1 | 1 | 0 | 4 | 0 | 2 | — | 0 | 1 | 0 | 4 |
| 5<br>*Leadership* | The university management shall demonstrate leadership and commitment with respect to the ISMS | **2.3** | 3 | 4 | 3 | 2 | 3 | 3 | 0 | 1 | 0 | 2 | 2 | 4 |
| | Document the information security policies | **1.6** | 1 | 3 | 2 | 1 | 3 | 0 | 1 | 2 | 0 | 2 | 2 | 2 |
| | Assign the roles and responsibilities of information security and communicate them | **2.3** | 3 | 3 | 3 | 2 | 5 | 1 | 1 | 1 | 1 | 2 | 1 | 5 |
| 6<br>*Planning (incl. risk management)* | Develop/plan the ISMS to fulfill requirements for dealing with risks | **0.9** | 1 | 0 | 1 | 0 | 3 | 0 | 1 | 0 | 2 | 0 | 0 | 3 |
| | Determine and apply an information security risk assessment process | **0.7** | 0 | 0 | 1 | 0 | 3 | 0 | 2 | 0 | 1 | 0 | 0 | 1 |
| | Document and apply an information security risk treatment process | **0.9** | 3 | 0 | 0 | 0 | 3 | 0 | 2 | 1 | 1 | 0 | 0 | 1 |
| | Establish and document information security objectives and plans | **1.4** | 1 | 3 | 1 | 0 | 4 | 0 | 1 | 2 | 0 | 1 | 0 | 4 |
| 7<br>*Support* | Determine the necessary resources for the ISMS and assign them to persons | **2.0** | 4 | 3 | 2 | 2 | 2 | 1 | 2 | 1 | 0 | 2 | 2 | 3 |
| | Determine, document, and make competences available | **2.0** | 3 | 1 | 2 | 2 | 3 | 1 | 2 | 2 | 0 | 2 | 2 | 4 |
| | Establish a security awareness program | **1.0** | 3 | 0 | 0 | 0 | 2 | 0 | 1 | 0 | 0 | 2 | 0 | 4 |
| | Determine the need for internal and external communications relevant to the ISMS | **1.9** | 3 | 3 | 3 | 0 | 2 | 0 | 2 | 0 | 2 | 3 | 0 | 5 |
| | Provide the documents required by the standard and the university | **1.8** | 3 | 3 | 1 | 1 | 3 | 0 | 2 | 2 | 0 | 1 | 1 | 5 |
| | Provide titles, authors, etc.; keep the formatting uniform; check and approve them | **1.4** | 2 | 4 | 0 | 0 | 3 | — | 0 | 1 | 0 | 1 | 0 | 4 |

| Clause | ISMS Requirement | Avg. | U 1 | U 2 | U 3 | U 4 | U 5 | U 6 | U 7 | U 8 | U 9 | U 10 | U 11 | U 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Manage the documents carefully | **2.0** | 3 | 4 | 1 | 0 | 4 | — | 1 | 0 | 0 | 3 | 2 | 4 |
| *8 Operation (incl. risk management)* | Plan, implement, control, and document the ISMS processes to manage risks (e.g., risk treatment plans) | **0.6** | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 1 | 2 | 0 | 0 | 1 |
| | Identify and document information security risks regularly and in the event of changes | **0.3** | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| | Implement a risk treatment plan and handle the risks; document the results | **0.5** | 2 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 2 |
| *9 Performance evaluation* | Monitor, measure, analyze, and evaluate the ISMS and the controls | **0.1** | 0 | 0 | 0 | — | 1 | — | 0 | — | 0 | 0 | 0 | 0 |
| | Plan and conduct internal audits of the ISMS | **1.8** | 2 | 1 | 1 | — | 3 | 2 | 2 | 0 | 1 | 2 | 2 | 4 |
| | Report regularly on the ISMS to the university management | **1.4** | 1 | 0 | 0 | — | 5 | 1 | 1 | 0 | 0 | 2 | 1 | 4 |
| *10 Improvement* | Identify, correct, and prevent the occurrence of nonconformities and document the activities | **1.2** | 1 | 0 | 3 | — | 3 | — | 0 | 0 | 1 | 1 | 0 | 3 |
| | Improve the ISMS continuously | **1.2** | 0 | 1 | 0 | — | 4 | — | 1 | 0 | 1 | 1 | 0 | 4 |

(Adapted from: Augsburg University of Applied Sciences)

**Table 4:** Audit Results to the Controls Specified in Annex A of ISO/IEC 27001 (or ISO/IEC 27002)

| Clause | Control | Avg. | U 1 | U 2 | U 3 | U 4 | U 5 | U 6 | U 7 | U 8 | U 9 | U 10 | U 11 | U 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *A.5 Information security policies* | 5.1.1 Policies for information security | **2.1** | 2 | 3 | 3 | 2 | 3 | 1 | 1 | 2 | 3 | 1 | 1 | 3 |
| | 5.1.2 Review of the policies for information security | **1.9** | 3 | 2 | — | 2 | 4 | 0 | — | 0 | 1 | 3 | 0 | 4 |
| *A.6 Organization of information security* | 6.1.1 Information security roles and responsibilities | **2.2** | 3 | 3 | 3 | 1 | 4 | 1 | 1 | 1 | 1 | 2 | 2 | 4 |
| | 6.1.2 Segregation of duties | **2.7** | 4 | 3 | 4 | 1 | 3 | 2 | 4 | 1 | 3 | 2 | 1 | 4 |
| | 6.1.3 Contact with authorities | **3.4** | 3 | 2 | 3 | — | 4 | 2 | 2 | 4 | 4 | 4 | 4 | 5 |
| | 6.1.4 Contact with special interest groups | **3.9** | 3 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 5 |
| | 6.1.5 Information security in project management | **2.3** | 2 | 3 | 2 | 1 | 3 | 1 | 3 | 2 | 3 | 3 | 3 | 2 |
| | 6.2.1 Mobile device policy | **1.4** | 0 | 0 | 1 | 2 | 4 | 0 | 1 | 3 | 3 | 3 | 0 | 0 |
| | 6.2.2 Teleworking | **3.4** | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 3 | 3 | 4 | 1 | 4 |
| *A.7 Human resource security* | 7.1.1 Screening | **4.5** | 4 | 4 | — | 5 | 5 | 4 | 5 | 5 | — | 4 | 5 | 4 |
| | 7.1.2 Terms and conditions of employment | **4.4** | 4 | 4 | — | 5 | 5 | 4 | 5 | 5 | — | 4 | 4 | 4 |
| | 7.2.1 Management responsibilities | **1.4** | 2 | 3 | 1 | 2 | 1 | 0 | 0 | 2 | 0 | 2 | 1 | 3 |
| | 7.2.2 Information security awareness, education and training | **1.4** | 3 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 0 | 1 | 1 | 2 |
| | 7.2.3 Disciplinary process | **4.1** | 4 | 4 | — | 4 | 5 | 4 | 4 | 4 | — | 4 | 4 | 4 |
| | 7.3.1 Termination or change of employment responsibilities | **3.8** | 3 | 3 | 3 | 5 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 5 |
| *A.8 Asset management* | 8.1.1 Inventory of assets | **3.0** | 3 | 3 | 1 | 4 | 3 | 3 | 3 | 4 | 2 | 3 | 3 | 4 |
| | 8.1.2 Ownership of assets | **2.6** | 4 | 3 | 0 | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 3 | 2 |
| | 8.1.3 Acceptable use of assets | **2.9** | 3 | 4 | 3 | 2 | 3 | 3 | 2 | 4 | 2 | 4 | 3 | 2 |
| | 8.1.4 Return of assets | **3.4** | 3 | 4 | 4 | 3 | 4 | 3 | 4 | 4 | 2 | 4 | 4 | 2 |
| | 8.2.1 Classification of information | **1.4** | 1 | 1 | 2 | 2 | 2 | 0 | 0 | 2 | 3 | 2 | 2 | 0 |

| **Clause** | **Control** | **Avg.** | **U 1** | **U 2** | **U 3** | **U 4** | **U 5** | **U 6** | **U 7** | **U 8** | **U 9** | **U 10** | **U 11** | **U 12** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 8.2.2 Labelling of information | **0.5** | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 3 | 1 | 0 |
| | 8.2.3 Handling of assets | **1.9** | 1 | 2 | 1 | 2 | 4 | 0 | 2 | 3 | 3 | 2 | 3 | 0 |
| | 8.3.1 Management of removable media | **1.3** | 1 | 0 | 4 | 0 | 1 | 3 | 0 | 2 | 0 | 3 | 0 | 2 |
| | 8.3.2 Disposal of media | **4.2** | 4 | 4 | 4 | 4 | 5 | 3 | 4 | 4 | 5 | 4 | 4 | 5 |
| | 8.3.3 Physical media transfer | **4.8** | — | — | — | — | — | 5 | 5 | — | 5 | — | 4 | 5 |
| *A.9 Access control* | 9.1.1 Access control policy | **2.2** | 2 | 1 | 3 | 3 | 3 | 0 | 4 | 3 | 1 | 1 | 2 | 3 |
| | 9.1.2 Access to networks and network services | **2.3** | 3 | 0 | 1 | 4 | 3 | 1 | 3 | 3 | 4 | 1 | 1 | 3 |
| | 9.2.1 User registration and de-registration | **4.1** | 4 | 3 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 |
| | 9.2.2 User access provisioning | **3.6** | 3 | 3 | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 3 | 4 |
| | 9.2.3 Management of privileged access rights | **3.9** | 3 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 3 |
| | 9.2.4 Management of secret authentication information of users | **4.3** | 4 | 4 | 4 | 5 | 4 | 5 | 3 | 5 | 5 | 5 | 3 | 5 |
| | 9.2.5 Review of user access rights | **2.7** | 2 | 2 | 4 | 3 | 3 | 3 | 4 | 3 | 1 | 1 | — | 4 |
| | 9.2.6 Removal or adjustment of access rights | **3.8** | 4 | 2 | 5 | 3 | 4 | 4 | 5 | 4 | 4 | 3 | 4 | 4 |
| | 9.3.1 Use of secret authentication information | **3.5** | 4 | 3 | 4 | 5 | 4 | 4 | 3 | 3 | 3 | 3 | 3 | 3 |
| | 9.4.1 Information access restriction | **4.1** | 4 | 2 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | — | 4 | 5 |
| | 9.4.2 Secure log-on procedures | **3.7** | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 3 | 3 | 4 | 3 |
| | 9.4.3 Password management system | **3.2** | 3 | 3 | 3 | 4 | 3 | 3 | 4 | 3 | 3 | 3 | 3 | 3 |
| | 9.4.4 Use of privileged utility programs | **3.0** | — | 3 | — | 4 | — | — | — | — | — | — | 2 | — |
| | 9.4.5 Access control to program source code | **4.7** | — | — | — | 5 | — | — | 5 | — | — | — | 4 | — |
| *A.10 Cryptography* | 10.1.1 Policy on the use of cryptographic controls | **1.1** | 1 | 1 | 0 | 0 | 2 | 0 | 0 | 1 | 1 | 2 | 3 | 2 |
| | 10.1.2 Key management | **3.9** | 4 | 4 | 4 | 4 | 5 | 4 | 2 | 4 | 4 | 4 | 4 | 4 |

| Clause | Control | Avg. | U 1 | U 2 | U 3 | U 4 | U 5 | U 6 | U 7 | U 8 | U 9 | U 10 | U 11 | U 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *A.11 Physical and environmental security* | 11.1.1 Physical security perimeter | **3.4** | 4 | 4 | 4 | 3 | 3 | 3 | 3 | 4 | 3 | 3 | 3 | 4 |
| | 11.1.2 Physical entry controls | **3.8** | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 3 | 4 | 4 | 5 |
| | 11.1.3 Securing offices, rooms and facilities | **3.7** | 3 | 4 | 5 | 4 | 2 | 3 | 4 | 4 | 2 | 4 | 4 | 5 |
| | 11.1.4 Protecting against external and environmental threats | **3.9** | 4 | 4 | 5 | 4 | 3 | 4 | 5 | 4 | 3 | 4 | 4 | 3 |
| | 11.1.5 Working in secure areas | **3.1** | 3 | 3 | 3 | 3 | 4 | 2 | 3 | 4 | 3 | 3 | 2 | 4 |
| | 11.1.6 Delivery and loading areas | **4.3** | 4 | 4 | — | 5 | 4 | 4 | 5 | 4 | — | 4 | 4 | 5 |
| | 11.2.1 Equipment siting and protection | **4.2** | 4 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 |
| | 11.2.2 Supporting utilities | **4.5** | 3 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 4 | 5 |
| | 11.2.3 Cabling security | **4.3** | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 4 | 4 | 4 |
| | 11.2.4 Equipment maintenance | **4.2** | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| | 11.2.5 Removal of assets | **5.0** | — | — | 5 | — | — | — | — | — | — | — | — | — |
| | 11.2.6 Security of equipment and assets off-premises | **4.3** | — | — | 5 | — | — | — | 5 | — | 3 | — | — | — |
| | 11.2.7 Secure disposal or re-use of equipment | **3.7** | 4 | 4 | 2 | 2 | 5 | 4 | 3 | 4 | 3 | 4 | 4 | 5 |
| | 11.2.8 Unattended user equipment | **3.8** | 3 | 3 | 3 | 5 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 |
| | 11.2.9 Clear desk and clear screen policy | **2.3** | 3 | 2 | 3 | 3 | 3 | 2 | 3 | 0 | 0 | 2 | 3 | 3 |
| *A.12 Operations security* | 12.1.1 Documented operating procedures | **3.2** | 2 | 3 | 3 | 4 | 4 | 2 | 3 | 3 | 4 | 4 | 3 | 3 |
| | 12.1.2 Change management | **3.4** | 3 | 4 | 3 | 3 | 4 | 3 | 4 | 4 | 3 | 3 | 3 | 4 |
| | 12.1.3 Capacity management | **4.1** | 4 | 3 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| | 12.1.4 Separation of development, testing and operational environments | **4.0** | 4 | 4 | 3 | 5 | 4 | 4 | — | 4 | 3 | 4 | 4 | 5 |
| | 12.2.1 Controls against malware | **3.8** | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 4 |

| Clause | Control | Avg. | U 1 | U 2 | U 3 | U 4 | U 5 | U 6 | U 7 | U 8 | U 9 | U 10 | U 11 | U 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 12.3.1 Information backup | **4.3** | 5 | 4 | 4 | 5 | 5 | 4 | 3 | 4 | 4 | 4 | 4 | 5 |
| | 12.4.1 Event logging | **2.3** | 2 | 2 | 2 | 2 | 3 | 1 | 2 | 3 | 3 | 3 | 1 | 4 |
| | 12.4.2 Protection of log information | **1.3** | 0 | 2 | 0 | 2 | 2 | 0 | 0 | — | 0 | 4 | 0 | 4 |
| | 12.4.3 Administrator and operator logs | **1.3** | 0 | 0 | 2 | 0 | 2 | 1 | 0 | 3 | 1 | 3 | 0 | 4 |
| | 12.4.4 Clock synchronization | **4.8** | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 |
| | 12.5.1 Installation of software on operational systems | **3.9** | 4 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| | 12.6.1 Management of technical vulnerabilities | **2.7** | 3 | 2 | 2 | 2 | 3 | 3 | 2 | 4 | 2 | 3 | 3 | 3 |
| | 12.6.2 Restriction on software installation | **3.4** | 3 | 4 | 3 | 4 | 3 | 3 | 4 | 3 | 3 | 4 | 4 | 3 |
| | 12.7.1 Information systems audit controls | **—** | — | — | — | — | — | — | — | — | — | — | — | — |
| *A.13 Communications security* | 13.1.1 Network controls | **3.9** | 4 | 4 | 3 | 4 | 4 | 4 | 5 | 4 | 3 | 4 | 4 | 4 |
| | 13.1.2 Security of network services | **4.3** | 5 | 4 | 3 | 5 | 4 | 4 | 5 | 5 | 3 | 4 | 5 | 4 |
| | 13.1.3 Segregation in networks | **3.8** | 4 | 4 | 2 | 5 | 3 | 4 | 4 | 4 | 3 | 4 | 4 | 4 |
| | 13.2.1 Information transfer policies and procedures | **1.8** | 1 | 2 | 2 | 0 | 3 | 3 | 1 | 3 | 1 | 1 | 2 | 3 |
| | 13.2.2 Agreements on information transfer | **3.5** | 3 | — | — | — | — | 4 | — | — | — | — | — | — |
| | 13.2.3 Electronic messaging | **3.4** | 4 | 4 | 2 | 3 | 4 | 4 | 3 | 4 | 2 | 3 | 4 | 4 |
| | 13.2.4 Confidentiality or non-disclosure agreements | **3.7** | 2 | 4 | 3 | 4 | 5 | 3 | 4 | 4 | 4 | 3 | 4 | 4 |
| *A.14 System acquisition, development and maintenance* | 14.1.1 Information security requirements analysis and specification | **2.5** | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 1 | 3 |
| | 14.1.2 Securing application services on public networks | **3.7** | 4 | — | 3 | — | 4 | 4 | — | — | 3 | — | 4 | 4 |
| | 14.1.3 Protecting application services transactions | **—** | — | — | — | — | — | — | — | — | — | — | — | — |
| | 14.2.1 Secure development policy | **0.4** | 0 | — | — | — | — | — | 0 | 2 | 0 | — | 0 | — |

| Clause | Control | Avg. | U 1 | U 2 | U 3 | U 4 | U 5 | U 6 | U 7 | U 8 | U 9 | U 10 | U 11 | U 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 14.2.2 System change control procedures | **4.0** | — | — | — | — | — | — | 4 | — | 4 | — | — | — |
| | 14.2.3 Technical review of applications after operating platform changes | **3.3** | 4 | — | 3 | — | — | — | 4 | 3 | 2 | 4 | — | — |
| | 14.2.4 Restrictions on changes to software packages | **—** | — | — | — | — | — | — | — | — | — | — | — | — |
| | 14.2.5 Secure system engineering principles | **1.6** | 2 | 3 | — | — | — | 3 | 0 | 3 | 0 | — | 0 | — |
| | 14.2.6 Secure development environment | **4.0** | — | — | — | — | — | — | 4 | — | — | — | 4 | — |
| | 14.2.7 Outsourced development | **3.0** | — | — | — | — | — | 3 | — | — | — | — | — | — |
| | 14.2.8 System security testing | **3.0** | — | — | — | — | — | 4 | — | — | — | — | 2 | — |
| | 14.2.9 System acceptance testing | **4.0** | — | — | — | — | — | 4 | — | — | — | — | 4 | — |
| | 14.3.1 Protection of test data | **4.5** | — | — | — | — | — | 5 | — | — | — | — | 4 | — |
| *A.15 Supplier relationships* | 15.1.1 Information security policy for supplier relationships | **2.7** | — | — | — | — | 2 | 3 | — | — | — | — | 3 | — |
| | 15.1.2 Addressing security within supplier agreements | **3.0** | — | — | — | — | — | 3 | — | — | — | — | — | — |
| | 15.1.3 Information and communication technology supply chain | **—** | — | — | — | — | — | — | — | — | — | — | — | — |
| | 15.2.1 Monitoring and review of supplier services | **4.0** | — | — | — | — | — | 4 | — | — | — | — | — | — |
| | 15.2.2 Managing changes to supplier services | **4.0** | — | — | — | — | — | 4 | — | — | — | — | — | — |
| *A.16 Information security incident management* | 16.1.1 Responsibilities and procedures | **3.2** | 3 | 3 | 4 | 0 | 4 | 4 | 1 | 3 | 4 | 4 | 4 | 4 |
| | 16.1.2 Reporting information security events | **1.8** | 2 | 0 | 3 | 0 | 1 | 1 | 0 | 2 | 2 | 3 | 3 | 4 |
| | 16.1.3 Reporting information security weaknesses | **1.5** | 2 | 0 | 3 | 0 | 0 | 0 | 0 | 1 | 3 | 1 | 3 | 5 |
| | 16.1.4 Assessment of and decision on information security events | **1.7** | 3 | 0 | 1 | 0 | 1 | 3 | 0 | 3 | 2 | 3 | 0 | 4 |
| | 16.1.5 Response to information security incidents | **2.7** | 3 | 0 | 4 | 0 | 4 | 4 | 0 | 3 | 4 | 4 | 2 | 4 |
| | 16.1.6 Learning from information security incidents | **2.2** | 4 | 0 | 1 | 0 | 3 | 1 | 0 | 4 | 4 | 4 | 0 | 5 |

| Clause | Control | Avg. | U 1 | U 2 | U 3 | U 4 | U 5 | U 6 | U 7 | U 8 | U 9 | U 10 | U 11 | U 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | 16.1.7 Collection of evidence | **—** | — | — | — | — | — | — | — | — | — | — | — | — |
| *A.17 Information security aspects of business continuity management* | 17.1.1 Planning information security continuity | **0.1** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
|  | 17.1.2 Implementing information security continuity | **1.1** | 0 | 1 | 2 | 0 | 0 | — | 4 | 0 | 2 | 2 | 0 | 1 |
|  | 17.1.3 Verify, review and evaluate information security continuity | **0.1** | 0 | 0 | 0 | 0 | 0 | — | 0 | 0 | 0 | 0 | 0 | 1 |
|  | 17.2.1 Availability of information processing facilities | **3.4** | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 3 | 2 | 3 | 4 | 3 |
| *A.18 Compliance* | 18.1.1 Identification of applicable legislation and contractual requirements | **3.5** | 4 | 4 | 4 | 0 | 5 | 4 | 0 | 4 | 4 | 4 | 4 | 5 |
|  | 18.1.2 Intellectual property rights | **3.3** | 4 | 4 | 3 | 2 | 4 | 3 | 1 | 3 | 4 | 4 | 4 | 3 |
|  | 18.1.3 Protection of records | **3.3** | 4 | 4 | 4 | 2 | 2 | 4 | 2 | 4 | 4 | 4 | 1 | 5 |
|  | 18.1.4 Privacy and protection of personally identifiable information | **4.3** | 4 | 4 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 5 |
|  | 18.1.5 Regulation of cryptographic controls | **2.8** | 2 | 4 | — | 3 | 3 | 3 | 4 | 2 | 3 | 3 | 2 | 2 |
|  | 18.2.1 Independent review of information security | **2.1** | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 4 |
|  | 18.2.2 Compliance with security policies and standards | **0.0** | 0 | 0 | 0 | — | 0 | — | 0 | 0 | 0 | 0 | 0 | 0 |
|  | 18.2.3 Technical compliance review | **2.1** | 4 | 2 | 3 | 0 | 2 | 0 | 0 | 1 | 3 | 3 | 3 | 4 |

(Adapted from: Augsburg University of Applied Sciences)

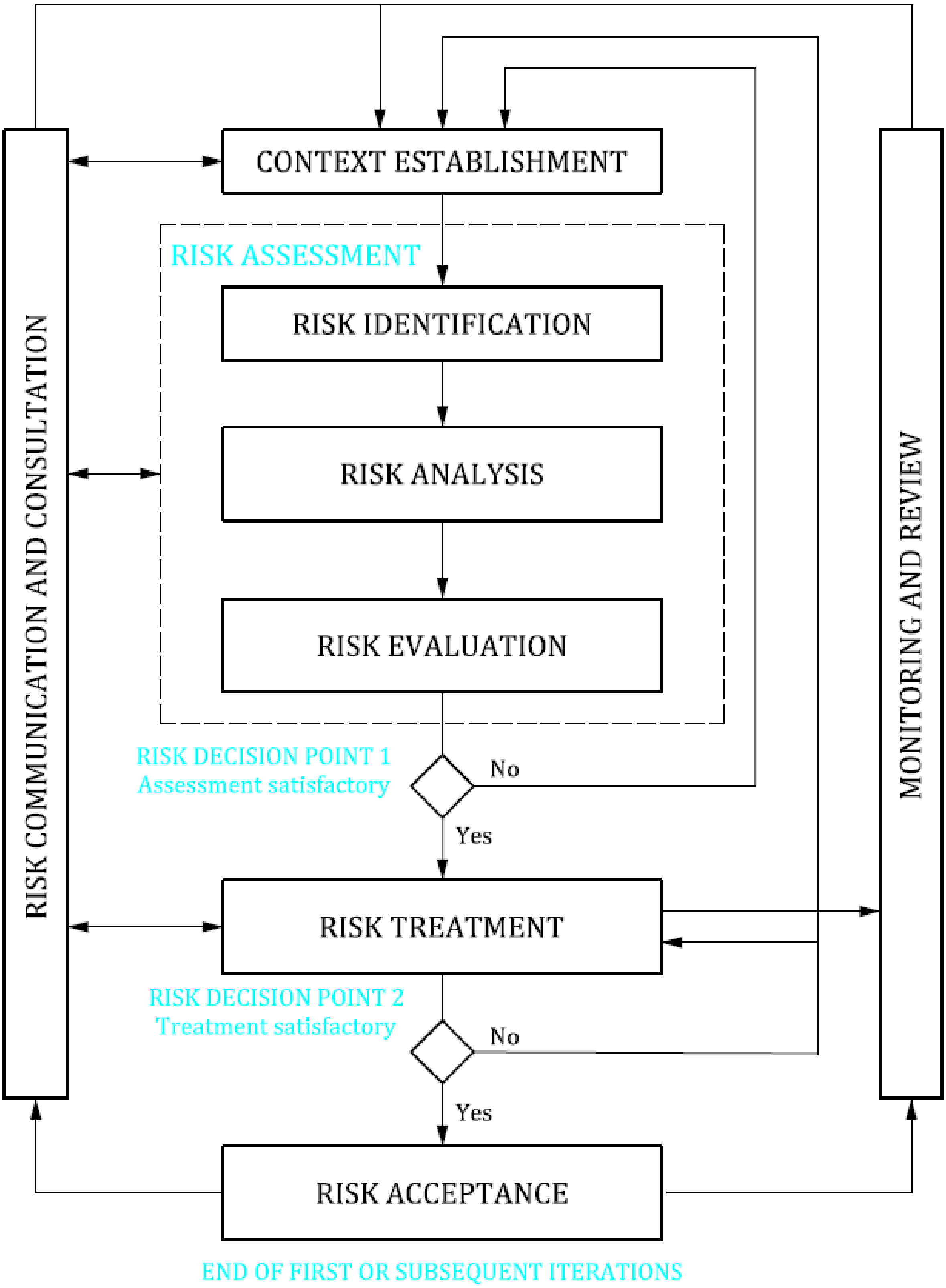
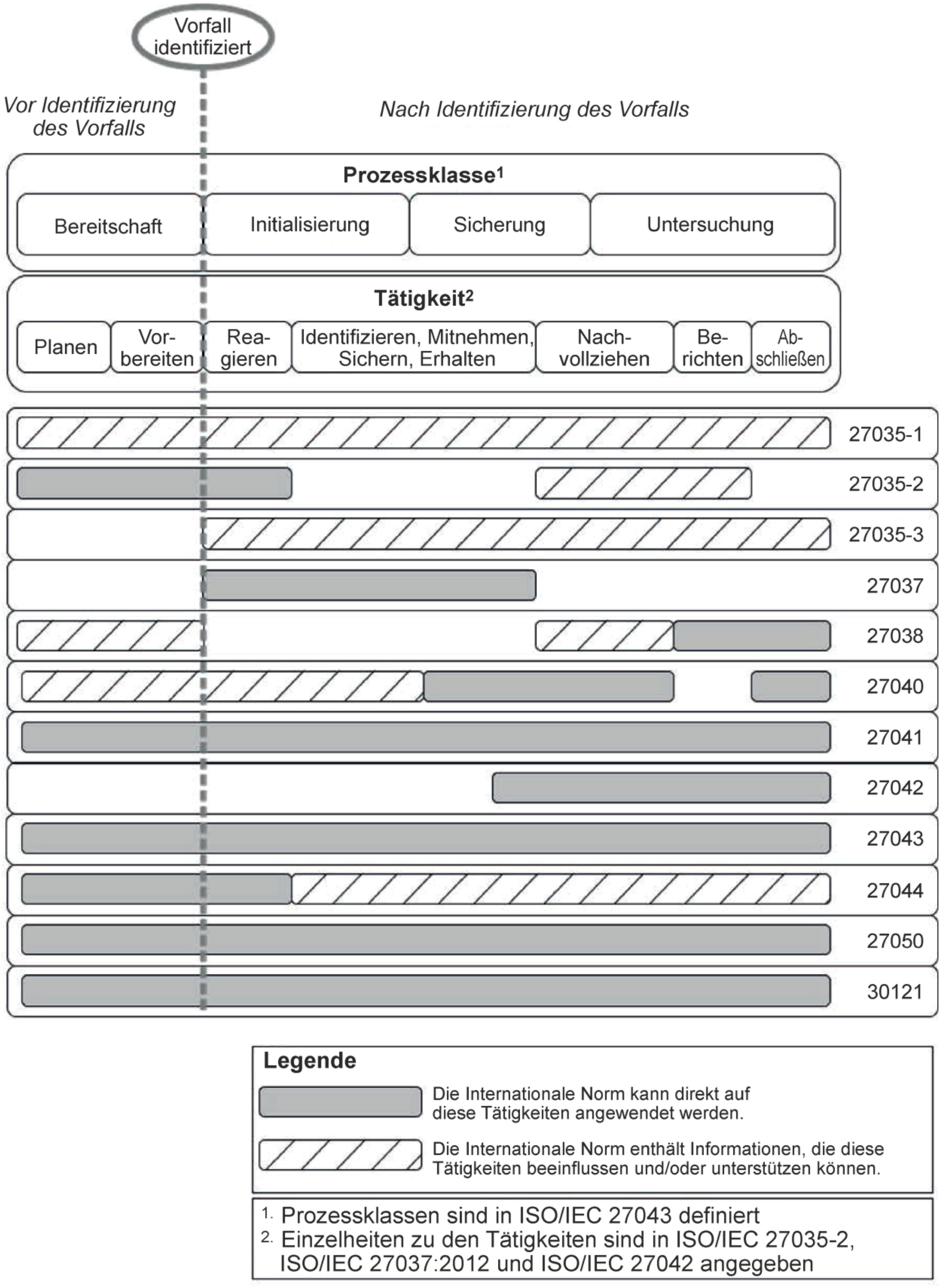


**Figure 5:** Information Security Risk Management Process

(Source: ISO/IEC, 2018b, p. 4)



Die Internationale Norm kann direkt auf diese Tätigkeiten angewendet werden.

Die Internationale Norm enthält Informationen, die diese Tätigkeiten beeinflussen und/oder unterstützen können.

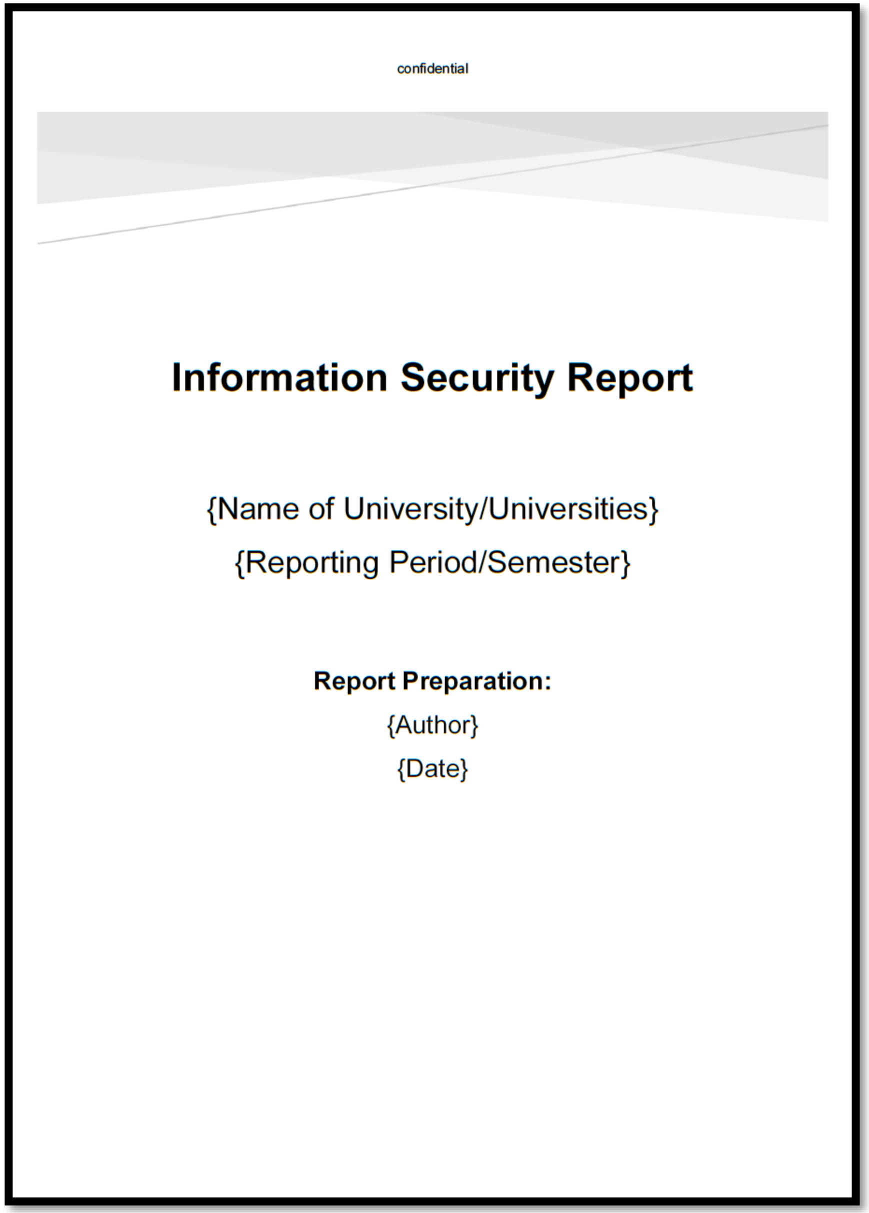
1. Prozessklassen sind in ISO/IEC 27043 definiert
2. Einzelheiten zu den Tätigkeiten sind in ISO/IEC 27035-2, ISO/IEC 27037:2012 und ISO/IEC 27042 angegeben

**Figure 12:** Applicability of the ISO/IEC Standards to the Examination Process Classes and Examination Activities (Incident Management)

(Source: DIN EN ISO/IEC, 2016, p. 9)

**Figure 18:** Information Security Report Template (English)

(Source: Own illustration)



confidential

# Information Security Report

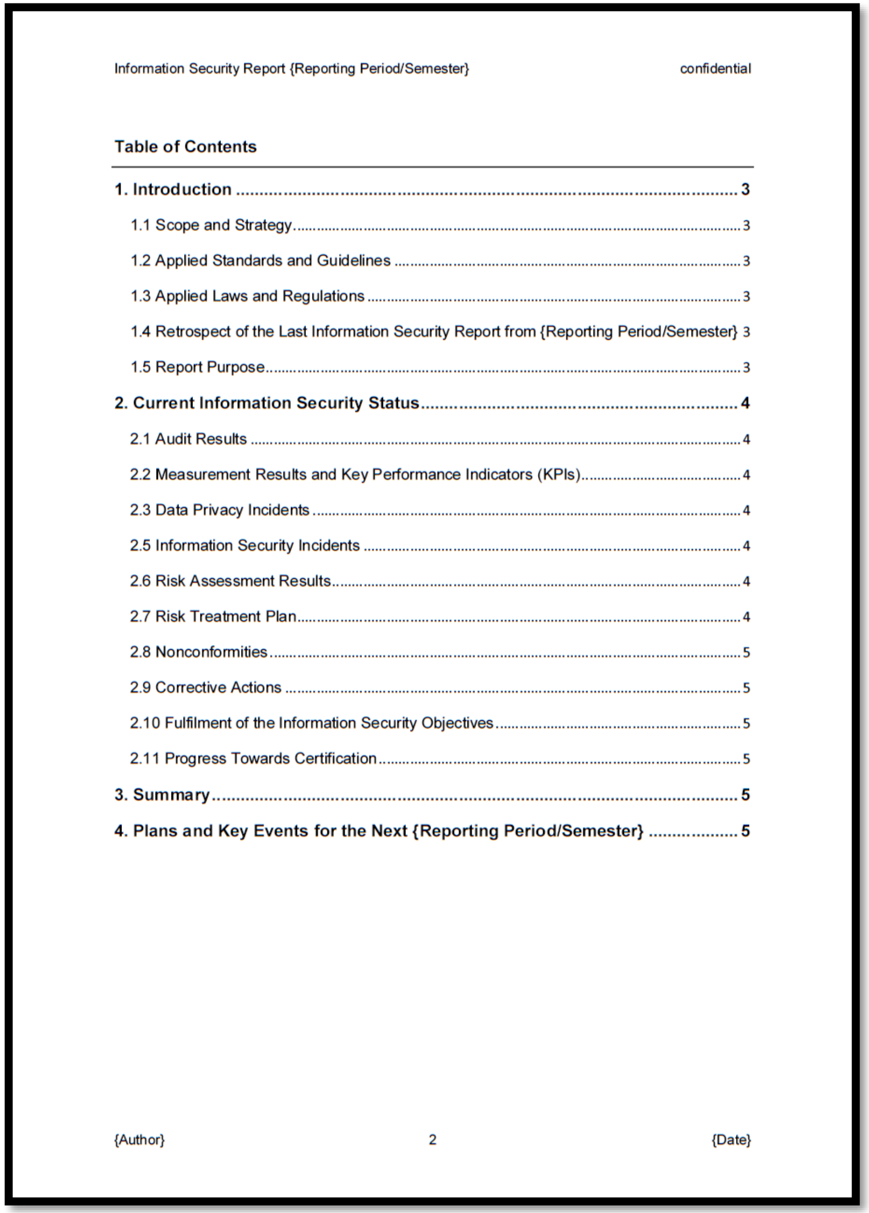
{Name of University/Universities}

{Reporting Period/Semester}

**Report Preparation:**

{Author}

{Date}



Information Security Report {Reporting Period/Semester} confidential

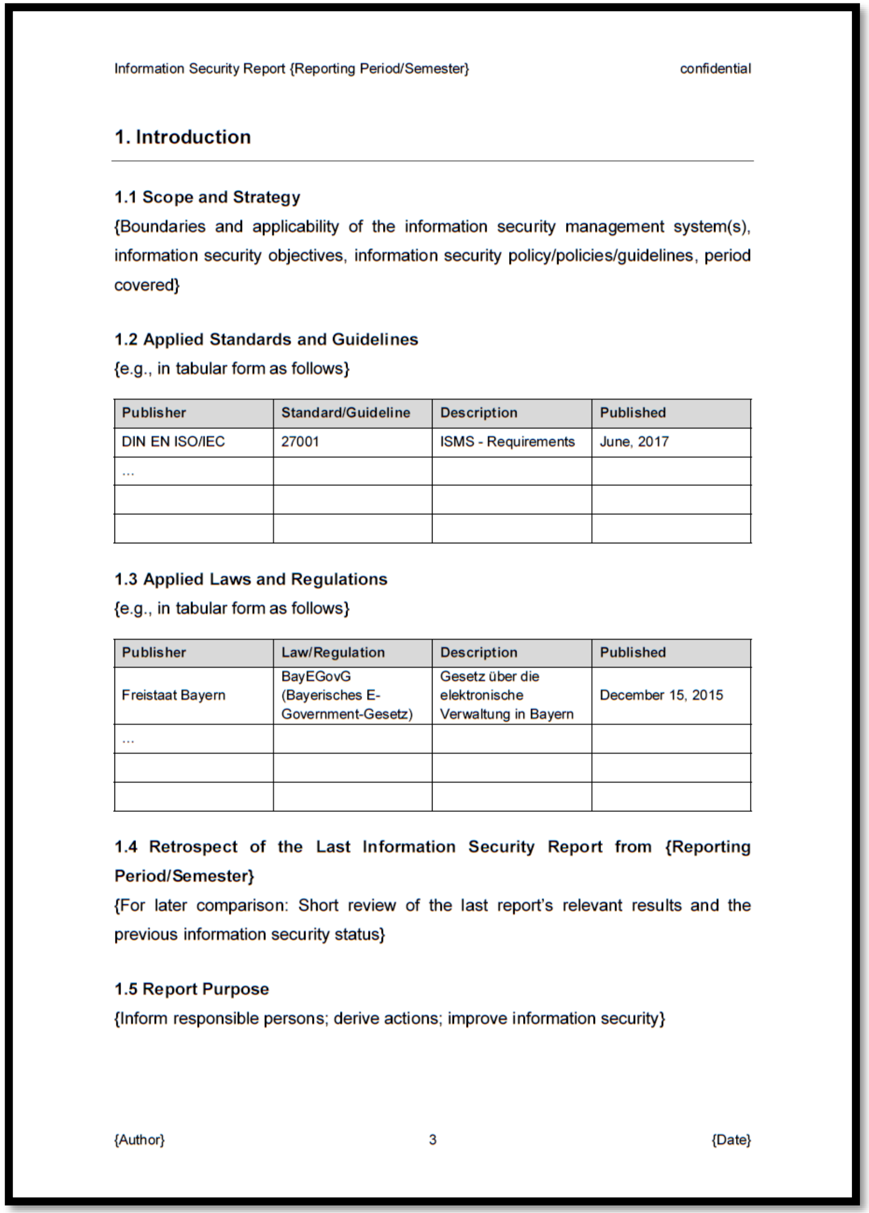
**Table of Contents**

{Author} 2 {Date}

*(continued)*

**Figure 18:** Information Security Report Template (English)

(Source: Own illustration)



Information Security Report {Reporting Period/Semester} confidential

## 1. Introduction

### 1.1 Scope and Strategy

{Boundaries and applicability of the information security management system(s), information security objectives, information security policy/policies/guidelines, period covered}

### 1.2 Applied Standards and Guidelines

{e.g., in tabular form as follows}

| Publisher | Standard/Guideline | Description | Published |
|---|---|---|---|
| DIN EN ISO/IEC | 27001 | ISMS - Requirements | June, 2017 |
| ... | | | |
| | | | |
| | | | |

### 1.3 Applied Laws and Regulations

{e.g., in tabular form as follows}

| Publisher | Law/Regulation | Description | Published |
|---|---|---|---|
| Freistaat Bayern | BayEGovG (Bayerisches E-Government-Gesetz) | Gesetz über die elektronische Verwaltung in Bayern | December 15, 2015 |
| ... | | | |
| | | | |
| | | | |

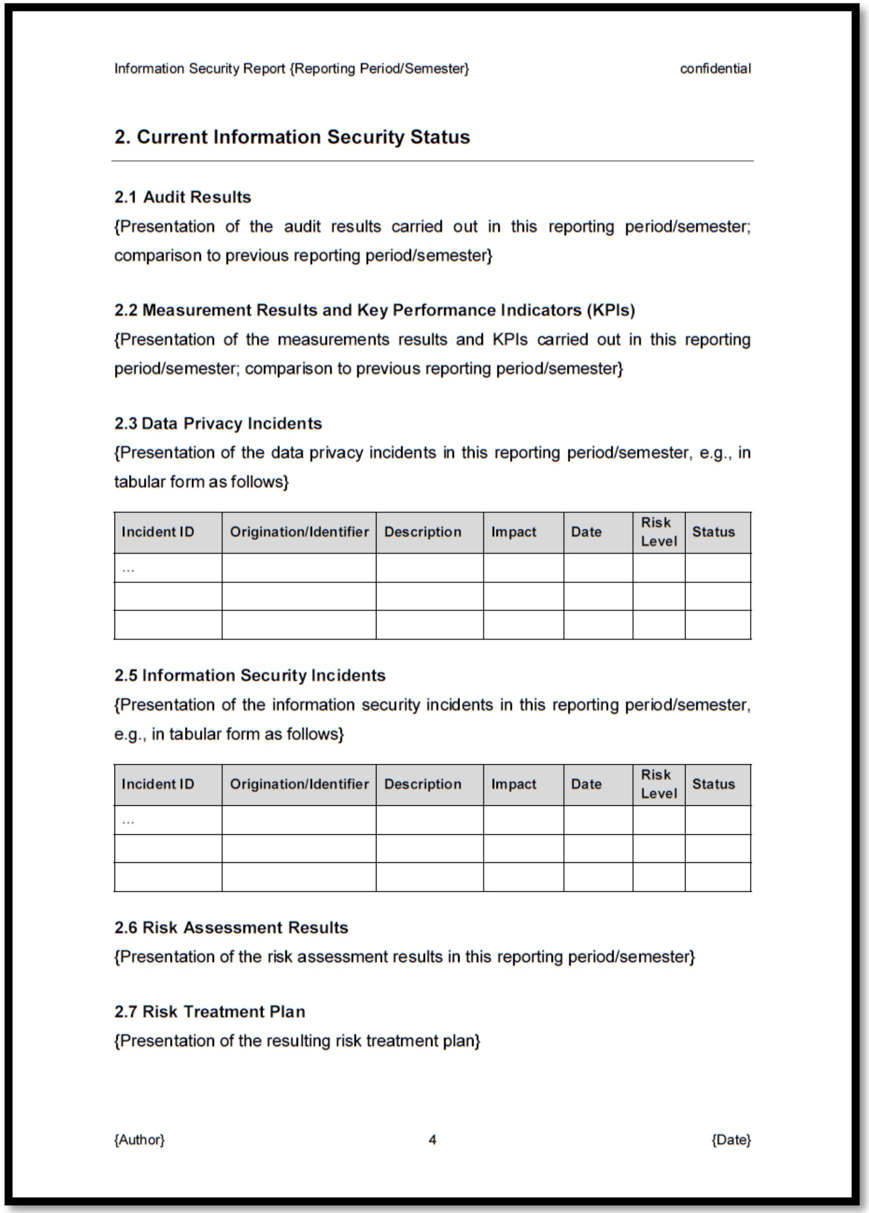
### 1.4 Retrospect of the Last Information Security Report from {Reporting Period/Semester}

{For later comparison: Short review of the last report's relevant results and the previous information security status}

### 1.5 Report Purpose

{Inform responsible persons; derive actions; improve information security}

{Author} 3 {Date}



Information Security Report {Reporting Period/Semester} confidential

## 2. Current Information Security Status

### 2.1 Audit Results

{Presentation of the audit results carried out in this reporting period/semester; comparison to previous reporting period/semester}

### 2.2 Measurement Results and Key Performance Indicators (KPIs)

{Presentation of the measurements results and KPIs carried out in this reporting period/semester; comparison to previous reporting period/semester}

### 2.3 Data Privacy Incidents

{Presentation of the data privacy incidents in this reporting period/semester, e.g., in tabular form as follows}

| Incident ID | Origination/Identifier | Description | Impact | Date | Risk Level | Status |
|---|---|---|---|---|---|---|
| ... | | | | | | |
| | | | | | | |
| | | | | | | |

### 2.5 Information Security Incidents

{Presentation of the information security incidents in this reporting period/semester, e.g., in tabular form as follows}

| Incident ID | Origination/Identifier | Description | Impact | Date | Risk Level | Status |
|---|---|---|---|---|---|---|
| ... | | | | | | |
| | | | | | | |
| | | | | | | |

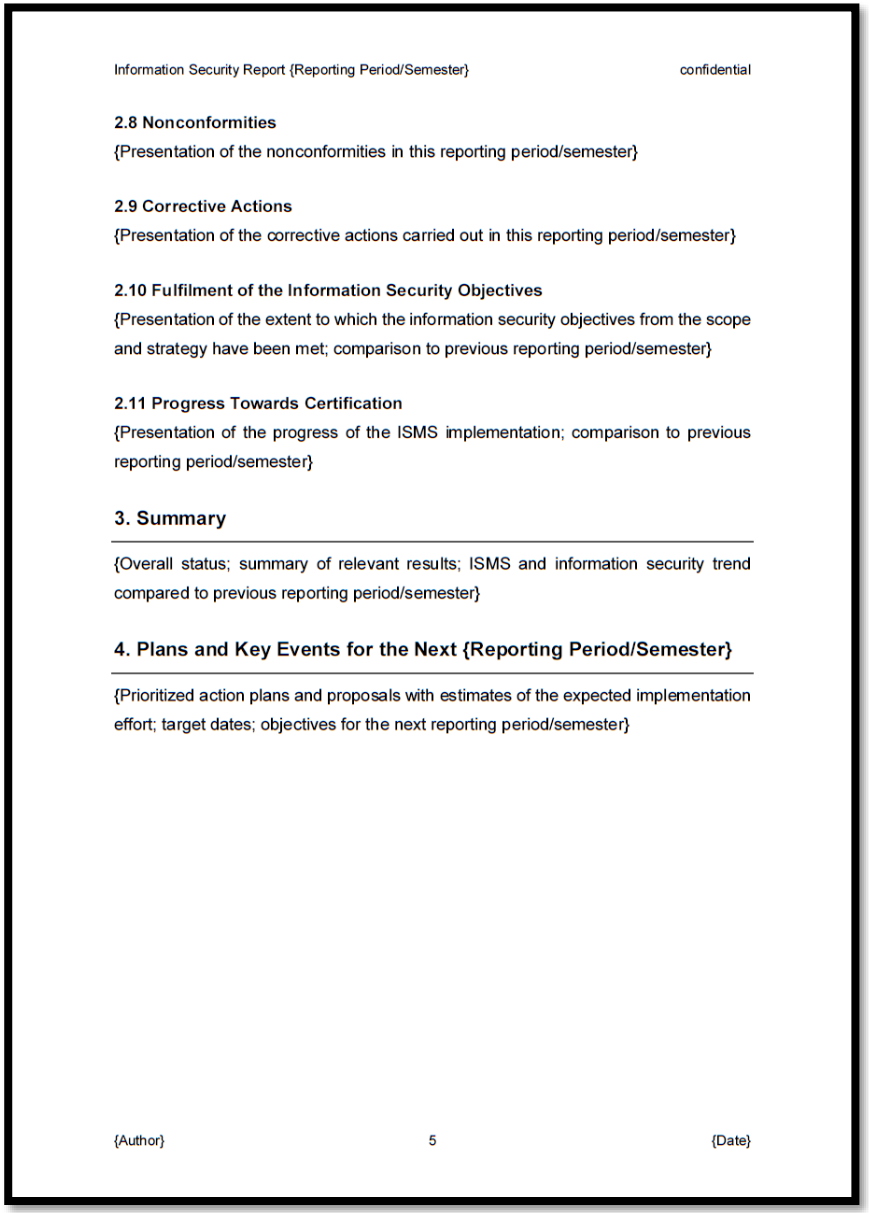
### 2.6 Risk Assessment Results

{Presentation of the risk assessment results in this reporting period/semester}

### 2.7 Risk Treatment Plan

{Presentation of the resulting risk treatment plan}

{Author} 4 {Date}



Information Security Report {Reporting Period/Semester} confidential

**2.8 Nonconformities**

{Presentation of the nonconformities in this reporting period/semester}

**2.9 Corrective Actions**

{Presentation of the corrective actions carried out in this reporting period/semester}

**2.10 Fulfilment of the Information Security Objectives**

{Presentation of the extent to which the information security objectives from the scope and strategy have been met; comparison to previous reporting period/semester}

**2.11 Progress Towards Certification**

{Presentation of the progress of the ISMS implementation; comparison to previous reporting period/semester}

**3. Summary**

{Overall status; summary of relevant results; ISMS and information security trend compared to previous reporting period/semester}

**4. Plans and Key Events for the Next {Reporting Period/Semester}**

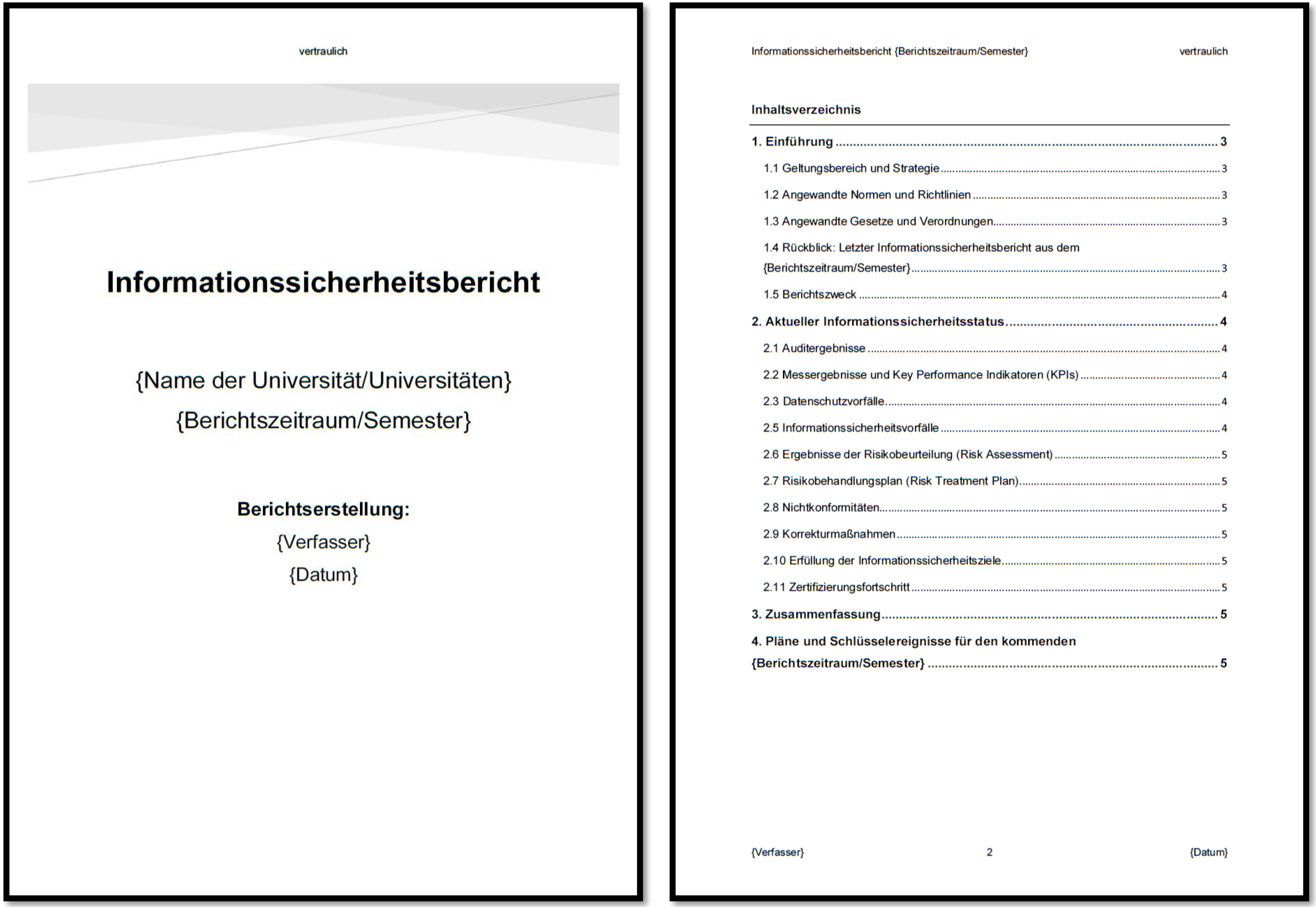
{Prioritized action plans and proposals with estimates of the expected implementation effort; target dates; objectives for the next reporting period/semester}

{Author} 5 {Date}

*(continued)*

**Figure 18:** Information Security Report Template (English)

(Source: Own illustration)



vertraulich

# Informationssicherheitsbericht

{Name der Universität/Universitäten}

{Berichtszeitraum/Semester}

**Berichtserstellung:**

{Verfasser}

{Datum}

Informationssicherheitsbericht {Berichtszeitraum/Semester} vertraulich

**Inhaltsverzeichnis**

{Verfasser} 2 {Datum}

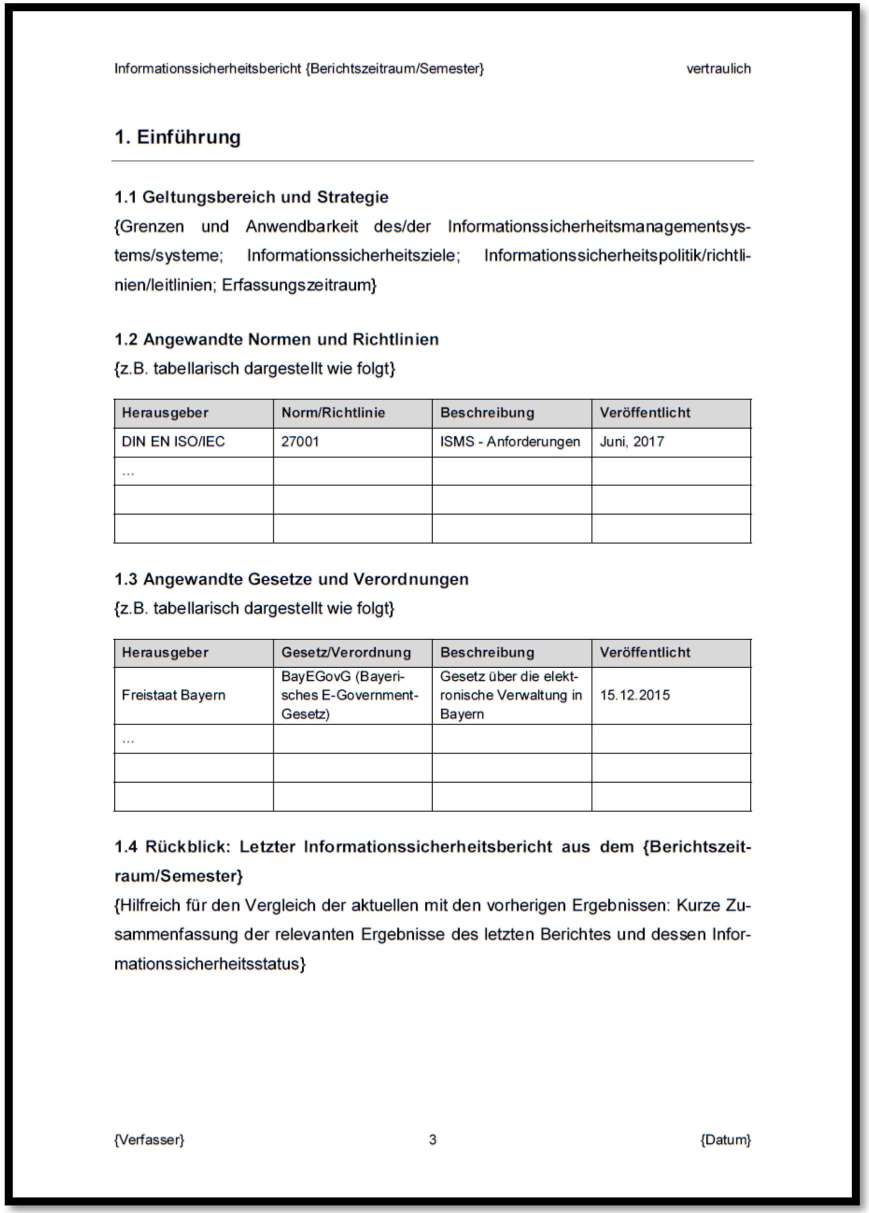
**Figure 19:** Information Security Report Template (German)

(Source: Own illustration)

*(continued)*

**Figure 19:** Information Security Report Template (German)

(Source: Own illustration)



Informationssicherheitsbericht {Berichtszeitraum/Semester} vertraulich

## 1. Einführung

### 1.1 Geltungsbereich und Strategie

{Grenzen und Anwendbarkeit des/der Informationssicherheitsmanagementsysteme/systeme; Informationssicherheitsziele; Informationssicherheitspolitik/richtlinien/leitlinien; Erfassungszeitraum}

### 1.2 Angewandte Normen und Richtlinien

{z.B. tabellarisch dargestellt wie folgt}

| Herausgeber | Norm/Richtlinie | Beschreibung | Veröffentlicht |
|---|---|---|---|
| DIN EN ISO/IEC | 27001 | ISMS - Anforderungen | Juni, 2017 |
| … | | | |
| | | | |
| | | | |

### 1.3 Angewandte Gesetze und Verordnungen

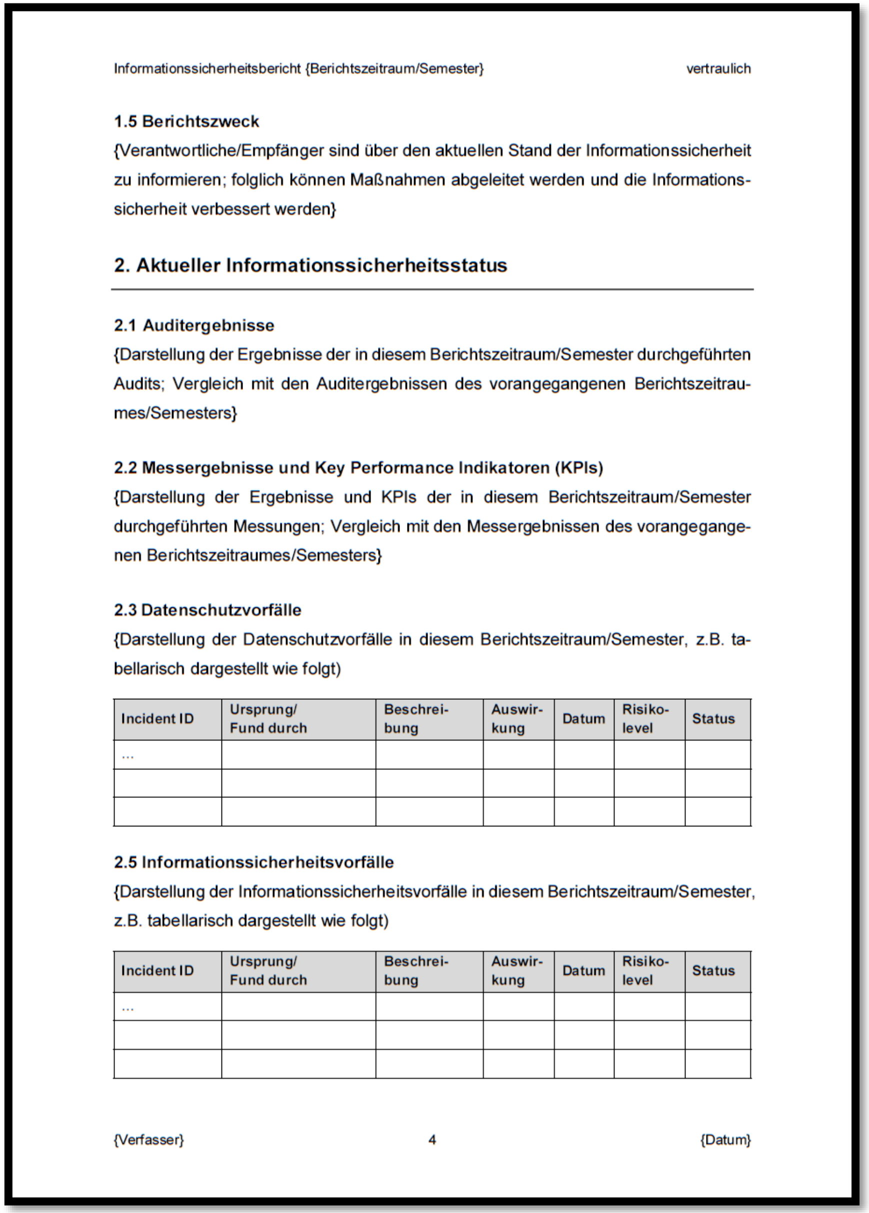
{z.B. tabellarisch dargestellt wie folgt}

| Herausgeber | Gesetz/Verordnung | Beschreibung | Veröffentlicht |
|---|---|---|---|
| Freistaat Bayern | BayEGovG (Bayerisches E-Government-Gesetz) | Gesetz über die elektronische Verwaltung in Bayern | 15.12.2015 |
| … | | | |
| | | | |
| | | | |

### 1.4 Rückblick: Letzter Informationssicherheitsbericht aus dem {Berichtszeitraum/Semester}

{Hilfreich für den Vergleich der aktuellen mit den vorherigen Ergebnissen: Kurze Zusammenfassung der relevanten Ergebnisse des letzten Berichtes und dessen Informationssicherheitsstatus}

{Verfasser} 3 {Datum}



Informationssicherheitsbericht {Berichtszeitraum/Semester} vertraulich

### 1.5 Berichtszweck

{Verantwortliche/Empfänger sind über den aktuellen Stand der Informationssicherheit zu informieren; folglich können Maßnahmen abgeleitet werden und die Informationssicherheit verbessert werden}

## 2. Aktueller Informationssicherheitsstatus

### 2.1 Auditergebnisse

{Darstellung der Ergebnisse der in diesem Berichtszeitraum/Semester durchgeführten Audits; Vergleich mit den Auditergebnissen des vorangegangenen Berichtszeitraumes/Semesters}

### 2.2 Messergebnisse und Key Performance Indikatoren (KPIs)

{Darstellung der Ergebnisse und KPIs der in diesem Berichtszeitraum/Semester durchgeführten Messungen; Vergleich mit den Messergebnissen des vorangegangenen Berichtszeitraumes/Semesters}

### 2.3 Datenschutzvorfälle

{Darstellung der Datenschutzvorfälle in diesem Berichtszeitraum/Semester, z.B. tabellarisch dargestellt wie folgt}

| Incident ID | Ursprung/ Fund durch | Beschreibung | Auswirkung | Datum | Risikolevel | Status |
|---|---|---|---|---|---|---|
| … | | | | | | |
| | | | | | | |
| | | | | | | |

### 2.5 Informationssicherheitsvorfälle

{Darstellung der Informationssicherheitsvorfälle in diesem Berichtszeitraum/Semester, z.B. tabellarisch dargestellt wie folgt}

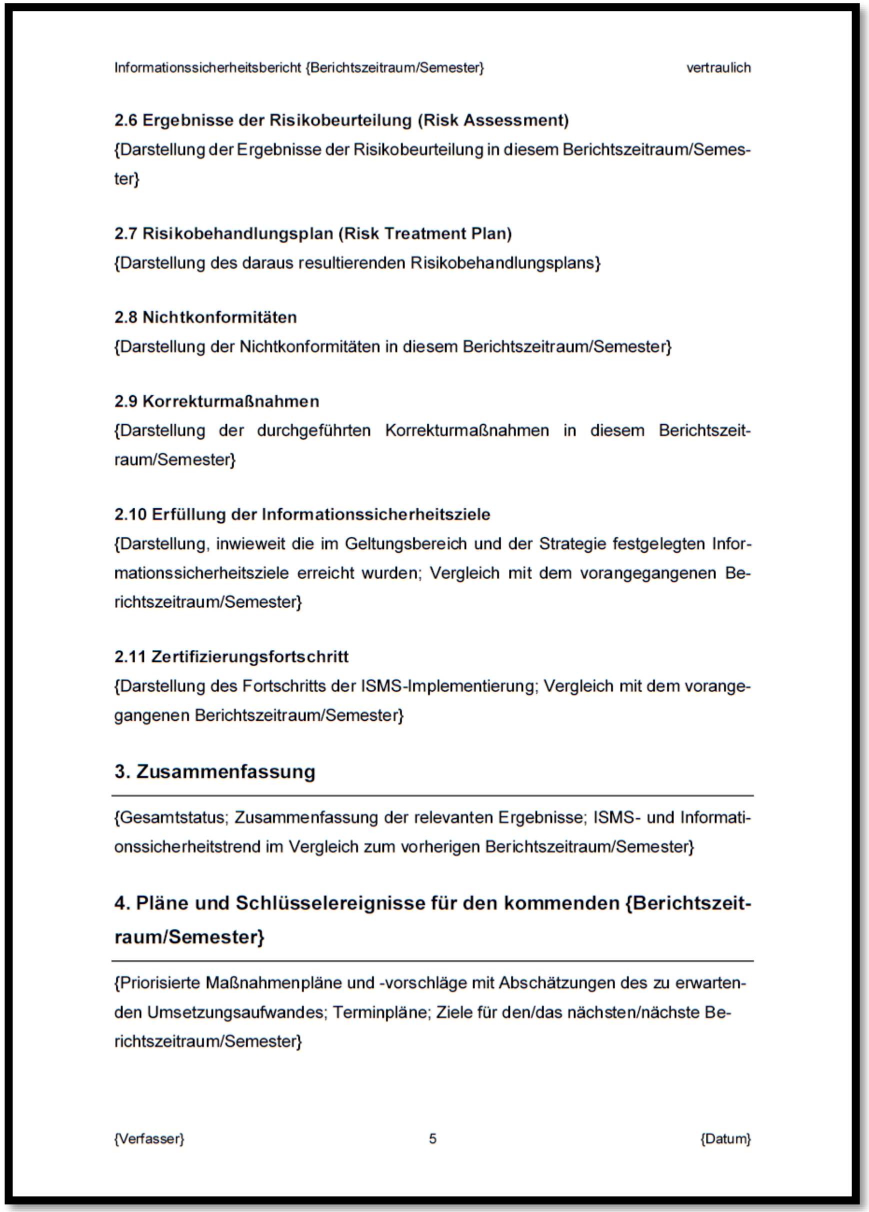
| Incident ID | Ursprung/ Fund durch | Beschreibung | Auswirkung | Datum | Risikolevel | Status |
|---|---|---|---|---|---|---|
| … | | | | | | |
| | | | | | | |
| | | | | | | |

{Verfasser} 4 {Datum}

*(continued)*

**Figure 19:** Information Security Report Template (German)

(Source: Own illustration)



Informationssicherheitsbericht {Berichtszeitraum/Semester} vertraulich

**2.6 Ergebnisse der Risikobeurteilung (Risk Assessment)**

{Darstellung der Ergebnisse der Risikobeurteilung in diesem Berichtszeitraum/Semester}

**2.7 Risikobehandlungsplan (Risk Treatment Plan)**

{Darstellung des daraus resultierenden Risikobehandlungsplans}

**2.8 Nichtkonformitäten**

{Darstellung der Nichtkonformitäten in diesem Berichtszeitraum/Semester}

**2.9 Korrekturmaßnahmen**

{Darstellung der durchgeführten Korrekturmaßnahmen in diesem Berichtszeitraum/Semester}

**2.10 Erfüllung der Informationssicherheitsziele**

{Darstellung, inwieweit die im Geltungsbereich und der Strategie festgelegten Informationssicherheitsziele erreicht wurden; Vergleich mit dem vorangegangenen Berichtszeitraum/Semester}

**2.11 Zertifizierungsfortschritt**

{Darstellung des Fortschritts der ISMS-Implementierung; Vergleich mit dem vorangegangenen Berichtszeitraum/Semester}

**3. Zusammenfassung**

{Gesamtstatus; Zusammenfassung der relevanten Ergebnisse; ISMS- und Informationssicherheitstrend im Vergleich zum vorherigen Berichtszeitraum/Semester}

**4. Pläne und Schlüsselereignisse für den kommenden {Berichtszeitraum/Semester}**

{Priorisierte Maßnahmenpläne und -vorschläge mit Abschätzungen des zu erwartenden Umsetzungsaufwandes; Terminpläne; Ziele für den/das nächsten/nächste Berichtszeitraum/Semester}

{Verfasser} 5 {Datum}

# Erklärung zur Abschlussarbeit

Hiermit versichere ich, die eingereichte Abschlussarbeit selbständig verfasst und keine andere als die von mir angegebenen Quellen und Hilfsmittel benutzt zu haben. Wörtlich oder inhaltlich verwendete Quellen wurden entsprechend den anerkannten Regeln wissenschaftlichen Arbeitens zitiert. Ich erkläre weiterhin, dass die vorliegende Arbeit noch nicht anderweitig als Abschlussarbeit eingereicht wurde.

Das Merkblatt zum Täuschungsverbot im Prüfungsverfahren der Hochschule Augsburg habe ich gelesen und zur Kenntnis genommen. Ich versichere, dass die von mir abgegebene Arbeit keinerlei Plagiate, Texte oder Bilder umfasst, die durch von mir beauftragte Dritte erstellt wurden.

Welden, den 18.03.2019

Ort, Datum

Matthias Mödinger

Unterschrift des/der Studierenden