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

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

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

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

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.

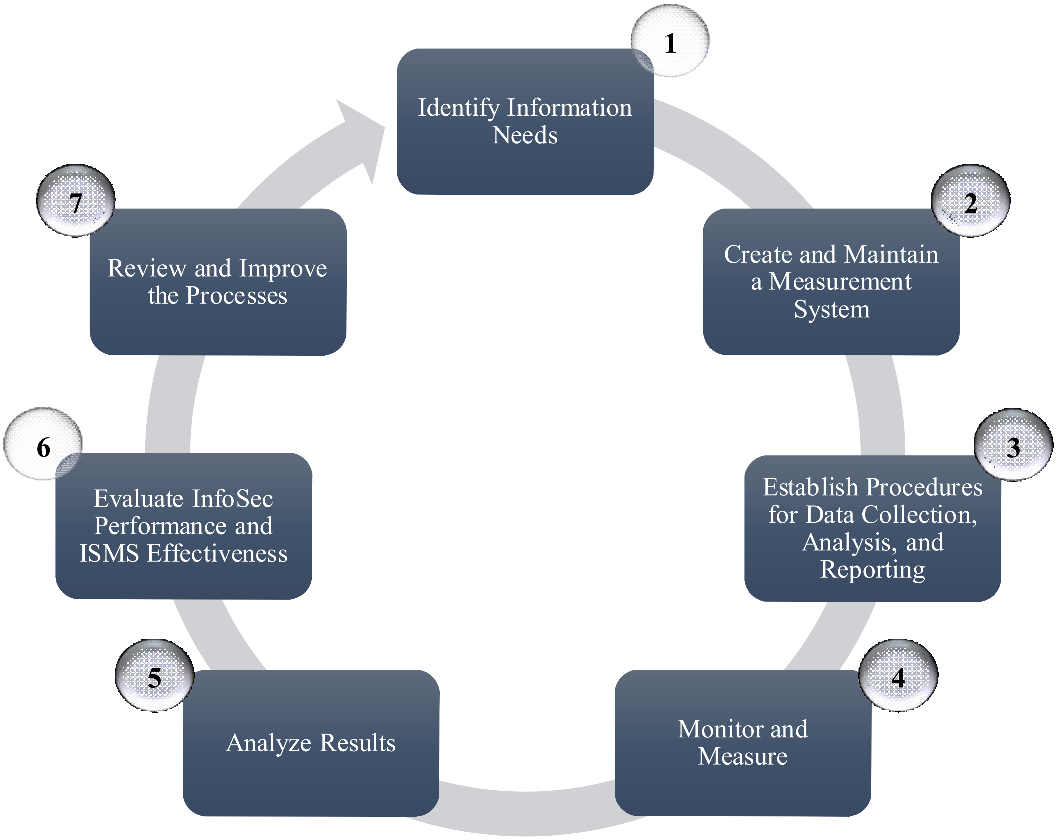

1
Identify Information Needs
2
Create and Maintain a Measurement System
3
Establish Procedures for Data Collection, Analysis, and Reporting
4
Monitor and Measure
5
Analyze Results
6
Evaluate InfoSec Performance and ISMS Effectiveness
7
Review and Improve the Processes

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)

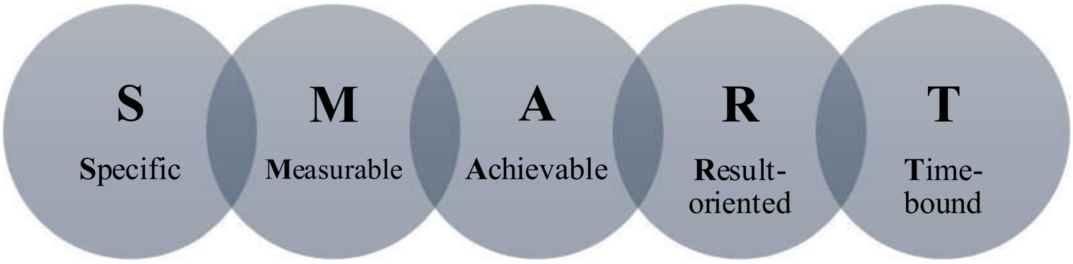


Figure 14: Characteristics of a Key Performance Indicator (‘SMART’ Acronym)

(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**.

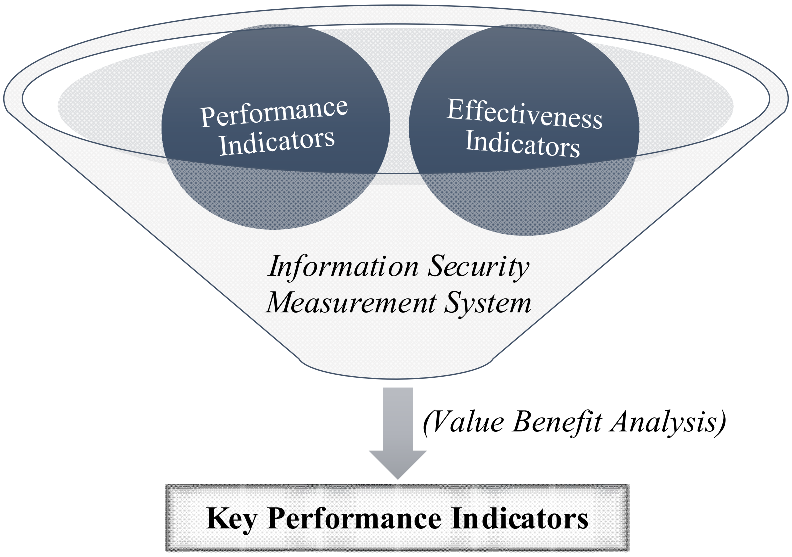


Figure 15: Information Security Measurement System Concept

(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**.

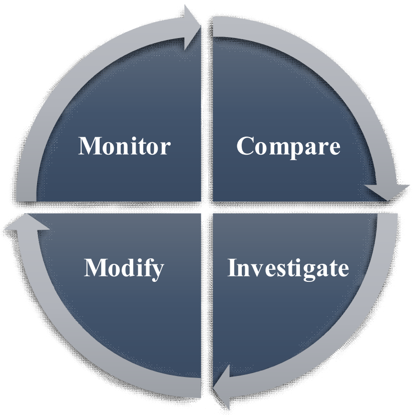


Figure 16: Procedure for the Ongoing Use of Metrics

(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	$EI_{\mathit{Resource\ Utilization}}$
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) ▪ 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	$\boldsymbol{PI}_{\textit{University Management Commitment}}$; $\boldsymbol{EI}_{\textit{University Management Commitment}}$
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 b) Average participation rates in university management InfoSec review meetings to date
Measure Type	a) Performance indicator b) Effectiveness indicator
Formula/scoring	a) $PI = \frac{InfoSec\ University\ management\ review\ meetings\ performed}{InfoSec\ University\ management\ review\ meetings\ scheduled}$ *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) $PI > 0.5$ (even if it fails, PI should be still over 0.5 to conclude the least achievement) 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 ▪ 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 ▪ Count the planned university management InfoSec review meetings held to date ▪ Count the unplanned university management InfoSec review meetings held to date ▪ Count the rescheduled university management InfoSec review meetings held to date ▪ For all university management InfoSec review meetings that were held, count the number of managers who attended
Frequency	▪ Collection: monthly ▪ Analysis and reporting: every semester ▪ Measurement revision: review and update every two years
Responsible parties	▪ Information owner and collector: quality system manager (information security manager; information security officer) ▪ 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: $PI \leq 60\%$ ▪ Green: no action is required ▪ Yellow: indicator should be watched closely for possible deterioration to red ▪ 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) ▪ 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. $EI = Percentage\ of\ training\ participants\ passed\ the\ test$
Target	Green: $EI \geq 90\%\ of\ people\ passed\ the\ test$, Yellow: $89\% \geq PI \leq 59\%\ of\ people\ passed\ the\ test$, Red: $PI \leq 60\%\ of\ people\ passed\ the\ test$ ▪ Green: no action is required ▪ Yellow: indicator should be watched closely for possible deterioration to red ▪ 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 ▪ Reporting: for each collection
Responsible parties	▪ Information owner and collector: information security officer (training manager) ▪ 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	$\boldsymbol{PI}_{\textbf{Policies Review}}$
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: $PI \leq 40\%$ ▪ Green: no action is required ▪ Yellow: indicator should be watched closely for possible deterioration to red ▪ 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 ▪ Reporting: for each collection
Responsible parties	▪ Information owner: policy owner who has approved management responsibility for the development, review, and evaluation of the policy ▪ Information collector: internal auditor ▪ 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	$\boldsymbol{EI}_{\textbf{Risk Potential}}$
Information need	Assess the hazard of the university to information security risks
Measure	a) High and medium risks beyond the acceptable threshold 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 $EI = Number\ of\ risks\ without\ status\ update$
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	$\boldsymbol{PI}_{\textbf{Audit program}}$
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 ▪ 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	$EI_{\text{Improvement Actions}}$
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 ▪ 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	$PI_{\text{Security Incident Costs}}$
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) ▪ Information collector: information security manager/officer ▪ 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) ▪ 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: $PI \leq 70\%$ ▪ Green: no action is required ▪ Yellow: indicator should be watched closely for possible deterioration to red ▪ 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 ▪ Reporting: every semester
Responsible parties	▪ Information owner: risk owner ▪ Information collector: CISO (CIO) ▪ 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	$PI_{\mathit{Physical\ Entry\ Controls}}$
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	$PI\ =\ Scale\ from\ 0-100\%$ 0%: There is **no access control system** 20%: There is an access system where **PIN code** (one factor system) is used for entry control 40%: There is an access control card system (**campus card system**) where passing the campus card (one factor system) is used for entry control 60%: There is a **campus card system** where passing card **and PIN code** is used for entry control 80%: There is a **campus card system** where passing card and **PIN code** is used for entry control and **log functionality** is activated 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: ▪ Access control card system evidence ▪ PIN code usage ▪ Log functionality ▪ Biometric authentication
Frequency	▪ Collection, analysis, and reporting: annually (every two semesters) ▪ Measurement revision: after twelve months ▪ Period of measurement: applicable twelve months
Responsible parties	▪ Information owner: facility manager ▪ Information collector: internal auditor/external auditor ▪ 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	$EI_{\mathit{Physical\ Entry\ Controls\ Effectiveness}}$
Information need	1. Ensure an environment of comprehensive security and accountability for personnel, facilities, and products 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) ▪ Information collector: computer security incident response team (CSIRT) ▪ 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	$\boldsymbol{PI_{Maintenance\ of\ Information\ Systems}}$
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) 2. Trend should be stable or close to $PI = 0$ days 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 ▪ Reporting: annually (every two semesters)
Responsible parties	▪ Information owner: security administrator ▪ Information collector: security staff ▪ 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 ▪ 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 ▪ 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 ▪ 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	$\boldsymbol{PI}_{\textit{\textbf{Log Files Review}}}$
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) ▪ Reporting: every semester ▪ Measurement revision: every two years ▪ Period of measurement: applicable: two years
Responsible parties	▪ Information owner: information security manager (information security officer) ▪ Information collector: security staff ▪ 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	$\boldsymbol{PI}_{\textit{\textbf{Vulnerability of Information Systems}}}$
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 ▪ Reporting: for each collection
Responsible parties	▪ Information owner: risk owner ▪ 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	$\boldsymbol{EI}_{\textit{Security Incident Management Effectiveness}}$
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 b) Define acceptable indicator thresholds for security incidents that exceed the category target time frame c) Compare the number of incidents whose resolution time exceeds the category target time frames with the indicator thresholds
Target	$EI = \textit{Number of incidents whose resolution time exceeds the category target time frames is within the defined indicator thresholds}$
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 ▪ Measurement revision: every semester
Responsible parties	▪ Information owner: managers responsible for the ISMS ▪ Information collector: Incident management manager ▪ 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	$\boldsymbol{EI}_{\textit{Security Incident Trend}}$
Information need	1. Trend of information security incidents 2. Trend of categories of information security incidents
Measure	1. Number of information security incidents in a defined timeframe (e.g., one month) 2. Number of information security incidents of a specific category in a defined timeframe (e.g., one month)
Measure Type	Effectiveness measure
Formula/scoring	$EI = \frac{\textit{Average number of information security incidents (of a specific category) of the last two timeframes}}{\textit{Average number of information security incidents (of a specific category) of the last six timeframes}}$ Define threshold values for the trend indicators, for example: ▪ Green: $EI < 1$ ▪ Yellow: $1 \leq EI \leq 1.3$ ▪ Red: $EI > 1.3$ 1. Perform analysis for all incidents 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) 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	$\boldsymbol{PI}_{\textit{\textbf{Security Events and Weaknesses Reporting and Assessment}}}$
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) ▪ Information collector: information security manager (information security officer) ▪ 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	$\boldsymbol{PI}_{\textit{\textbf{Availability of IT Services}}}$
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 ▪ Information collector: IT quality ▪ Measurement client: CIO
Data source	Monitoring tools
Reporting format	For each IT service, two lines in the chart: ▪ line linking the actual availability (percentage) of each sampled period ▪ 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	$0.8 \le PI \le 1.1$ (to conclude the achievement of the control objective; no action required) $PI > 0.6$ (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 ▪ Measurement revision: reviewing and updating every two years ▪ Period of measurement: applicable: two years
Responsible parties	▪ Information owner: managers responsible for the ISMS ▪ Information collector: internal auditor; quality manager ▪ 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%)

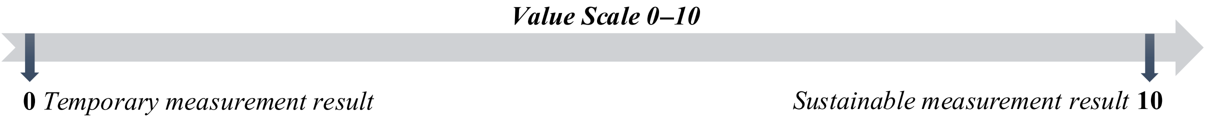
High effort and high costs for the collection and provision of data or information that are required for the measurement always involve a risk. It is counterproductive if many resources concerning a lot of personnel, time, and high costs are spent on a measurement and then the benefit or efficiency of 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.

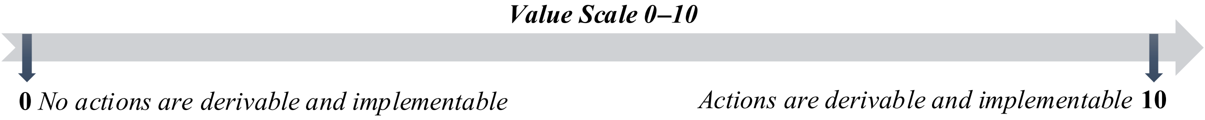
This is important for the achievement of long-term goals and continuous improvement processes and, therefore, it is weighted by 20%.



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

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

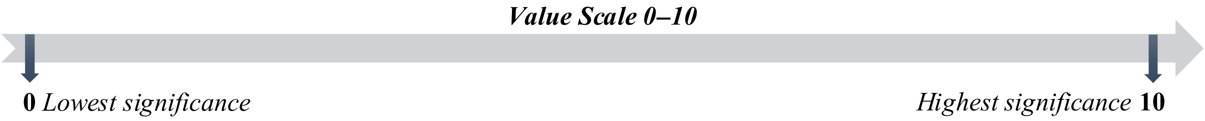
As **Figure 13**, **p. 48** has shown, the monitoring, measurement, analysis, and evaluation processes have to be continuously reviewed, updated, and improved to achieve the desired objectives. Suitable and targeted conclusions must be drawn from KPIs in order to optimize measurement results and improve 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).

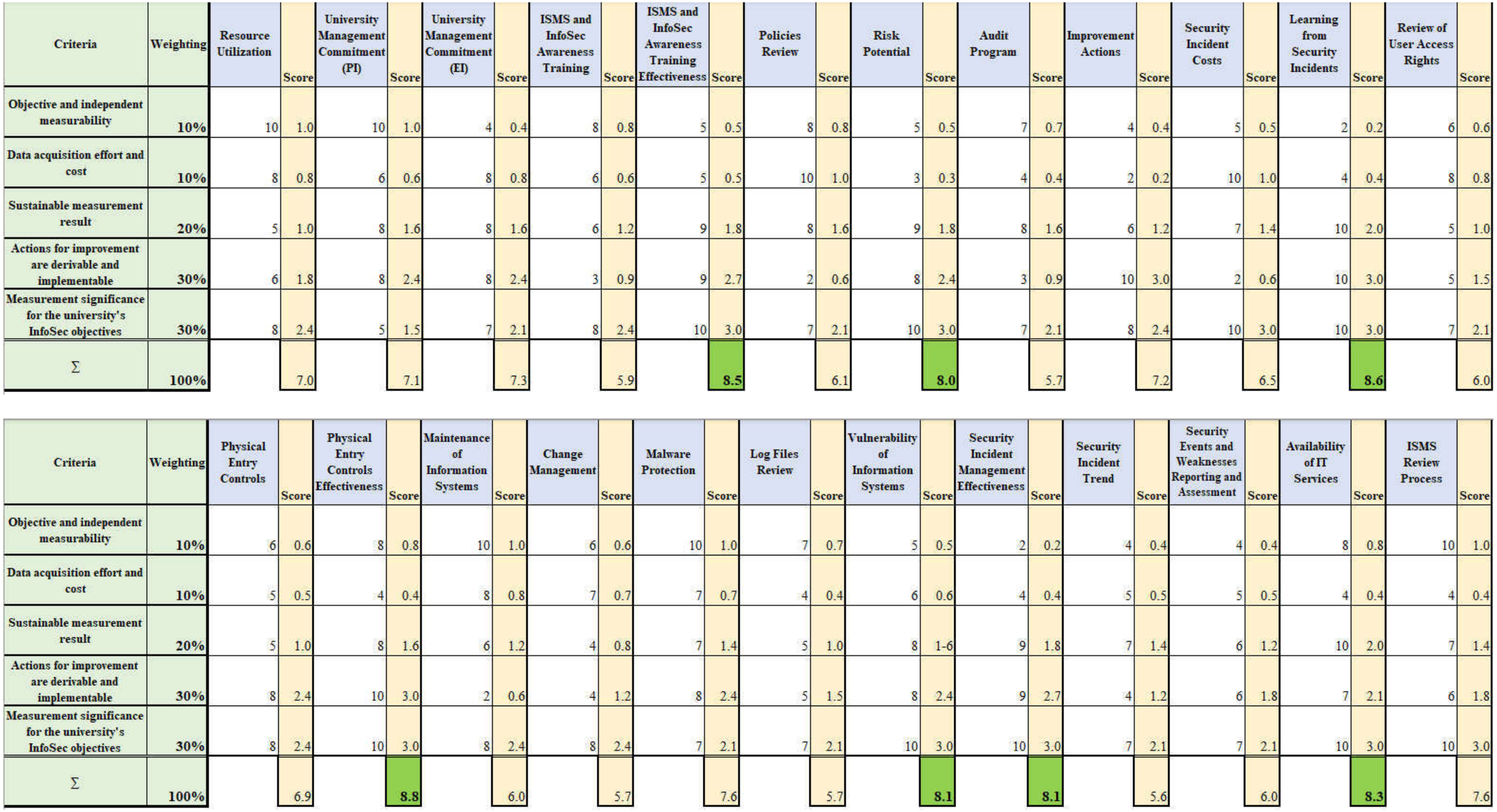
The KPI range was set from 8.0 to 10.0. As a logical consequence, the measurements with a total score of at least 8.0 (green marked) determine a key performance indicator. The following KPIs were calculated and result from this model:

Table 30: Key Performance Indicators for Universities

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

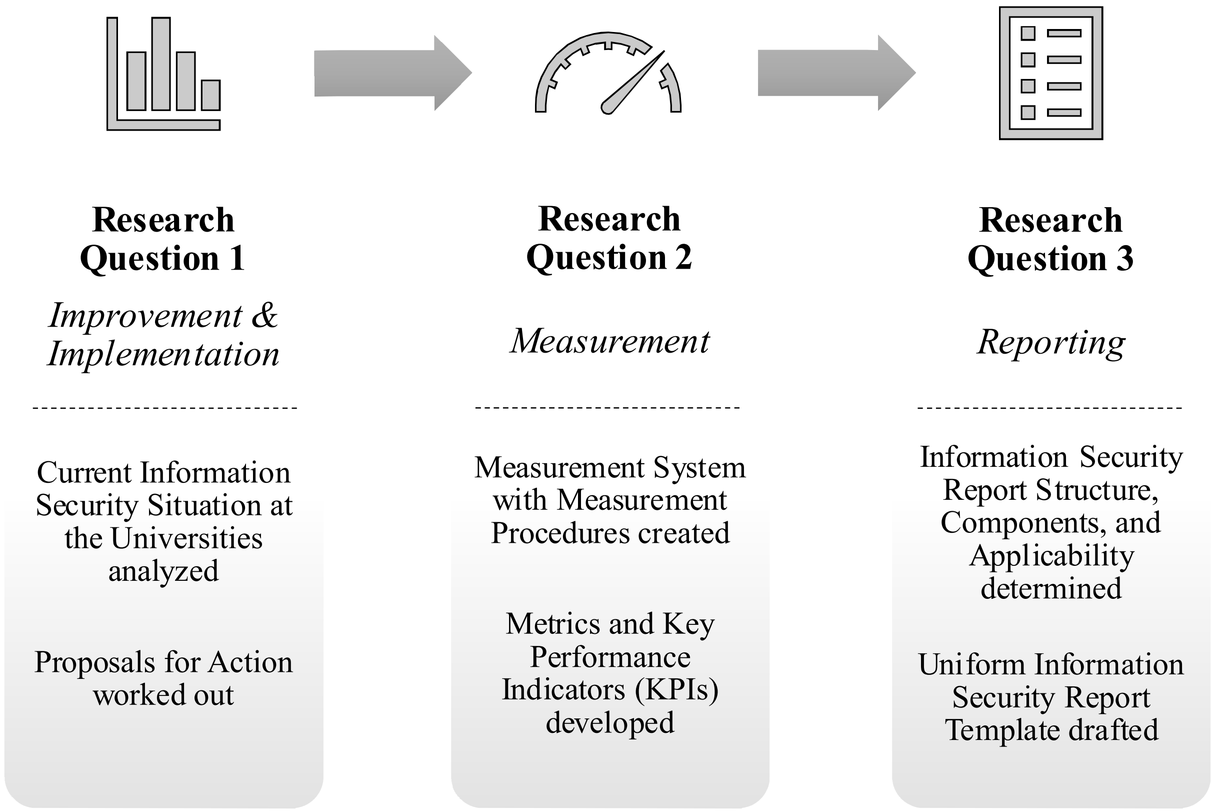
Due to the fact that the establishment of an ISMS at the universities is based on the ISO/IEC 27000-series, a requirements elicitation of the report structure and components was carried out according to this series of standards to guarantee standard conformity. The audit results, the measurement results 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.

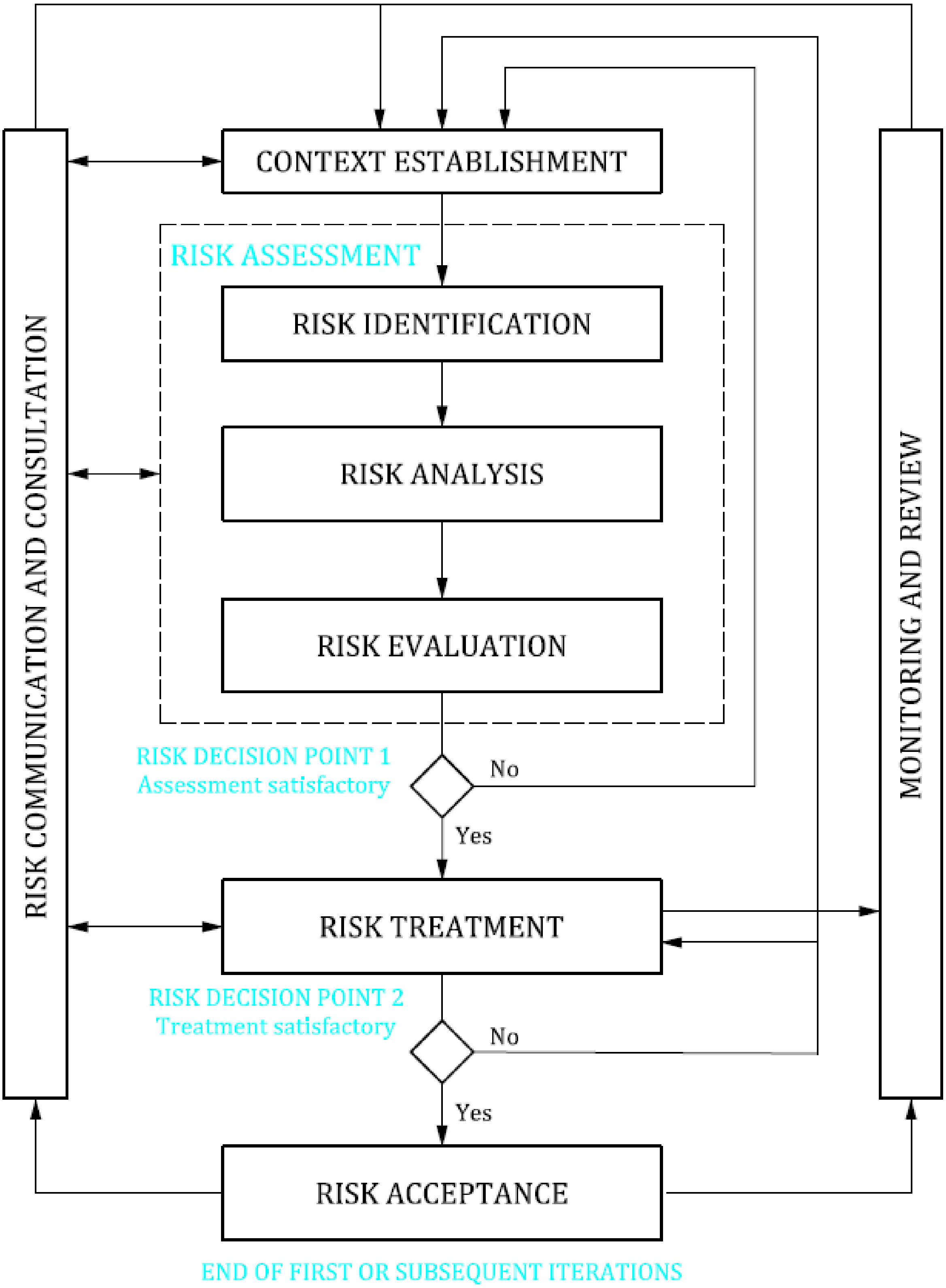


Figure 5: Information Security Risk Management Process

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

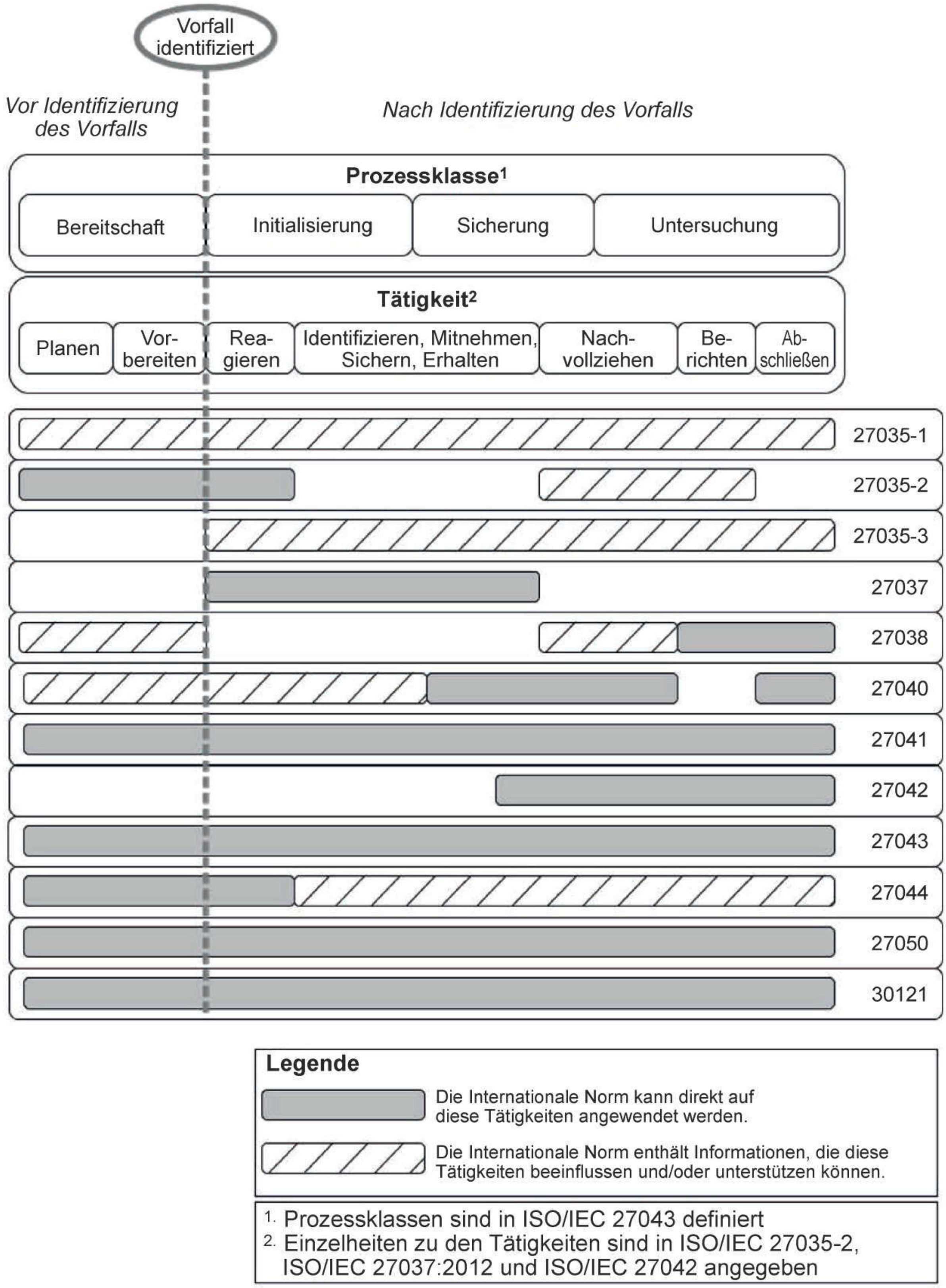
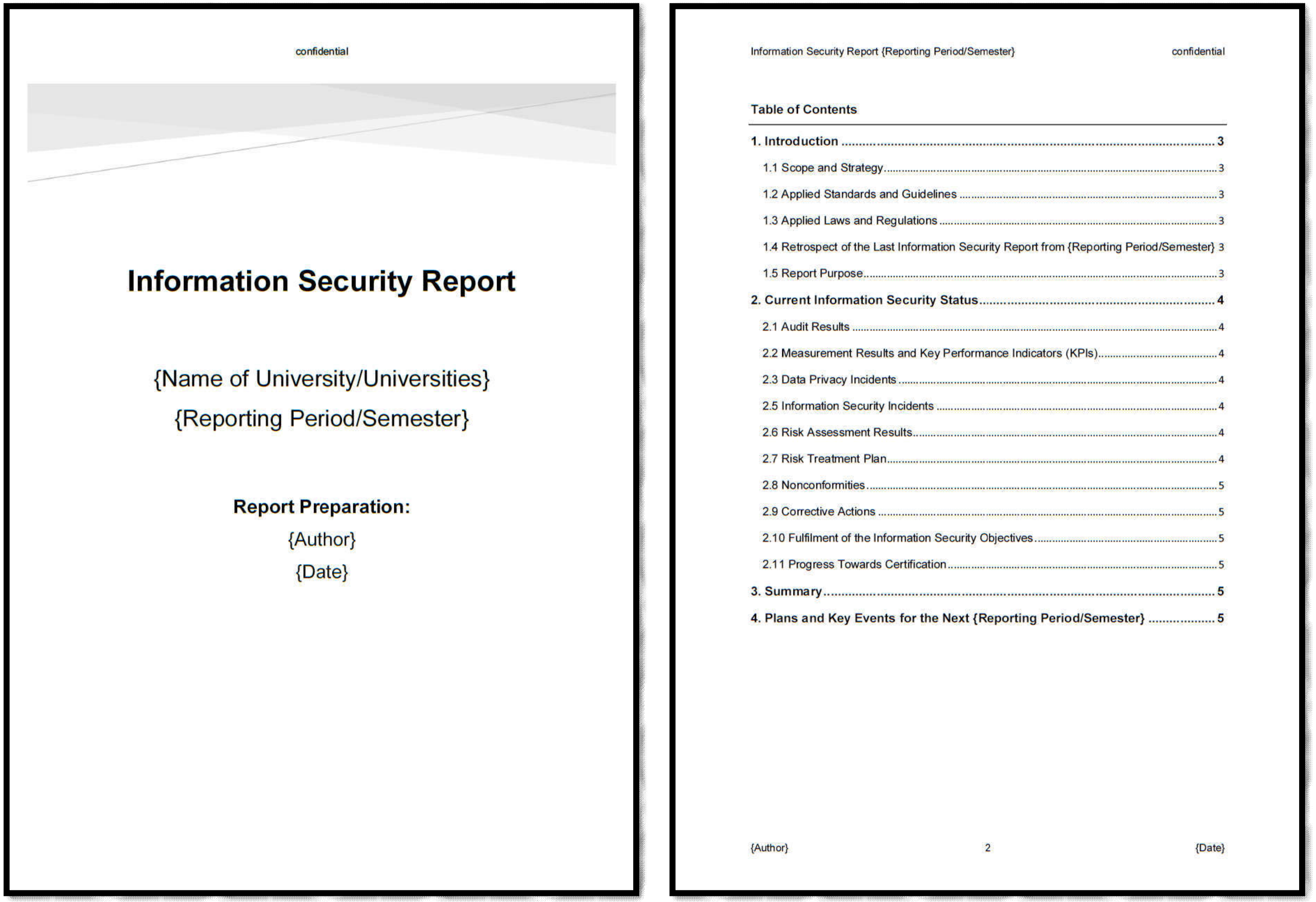

Vorfall identifiziert
Vor Identifizierung des Vorfalls
Nach Identifizierung des Vorfalls
Prozessklasse¹
Bereitschaft
Initialisierung
Sicherung
Untersuchung
Tätigkeit²
Planen
Vor-bereiten
Rea-gieren
Identifizieren, Mitnehmen, Sichern, Erhalten
Nach-vollziehen
Be-richten
Ab-schließen
27035-1
27035-2
27035-3
27037
27038
27040
27041
27042
27043
27044
27050
30121
Legende
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

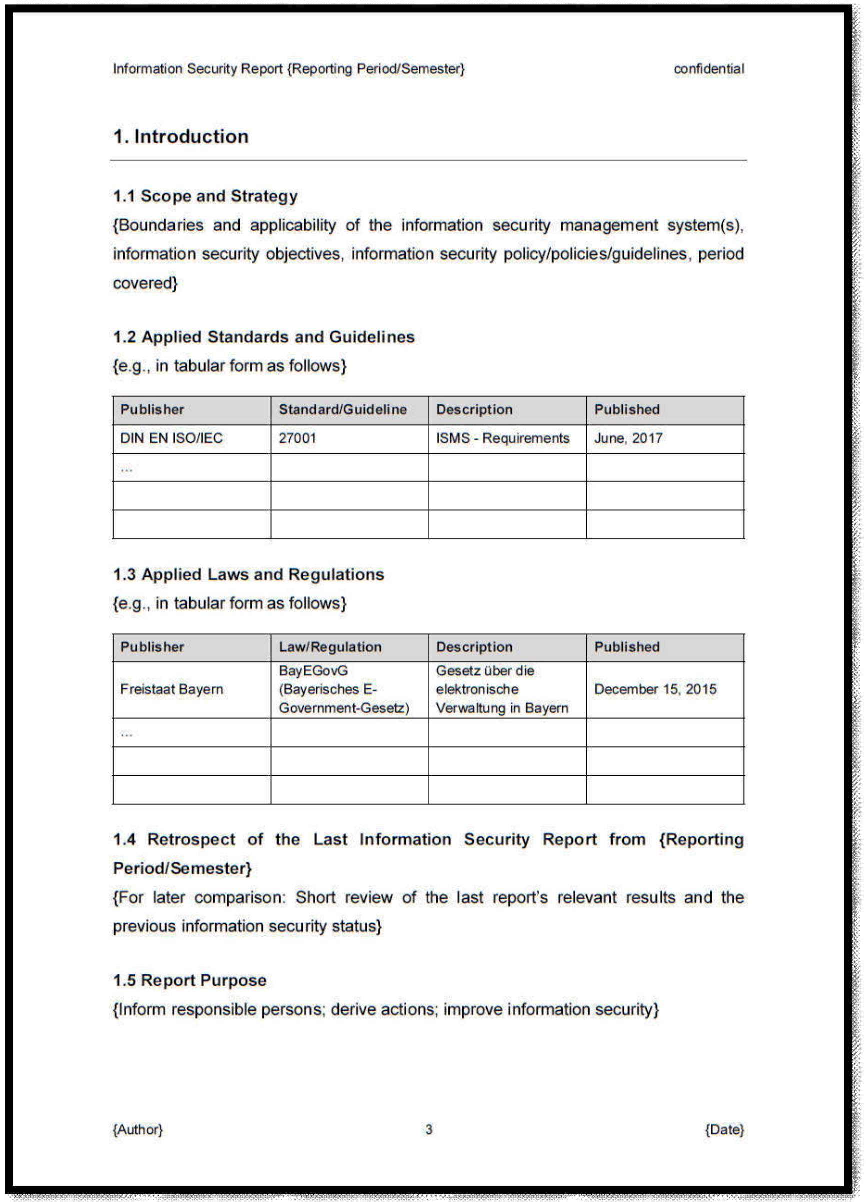
Table of Contents

{Author} 2 {Date}

(continued)

Figure 18: Information Security Report Template (English)

(Source: Own illustration)



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}

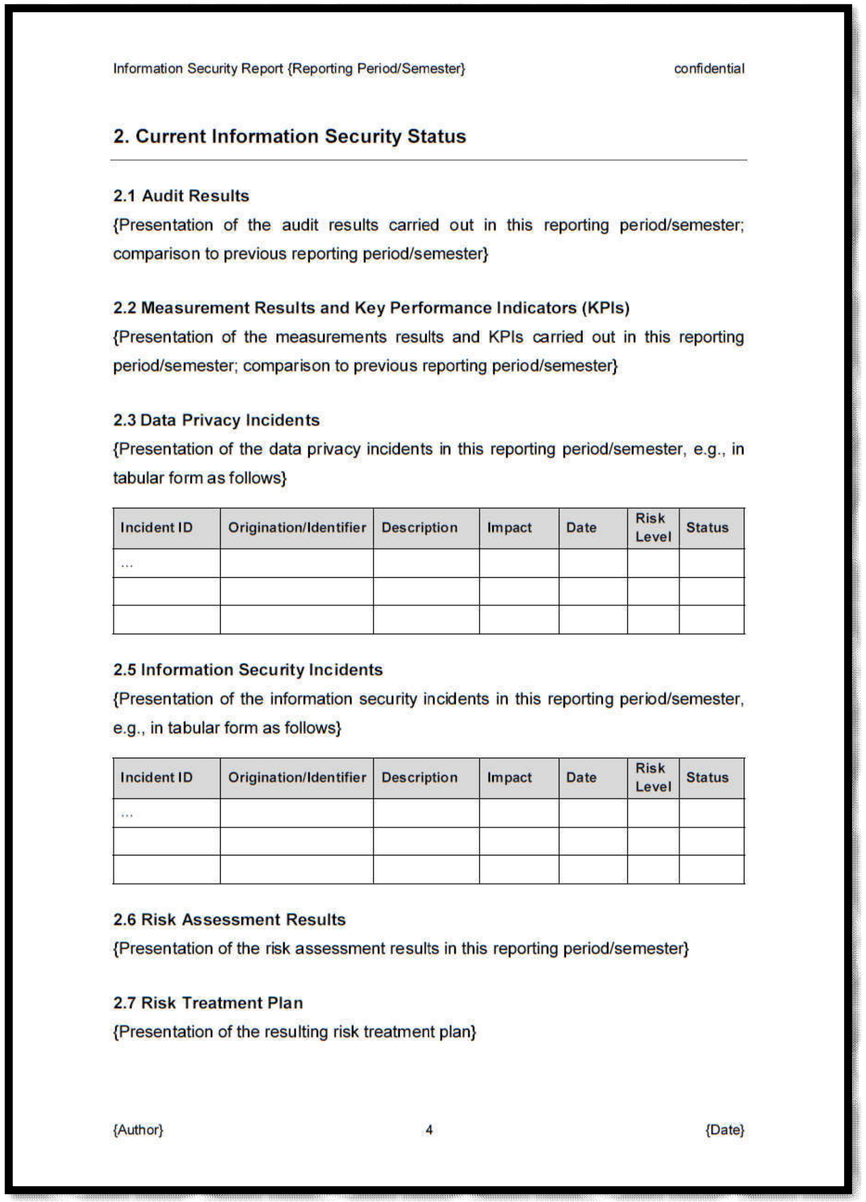
Publisher	Law/Regulation	Description	Published
Freistaat Bayern	BayEGovG (Bayerisches E-Government-Gesetz)	Gesetz über die elektronische Verwaltung in Bayern	December 15, 2015
...			

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}



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}

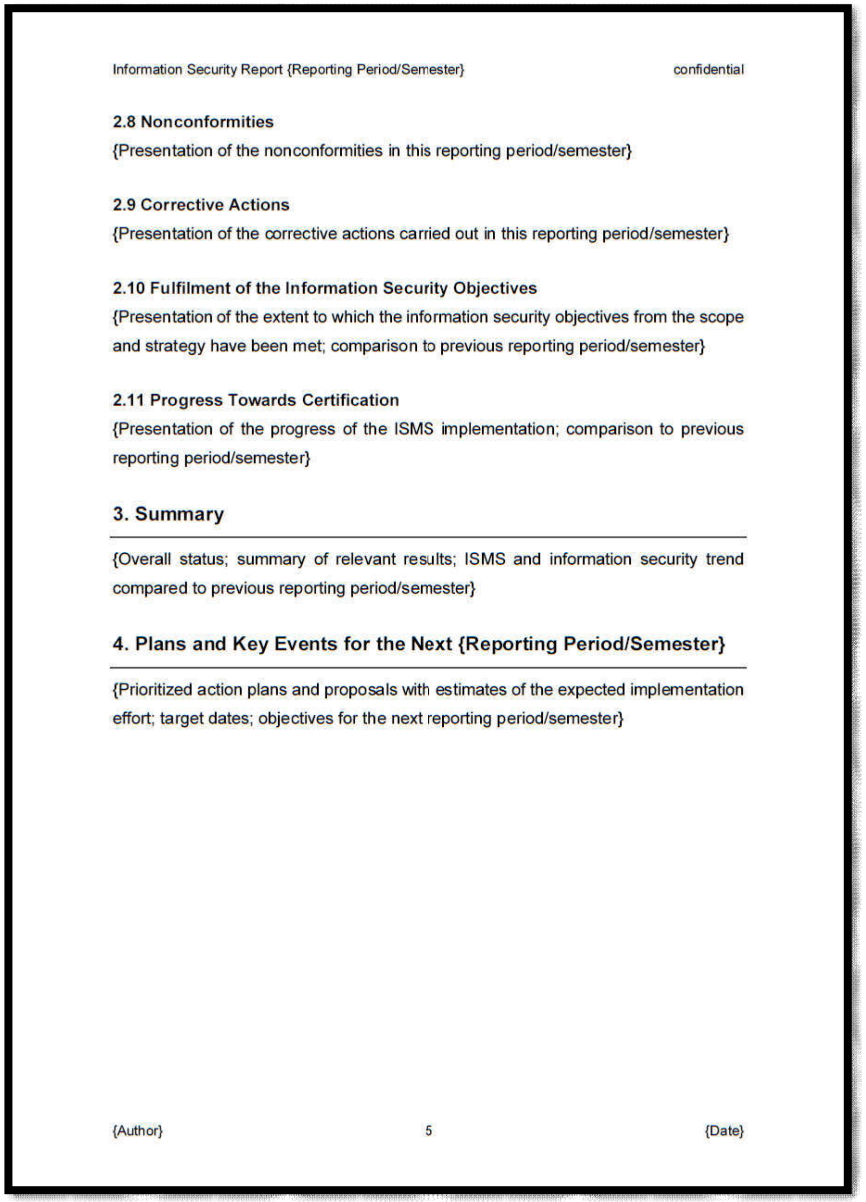
2.7 Risk Treatment Plan

{Presentation of the resulting risk treatment plan}

(continued)

Figure 18: Information Security Report Template (English)

(Source: Own illustration)



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}

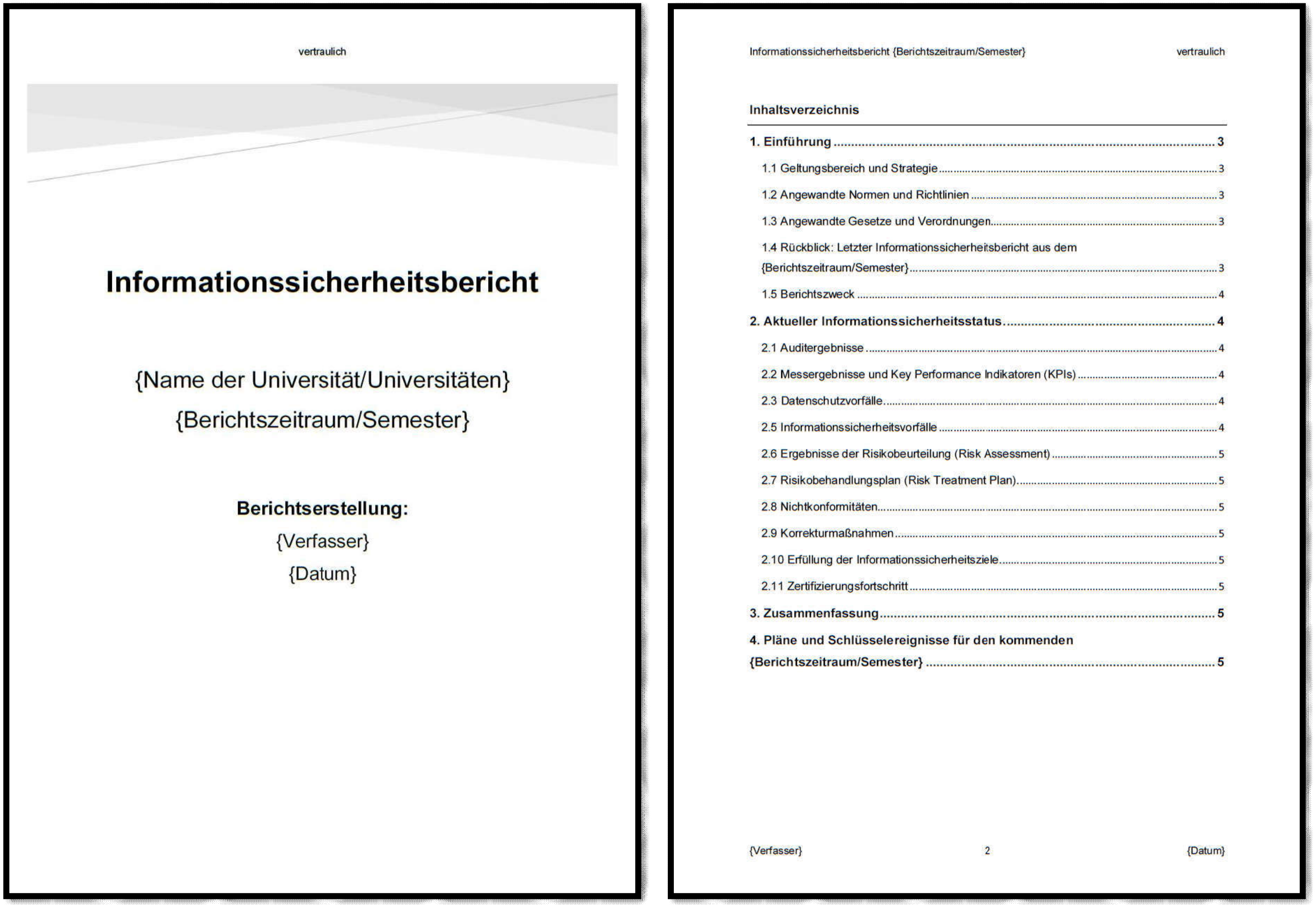
4. Plans and Key Events for the Next {Reporting Period/Semester}

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

{Author} 5 {Date}

Figure 19: Information Security Report Template (German)

(Source: Own illustration)



vertraulich

Informationssicherheitsbericht

{Name der Universität/Universitäten}

{Berichtszeitraum/Semester}

Berichtserstellung:

{Verfasser}

{Datum}

Informationssicherheitsbericht {Berichtszeitraum/Semester} vertraulich

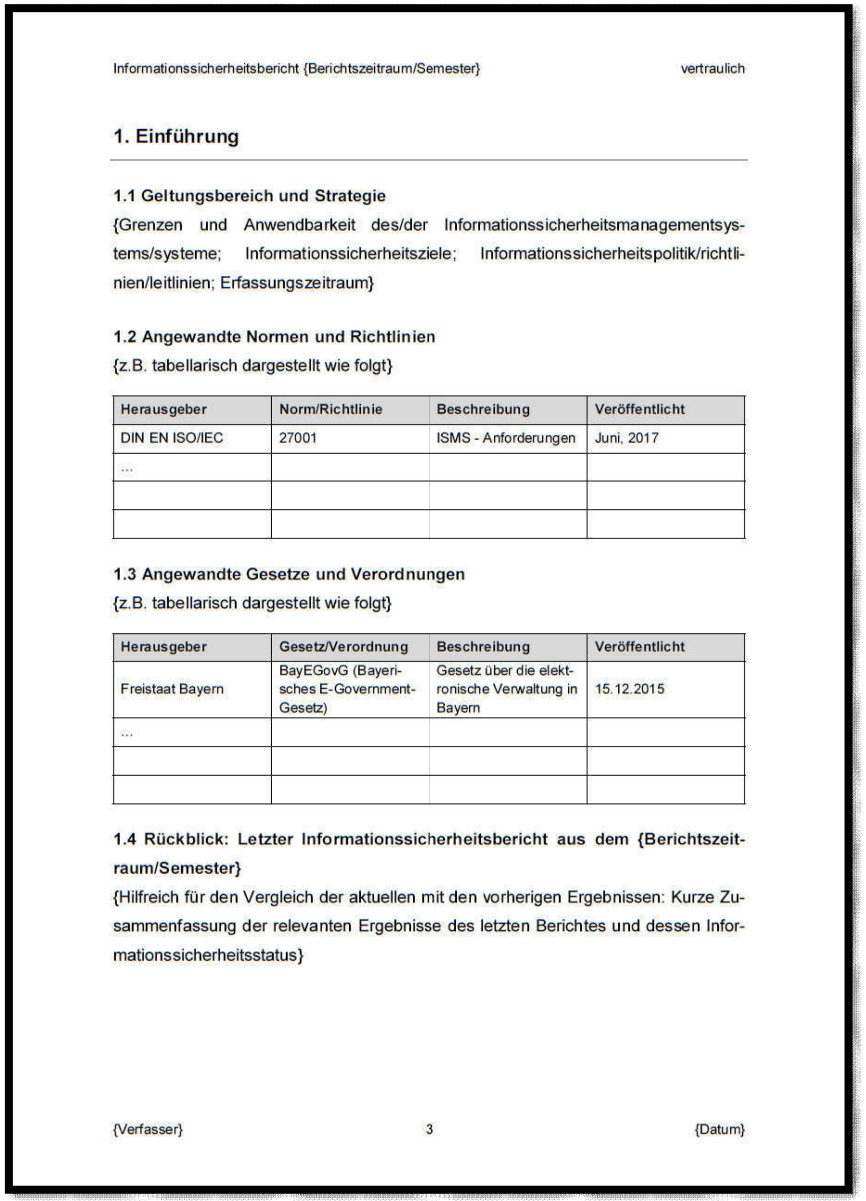
Inhaltsverzeichnis

{Verfasser} 2 {Datum}

(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 Informationssicherheitsmanagementsystems/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

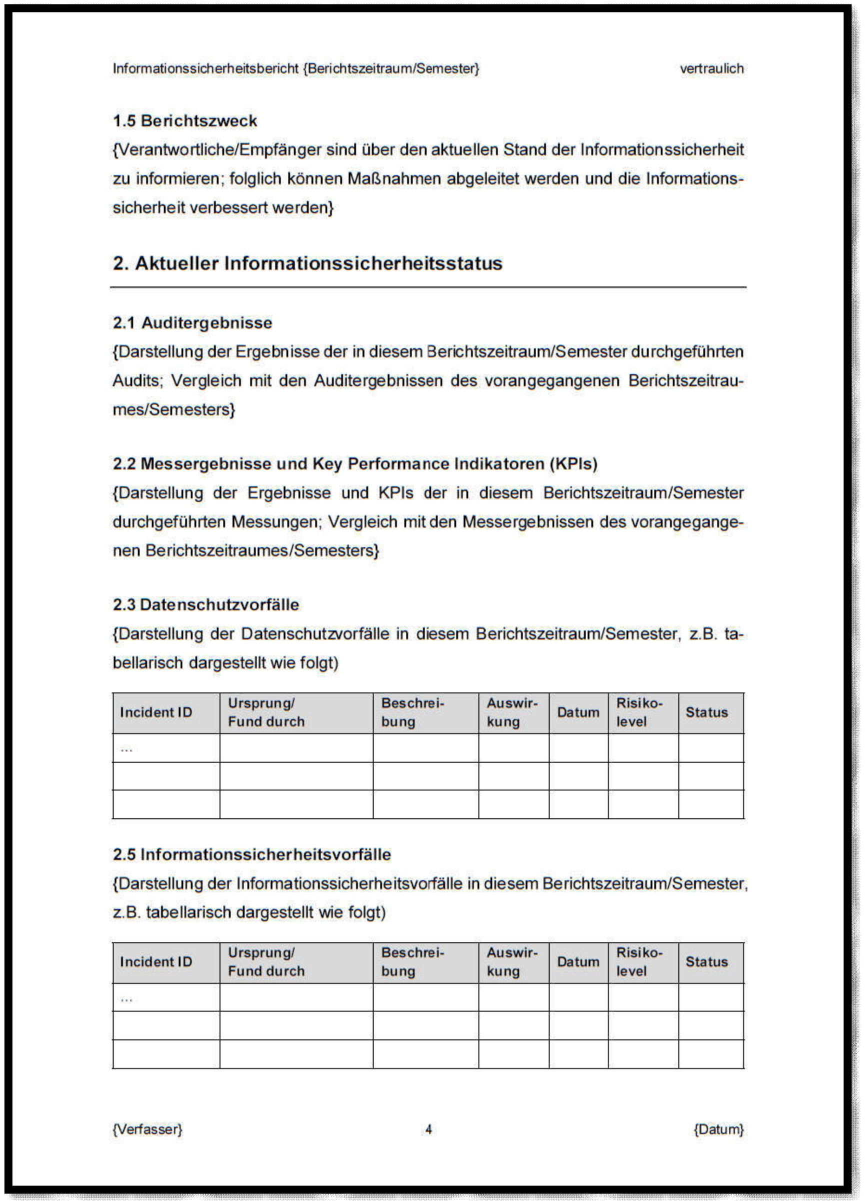
{z.B. tabellarisch dargestellt wie folgt}

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
...						

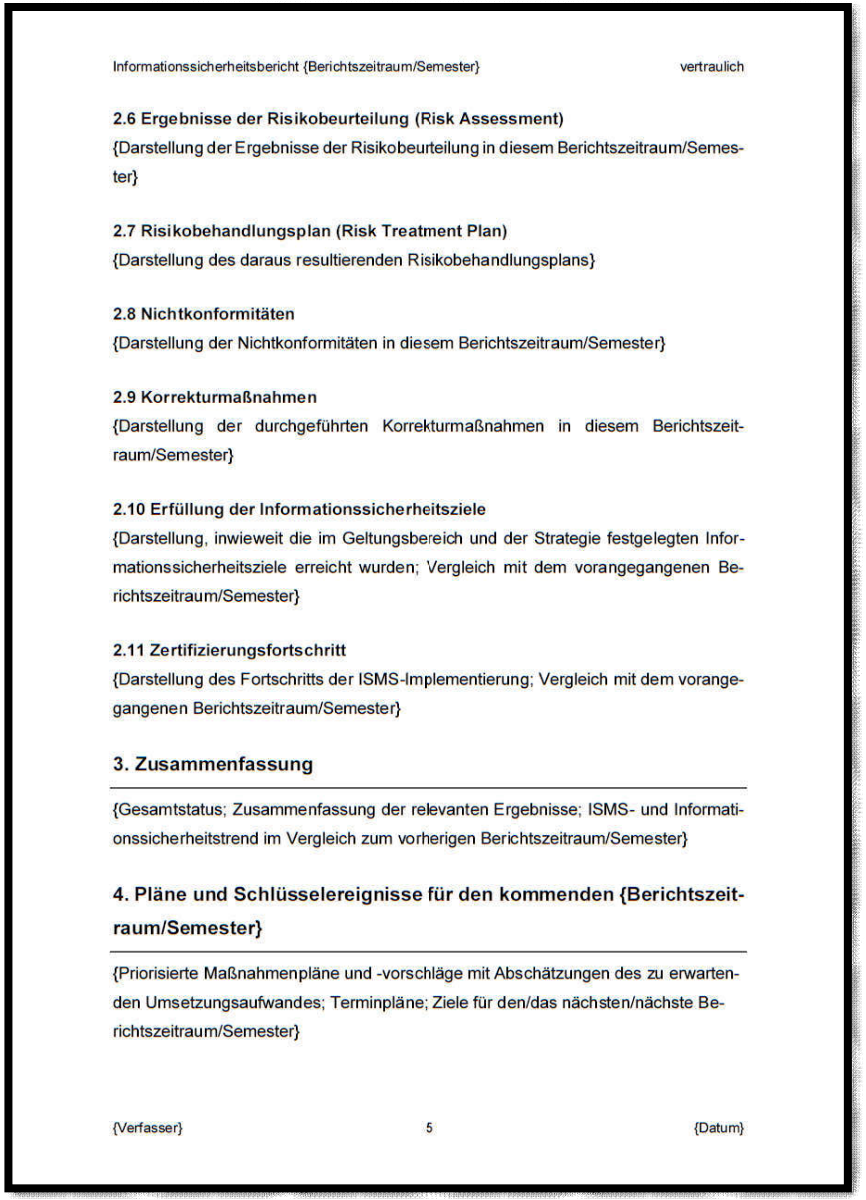
2.5 Informationssicherheitsvorfälle

{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)



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}

Figure 19: Information Security Report Template (German)

(Source: Own illustration)

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