Hochschule
Augsburg University of
Applied Sciences

Fakultät für
Informatik

Master Thesis

Studienrichtung

Master of Applied Research

Sabine Schnitzler

A universal guideline for the implementation of a specific ISMS for all Bavarian universities and universities of applied sciences using the example of the University of Applied Sciences Augsburg

Prüfer: Prof. Dr. Clemens Espe,
Christian Fötinger, MSc.

Abgabe der Arbeit am: 02.02.2018

Hochschule für angewandte
Wissenschaften Augsburg
University of Applied Sciences
An der Hochschule 1
D-86161 Augsburg
Telefon +49 821 55 86-0
Fax +49 821 55 86-3222
www.hs-augsburg.de
info@hs-augsburg.de

Fakultät für Informatik
Telefon: +49 821 5586-3450
Fax: +49 821 5586-3499

Verfasser der Master Thesis:
Sabine Schnitzler
Kopernikusstr. 12
86179 Augsburg
Telefon:+49 176/ 211 60 798
Sabine.schnitzler@hs-augsburg.de

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.

Ort, Datum	Unterschrift

I. ABSTRACT

A number of factors have made information security a very significant, critical issue across industries and organizations during the recent years.

Reasons are for instance the ever-increasing networking of IT systems and the ubiquitous presence and availability of information of all kinds, while the network boundaries are fading away. At the same time, this situation has led to a sharp increase in cybercrime attacks such as "Wanna Cry".

Particularly in a research- and knowledge-intensive sector, where universities of all kinds are part of, data and information are the most valuable assets, and there is a strong need to ensure the fundamental values of confidentiality, integrity and availability of data. On the other hand, the freedom of research and teaching must be maintained.

A number of laws, standards and guidelines at various legislative levels also underline the need to introduce an information security management system (ISMS). Not only due to the “bill concerning the digitized governance in Bavaria” (BayEGovG) in combination with the “Bavarian bill on data protection” it is compulsory to implement a corresponding information security concept at all Bavarian higher education institutions until 01.01.2019.

Although there are many different standards, nouns, approaches and procedures in the field of information security with very different quality and quantity, there is still no specifically individual solutions for the knowledge-intensive university and higher education sector.

In the author’s research report, the different approaches and procedures already existing were analyzed, compared and evaluated with respect to the specifically relevant criteria for the university and higher education sector.

As a result, it was possible to identify both the strengths and weaknesses of the prioritized solution alternatives based on the partial utility values and to carry out an overall assessment of the variants. It became obvious that there is a need for a solution that is specifically tailored to the knowledge-intensive university sector, since none of the solutions examined completely fulfills all necessary requirements on its own.

Hence, this master thesis develops a sophisticated ISMS, a so-called “UNI-HS-ISMS”, specially tailored to the requirements of the higher education sector. With this master thesis, this UNI-HS-ISMS can be established, implemented, maintained and improved in eight consecutive steps at all Bavarian universities and universities of applied sciences.

Based on a case distinction for the individual protection needs of each university and universities of applied sciences, an individual method for risk management within the HS-UNI-ISMS will be presented.

In addition, checklists have been developed in this master thesis for each phase of the UNI-HS-ISMS to facilitate the handling of the ISMS in the Bavarian higher education sector.

This ISMS-guideline is developed using the University of Applied Sciences Augsburg as an example and at the same time is designed to be so universal that all Bavarian universities and universities of applied sciences can use it.

Based on the results of a performed risk tolerance table, the highly sensitive processes "access control with the campus card" and "recording of marks" are treated as prototypes within the framework of the special UNI-HS-ISMS at the University of Applied Sciences in Augsburg.

In particular, in addition to scope and boundaries determination, an information security requirements analysis is carried out for these sensitive processes, in which the assets are determined and classified. Based on this, a meaningful risk assessment is conducted by identifying, estimating, assessing and managing risks.

By applying this master thesis, an enormously important step is taken to ensure information security at all Bavarian universities and universities of applied sciences.

II. TABLE OF CONTENTS

III. IMAGE INDEX

IV. ABBREVIATION INDEX

ALG	Application Level Gateway
BSI	Bundesamt für Sicherheit in der Informationstechnik - Federal Office for Information Security
DIN	Deutsches Institut für Normung e.V. - German Institute for Standardization
DoS	Denial of Service
HIS	Hochschulinformationsystem - university of applied sciences information system
HSA	Hochschule Augsburg - University of Applied Sciences Augsburg
IDM	Identity Management
IEC	International Electrotechnical Commission
ISIS 12	Informationssicherheitsmanagementsystem in 12 Schritten - Information Security Management System in 12 steps
ISMS	Information Security Management System
ISO	International Standard Organization
KRITIS	Kritische Infrastrukturen- critical infrastructure
NDA	Non-Disclosure Agreement
PDCA	Plan-Do-Check-Act
PT	Personentage - man-days

1 Introduction and Motivation

Information security has become more and more an essential issue across industries and organizations dealing with sensitive data during the recent years. This is due to not only the increasing degree of crosslinking of IT systems and the ubiquitous presence and availability of all types of information, while network boundaries are more and more disappearing. In addition, the simultaneous increase of cybercrime attacks in the last decade shows that information security is a sensitive topic.

The most recent cybercrime attack, “Wanna Cry”, a ransomware attack, shows the vulnerability of the internet technology and underlines the necessity of effective safeguards to guarantee the information security protection goals confidentiality, integrity and availability. “Wanna Cry” caused a huge damage cross-sectoral. The crypto-trojan spreads worldwide, slowing down hundreds of thousands non-patched or obsolescent PCs especially in the critical infrastructure (KRITIS). For example in the United Kingdom, the PCs of the National Health Service (NHS) were affected, critically ill had to be transferred in non-affected hospitals. In Spain and Portugal, the network operators Telefónica and Telecom were stroked, in Germany “The Deutsche Bahn" was also affected. As a consequence of this attack the German Federal Minister for Digital Infrastructure, Alexander Dobrindt, says that the IT-security level must be strongly increased.[1], [2], [3].

Particularly the situation in the public sector is classified as critical, because standard security measures, such as strong passwords or regular updates or the economy of data according to § 3a Bavarian data protection law “Bayerischen Datenschutzgesetzes (BDSG)“, are often not existent [4].

This is also true for the knowledge-intense environment, especially for universities and for universities of applied sciences. As administration processes meanwhile are also supported by information technology in the public sector, especially in the field of universities, data are the most valuable asset and have to be protected appropriately.

Not only due to the “bill concerning the digitized governance in Bavaria” (BayEGovG) in combination with the “Bavarian bill on data protection” it is mandatory to implement an adequate information security concept at all Bavarian universities until 01.01.2019 [5]. The information security concept is a part of an information security management system (ISMS).

Because information security is considered as a holistic approach, not only the IT-technical, but also the personnel, organizational and the infrastructural components have to be taken into account. To assure the indemnification of the basics confidentiality, integrity and availability, it is essential to establish a structural methodology for the protection of information security. By means of an appropriate model establishing an ISMS, it is possible to guarantee the organizations’ or public authorities’ overall information security.

Special challenges pose the introduction of an ISMS in the knowledge-intense environment, like the universities. To meet the requirements on the one hand the

freedom of research and teaching and on the other hand, the high protection requirements of sensitive data, such as for instance personnel data or results of the examination or research data, have to be considered. As a result of this, it is necessary to establish an ISMS that is especially matched with the requirements of the environment of universities [6], [7], [8], [9], [10].

Not to forget, a university respectively a university of applied sciences is a two-tier construct. On the one hand, the Bavarian university administrations are subject to mandatory guidelines for IT-security (such as the “BayITSiLL” [11] an IT Security Policy for the Bavarian public administration or the “BayITSiR-02” [12], a special policy for the “Operation of the transition to the Internet”), and on the other hand, they need a sophisticated ISMS for their sensitive research data from the field of research and teaching.

However, there are many different approaches and procedures both with respect to quantity and quality in the field of information security. Specifically, in the knowledge-sensitive field the universities represent, there are up to now no suitable individual solutions available to develop, implement and maintain or eventually improve an ISMS.

In the course of the authors’ research report [13] the different approaches and procedures already existing were analyzed and compared. Based on that, the prioritized procedures were evaluated based on a value benefit analysis – with respect to the specifically relevant criteria for the university sector. This made it both possible to identify the strengths and weaknesses of the prioritized solutions based on partial use values and define an overall use value per solution.

Finally, the necessity of a solution that is specifically adapted to the university sector was lined out, as none of the evaluated solutions can fulfil all requirements completely on its own.

Within the framework of this master thesis, the various analyzed and evaluated methods and approaches are combined with their respective strengths, depending on the requirements of the university sector, so that a sophisticated ISMS can be created that is specially tailored to the university sector.

With the help of this approach, a universal guideline to be edited specifically for the knowledge-intensive higher education sector, applicable to all Bavarian universities and universities of applied sciences for the introduction, implementation, maintenance and improvement of a "HS-UNI-ISMS" will be created.

Starting with a case distinction to determine the need for protection, this Master's thesis shows the appropriate method for the respective university or respectively the university of applied sciences to deal with the core of the HS-UNI-ISMS, the appropriated risk management.

Based on this, a process flow diagram is used to develop an exact and at the same time universal procedure for all Bavarian universities and universities of applied sciences to handle a HS-UNI-ISMS.

This procedure is intended to enable all Bavarian universities and universities of applied sciences to create a universal HS-UNI-ISMS, which can be scaled at the same time for the individual special requirements of each university.

Using checklists in every process phase, this master thesis enables all Bavarian universities and universities of applied sciences to develop a precisely tailored HS-UNI-ISMS for them.

In addition, an example of how a HS-UNI-ISMS handles the critical process of recording of marks and the infrastructural component - access control with the campus card - will be demonstrated using the University of Applied Sciences Augsburg as an example.

In this process, all the components necessary for information security such as hardware, software, organizational and personnel aspects are taken into account in order to create a meaningful and effective risk management.

With the help of this master thesis, a prototype of the mentioned areas is developed for the application of a sophisticated HS-UNI-ISMS.

Finally, the aim of this master thesis is to develop a universal, but also individual tailored guideline for the implementation of a specific ISMS (“HS-UNI-ISMS”) for all Bavarian universities and universities of applied sciences using the example of the University of Applied Sciences Augsburg.

With the support of this master thesis, an enormously important step is being taken towards guaranteeing information security at all Bavarian universities and universities of applied sciences.

The structure of this master thesis is organized as follows:

Chapter one chapter one contains the introduction and the motivation.

Chapter two describes not only the definitions relevant for comprehension, but also the requirements of the public administration, especially in the higher education sector, the procedure in the master thesis, as well as the object of investigation and its limits.

The next chapter three explains the existing concepts in the field of information security in the higher education sector. In addition, relevant norms, standards and general conditions are described which present themselves as influencing factors on management systems for information security.

Chapter four, based on the author's research report, analyses and prioritizes the different approaches of dealing with an ISMS and evaluates them by means of a benefit analysis. Based on these results, a model is developed to determine the need for protection requirements.

Based on this, a special ISMS for the higher education sector is developed in chapter five, a so-called "HS-UNI-ISMS".

Chapter six contains exactly matching checklists for the individual HS-UNI-ISMS steps.

In chapter seven, the newly created HS-UNI-ISMS is used as a prototype model for the critical processes "Access control with the campus card" and "Recording of marks". Finally, suggestions for further scientific work are given in the last chapter.

2 Terms and definitions, approach, object of investigation, delimitation and requirements

2.1 Terms and definitions

This subchapter defines the terms necessary for a common basis, since different definitions exist.

Public administration is the generic term for administrations that perform tasks of the state, including public law institutions. The public administration is administered by the Federal Government, the states and the municipalities. The higher education sector is therefore also covered by this term.

State or public IT refers to the public and non-public components of information technologies that are operated under the responsibility of the public sector. This includes IT at all levels of government and supranational, i.e. at international, European, federal, state and local levels as well as within the framework of alliances.

Information security extends the term IT security to include the personnel, organizational, procedural and infrastructural components in which the basic values of confidentiality, availability and integrity are guaranteed.

Information Security Management (ISM) is the planning, management and control task necessary to establish and continuously implement a well thought-out and effective information security process. This is a continuous process, whose strategies and concepts have to be constantly checked for their efficiency and effectiveness and, if necessary, updated [6].

In accordance with the ISO/IEC standard 27001 [14] as well as the BSI standard 100-1 [15] and the aspects according to Müller [16], an information security management system (ISMS) is defined as the entirety of all processes, responsibilities, procedures, methods and resources as well as aids to enable the management level with an efficient organizational structure to steer and document all activities and tasks oriented towards information security in a comprehensible manner. In addition, an effective ISMS includes iterative security, continuity and risk management processes. With the help of an ISMS, information security is integrated into the lifecycle of processes, resources, organization, products and services. Some procedures contain different sub-areas or core elements of an ISMS in varying degrees of completeness, detailing, concretization and quality [17].

The IT Security Policy documents the IT security goals and the strategy for their implementation. The IT Security Concept and the IT Security Organization are the tools of the management level for implementing the IT Security Strategy. [18], [19]

Policies are guidelines for the behavior of managers and employees and their actions within the company. They can be issued as guidelines from both the normative and

operational management levels. As such, they communicate how the goals and requirements of the respective levels are to be implemented. In this way, they also define how the tasks, responsibilities, competencies and resources are allocated within the company. [18]

Information security risk is the potential by exploiting the threat of a vulnerability and causing damage. The risk consists of the combination of the probability of an event and its consequences [19].

Risk management is understood to mean the collection, analysis, evaluation, adjustment or treatment, monitoring, early identification of risks as well as the target-oriented and requirements-compliant management, reporting and communication of risks [16], [20].

The risk management process includes the systematic iterative approach such as management policies, procedures and practices to identify and assess all potential risks, determine the context, and then select and implement appropriate risk management measures, such as the management, monitoring and review of risks, at both strategic and operational levels. In addition, the risk management process is subject to continuous improvement measures [20], [21].

Risk analysis is a process for understanding the nature of the risk and determining the level of risk. The risk analysis provides the basis for risk assessment and decisions based on the risk treatment [20].

2.2 Object of investigation and delimitation

The present master thesis contains an analysis, prioritization and evaluation of the different existing models in the handling of an ISMS. The different approaches are assessed based on requirements and relevant criteria defined for the university sector. Based on the independent evaluation of the author's research report, this master thesis develops a sophisticated ISMS, a so-called "HS-UNI-ISMS", specifically tailored to the university and higher education sector, based on the strengths of the respective approaches.

With the help of newly created checklists for each phase of the HS-UNI-ISMS, this master thesis develops a universal guideline that enables the creation of an individual HS-UNI-ISMS, which is tailored to the requirements of each Bavarian university and university of applied sciences. In addition, this master thesis describes the challenges of each phase in order to facilitate the user's handling of the HS-UNI-ISMS. Finally, the newly developed HS-UNI-ISMS will be used as a prototype model for critical processes "Access control with the campus card" and "Recording of marks" at the University of Applied Sciences Augsburg.

The complete implementation of the HS-UNI-ISMS at the University of Applied Sciences Augsburg is not part of this work. In addition, the HS-UNI-ISMS is only applied to the above-mentioned processes as a model, so that there is no claim to

completeness. In particular the steps "obtaining management approval for initiating an ISMS project, determining an ISMS policy, obtain resources, awareness of all university s' members and designing the ISMS" of HS-UNI-ISMS are not detailed in chapter seven.

The master thesis is a snapshot and is considered to be final at the time of the document.

2.3 Approach

In a first step the general requirements, the frame conditions and the context definitions in the public authorities, especially in the field of the university and university of applied sciences will be defined. Next, based on the results of the authors´ research report, the analyzed and assessed concepts and standards in the field of information security will be illustrated. Derived from step one, the criteria specific for the knowledge-intensive sector as the universities are defined.

With the aid of the use-value analysis, the strengths and weaknesses of the different methods and concepts in the field of information security are represented.

Depending on the protection requirement, a case decision, what kind of risk assessment, will be developed. Based on these results, a step by step combination of the different methods´ and concepts´ strengths will be created, whereas the concepts´ weaknesses will be replaced through a new action.

Based on this, this master thesis develops a special, sophisticated ISMS for the higher education sector, a so-called "HS-UNI-ISMS".

Depending on the protection requirements of each university, the appropriate approach to risk management is used. In addition, this master thesis discusses the challenges of each phase in order to make it easier for the user to handle the HS-UNI-ISMS.

In this context, universal checklists will be developed in order to introduce, implement, maintain and improve a HS-UNI-ISMS.

In a next step, the newly developed HS-UNI-ISMS will be implemented exemplary in the sub-processes "Access control with campus card" and „Recording of marks“ at the University of Applied Sciences Augsburg.

As a result of this master thesis a universal guideline for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a specific ISMS for the knowledge-intense sector of the universities and universities of applied sciences in Bavaria will be developed, which will be based on the test case of the University of Applied Sciences Augsburg.

The guideline will be universal, but also scalable to meet the individual local requirements of each university. The results of this master thesis base among others on the results of the authors research report, the information of the Bavarian IT-

Sicherheitscluster e.V., on the analysis of the ISO/IEC 2700x family of standards and of the BSI IT-Grundschutz. The results of [22], [23], [24], [10], [9] influence the assessment.

Within the framework of this master thesis, structured interviews were conducted, analyzed and evaluated with the employees of the computer center and the examination office. Thus, the results are based on this.

2.4 General requirements for public administration in specific for universities

The facilitation of science, research and teaching is a common and central task of government and society and has constitutional rank based on article 91b/1 GG [25].

Particularly in the university sector, freedom of research and teaching must be guaranteed on the one hand, and sensitive data such as personal employees and student data, examinations, certificates or research results must be protected on the other. Ensuring availability, confidentiality, integrity, authenticity and traceability is an elementary prerequisite of any IT process.

As in the meantime the majority of all administrative processes in the public sector - particularly in the science, research and university sector - is supported by or even based on information technology systems, its ability to perform the required tasks is largely relying on the availability, confidentiality and integrity of data. A major goal of the federal "e-governance-bill", which has entered into force from 01.08.2013, is to provide user-friendly, efficient and cross media electronic administration tools and processes to all levels of the public sector. The IT-Council is, based on the IT-inter-state-treaty in charge of the alignment of the minimum requirements of both the federal and states' administrations. Hence, the "guideline regarding the information security in the public sector" that has been passed [26] is valid for all authorities and institutions of the federal and state governments. In this guideline, the minimum requirements for IT-Security for the federal and state administrations are defined. Nevertheless, the specifications defined in this guideline have to be implemented by the federal and state authorities in their respective areas of responsibility on their own [27]. The definition of the minimum-security level is based on the "IT-Grundschutz" of the BSI.

The public sector is facing specific challenges to their IT-Systems, such as a hierarchical environment, a huge number of regulations (bills, decrees, and service regulations), budgetary rules and traditionally strong and detailed specifications for each end every process. Furthermore, IT-standards for the public sector are mainly developed locally, due to its decentralized organization, the federal structure of the state and the departmental principal. Quite naturally, this approach leads to large variety of results [28]. It is clear that a central institution to achieve common IT-security-standards makes sense.

Based on [29], [30] the basic prerequisite for a successful implementation of an ISMS in the public sector is a healthy human resources management, such as investing in

highly qualified experts in the field of information security, training and awareness raising measures.

Taking into consideration the whole university landscape in Bavaria, one can no longer assume a standard agency (not more than 500 employees, homogenous IT-basis – infrastructure, no dislocated subsidiaries linked through unprotected public networks, normal protection requirements, no high-level availability requirements regarding the IT-Systems, no critical applications in terms of KRITIS) according to BSI standards. Even each university on its own has more than 500 members. In addition, there are dislocated subsidiaries linked through unprotected public networks and the protection requirements especially for research results and exam data is beyond a normal level. Mostly, there is also not a homogenous IT-infrastructure, as the individual faculties act independently. In case thousands of students are using online-services such as Email or E-learning services, high-level availability requirements exist. Further on it is open for discussion whether universities are to be seen as KRITIS (critical infrastructure) – in case the computing center has an average annual power of more than 5 MW or for instance a university with a medical faculty is supporting the emergency medical service, this could be affirmed [31], [32], [14].

3 Existing Standards in the field of information security

3.1 General

There are many standards and norms in the field of information security with different characteristics in terms of quantity and quality. Depending on the target group and its protection needs, some of them are very suitable, while others are not applicable. The most important standards and norms with regard to information security are briefly listed below. The author's research report can be read for further details.

- ISO/IEC 2700x

The international family of standards ISO/IEC 2700x provides besides requirements for an ISMS also detailed guidelines for the establishment, implementation, maintenance or improvement of an ISMS at a total procedural view. This guideline is based on international standards and allows all organizations, no matter of which kind or size, to develop a framework for maintaining and managing the security of their assets. The family of standards consists for instance of ISO/IEC 27001 (Information security management systems Requirements) ISO/IEC 27002 (Code of practice for information security controls) or ISO/IEC 27005 (Information security risk management) and many more. This family of standards has - in comparison to other standards - a very abstract character [20], [33].

- IT-Grundschutz of the BSI

The IT-Grundschutz was published by the German Federal Institute "*Bundesamt für Sicherheit in der Informationstechnologie (BSI)"*. This standard provides recommendations for methods, processes and procedures. The *IT-Grundschutz* is divided in four BSI-Standards (100-1 or the newer 200-1 describes requirements; 100-2 or the newer 200-2 specifies guidelines for implementation of an ISMS; 100-3 or the newer 200-3 depict a risk analysis; 100-4 or the newer 200-4 describes a Business Continuity Response Plan) and the basic protection catalogue. The basic protection catalogue consists of modules, threats and measures.

This simplified risk analysis of the standard 200-3 for a minimum high protection requirement is used, if the existing measures in the basic protection catalogues are not enough. Indeed, this procedure is more comparable to an analysis of the rest risk in ISO/IEC 27005 than a completely risk management method. The *IT*-Grundschutz pursues the goal to reduce the effort for the information security process using already known security measures [34], [35], [36], [37], [21], [24], [38], [19].

- ISIS 12

The ISMS in 12 steps (ISIS 12) was developed by the Bavarian "*IT-Sicherheitscluster e.V*." in the year 2009 and has been updated ever since. This guideline pursues the aim „as simple as possible but not simpler" by using the BSIs´ reduced basic protection catalogue and not using the abstract elements of ISO/IEC 27001. This method has to pass through a 12 sequential steps cycle, only focusing on a few critical applications. This method is very flexible and very scalable. Originally, the method was developed for small and medium-sized businesses. It is also applicable for a so called „standard agency" in the public sector. Due to the easy scalability of this guideline the most important steps to establish an ISMS can be completed with comparably little efforts and a later implementation of more complex standards is still simplified [39], [40], [22].

- Guideline of the Bavarian Innovation Foundation

This tool was developed in December 2016 by the Bavarian Innovation Foundation of the *„Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB*) "and is based on ISIS 12 and the IT-Grundschutz. However, this method only comprises of a significantly reduced measure catalog for self-estimation and the use of the tool cannot be certified and it is not a substitute for an ISMS, it can only be seen as a starting point for smaller municipalities that have so far not dealt with information security questions. That is why this tool will not be dealt with in this master thesis [41].

- Other standards related to information security

There are also other standards, which affected the information security, for example COBIT, ITIL, ISO/IEC 20000-1. For example, the COBIT-framework has a 90% accordance with the ISO/IEC 27001 and the ISO/IEC 20000-1, whereas ISO/IEC 27001 is to far more extent detailed. The security measures in ISO/IEC 20000-1 are more general and refer to ISO/IEC 27002. Also ITIL has a significant amount of communalities with ISO 27001.For this reason this master thesis will also not deal with these [42], [43], [44], [45], [46].

3.2 Specific guidelines for universities and universities of applied sciences

In the university sector, guidelines for the treatment of information security already exist. However, these guidelines are very restrained and deal only with the area of it-security and are therefore not suitable for dealing with the complex feld of information security, or only in very limited areas. The existing guidelines are briefly listed below. For more information please read the author's research report.

- Working Group „ Information security of the IT Planning Council (IT-PLR)“

The IT Planning Council (IT-PLR) is, based on the interstate treaty on IT-questions, in charge of aligning the common minimum-security requirements e. g. securing the network infrastructure of public administration, uniform security standards for cross-level IT procedures, joint defense against IT attacks or standardization and product security, between the federal and state governments and institutions. Hence, it is also in charge for the development, signing or find further development and success control of the guidelines regarding the information security. One of the most important goals of this guideline is to develop and establish an information security management in the public sector, which needs to be implemented by 01.01.2018 [47], [26].

- Research Group „IT-Security of the ZKI“

When these Information security requirements where defined in 2005 by „*Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI)* “, no differentiation was made between information security and IT-Security. It was meant to deal with aspects such as a security policy or an overall guideline for IT-Security at universities [48], [27], [49].

- Information security guideline of the “Free University of Berlin”

The overall guideline for information security developed in 2005 by the „ *Free University of Berlin* “ is mainly comparable to the IT-Grundschutz. This concept is - due to its development date and the sources it is based on (such as the security guideline of 1992 and the „*Grundschutzhandbuch*“of 2002) - not providing an iterative process with improvement measures such as the PDCA-Cycle, but is rather a snapshot of the current situation [50].

4 Analyzing, prioritization and assessment of information security methods and determination of the protection requirement

4.1 Research Report

This subchapter summarizes the results of the author's research report. The prioritized approaches, namely of ISIS 12, of ISO/IEC 2700x family of standards and of the BSI IT Grundschutz, for establishing an ISMS at all Bavarian universities and universities of applied sciences are assessed with the aid of the benefit value analysis.

This way a substantial basis is created for an appropriate approach for establishing, implementing, maintaining and improving an ISMS for all Bavarian universities and universities of applied sciences.

Based on the requirements in the knowledge-intensive university sector, the prioritized methods are analyzed and assessed with their individual weaknesses and strengths. These three prioritized approaches are all suitable to establish an ISMS – even if only to a different degree.

Because of non-fulfilling this criterion at all, the method of the Bavarian innovation foundation is excluded from the following assessment.

Based on the criteria relevant for the university sector, the different alternatives are assessed with the aid of the benefit value analysis.

In this process, each alternative is given a benefit value, based on which a prioritization is done leading to a final result.

First, the relevant decision alternatives are selected. Subsequently, important criteria for the decision finding are defined. Attention should be paid to the fact that only the sum of the criteria defines the solution for the underlying problem. Furthermore, every criterion has to be important for the decision and reproducible. After identifying all relevant criteria, they have to be weighted depending on their importance. The overall sum of the weight has to be exactly 100 %. Next the criteria are associated to the marks in reverse order from 1 („ criterion is not at all or hardly fulfilled “) to 6 („ criterion is very well fulfilled “). A clear scale is important as follows:

- 1: criterion is not at all or hardly fulfilled
- 2: criterion is only fulfilled while accepting major restrictions
- 3: criterion is sufficiently fulfilled
- 4: criterion is fulfilled satisfactory
- 5: criterion is well fulfilled
- 6 criterion is very well fulfilled

For each criterion, an estimation is done in how far it is fulfilled or useful for the respective decision alternatives. After that, all scores are multiplied by the weighting factor. Hence, these values (partial benefit values) are reflecting how well the respective criterion is fulfilled by a decision alternative. Finally, all partial benefit values are summed up per decision alternative. This sum is defined as the benefit value, upon which the decision alternatives are assessed [51], [52] ,[53].

4.2 Criteria

4.2.1 Target group applicability

The criterion “Target group“ is describing the applicability of the respective approach for the university area. It reflects in how far it can be used for the known-intense area with highly sensitive data and therefore high protection requirements, such as research results or examination results. The definition of a “standard authority” as given by the BSI does not fully comprise this area. Even if each university is examined on its own, there are more than 500 members. Neither are homogeneous IT-Infrastructure nor protected external subsidiaries that are linked via public networks to be found. The definition of a low or average protection requirement can be ruled out. As described in chapter 2.3. there are high level availability requirements for IT-systems and even the term “KRITIS” might be appropriate under certain circumstances. It plays a vital role for which target group the respective solution alternative for the creation, implantation, sustaining and improvement of an ISMS for all Bavarian universities is most suitable.

As this criterion is the most decisive component in the decision making process, it is weighed with 20%.

4.2.2 Efficiency

The criterion resource efficiency is also highly important and therefore is weighed with 15%. It reflects on the one hand the internal time-, cost- and staff requirements that are needed for the implementation and sustaining of an ISMS. On the other hand, it reflects the external requirements for the certification, which is quite different for each solution alternative. For the internal requirements, both strategic, one-time demands (such as creation of a security team, information security concepts and an IT-security policy) and ongoing organizational tasks (such as the validation of IT-security concepts, IT-emergency concepts and staff training) have to be considered. To implement and maintain an ISMS both the IT-Security-counselor as well as the IT-Security team needs to have found and specific related knowhow, which leads to high personnel costs, which have a substantial share in the indirect costs of an organization.

In the public sector resources are a key factor due to the specific budget planning for third-party funds, so this criterion is reflecting their high impact. .[54]

4.2.3 Scalability

The criterion scalability is highly important, as the circumstances under which the ISMS needs to work are rapidly changing. Hence, it needs to be scalable in both a quantitative as well as a functional way. This criterion is reflecting how the respective approach reacts on quantitative changes (for instance-increased number of universities or their members) and functional circumstance (such as changes of the threats and weaknesses, change in protection requirements). Based on its importance it is weighed with 13%.

4.2.4 Risk management

A powerful risk management is the core of each ISMS [55]. Therefore, this criterion is weighed with 19%. It reflects in how far the respective approach fulfill the requirements to identify and evaluate all potential risks and to execute the necessary measurements for the risk handling, risk control. In addition, the early detection of risks and the target oriented and requirements adapted management, reporting and communication of risks is evaluated, both on a strategic and operational level. The risk management process is subject to continuous improvements, due to its iterative nature. As described in [56]”virus infection for hosts and phishing” are serious risks in the field of universities, which can be successfully treated with a found risk management

4.2.5 International significance

The international significance of the approaches presented here is of far-reaching significance in a knowledge-intensive university sector. International recognition of an ISMS is very important, particularly in relation to the Bologna Process, where the promotion of spatial and cultural mobility, international competitiveness and employability has been established by integrating the European Higher Education Area with the European Research Area, in particular by integrating the doctoral phase. The establishment, implementation and maintenance of an effective ISMS in the university sector should be internationally recognized, especially against the background of the desired certification. The evaluation standard is based on the extent to which the international recognition of the respective alternative is high. For this reason, this criterion is valued at 12%.

4.2.6 Tool support

Successful introduction, implementation and maintenance of an ISMS in a knowledge-intensive area requires adequate tool support. From a document management system to complex process planning with a meaningful risk management system, an ISMS should be supported by powerful and user-friendly tools. This criterion primarily examines the availability of appropriate tools for each decision alternative. As described in chapter 2.2, the detailed contents of the tools are not the subject of this research report. Thus, the criterion tool support is 5 %.

4.2.7 Given process steps

Predefined process steps lead the user through the whole process in a systematic and structured way. This significantly reduces the implementation process and makes it possible to perform this task with less in-depth know how as if the process needs to be started from scratch. However these predefined process steps should be set up flexibly enough, that the process can be extended or shortened adapted to the given situation. Hence, this criterion is weighed with 5%.

4.2.8 Minimum requirements of the IT-PLR

As described in chapter 3.2, the „IT-Planning council“ is, among other tasks, in charge of the creation and establishment of the information security management in the public authorities. Based on this it is evaluated in how far the minimum requirements for an ISMS in the university sector is fulfilled by the respective approaches. This criterion is weighed with 5%.

4.3 Assessment

The subsequent evaluation matrix shows the explicit subdivision of the partial utility values of each presented decision alternative as well as the total utility value of each variant. This makes the strengths and weaknesses of the respective procedure visible on the one hand, and on the other hand, an overall assessment is possible.

The benefit analysis carried out shows that the ISO/IEC 2700x decision alternative with 4.80 has the highest utility value. The decision alternative ISIS 12 has the second highest utility value of 3.10, closely followed by the third alternative IT basic protection with 3.08. In order to be able to provide a meaningful evaluation with a sound result, the strengths and weaknesses of the three decision variants must be explicitly

considered on the one hand, and on the other hand, the background of the value grading of the individual criteria for each alternative must be analyzed in detail. Based on the evaluation matrix, the following results are produced.

Criteria	Weight	ISIS 12		IT-Grundschutz		ISO/IEC 2700x	
	G	P	W	P	W	P	W
target group applicability	21%	1	0,21	5	1,05	6	1,26
efficiency	15%	6	0,9	2	0,3	1	0,15
scalability	13%	6	0,78	2	0,26	6	0,78
risk management	19%	1	0,19	2	0,38	6	1,14
international significance	12%	1	0,12	2	0,24	6	0,72
tool support	10%	3	0,3	4	0,4	4	0,4
given process steps	5%	6	0,3	3	0,15	1	0,05
minimum requirements of the IT-PLR	5%	6	0,3	6	0,3	6	0,3
Sum	100%		3,10		3,08		4,80

Figure 1: Rating Matrix [own preparation]

4.3.1 ISIS 12

The ISIS 12 approach does not fulfill the criterion “Target group“ at all or only hardly. Even though it is optimized for medium sized companies and smaller public authorities that are to be seen as a „standard authority“ it cannot fully cover the needs described in the criterion „target group“. This is because universities and universities of applied sciences deal with highly sensitive data, such as research results, staff data or exam results, hence the protection requirements can't be classified as „normal“. Furthermore, each university on its own has already more than 500 members and there is no homogeneous IT-infrastructure nor are there branches that are linked through public networks in a protected way. In case several thousands of students are

accessing simultaneously on a certain application (for instance Email or eLearning service or examination results) high-level availability requirements on these systems occur. As even the term „KRITIS“ can be used appropriately under certain circumstances (see 2.4.), the ISIS 12-Approach does not fulfill the criterion “Target group“ at all.

The criterion „resources“ is fulfilled to a very good extent. Due to the reduced measure catalogue and the predefined process steps the internal time-, financial and staff, requirements are pretty small compared to other solutions.

If only the internal efforts are taken into consideration, the case study for a standard authority following the BSI “IT-Grundschutz” approach shows that HR-resources of 160 Man-Days (md) for one-time, strategic work can be expected and 180 md for operational tasks on a regular basis are required. As ISIS12 is derived from the BSI approach, but has a significantly reduced catalogue of measures one can assume that necessary resources are respectively smaller. In addition to that, the predefined process steps of the ISIS12 approach help to reduce the process lead-time, which also reduces the required resources. Additionally, the external resource requirements for a potential certification can be estimated to be two md for an initial certification and one md for a repetitive audit.

In the university area the resource aspect, regarding for instance staff, time, plays a huge role due to the economic feasibility studies and the budget planning. The ISIS 12 approach fulfills this approach very good. The criterion scalability is also well fulfilled by this approach. The ISIS 12 approach is easily adaptable to quantitative (for instance number of employees) and qualitative (changes of threats, weaknesses, protection requirements) changes of the underlying scenario. Additionally, user specific work packages can be integrated in the predefined catalogue. This flexible modular approach is of high importance in a rapidly changing environment in which knowhow related data is the most important good. Hence, the ISIS12 approach fulfills this requirement very well. However, the criterion risk management is only fulfilled poorly due to its design criterions. The ISIS12 approach, which is largely based on the BSI Grundschutz, only provides an immanent risk analysis. The safety measures that need to be taken during the first two phases only cover the general threats for low or intermediate protection requirements. As in a knowledge- intense sector the protection requirements cannot be considered to be low or intermediate any more, the immanent risk analysis of ISIS12 fulfills this criterion not at all or only poorly. The goal of a successful risk management that is based on a sensual risk analysis is to identify all relevant threats, estimate all arising risks and reduce them to an acceptable degree by using corresponding countermeasure whilst creating transparency for all remaining risks. In addition, it follows an iterative approach with a continuous improvement process, which is not available in ISIS 12 also. As a powerful risk management is the core of an ISMS, ISIS 12 fulfills this criterion only very poorly. The criterion “international relevance” is also only fulfilled very poorly.

The ISIS 12 approach is nevertheless known more and more among midsized companies and partially also public authorities in the German speaking countries while it is not at all renowned on a truly international basis. However, as this is required in

the university environment, especially due to the bologna process, this criterion is only fulfilled very poorly or not at all.

There is a dedicated software tool for the ISIS12 standard and in addition to that also a commercial tool. Making use of such a tool is recommended, however it is possible to use and / or certify an ISIS12 application without it, even if that is very resource intensive. Hence, ISIS12 fulfills this criterion to a satisfactory extent. The next criterion “predefined process steps” is fulfilled very well by ISIS12, as the user is led following a top-down approach using the sequential predefined process steps through the creation, implementation, maintenance and improvement of an ISMS. The 12 process steps are consolidated into 3 main phases (starting phase, definition of the organization, development and implementation of the ISIS12-concept), which need to be followed in a chronological order by the user.

Besides that, the specified process steps reduce the necessity of detailed subject matter knowhow compared to setting up the process from scratch. Additionally, the criterion “minimum requirements of the IT-PLR” is very well fulfilled by ISIS12. As the IT-PLR is among others responsible for the establishment of an ISMS for public authorities, this criterion helps to analyze in how far the minimum requirements for an ISMS in the university area can be fulfilled using the ISIS 12 approach.

The ISIS12 approach contains the in chapter 3.2 described minimum requirements for an ISMS. The later ones (appropriate and harmonized training of the information security officers, annual conferences of the information security officers for exchange on the experiences) are not directly linked to an ISMS but are by far more aiming towards qualification methods for information security officers. Hence, they are only partially available in ISIS12.

4.3.2 IT-Grundschutz

The solution approach „IT-Grundschutz“ of the BSI fulfills the criterion target group pretty well. It is especially in the public sector usable without almost no restrictions, this is of course also true in the field of universities as they are part of the public sector. Nevertheless, the IT-Grundschutz is assuming low to medium protection requirements when applying the Standards, 100-1,100-2 and 100-4. As already explained in the assessment of the ISIS12 approach, a low or medium protection requirement can no more be assumed in the university area. If at minimum a high protection requirement is assumed, the IT-Grundschutz makes use of the standards 100-3 or 200-3 respectively. If there are non-standard threats that require the corresponding countermeasures, the IT-Grundschutz is no longer sufficient. It leaves the choice of the necessary risk analysis up to the user. It can hence be used as an initial alternative in an adequate way. If – in the course of the appliance of the IT-Grundschutz – it turns out that there are non-standard threats, which require the respective countermeasures, other approaches can be used based on the already performed process steps of the IT-Grundschutz.

The criterion resource efficiency is only fulfilled by the IT-Grundschutz when accepting a number of deficits. The use of resources is divided into external and internal resources. As described in the case study [23], the creation, implementation, maintenance and improvement of an ISMS requires 160 man-days (PT) of internal resources for one-off, strategic and regular operational work of 180 PT. These specifications refer to the definition of a standard authority. Appropriate surcharges are added for the factors, more than 500 employees, the degree of heterogeneity of the IT landscape and IT processes, the number of branch offices to be supported, the proportion of IT applications with a protection requirement higher than "normal", and the high availability requirements for IT applications. In addition, the external resources required for a possible certification are at least 15 PT. This is considered to be independent of the scope of application without any handling of defects and queries by the certification body. Experience has shown that this effort is estimated by the BSI at 14 to 30 PT. The decisive factor in this evaluation criterion is also the very extensive and complex catalogue of basic IT protection components and measures, the selection and processing of which requires a high degree of time, cost and personnel input. As the process steps, as described in chapter 4.2, are formulated rather vaguely, the process creation and processing is associated with additional resources. If the basic IT protection is evaluated on the basis of scalability, it meets the requirements of an ISMS in the higher education and university sector rather moderately. The modules are self-contained and can only be improved and updated by the BSI itself. In addition, the prefabricated modules with safety measures are only designed for standard hazards. Should new standard deviation hazards develop in such a rapidly evolving knowledge-based field, the basic IT protection of the BSI is no great help here. This means that the criterion is only fulfilled if essential defects are accepted.

Similarly, the risk management criterion is only fulfilled by the decision alternative of basic IT protection if essential deficiencies are accepted. On the one hand, the 100-1 and 100-2 standard is only designed for the low to medium protection requirements, which is not promising in a knowledge-intensive higher education and university sector. Even if the basic IT protection refers to the standard 100-3 or 200-3 for high protection requirements, the basic IT protection assumes that the existing pool of standard security measures is sufficient. In this case, a downstream safety analysis is carried out in which general categories of hazards are used, so that a time-consuming risk analysis is unnecessary. On the other hand, the basic protection modules used are considered to be self-contained. An iterative improvement process is difficult for the basic protection user because improvements are only carried out by the BSI. However, this approach does not reflect the core of effective risk management with an iterative improvement process. If standard deviating measures are required due to standard deviating hazards, the BSI is not applicable. However, basic IT protection leaves the choice of the risk analysis to the user, so that basic IT protection can at least be used to identify all standard hazards and the associated countermeasures.

The IT-Grundschutz is relatively well known in the German-speaking countries, especially in the public sector. However, especially in view of the Bologna background, international recognition in higher education is of great importance. The establishment, implementation and maintenance of an effective ISMS in the university sector should

be internationally recognized, especially in the case of the desired certification. However, the IT Grundschutz cannot meet this requirement. This means that this criterion is only fulfilled if essential defects are accepted.

The IT-Grundschutz was supported by the gstool tool, which was individually developed for the BSI. However, sales were discontinued as of December 31, 2014 and support until the end of 2016 [57]. However, there are other licensed tools such as Sidoc ® -Security Management, INDART® Professional, Verinice Open Source ISMS Tool, HiScout Basic Protection to support the basic IT protection approach, so that this criterion is satisfactorily met.

The IT-Grundschutz approach includes a vaguely managed process structure with the process described in chapter 4.2. The user can view the predefined process steps such as initiation of the security process, creation of a security concept, implementation of the security concept and maintenance and improvement as a rough guide. However, compared to other decision alternatives, the user is not guided through the process in such detail. Although the user does not have to reinvent the process completely, there are no precisely defined process steps in this alternative solution. In this way, the criterion is sufficiently fulfilled.

The IT-PLR fulfils the last criterion of minimum requirements for an ISMS very well with the IT-Grundschutz procedure. The IT-Grundschutz includes all minimum IT-PLR requirements specified in [13]. Since the latter requirements (requirements-based and uniform advanced training of the Information Security Officers, annual meetings of the ISB for the mutual exchange of experience) are not direct requirements for an ISMS, but serve much more as qualification measures for the vocational competences of information security officers. These requirements are only partly available IT-Grundschutz.

4.3.3 ISO/IEC 2700x

The ISO/IEC 2700x family of standards fulfils the criterion target group in the university sector very well, as it is fully applicable. This solution is suitable for both low and very high protection requirements. Since highly sensitive data such as research results, examination results or personal data are handled in the university sector, which means that a very high level of protection is required, at least in relation to the requirements of this criterion, this alternative decision is fully in line with this criterion. The limitations of a standard authority are not taken into account in this alternative. The demand for a maximum number of 500 members, a homogeneous basic IT infrastructure, branch offices that are connected via public networks and no high availability requirements for IT systems is meaningless. Even the definition of KRITIS can be covered by this decision variant. Thus, it is irrelevant whether the knowledge-intensive university sector can fall under the term KRITIS under certain conditions (see chapter 2.4). The creation, implementation, maintenance and improvement of an ISMS at Bavarian

universities and colleges is completely covered by this decision alternative with regard to the criterion target group.

However, the ISO/IEC 2700x decision alternative does not adequately meet the criterion of resource use. Due to the very abstract character without prescribed technical implementation details, as well as the rather unmanaged implementation process, the resource expenditure is very high. It requires highly qualified personnel to create, implement, maintain and improve an ISMS in a knowledge-intensive area. This decision alternative contains 114 generic measures and controls divided into 14 control groups. However, these measures and controls are not conclusive and serve as a guide for highly qualified specialists rather than a concrete guided implementation aid. Due to its generic character, this alternative solution offers a collection of possible measures and controls in the environment of an ISMS rather than precisely defined process steps. Thus, a process in the area of an ISMS for higher education and university needs to be newly established. This results in high time, cost and personnel costs. Highly qualified personnel resources entail high costs. In addition, the external resources required for certification, which is calculated in accordance with ISO 27006 and is primarily dependent on the number of employees in the area of application, is relatively high at 5 PT for the first audit (+-30% for specific factors such as complexity, locations, etc.). In the university sector, the resource aspect is of great relevance due to the economic efficiency analysis and budget planning.

The ISO/IEC 2700x family of standards fulfills the criterion of scalability very well. Thus, changes can be made at any time both in quantitative (e. g. change in the number of higher education institutions or universities, change in the number of university and higher education staff) and qualitative (e. g. change in threats and vulnerabilities, change in the need for protection) respects. In addition, the measures and controls are not conclusive and can be extended or adapted as required depending on the situation. Especially in a knowledge-intensive field that is developing so quickly, it is of enormous importance that a flexible situation-dependent reaction can take place.

The decision variant of the ISO/IEC 2700x family of standards fulfils the criterion of risk management very well. ISO/IEC 27005 contains a comprehensive risk management system with an upstream risk analysis. Risk management is carried out in accordance with the PDCA cycle according to Deming, as described in [13]. The individual steps, such as the definition of framework conditions, risk assessment, risk identification, risk assessment, risk assessment, risk evaluation, risk treatment, risk acceptance, risk communication, risk monitoring and improvement must be carried out as iterative processes. The risk management according to ISO/IEC 27005 [58] decision variant is applicable for a low to medium, but also especially for a high to very high protection requirement. This property is very important against the background of a knowledge-intensive area where data with high or very high protection requirements exist.

This iterative approach makes it possible to respond very promptly to changes in any aspect, such as changing the context, threats or risks, and to implement improvement measures. In addition, this risk management approach can be adapted to suit individual requirements, even with regard to standard deviating hazards. Whether a quantitative or qualitative risk analysis method is used depends on the user's decision.

Since highly sensitive data exist in the university and higher education sector, which require a high to very high level of protection, this decision alternative is very well suited for risk management. In this knowledge-intensive field, which is developing at a very rapid pace, it is also of far-reaching significance if changes, especially those deviating from the standard, can be identified at an early stage and thus promptly reacted to.

The ISO/IEC 2700x family of standards is an international standard that enjoys unrestricted international recognition. Since international recognition, especially in the field of universities, is an influential factor, especially against the backdrop of Bologna, the ISO/IEC 2700x family of standards fulfills the criterion of international importance very well. In addition, international recognition should be available in view of any aspired certification.

There are several tools on the market, such as ChaRMe, verinice or ISMS Toolbox, which support an ISO/IEC 2700x family of standards [32]. However, there are considerable differences in quality and costs. Before starting an ISMS implementation, especially in the university sector, the available tools should be analyzed according to the required requirements. Due to the availability of different tools for ISMS support, the ISO/IEC 2700x family of standards satisfies this criterion to a satisfactory extent.

Since the ISO/IEC 2700x family of standards does not exactly specify the process steps, but rather sets out requirements, measures and objectives for action, the criterion of predefined process steps is not sufficiently fulfilled. Compared to the other decision alternatives, there is no precisely predefined guided process with individual concrete recommendations for action. Therefore, a process specifically defined for the university sector must first be redefined. This new process definition requires more qualified specialist knowledge than if the entire process is already precisely specified with concrete recommendations for action.

The minimum requirements for an ISMS of the IT-PLR described in chapter 3.2 and in [13] are met by the ISO/IEC 2700x family of standards. This means that the ISO/IEC 2700x family of standards meets the criterion very well. Since the latter requirements (requirements-based and uniform advanced training of the information security officers , annual meetings of the information security officers for the mutual exchange of experience) are not direct requirements for an ISMS, but serve much more as qualification measures for the professional competences of information security officers, these requirements also only partly exist in the ISO/IEC 2700x family of standards.

4.4 Results

In summary, it can be concluded that the ISO/IEC 2700x standard family achieves the highest utility value with 4.80 %, the second highest utility value of 3.10 % is achieved by the ISIS 12 method, followed by the basic IT protection procedure with a utility value of 3.08 %.

However, the ISO/IEC 2700x approach also has weaknesses in the criteria of resource usage and prescribed process steps, despite the highest utility value. The ISO/IEC 2700x family of standards meets the criteria of target group orientation, scalability, risk management and international significance very well.

The basic IT protection approach has no such clear strengths and weaknesses. In this alternative, the target group criterion is well met, whereas the criteria of resource use, scalability, risk management and international significance are only met with moderate success.

In contrast, the third alternative, the ISIS 12 approach, clearly demonstrates its strengths in terms of economic resource requirements, scalability and the given process steps, whereas the weaknesses lie in terms of resource usage, scalability, risk management and international significance.

As a result, the necessity of an individual solution for the knowledge-intensive university and higher education sector is made clear, since no alternative solution studied covers all the necessary requirements completely on its own. In order to be able to create a suitable model for the introduction, implementation, maintenance and improvement of an ISMS for universities and colleges, it makes sense to select the respective strengths of the three models from synergy effects and to neglect the respective weaknesses.

For this reason, in spite of the non-compliance with the standard authority definition, it may make sense to orientate oneself in the initial phase according to the specified steps of ISIS 12 procedure in order to carry out the initialization work such as the creation of a guideline, sensitization of the employees in a resource-optimized manner.

In addition, the ISIS 12 procedure can be used to carry out the organizational structure and process organization, such as setting up an information security team (-? calculation of personnel expenses BSI), and the preparation of IT documentation for process optimization reasons. The ISIS 12 alternative can be used as an entry aid to identify reduced standard hazards due to its high scalability, even if this alternative is only intended for low to medium protection requirements.

If it is found during this risk identification process that the pool of hazards and measures is not sufficient, the BSI IT-Grundschutz's more comprehensive pool of building blocks can be replaced. However, this very extensive pool of measures is only designed for standard hazards, which in principle also cover a low to medium protection requirement. In case of high protection requirements with standard endangerment, the existing pool of basic IT protection 200-3 measures can be used.

However, if there is a need for at least a high level of protection with standard deviating hazards, it is possible to switch to the alternative of the ISO/IEC 2700x family of standards. The synergy effects can be used to build on the steps already taken.

Particularly for risk management in the knowledge-intensive higher education sector, the approach of the ISO/IEC 2700x family of standards, with its preceded, perfect risk analysis and iterative improvement approach, should be used. In such a rapidly developing knowledge-intensive environment, it is of great importance to use a risk

management system that follows an iterative approach with a continuous improvement process in order to be able to react promptly to all changes (e.g. changes in the hazards, changes in context). Unfortunately, the procedures according to ISIS 12 and IT-Grundschutz do not follow this iterative improvement approach of risk management.

4.5 Determination of the protection requirement

A sophisticated risk management is the key factor for an effective ISMS. For this reason, the determination of the requirement for protection is one of the most important issue before selection the subsequent risk assessment approach. With the aid of the following case-by-case analysis for the protection requirement in this section, this master thesis illustrated a model for choosing the adequate risk management approach depending on the individual protection requirement. This model only consider the selection of the adequate risk management approach, irrespective of the selected method for the initialization and planning phases of the ISMS.

Exemplary the protection requirement of the University of Applied Sciences Augsburg for personal data, critical research results or exam data is at least high. Because there are more than 500 employees which could pose a threat source. In addition, there are dislocated subsidiaries linked through unprotected public networks. Furthermore, there is no homogenous IT-infrastructure, as the individual faculties act independently. In addition high-level availability requirements exist, in case thousands of students are using online-services such as Email or E-learning services like moodle. Further, on the computing center has an average annual power of more than five MW, so the University of Applied Sciences Augsburg could be regarded as KRITIS according to the definition in chapter 2.4. Therefore, the risk management method of ISIS 12 or BSI 100-1/100-2 cannot cope with beyond medium protection requirement.

As in section 3.1 already described, the risk management method of BSI 200-3 can fulfill high protection requirement for standard threats. In this case, an additional security analysis is conducted, in which is decided, if more measures have to be realized.

However, it must be pointed out, it can only used if the existing pool of measures is satisfactory. Because of using general categories of threats, an elaborate risk analysis can be omitted. However, this projection doesn´t reflected the core of a perfected risk analysis.

In addition, improvements can only be made by the BSI because the building blocks are self-contained. Consequently, there is no iterative improvement process possible by the user. Nevertheless, the procedure according to the BSI leaves to the user what kind of risk management used. In this very fast changing environment, in which data are the most valuable asset, an iterative sophisticated risk management, especially for non-standard threats, is essential for an effective ISMS. Therefore, to meet the University of Applied Sciences Augsburg s ´high protection requirement, the risk

management method ISO/IEC 27005 is the reasonably variant. The detailed risks are specified in chapter seven.

Nevertheless, each higher education institution can use the following model to decide for itself what kind of risk management method it wants to apply on the basis of its protection requirements.

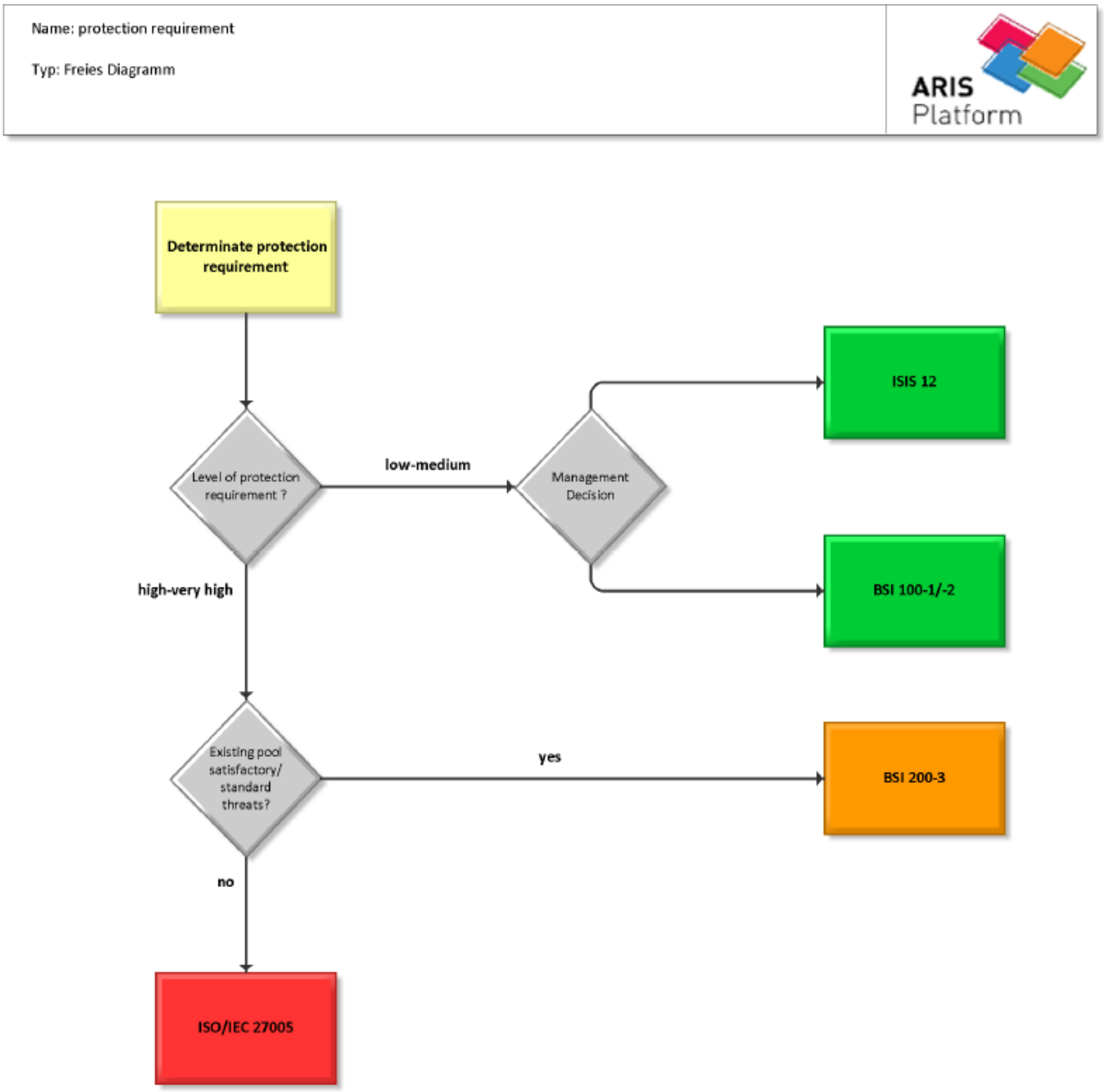


Figure 2: Protection Requirement [own preparation]

5 General steps for Implementation an ISMS at universities and universities of applied sciences the “HS-UNI-ISMS”

As mentioned above in section 4.4, none of the already existing standards and methods fulfill the required criteria for implementation of a specific ISMS for the knowledge-intensive sector.

Depending on several factors, such as the detected protection requirement, the business and security objectives, the security risks and the control requirements, the employed processes and the size or the structure of the university respectively of the university of applied sciences, the design and the implementation of an ISMS differs a lot.

For example, a small university with only low protection requirement needs only a simple ISMS with a simple risk analysis, whereas a large university with high protection requirement such as the University of Applied Sciences Augsburg, needs a well matured ISMS with a sophisticated risk management (see chapter 4.5).

Therefore, based on the results of the authors research report and the specific required criteria, in this section, the conducting phases and steps for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a specific ISMS tailored for the knowledge-intensive sector with high protection requirement are specified.

This is done combining the strengths of the different approaches as described in chapter 4 and mainly based on those and the authors recommendations.

Furthermore, the challenges arising from each step are discussed.

For handling a sophisticated ISMS at universities and universities of applied sciences, a so-called “HS-UNI-ISMS”, there are different constructive steps necessary.

The specific ISMS “HS-UNI-ISMS”, is constructed scalable in a way that is adaptive for all Bavarian universities and universities of applied sciences irrespective of their individual business and security objects, their employed process, or their size and structure. Relating to their protection requirement (see chapter 4.5), an individual case-by-case decision for what kind of risk management method is possible in step seven. Considering in general, the implementation of an ISMS is a strategic decision. Therefore, at the very beginning, it is obligatory to obtain management approval for initiating an ISMS project, afterwards determining the scope and boundaries of the information security management system, subsequently determining or adopting an ISMS policy. To manage all the requirements regarding to an ISMS it is necessary to build an information security team. In a next step conducting awareness and training programs of all organizations ‘employees and staff.

After completing the initialization phase, the operational phase starts with conducting information security requirements analysis, following with the risk assessment and planning risk treatment. Afterwards starting with the designing of the ISMS, including the final ISMS project implementation plan, the performance evaluation measures, the continual improvement and communication between all concerned parties. An all-over and exact documentation about every action is obligatory. In addition, a certificate according to ISO/IEC 27001 can be seeked for.

Attention should be paid to that the risk assessment as well as the whole ISMS process is an iterative cycle with continuous controls and improvements corresponding to the ”Plan-Do-Act-Check” by Deming.[59],[60],[58]. The afterimage, illustrate the single items.

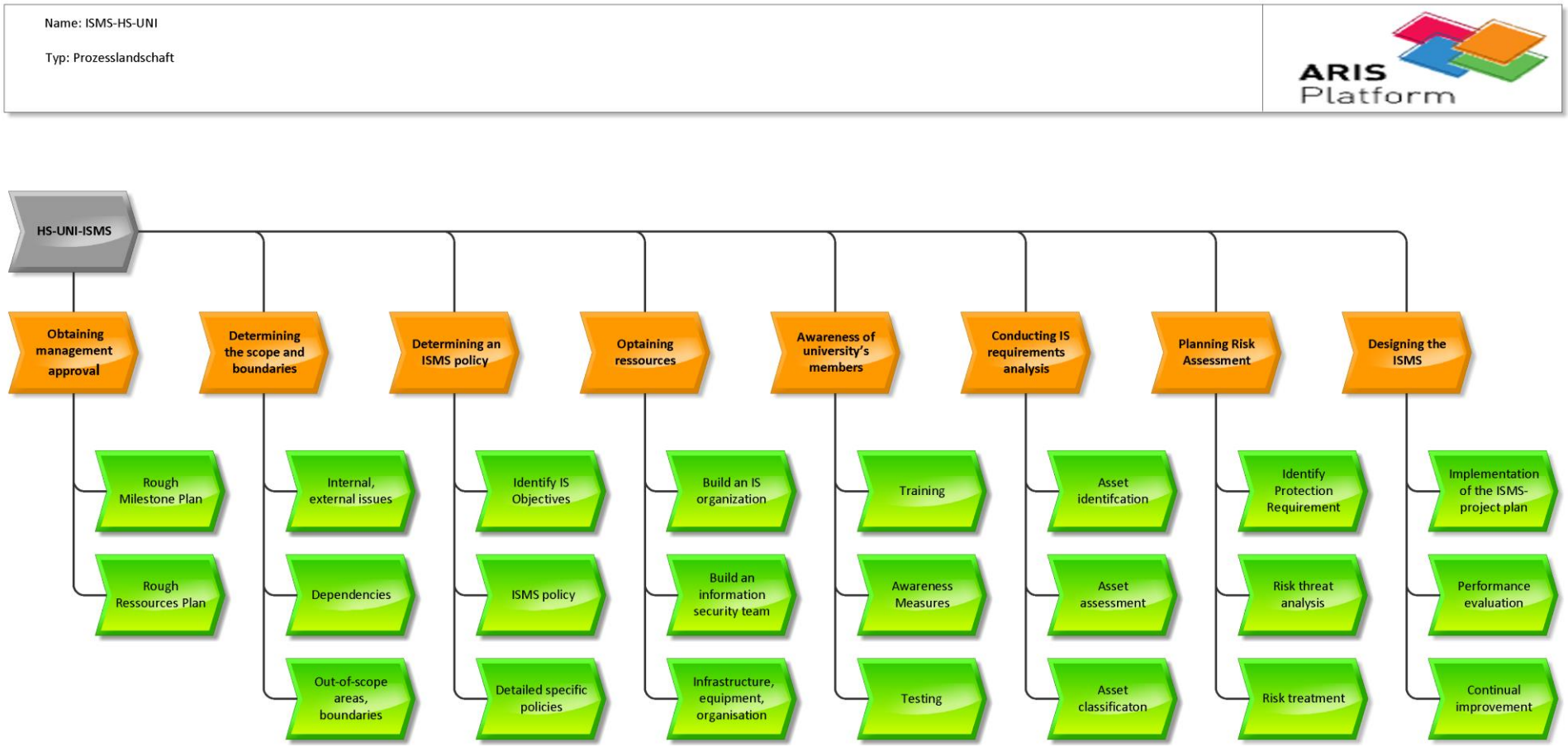


Figure 3: HS-UNI-ISMS: single steps [own preparation]

5.1 Obtaining management approval for initiating an ISMS project

For establishing a sophisticated ISMS it is obligatory to have the top management approval for initiating an ISMS project. In the university sector, the top management of the university consists of the executive committee with a president, a vice president, the senator and the chancellor, of the relevant university. In general, the Top management has the overall responsibility for the ISMS, by delegating authority in the university or providing resources to actually perform activities.

The executive committee can actively support the information security by overt weaving the IT-strategy in the strategy of the university, giving clear direction by singing different policies. Furthermore, the management of the university should demonstrate leadership and the university´s commitment by assigning information security responsibilities to highly qualified manpower.

For the success of an effective ISMS, the management of the university has to approve the information security policy at the very beginning of the iterative ISMS process, should allocate resources with financial resources, facilities, technical infrastructure and high-qualified employees by assigning security roles with decision-making power. These resources are necessary both for the establishment, the implementation, the maintenance and the improvement of an ISMS, as well as for implementing information security controls and their improvement.

In addition, the management of the university has to guarantee that the information security objectives are compatible with the strategic direction of the university and the integration of the requirements and of the controls in the university´s processes.

In this respect the top management has to nominate a person, a so called “information security officer” who is responsible for the university’s´ information security by coordinating and controlling all security processes.

In the last part of the iterative ISMS process, the management of the university should review the implementation of the ISMS across the university accordingly the university of applied sciences.

Furthermore, it is the responsibility of the management to assess resource needs during the management reviews.

It should be noted that the Senator has to sign the policy with external effect, while the Chancellor is responsible for signing the policy with purely internal influence.

Challenges:

Information security is often a critical issue, which is often cohered with fear of control by people. Therefore, it is vitally important to remove the potential fear of the decision maker by illustrating the advantages and the benefit of the ISMS. It is very helpful to have an already finished concept with convincing arguments for information security, so as to create confidence in the whole university. Reasons are – among others- that proactive information security is much cheaper than damage repression, an effective defense against hackers or act of God. Further risks and negative impacts of non-implementation an effective ISMS, such as loss of repudiation as a consequence of thieving or manipulating sensitive research data, ask for ransom or a huge financial damage should be demonstrated. In addition, before asking for management approval you should have a rough concept with a rough mile stone plan, including a financial, personal and functional planning to establish the ISMS. It is easier and more probable to get an effective management support with a correct disclosed elaborated pre-concept.

Even if the Bavarian Data Protection Act requires that an information security concept must be established by 01.01.2018, it is nevertheless essential that the management wants and supports an ISMS. To do this, you need to convince management of information security and the need for an effective ISMS. Not to be forgotten are often personal problems between the individual decision-makers within top management, which can slow down decision-making processes. In preparation for the introduction of an ISMS, it is helpful to know which decision-makers have a positive attitude and implement an effective stakeholder management.

5.2 Determining the scope and boundaries of the information security management system

If the management approval is given, one can start with determining the scope and boundaries of the information management system.

In order to identify the scope and boundaries of the information security management system, it can be helpful to define a rough risk tolerance table at the beginning. In this table, the most important global problems and risks of each university are categorized according to four different levels (non-significant, serious, very serious and seriously critical). This table in turn simplifies the derivation of all information security objectives and strategic goals.

An important part of the ISMS is the continuous analysis of the concerning institution- the university- and the world surrounding it. This analysis is applied to the internal and external needs affecting the information security and their objectives and how managing information security. The aim of this analysis is to understand the context in order to define the scope of the ISMS.

Establishing the scope is a key factor for building the necessary fundament on which all following activities in the ISMS such as risk assessment, risk treatment or determining the counter measures, are based. All the following activities give only a correct and valid result, if the scope is precisely defined. Consequently, exact knowledge of the scope, boundaries, interfaces and dependencies between actors, systems, hardware and the organization is vital for implementing an effective ISMS.

The scope of the ISMS is depending on the context of the university, the external and internal issues and the interest third parties and should accordingly be signed by the management.

The relevant external and internal interests are continually present issues and depend on the universities specific priorities and its situation.

Analyzing the external issues, the environment of the university, the following aspects should be considered:

- social and cultural
- political, legal, normative and regulatory
- financial and macroeconomic
- technological
- natural
- competitive

In contrary to external issues, the internal issues are subject to the university's control. Analyzing the internal issues, the following areas should be considered:

- the university´s culture
- policies, objectives, and the strategies to achieve them
- governance, organizational structure, roles and responsibilities
- standards, guidelines and models adopted by the university
- contractual relationships
- processes and procedures
- resources and knowledge (e.g. capital, time, persons, processes, systems and technologies)
- physical infrastructure and environment
- information systems, information flows and decision making processes (formal and informal)
- previous audits and previous risk assessment results

The question, "how does a certain category of interests (see above) affect the information security objects?" can be asked to identify the important interests. For instance, determining internal issues, you should identify all relevant IT systems and the corresponding relevant information flows between these systems and the relevant decision making processes (see chapter 5.6).

For determining the scope regarding the interested external third parties (e.g. industry associations or regulators and legislators) and internal (e.g. decision makers including top management, employees or students) third parties have to be considered, because they can have specific needs, exceptions or requirements for the university´s information security. Furthermore both the supported activities that are necessary to support the university's´ business activities (e.g. facility management of buildings, physical zones, essential services and utilities, human resources management or IT services) and the outsourced activities (e.g. hosting of Webserver) or the surrounding activates with third parties (e.g. research project with companies) influence the scope of the ISMS.

Because the external and internal issues and the issues of the interested parties change from time to time, one has to continually has to review the scope and the requirements of the ISMS.

One should bear in mind that any exclusion from the scope of the ISMS has to be justified and -most notably -documented. Keep in mind that out of scope areas are inherently less trustworthy, nevertheless additional security controls for any business or administration processes passing information across the boundaries could behooved.

For determining the scope, following steps are necessary:

- to define the broad scope only by a small representative group of university's´ management representatives in order to accelerate the process
- to define the rarefied scope: in this activity all supported activities that are necessary to support the business activities of the university are defined.
- to define the final scope: the rarefied scope is assessed by all members of the university's management. If it is behooved, it is adjusted and documented
- approval of the scope: the documented scope is formally approved by top management of the university [61]

As in all subsequent steps of the process it is already now mandatory to have a consistent terminology of terms used in the ISMS field in order to guard against misunderstandings.

In order to identify a complete ISMS policy, it can be helpful to define a risk tolerance table. In this table, the most important global problems and risks of each university are categorized according to four different levels (non-significant, serious, very serious and seriously critical). This table in turn simplifies the derivation of all information security objectives and strategic goals.

Challenge:

Information security is a largely cross-linked issue with networked information and networked processes including many sub processes. Therefore it is obligatory to define exactly the concerning area and especially the non-including aspects. For demarcating the scope of the ISMS it is vital to have at least a rough overview of the regarding institution with its infrastructure, its software and hardware, its organization with the administration processes and of the involved people with their function. This can be very difficult, if there are only lived processes, but no documented processes. You could encounter difficulties, if the person in charge do or want not to know what their responsibilities exactly are. Furthermore, it could be a big challenge to get all-important information for defining the scope of an ISMS, if there are knowledge gaps between the processes or between the knowledge carriers and the responsible persons of each area of responsibility.

Identifying all-important information for defining the scope can sometimes be like a police interrogation. Especially if there are knowledge-gaps between processes or knowledge-supporter, it could make difficulties. The information security officer should have a sure instinct for identifying the necessary information. Often the knowledge-supporter may be unsecure or they may be afraid of making something wrong. Consequently, they may keep important information secret. Hence, especially the knowledge-gaps between processes, organization or persons are an important information, which could lead to security breaches. In addition, it could be a challenge getting the essential information for defining the scope if there is internal disagreement between persons that are working together. The information security officer should be emphatic, listening and catching the right information. If this important step is finished, you can start with determining an ISMS policy.

5.3 Determining an ISMS policy

The information security policy is on top of all following security documents, by reflecting the university's´ business situation, issues, culture, requests and attitude related to information security. Because of the strategic character of this important document, the top management of the university establishes the information security policy. In this document the top management of the university gives a clear statement on its commitment to satisfy information security requirements and support the continuous improvement of all activities concerning the university's´ information security.

In order to establish an effective information security policy, it is important to identify and define the information security objectives, because the objectives of information security help to implement the strategic goals of an organization and the information security policy.

When planning how to meet the information security goals, the university determines what is being done, what resources are needed, who is responsible, when it will be

completed and how the results will be evaluated. The objectives of information security should be based on the requirements of information security.

Since the requirements for information security can change at any time, the security objectives and thus the information security policy must always be kept up to date.

Information security objectives can be formulated in different ways. The expression should be appropriate to fulfil the requirement of measurability. The objectives for information security can be expressed as follows, for example:

- Numerical values with their limit values, e. g." do not exceed a certain limit" and "Achieve level 5";
- Objectives for measuring information security performance
- Objectives for measuring the effectiveness of the ISMS (see 5.8)
- Compliance with the requirements of a certain standard
- Compliance with ISMS procedures
- Risk criteria to be fulfilled

With the aid of the information security policy, information security activities are directed in the university. The information security policy defines the objectives of information security or provides a framework for setting the objectives.

The policy is tailored to the particular needs and to the actual context of the university. To achieve high security for the university, the policy should imply short comprehensible statements of direction and guidance at a high level concerning the university's information security. The policy can also have a larger coverage as the scope of the ISMS. All following detailed policies, procedures, activities or objectives related to the university's´ information security are based on the information security policy.

The extent of the information security policy should find the trade off between completeness and comprehensibility, so that the users of the policy can identify themselves with the strategic direction of the policy.

This main guiding policy either contains objectives of information security or contains a framework how to achieve these objectives in the university. The information security policy can be an individual standalone policy or can be a part of comprehensive policy of the whole university (high-level general policy).

When the information security policy is established by the top management of the university, it is important to announce it in a documented form to all within of scope participants. It the university's´ top management decides the information security policy is also for external third parties, such as students, customers, suppliers or contractors, the document must not contain confidential information, of course.

Typically, the hierarchy of the information security policy is as follows. The information security policy is on top or as a part of a general high-level policy of the university. Many topic-specific policies, called "standards", "directives" or "rules" are based on the

information security policy. These topic-specific policies for example are related to physical and environment security, access control, strong passwords or information classification among others.[60],[61],[11]

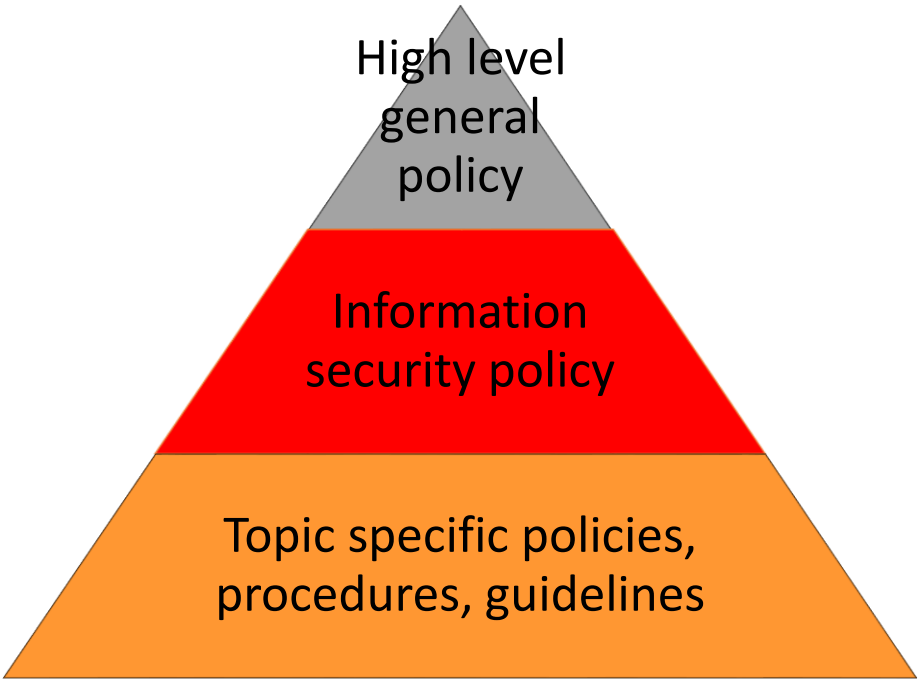


Figure 4: Hierarchy of policies [own preparation]

When developing any policy, you should regard the following aspects:

- the aims and objectives of the university
- strategies adopted to achieve the university´s objectives
- the structure and processes adopted by the university
- aims and objectives associated with the topic of the policy
- the requirements of related higher-level policies
- the target group of the policy

Consider the following structure, when developing any policy.

- Administrative: policy title, version, publication/validity dates, change history, owner(s) and approver(s), classification, intended audience etc.

- Policy summary: a brief overview (1-2 sentences), can be in combination with the introduction
- Introduction: a brief explanation of the topic of the policy
- Scope: describes the parts or activities of the university affected by the policy or illustrates lists of other policies that are supported by this policy
- Objectives: describes the intention of the policy
- Principles: describes the rules concerning actions for achieving the objectives. It can be helpful to identify the key processes associated with the topic of the policy
- Responsibilities: describes who is responsible for actions to meet the requirements of the policy
- Key outcomes: describes the business outcomes if the objectives are met. Sometimes you can merge this with the objectives
- Related policies: describes other policies relevant to achieve the objectives by providing additional detail specific issues
- Policy requirements: describes the detailed requirements of the policy

Challenge:

The Bavarian universities and university of applied sciences consist of two parts. One part is research and teaching and the second part is the university's administration with access to the governmental network.

In the second part, the Bavarian Standard "Standards and Guidelines for Information and Communication Technology (ICT) in the Bavarian Administration (IuKSR)[22]", which is supported by a number of different binding general and specific topics and standards and rules, such as e. g. the "BayITSiLL "- a Security Policy [21] or the "BayITSiR-02", a specific guideline for the operation of a transition to the Internet [22], is to be followed. Although this standard was created on the basis of BSI IT-Grundschutz, you have to control the application of the standard.

Thus, on the one hand, you have to comply with the freedom of research and teaching when developing an information security policy and, on the other hand, you have to meet the requirements of the Bavarian standard "IuKSR" for the administrative part of the university.

For the preparation of this master thesis, it was already a great challenge to gain access to the network of public authorities in order to gain access to the Bavarian standards and rules. In order to gain access to the public authority network, it requires a written request from the supervisor. In a next step, the application must be considered before accessing the administration network. It is a time-consuming and tedious process to obtain simple but necessary information. The entire information retrieval process took six weeks.

The ISMS policy developed must be communicated and made accessible in the appropriate form to all employees, professors and students, as well as third parties involved (see above). An information security policy for the University of Applied Sciences Augsburg is developed in Annex A.

5.4 Obtaining resources

It is imperative for the establishment, implementation, maintenance and improvement of an ISMS that sufficient resources are made available by the university management or the Bavarian State Administration.

Resources are vital to perform any kind of ISMS-related activities. There are external and internal resource costs. Certification falls within the scope of external resources. The internal resources used include one-off strategic issues (e. g. setting up an information security team, developing an information security concept) and continuously sustainable operational organizational aspects (e. g. controlling of information security concepts, training and awareness measures, audits) [23].

To establish, to implement, to maintain and to improve an ISMS the following categories of resources are necessary:

- human resources to drive and operate the activities
- time resources to perform activities
- financial resources to acquire, develop and implement what is needed
- information resources to support decisions, measure performance of actions and improve knowledge
- infrastructure and other means for assessing, acquiring, maintaining or improving information security (e.g. license of sophisticated tools)

The management of the university acquire, provide, maintain and review the needed resources across the whole ISMS process

5.4.1 Build an information security organization

Depending on the size, structure and protection requirement of each university, the information security organization differs a lot. For a medium till big university, such as the University of Applied Sciences Augsburg the following organization structure can be applied.

The information security officer and his or her team should have clearly defined tasks determined by the university's top management. To perform their tasks they should be integrated in all relevant decisions and processes. The roles should be embedded in the university's structure in that way that all participants are able to communicate to each other.

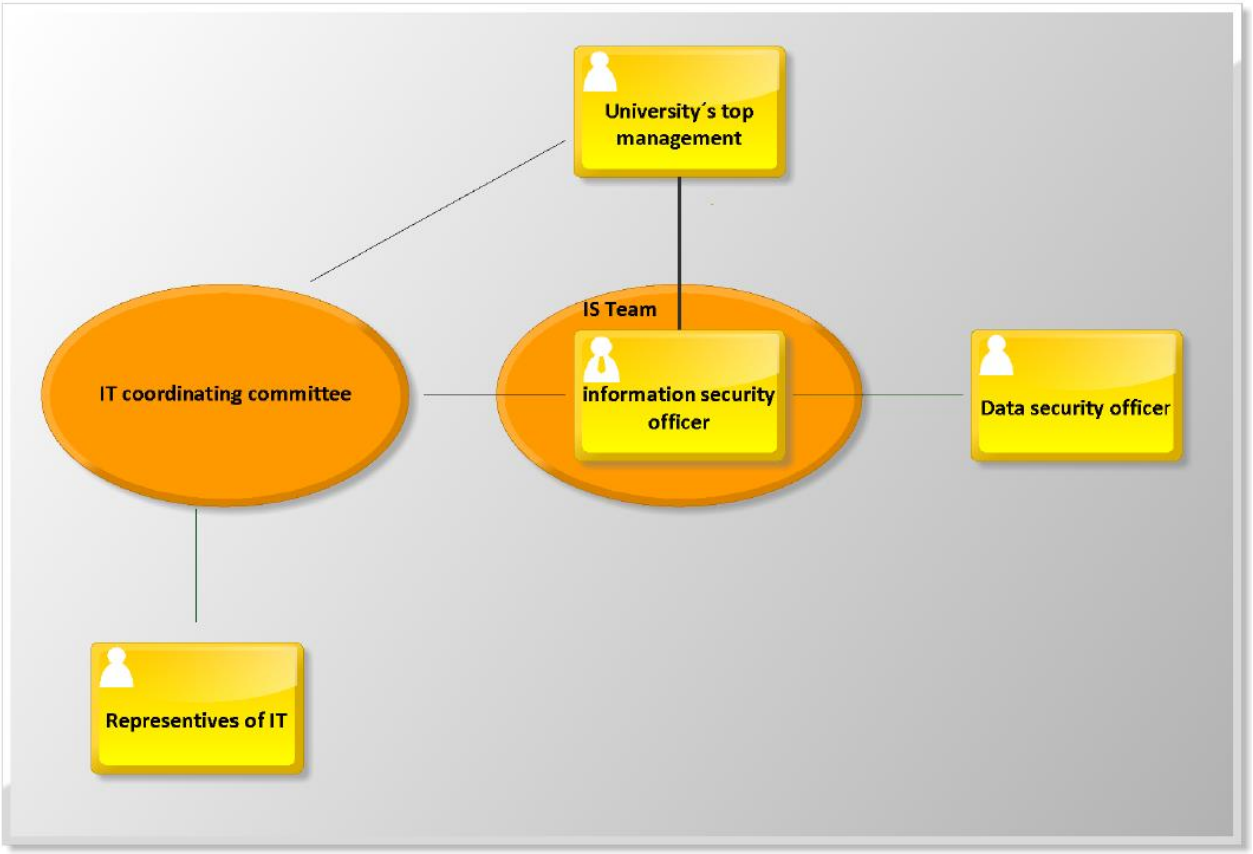


Figure 5: IS organization structure [own preparation according to [[62]]

5.4.2 Build an information security team

Depending on the structure and size of the university an information security team consists of an information security officer, a qualified reprehensive of him or her, and other information security members.

The information security officer has initial tasks such as building up an information security team, estimating the resources needed for all activities concerning the ISMS in terms of quality and quantity, developing an information security policy, creating an

information security concept, an incident response plan and a concept for continuous management. In addition, ways of reporting have to be established in case of an incident. Before beginning his or her job, the information security officer should do an advanced information security-training course.

Furthermore, the information security officer has regular tasks such as the controlling, maintenance and the improvement of the whole ISMS. The key aspects are the maintenance, controlling and adjustment of the concepts concerning the information security, the monitoring and the updating of the incident response, business continuity management and crisis management concepts, awareness of the employees, evaluation of the overview of the situation, monitoring of the effectiveness of the security measures, assessment of information about the ongoing security risks, analysis of the security incidents and the consulting and reporting to the university's management. Furthermore, he or she should participate in advanced training courses and visit conferences.

Because of the new working environment and the fast-changing security situation networking with other information security experts are vital for the information security officer. For an information security officer, it is essential to train his or her employees and not to forget to better himself or herself in order to stay on the state of the art.

The information security officer should be a standalone and independent job position instead of being simultaneous an IT-administrator who gets directions from other parties. The information security officers' main task is to support the university's top management by theirs exercise of functions accordingly the information security and to support them by their implementation. Furthermore, the information security officer has the following tasks:

- steer an information security process and participate in all related tasks,
- support the university's top management in the creation of the information security policy
- Coordinate the development of the security concept, the incident response concept and other supporting guidelines and specific policies, as well as other guidelines and regulations on information security
- initiating and reviewing the implementation of security measures,
- report to the management and the IS Management team on the status quo of information security
- coordinating security-related projects
- investigate security incidents
- initiate and coordinate information security awareness and training activities

For doing a good job the information security has to have a direct right to audition to the university's top management at all times. The IT Security Officer shall also be involved in all major projects that have a significant impact on information security such as the introduction of new applications and IT systems, to ensure compliance with security aspects in the various project phases.

Depending on the university's size, its protection requirements and its resources the information security consists of different number of members. In an extreme case, it consists only of one single person, the IT security officer, who in this case is responsible for all tasks in the ISMS. The IS management team supports the IT security officer by coordinating comprehensive measures in the overall organization, gathering information and carrying out control tasks. Furthermore, the information security team has the following tasks:

- determine information security goals and strategies, and develop the information security policy
- review the implementation of the security policy
- initiate, control and supervise the security process
- participate in the development of the security concept
- verify that the security measures envisaged in the security concept function as intended and are appropriate and effective
- design information security training and awareness raising programs
- advise the IT Coordination Committee and the university´s top management on information security issues

In order to be able to carry out the task the members of the information security team should have knowledge of information security, technical knowledge of IT systems and experience with organization and administration. The IS Management team should have at least the following roles: IT responsible person, the information security officer and a representative of the users. As personal data is often also affected, the Data Protection Officer should also be a member of the IS Management Team or be available as an independent consultant.

According to [23] the minimum personnel requirement for establishing, implementing, maintaining and improvement of an ISMS for the definition of a "standard authority" (see chapter 2.4)as a meta model is due to a basis value of allover 340 man-days (PT), whereas 205 man-days correspond to 1 employee per day.

In the first year, the initialization tasks and the regular task with the exception of monitoring and updating of the information security and the incident response concept, with a minimum personnel requirement of 250 PT are handled. As a result the need of staffing is 1,22 in the first year.

In the next years, the regular tasks with a minimum personnel requirement of 180 PT are executed. As a result the need of staffing is 0,88 in the next years.

	IT-Sicherheitsaufgabe	Typischer Aufwand in Personentagen	Zuschlag für Anzahl der Mitarbeiter	Zuschlag für Heterogene IT-Landschaft und IT-Verfahren	Zuschlag für Außenstellen	Anteil der IT-Anwendungen mit hohem Schutzbedarf (verhältnismäßig zu allen IT-Anwendungen)	Zuschlag für Schutzbedarf mit Hochverfügbarkeits-anforderung	Summe in Personentagen (ohne Outsourcing)
	Metamodell Standardbehörde		500	A	0	0%		
initiale Aufgaben	Toolunterstützte Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz), Kryptokonzept	120	0 %	0%	0 %	0%		120
	Erstellung IT-Notfallvorsorge-konzept sowie IT-Notfall- und IT-Krisenmanagementkonzept, BSI-Standard 100-4	40	0 %	0%	0 %	0%	0 %	40
Aktualisierung und Fortschreibung	Überprüfung und Fortschreibung Sicherheitskonzept und Kryptokonzept	60	0 %	0%	0 %	0%		60
	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und IT-Krisenmanage-mentkonzept inkl. Übungen , BSI-Standard 100-4	30	0 %	0%	0 %	0%	0 %	30
	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungs-aufwand, ohne Schulungsaufwand)	20	0%	0%	0%	0%		20
	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Revision und Audits	30	0%	0%	0%	0%		30
	Untersuchung sicherheitsrelevanter Vorfälle, ajour halten (z.B. Heise-Ticker, CERT-Meldungen)	20	0%	0%	0%	0%		20
	Beratung (auch. in IT-Fachverfahren) und Berichterstattung	20	0 %	0%	0 %	0%		20

ERGEBNIS		
1. Jahr	250,00 PT	1,22 Kräfte
Folgejahre	180,00 PT	0,88 Kräfte

OUTSOURCING	
Prozentuale tatsächliche Entlastung der IT-SiBe durch ausgelagerte IT	0%

Figure 6: values for staffing for the meta model of the standard agency [23]

However, these values are only valid for the meta model “standard authority”. There are overtime rates for the following relevant additional factors:

- more than 500 employees,
- degree of heterogeneity of the IT-basis infrastructure,
- number of dislocated subsidiaries,
- quota of IT-application with more than normal protection requirement,
- high level availability requirements regarding the IT-Systems,

The overtime rates and accordingly the number of employees result from one time tasks (security concept and other concepts) and regular long-time tasks (adjusting all different concepts, awareness of the employees, control of the effectiveness of the security measures, analysis of incidents, consulting and reporting). Per each 500 step, the next overtime rate is applied. (see figure 7)

ZUSCHLAGSTABELLE ANZAHL MITARBEITER

Sicherheitskonzept (eimalig)

		Zuschlag	
ab	0	0	%
	501	20	%
	1001	50	%
	1501	70	%
	2501	90	%
	3001	120	%
	4001	200	%
	5001	350	%
	6001	500	%
	8001	700	%

Weitere Konzepte (eimalig)

		Zuschlag	
ab	0	0	%
	501	5	%
	1001	12	%
	1501	20	%
	2501	22	%
	3001	30	%
	4001	50	%
	5001	90	%
	6001	125	%
	8001	180	%

Fortschreibung Sicherheitskonzept (dauerhaft)

		Zuschlag	
ab	0	0	%
	501	20	%
	1001	50	%
	1501	70	%
	2501	90	%
	3001	120	%
	4001	200	%
	5001	350	%
	6001	500	%
	8001	700	%

Fortschreibung Weitere Konzepte (dauerhaft)

		Zuschlag	
ab	0	0	%
	501	20	%
	1001	50	%
	1501	70	%
	2501	90	%
	3001	120	%
	4001	200	%
	5001	350	%
	6001	500	%
	8001	700	%

Sensibilisierung der Mitarbeiter

		Zuschlag	
ab	0	0	%
	501	20	%
	1001	50	%
	1501	70	%
	2501	90	%
	3001	120	%
	4001	200	%
	5001	350	%
	6001	500	%
	8001	700	%

Kontrolle Wirksamkeit von Sicherheitsmaßnahmen

		Zuschlag	
ab	0	0	%
	501	20	%
	1001	50	%
	1501	70	%
	2501	90	%
	3001	120	%
	4001	200	%
	5001	350	%
	6001	500	%
	8001	700	%

Untersuchung (sicherheits-relevanter Vorfälle

		Zuschlag	
ab	0	0	%
	501	20	%
	1001	50	%
	1501	70	%
	2501	90	%
	3001	120	%
	4001	200	%
	5001	350	%
	6001	500	%
	8001	700	%

Beratung und Berichterstattung

		Zuschlag	
ab	0	0	%
	501	20	%
	1001	50	%
	1501	70	%
	2501	90	%
	3001	120	%
	4001	200	%
	5001	350	%
	6001	500	%
	8001	700	%

Figure 7: Table of overtime rates for the number of employees [23]

The University of Applied Sciences Augsburg has with about 6000 students and more than 500 employees. Attention should be paid to about 9300 campus cards circulating. Because of having access to the university of applied science environment, the value of 9300 is relevant for assessing information security as a holistic approach consequently for assessing the necessary personal staffing for the information security team.

For the degree of heterogeneity of the IT-basis infrastructure there are three different categories (A = no heterogeneity, B = an average heterogeneity with regularly two operation systems, C = high heterogeneity). The University of Applied Sciences Augsburg falls in the category “C”, because it acts as an IT-service provider with more than an average heterogeneity because of its special and high complex IT-processes and operation systems.

Furthermore, there are following overtime rates for the dislocated subsidiaries. The overtime rates is carried out in one time tasks (security concept and other concepts) and regular long-time tasks (adjusting all different concepts, awareness of the employees, control of the effectiveness of the security measures, analysis of incidents,

consulting and reporting). The overtime rate begin from one dislocated subsidiaries with 5%.

The university of applied sciences Augsburg has three dislocated subsidiaries (campus at the “roten Tor”, at “Nördlingen”, at “Memmingen”) therefore it falls in the category from one dislocated subsidiaries and get consequently 5% respectively 10% (for other one-time concepts) of overtime rate.

ZUSCHLAGSTABELLE ANZAHL AUßENSTELLEN

Sicherheitskonzept (einmalig)

ab	Zuschlag
0	0 %
1	5 %
15	10 %
30	40 %
60	80 %
100	100 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Weitere Konzepte (einmalig)

ab	Zuschlag
0	0 %
1	10 %
15	30 %
30	80 %
60	160 %
100	200 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Fortschreibung Sicherheitskonzept (dauerhaft)

ab	Zuschlag
0	0 %
1	5 %
15	10 %
30	40 %
60	80 %
100	100 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Fortschreibung Weitere Konzepte (dauerhaft)

ab	Zuschlag
0	0 %
1	5 %
15	10 %
30	40 %
60	80 %
100	100 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Sensibilisierung der Mitarbeiter

ab	Zuschlag
0	0 %
1	5 %
15	10 %
30	40 %
60	80 %
100	100 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Kontrolle Wirksamkeit von Sicherheitsmaßnahmen

ab	Zuschlag
0	0 %
1	5 %
15	10 %
30	40 %
60	80 %
100	100 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Untersuchung (sicherheits-relevanter Vorfälle

ab	Zuschlag
0	0 %
1	5 %
15	10 %
30	40 %
60	80 %
100	100 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Beratung und Berichterstattung

ab	Zuschlag
0	0 %
1	5 %
15	10 %
30	40 %
60	80 %
100	100 %
250	300 %
500	400 %
1.000	500 %
1.500	600 %

Figure 8: table of overtime rates for the number of dislocated subsidiaries [23]

Additional for the quota of IT-application with more than a normal protection requirement there is also an overtime rate. Depending on the quota of the IT-application with more than normal protection requirement, follows a corresponding overtime rate.

Circumspectly calculated the University of Applied Sciences Augsburg has minimum 10% of application with more than a normal protection requirement. Consequently, the overtime rate is in this case 10%. For example, the HIS database with critical personal

data, marks or certificates or the own cloud with sensitive research data have more than a normal protection requirement.

The high-level availability requirements regarding the IT-Systems gets also a staggered across the board overtime rate from 50%.

In the University of Applied Sciences Augsburg there are high-level availability requirements regarding the IT-Systems available. In case, thousands of students are using online-services such as Email, E-learning services or register to exam the high-level availability requirement is existent.

- Results:

The following table illustrates the personnel forecast depending on the above-mentioned factors specify for the university of applied sciences Augsburg.

	IT-Sicherheitsaufgabe	Typischer Aufwand in Personentagen	Zuschlag für Anzahl der Mitarbeiter	Zuschlag für Heterogene IT-Landschaft und IT-Verfahren	Zuschlag für Außenstellen	Anteil der IT-Anwendungen mit hohem Schutzbedarf (verhältnismäßig zu allen IT-	Zuschlag für Schutzbedarf mit Hochverfügbarkeits-anforderung	Summe in Personentagen (ohne Outsourcing)
	HSA		9.300	A	4	10%	X	
initiale Aufgaben	Toolunterstützte Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz), Kryptokonzept	120	700 %	0%	5 %	10%		978
	Erstellung IT-Notfallvorsorge-konzept sowie IT-Notfall- und IT-Krisenmanagementkonzept, BSI-Standard 100-4	40	180 %	0%	10 %	10%	50 %	140
Aktualisierung und Fortschreibung	Überprüfung und Fortschreibung Sicherheitskonzept und Kryptokonzept	60	700 %	0%	5 %	10%		489
	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und IT-Krisenmanage-mentkonzept inkl. Übungen , BSI-Standard 100-4	30	700 %	0%	5 %	10%	50 %	260
	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungs-aufwand, ohne Schulungsaufwand)	20	700%	0%	5%	10%		163
	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Revision und Audits	30	700%	0%	5%	10%		245
	Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten (z.B. Heise-Ticker, CERT-Meldungen)	20	700%	0%	5%	10%		163
	Beratung (auch. in IT-Fachverfahren) und Berichterstattung	20	700 %	0%	5 %	10%		163

ERGEBNIS		
1. Jahr	1.851,50 PT	9,03 Kräfte
Folgejahre	1.482,00 PT	7,23 Kräfte

Figure 9: table of the necessary personnel stuff for building the information security team [own calculation according to [23]

As illustrated in the table above there are for initial tasks and regularly updating tasks in the first year a minimum of 1.851,50 PT corresponding to 9,03 man-power necessary for establishing and implementing an ISMS in the university of applied sciences Augsburg. For the following years there is a minimum of 1.482,00 PT corresponding to 7,23 man-power essential. The calculation is made without outsourcing capacities. As mentioned above the most pivotal factor is the number of employees respectively the number of persons involving in the information security process. Because here is the highest working surface for crime such as social engineering. Therefore, the costs for instance of awareness and training measures rise correspondingly to the number of employees respectively the number of persons involving in the information security process.

However, bear in mind that this is the minimum necessary staffing for building the information security team at university at applied sciences Augsburg. It must be pointed out that many tasks and issues are not calculated in this evaluation. For example, the education and the further education are not charged either in quality or in quantity. Furthermore, efforts for the operative information security management (such as e.g. project working tasks, day-to-day business, consulting of the employees, consulting with the work council and the data security officer) are not completely itemized. In Addition, the organization of the information security team cannot be illustrated quantitatively. Furthermore, the reaction of the ongoing situation of security (e.g. patches, updates) is not able to execute from a single person, but also needs the organization and management of corresponding security measures within the information security team. For this tasks and activities, additional overtime rates have to be calculated.

5.4.3 Provide resources for the infrastructure, the equipment and the organization

For establishing, implementation, maintenance and improvement of the UNI-HS-ISMS, the university’s top management has to provide adequate resources for the infrastructure, the equipment and the organization. The arrangement of the security strategy has to be in accordance with the cost-effectiveness issues of the university. If the provided resources cannot fulfil the necessary security measures, the security strategy has to be changed. Keep in mind that every security measures has to fulfill the cost-benefit ratio. For a significant improvement of the security level, first invest in simple low cost organizational regulation instead of expensive complex technical infrastructure. Not before realizing basic security measures, investing in technical security infrastructure and equipment makes sense. Technical security measures always have to be embedded in appropriated organizational framework with corresponding personnel, timed and financial resources.

Challenge:

First one can often encounter difficulties to enforce the necessary number of information security experts by the management of the university respectively the by the Bavarian public administration. Furthermore, it is a huge challenge to hire enough sophisticated information security experts. For example, for an information security officer you need a person who has on the one hand a technical understanding for the IT systems and infrastructure and on the other hand even more important an analytical, structured mindset for the whole organization, infrastructure, people, activities and processes concerning information security. If the person is only sophisticated in penetration testing for instance, he or she is not qualified enough. In addition, she or he needs a huge assertiveness for applying the security measures and otherwise she or he has to be people oriented to get the important information for establishing, maintaining and improving the ISMS from every person within or even out of scope. The persons has to consider him or herself trustworthy for effective awareness and training measures. The information security officer and her or his information security team members have to have a high ability to communicate: they need the ability to both debate with the university's top management, advance the technical view and to talk with the cleaning personnel having also an access to the university's building depending on every situation.

The information security officer and her or his team members should have a huge intuition to get the necessary information depending on the individual situation, the particular character and the relative points of use. Furthermore, the information security officer should have the ability to cooperate and work in a team, but also assertiveness because the task requires so much skill and skill in dealing with other people of different characters, position and subject area.

For recording of processes the interviewee could be awed or could be afraid of doing something wrong, so the information security expert has to be emphatic to get the necessary information nevertheless. Particularly in partly hierarchic governmental and academic environment, it could be a great challenge to improve old long-living processes or to establish new ones. In the public sector, within the university sector is partly associated, the employees do a long time a good work and with the establishing of information security, their work and the related processes are a-rayed, controlled and improved. Therefore, it is comprehensible that employees regard information security often with suspicion. The information security officer and the information security team use this change to illustrate the advantages and benefits of information security in order to create confidence.

It poses a big challenge that the information security officer and the information security team have no direct authority to give directives. He or she only pronounces recommendations concerning the university's information security. These recommendations are only binding if it is fixed in the information security policy signed by the university's top management.

Another challenge is that there is no information security officer who has the authority to issue instructions for all Bavarian universities and universities of applied sciences.

Consequently, the central information security officer only gives recommendations, and every university and university of applied sciences do their own information security work. For example, the top management of one university may decide they do not need a sophisticated risk management method for resources reasons, although they have critical data with high protection requirement, or the university's top management decide for an unappropriated, ineffective procedure for implementing an ISMS.

In a worst case there are 37 different procedures handling the information security at the Bavarian universities and universities of applied sciences. For establishing a standardized procedure for handling the universities information security in Bavaria, the central information security officer needs an authority to give directives for all information security issues.

5.5 Awareness of all university's members

If the all the initial work (establish the information security policy, and the supporting policies, the initial concepts and the information security team is build) you can start with awareness and training measures of all university's employees and staff. All the persons within the scope of the ISMS, especially the university's employees, professors, staff and students are made aware of the information security policy and the relevant supporting detailed policies, their contribution to the effectiveness of the university's ISMS and the benefits of improved information security performance. An awareness concept for different target groups (e.g. management, administrator, user, students) should be established.

Furthermore, the negative consequences of not conforming to the requirements of the ISMS are illustrated.

The persons working under the university's control should know, understand and accept the information security policy and the expected requirements regarding to information security. Furthermore, they should get an awareness of information security and get a motivation for complying with information security aspects and for improving the university's information security situation. All within the scope persons should know that there is an information security policy and where to find the information about it. Not all within the scope persons have to know exactly the detailed content of the information security policy. Instead of this, they should know, understand, accept and implement the information security objectives and requirements derived from the policy that regard their job respectively their area of responsibility. They should support the university's information security objectives and follow the rules concerning information security to correctly do their daily tasks. For establishing an effective awareness of information security the university should

- prepare a further education program for all university's employees and staff depending on the specific issues focused on each audience (employees, staff, professors or students). The further education program should be consistent

with university's objectives, information security policy in due consideration of the protecting assets of the university

- compile a plan to communicate important issues in regular intervals or in every change of the general policy of the university or the information security policy
- inform persons about general procedure concerning information security (e.g. ways of reporting incidents, illustrate contact persons) and basic security measures (e.g. strong passwords, regular updates)
- encourage persons taking responsibility for their own behavior for protecting the university's assets
- test the knowledge and understanding of information during and after an awareness training
- call on persons to notify the contact person in case of noticed vulnerabilities
- illustrate the implications of non-conform behavior for information security or repercussions for the person
- establish ways of reporting in case of an incident
- determine contact persons
- test whether persons act according to the communicated information

Note the co-determination right of the works council by conducting awareness measures. Furthermore, the further education training programs should take place regularly. The distribution of important information should take place in an easy way and simple accessible (e.g. university's portal, newsletter).

Challenge:

All in the scope persons, especially the university's employees and staff have to want information security. The success of awareness and training programs and consequently of information security depends on the participating people. Therefore, the information security officer and the information security team has to convince them and illustrate them the benefits and advantages of information security. On the one hand, the information security has to create confidence and on the other hand, he or she has to show the negative consequence of neglecting information security for the university's information security and for the repercussions for the person.

Furthermore, the university's top management has to provide appropriate resources for regular training and awareness measures. Both for new employees and for long-term employees. The more employees, staff and students the more necessary resources for awareness and training programs are needed. See also point 5.4.

5.6 Conducting information security requirements analysis

For conduction the information security requirements analysis one has to start with identifying and assessing the university's assets. Afterwards a classification of the university's assets is executed. The identification, the assessment and the classification of the university's assets are the fundament of an effective risk and threat analysis.[63] Without an exact identification, assessment and a classification the next steps are not possible, and consequently an effective ISMS cannot be established. The level of detail used for asset identification influences the extent of the risk management.

For example in the ISIS12 method there is no identification, assessment or classification of all university's assets. Instead of only the identification of critical application is conducted [40]. However, how can you identify an application as critical without identifying, assessing and classifying all university's assets?

Furthermore, for example, in the ISMS method of BSI [35], only an analysis of the "IT-Verbund" is carried out, i.e. primarily the technical components of the scope. In addition, organizational and personnel regulations and information are also to be included, but the scope is more likely to be defined here than a necessary value determination. No necessary classical determination of values is therefore made here.

An inventory of all universities' information assets should be recorded, administered and controlled by a responsible person. It is important that the inventory is exact and up to date. The asset owner ascertains that all assets are inventoried, classified and secured, even he may not have property rights to the asset. Furthermore, the asset owner regularly controls the access to the inventory and guarantees a correct handling of deleting the assets. Often the asset owner is the most suitable person to identify the university's assets value.

For identification of the university's assets two different kinds of assets can be distinct. The primary assets and the supporting assets. The primary assets (business processes and activities, information) concern usually the university's core processes and activities and their information.

The **primary** assets consist of two types:

- Business processes (or sub-processes) and activities

Business processes or sub-processes are essential processes for example for carrying out the universities mission (e.g. research and teaching) or processes with confidential information involving critical technology (development of critical technology). Furthermore, processes that are essential to comply with legal or regulatory

requirements such as for instance registration of marks, notice of marks, and certification of enrollment.

- Information:

Information can be vital information for the universities mission such as research and teaching data, or personal data, high-cost information whose gathering and storage necessitate a long time or include a high acquisition cost.

The **supporting** assets are assets which support the primary elements of the scope. The supporting assets consist of various types of hardware, software, network, personnel and the university's structure.

- Hardware: The hardware type consists of all the physical elements supporting processes
    - Data processing equipment (active): Automatic information processing equipment including the items required to operate independently.
    - Transportable equipment: computer equipment which is portable
      Examples: laptop computer, Personal Digital Assistant (PDA).
    - Fixed equipment: Computer equipment used on the organization's premises. Examples: server, microcomputer used as a workstation.
    - Processing peripherals: Equipment connected to a computer via a communication port (serial, parallel link, etc.) for entering, conveying or transmitting data.
      Examples: printer, removable disc drive.
    - Data medium (passive): media for storing data or functions.
    - Electronic medium: An information medium that can be connected to a computer or computer network for data storage. Despite their compact size, these media may contain a large amount of data. They can be used with standard computing equipment.
      Examples: CD ROM, back-up cartridge, removable hard disc, memory key, USB-sticks
    - Other media: Static, non-electronic media containing data.
      Examples: paper, slide, transparency, documentation, fax.

- Software: consists of all the programs contributing to the operation of a data processing set.
    - Operating system: all the programs of a computer making up the operational base from which all the other programs (services or applications) are run, including a kernel and basic functions or services. The main elements are all the equipment management services (CPU,

memory, disc, and network interfaces), task or process management services and user rights management services.

- Service, maintenance or administration software: it complements the operating system services and is not directly at the service of the users or applications

- Package software or standard software: provide services for users and applications, but are not personalized or specific in the way that business applications are.
  Examples: data base management software, electronic messaging software, groupware, directory software, web server software, etc.

- Business application
  Standard business application
  This is a commercial software, that gives users direct access to the services and functions in their professional environment.
  Examples: accounts software, machine tool control software, customer care software, personnel competency management software, administrative software, etc.
  Specific business application
  This is a piece of software that has been specifically designed to provide users with direct access to the services and functions they need from their information system, through various aspects (especially support, maintenance, upgrades, etc.).
  Examples: Invoice management of telecom operators' customers, real time monitoring application for rocket launching

- Network: the network type consists of all telecommunications devices used to interconnect several physically remote computers or elements of an information system.

  - Medium and supports: Communications and telecommunications media or equipment are characterized mainly by the physical and technical aspects of the equipment (point-to-point, broadcast) and by the communication protocols (link or network - levels 2 and 3 of the OSI 7-layer model).
    Examples: Public Switching Telephone Network (PSTN), Ethernet, GigabitEthernet, Asymmetric Digital Subscriber Line (ADSL), wireless protocol specifications (e.g. WiFi 802.11), Bluetooth, FireWire.

  - Passive or active relay: This sub-type includes all devices that are not the logical terminations of communications (IS vision) but are intermediate or relay devices. Relays are characterized by the supported network communication protocols. In addition to the basic relay, they

often include routing and/or filtering functions and services, employing communication switches and routers with filters. They can often be administrated remotely and are usually capable of generating logs.
Examples: bridge, router, hub, switch, automatic exchange.

- Communication interface: They are characterized by the media and supported protocols, by any installed filtering, log or warning generation functions and their capacities and by the possibility and requirement of remote administration.
  Examples: Universal Mobile Telecommunication System (UMTS), Ethernet adapter

- Personnel: The personnel type consists of all the groups of people involved in the information system.
  - Decision maker: Examples: top management of the university, IT-project leader.
  - Users: They may have special access rights to the information system to carry out their everyday tasks.
    Examples: human resources management, financial management, student department
  - Operation/ Maintenance staff: Personnel in charge of operating and maintaining the information system.
    Examples: system administrator, data administrator, back-up, Help Desk, application deployment operator, security officers.
  - Developers
    Developers are in charge of developing the university's applications. They have access to parts of the information system with high-level rights but do not take any action on the production data.
    Examples: developer of the HIS-database, business application developers

- Site: site type comprises all the places containing the scope, and the physical means required it to operate.
  - Location: External environment: This concerns all locations in which the organization's means of security cannot be applied.
    Examples: homes of the personnel, environment outside the site (urban area, hazard area).
  - Premises: This place is bounded by the organization's perimeter directly in contact with the outside. This may be a physical protective boundary obtained by creating physical barriers or means of surveillance around buildings.
    Examples: establishment, buildings.

- Zone: A zone is formed by a physical protective boundary forming partitions within the organization's premises. It is obtained by creating physical barriers around the organization's information processing infrastructures.
  Examples: offices, reserved access zone, secure zone.

- Essential services: All the services required the organization's equipment to operate.
- Communication: Telecommunications services and equipment provided by an operator.
  Examples: telephone line, PABX, internal telephone networks.
- Utilities: Services and means (sources and wiring) required for providing power to information technology equipment and peripherals.
  Examples: low voltage power supply, inverter, electrical circuit head-end, water supply, Waste disposal, services and means for cooling the air

- Organization: it describes the organizational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

  - Authorities: organizations from which the analyzed university derives its authority. They may be legally affiliated or external. This forces constraints on the analyzed university in terms of regulations, decisions and actions.
    Examples: administrating body, Head office of the university, the Bavarian public administration.
  - Structure of the organization: different parts of the university, including its cross-functional activities, under the control of its management.
    Examples: human resources management, IT management, student department, registrar's office, computing center, building safety service
  - Project or system organization: This concerns the university set up for a specific project or service.
    Examples: new application development project, information system migration project, research project
  - Subcontractors / Suppliers / Manufacturers: organizations that provide the university with a service or resources.
    Examples: facilities management company [61]

After identifying all the university’s assets within the scope, one starts with the valuation of the assets. For the valuation of the assets, the university itself can decide if they use a quantitative or qualitative scale depending on the university needs for security, university size, and other university specific factors.

For the University of Applied Sciences Augsburg, a qualitative scale form "negligible, low, medium and high" is applicable.

The criteria used as the basis for assigning a value to each asset should be unambiguous. Criteria for determining an asset´s value could contain its original cost, its replacement or re-creation (e.g. the value of a university's repudiation). Furthermore, the basis for the valuation of assets could be the costs resulting due to the loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability in case of a security incident. For realizing the asset valuation, the university needs to select specific criteria relevant to its knowledge-intensive sector and to the security requirement. The following criteria of negative consequences in case of an incident can be applied:

- Violation of legislation and/or regulation
- Interruption of service/ inability to provide the service
- Loss of economy/research company confidence
- loss of credibility in the internal information system
- Disruption of internal operation
- additional internal cost
- Disruption of a third party's operation (e.g. a research project with company's)
- inability to fulfill contractual obligations
- Impairment of business performance
- Loss of goodwill/negative effect on reputation
- Breach associated with personal information
- Endangerment of personal safety
- Breach of confidentiality
- Financial costs for emergency or repair:
  - in terms of personnel, equipment, studies, research reports
- Disruption to business activities
- Loss of goods, funds, assets

Nevertheless, note, these criteria are only exemplary and not concluding. Depending on the university's security situation more criteria have to be added or unappropriated criteria has to be neglected.

For valuation of the university's assets an appropriate scale with appropriate numbers of levels and theirs limits has to be established. Furthermore, it is important to identify the dependencies of assets on business processes and other assets, because they could influence the value of the assets.

For example, the integrity of information depends on the hardware and software used for its storage and processing. Hence, the hardware depends on the power supply and possibly air conditioning, this information about dependencies are the basis for the following identification of threats and vulnerabilities.

If one has finished this step, a list of assets and their values according to disclosure (preservation of confidentiality), modification (preservation of integrity, authenticity,

non-repudiation and accountability), non- availability and destruction (preservation of availability and reliability), and replacement cost are conducted.

The following table gives an example of the University's of Applied Sciences Augsburg assets. Nevertheless, pay attention this table is not concluding, but rather it is used as a guideline.

- Primary assets:

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Business processes and activities	Registration of marks				x	Mrs. Example
Business processes and activities	certification of enrollment			x		Mrs. Example
Information	Marks				x	Mrs. Example
Information	Research Data				x	Mrs. Example
Information	Personal Data				x	Mrs. Example

- Supported assets:

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Hardware	Fixed equipment (Server)				x	Mrs. Example
Hardware	Transportable equipment (laptop)			x		Mr. Xy
Hardware	Data medium (door opener-de-energized contact)			x		Mrs. Example
Hardware	Other media non digital (slides about processes *)	x				Mrs. Example
Hardware	…					
Software	Operating system (user rights administration LDAP)				x	Mr. Xy
Software	Business application software (e.g. HIS database)				x	
Software	Standard software (e.g. word)		x			
Software	Business application (e.g. administration software atoss)		x			
Software	…					
Network	Medium and supports (everything from the second and third OSI layer)					
Network	Passive or active relay					

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
	(e.g. routers, switches)					
Network	…					
Personnel	Decision maker (e.g. university's top management)				x	
Personnel	Users (e. g. human resources management)				x	
Personnel	Users (e.g. department of students)				x	Mr. Xy
Personnel	Developers (e.g. developers of sogo webinterface)			x		
Personnel	Users (e.g. students with theirs individual account)		x			
Personnel	…					
Site	Zone (e.g. offices from the student administration)				x	
Site	Zone (e.g. offices from the professor)				x	
Site	Zone (e.g. server room)				x	
Site	Zone (e.g. laboratory)				x	
Site	Premises (e.g. parking with bounds)	x				
Site	Communication (e.g. telephone lines)		x			
Site	Utilities (e.g. services for cooling the air)				x	
Site	…					

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Organization	Authorities (e.g. Head office of the university)				x	
Organization	Structure of the organization (e.g. computing center)				x	
Organization	Structure of the organization (e.g. student department)				x	
Organization	Project organization (e.g. research project)				x	
	…					

Figure 10: Asset identification and classification [own preparation]

The values were classified according to the following criteria.

- Negligible = no costs/ no negative repudiation/ no disruption of operations/ no impairment of business performance / no breach of confidentiality
- Low = low costs/low negative repudiation/ low disruption of operations/ low impairment of business performance /low breach of confidentiality
- Medium = medium costs/ negative repudiation/ disruption of operations/ impairment of business performance /breach of confidentiality
- High = high costs/high negative repudiation/ high disruption of operations/ high impairment of business performance / high breach of confidentiality

* no slides about critical processes exist.

Challenge:

It is important to identify all assets within the scope. Because only by identify all the university's assets an appropriated classification is possible and consequently an effective risk management can be conducted. Note the identified assets has to described exact accordingly their context in which they are used. For instance, with a "*" the context can be described exactly (see above). Furthermore, an asset owner has

to be notched who is responsible for the classification for the assets, the maintenance and the right handling of them. Often it is difficult to identify really all assets. Furthermore, it can be a challenge to describe the used assets and its context in a correct and exactly way that there exist no misunderstanding. In addition, it could be difficult to find a person who want to be responsible for the inventory. It could be helpful to call the head of each department to account for theirs assets, because she or he have the best knowledge about the assets, their values and their criticality in case of an incident. A complete and sophisticated asset classification is the basis for the success of an effective risk management.

5.7 Planning risk assessment – Identification-Estimation-Evaluation

Based on the complete and meaningful value determination and classification, risk management is carried out in this step. Effective risk management is at the heart of every ISMS. Without a sophisticated risk management, an effective ISMS cannot be implemented, operated, maintained or improved[64],[65].

- Protection requirement

As described in chapter 4.5, the nature and manner of the preferred risk management method depends on the determination of the protection requirements.

For the University of Applied Sciences Augsburg and any other Bavarian higher education institution and university comparable in terms of protection requirements, the risk management method according to ISO/IEC 27005 [31], with their preceded, thorough risk analysis and iterative improvement approach, was used for the reasons mentioned in chapter 4.5.

In the knowledge-intensive university and higher education sector, in such a rapidly developing environment, it is of great importance to use a risk management system that pursues an iterative approach with a continuous improvement process in order to be able to react promptly to all changes (e.g. changes in risks, changes in context).

The process of information security risk management according to ISO/IEC 27005 can be integrated as a self-contained sub-process of the creation of an information security concept into the phases of the “plan-do-check act” or "PDCA circle" of an ISMS.

The process-oriented approach of this model is also used in other ISO/IEC standards, such as ISO/IEC 9001 [66] and ISO/IEC 20000-13, and in the previous version of ISO 27000 (DIN ISO/IEC 27000:2011) [67] , the overall process of creating, maintaining, controlling and improving an ISMS is still based on the "Plan-Do-Check-Act-Process". For optimization reasons, the "PDCA circle" is only used for the self-contained sub-process of information security risk management. The following table compares the

information security risk management process measures with the PDCA group of an ISMS.

Table 1 — Alignment of ISMS and Information Security Risk Management Process

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Figure 11: Alignment of ISMS and information security risk management process [58]

In the first phase of the "planning", the framework conditions are defined as well as the risk assessment, a risk treatment plan is drawn up and risk acceptance is examined. The next phase of implementation describes the implementation of the risk management plan, i. e. all selected measures and objectives are carried out based on the plan. In the subsequent "control" phase, the phases that have already been completed are monitored and the risks reviewed. Finally, in the final phase of the "action", the entire information security management process is maintained and, if necessary, improved so that the cycle can start again from the beginning.

The focus of an information security concept is the implementation of an information security risk management. In order to systematically identify, evaluate, treat and monitor information security risks, the following risk management process must be carried out in accordance with DIN ISO 27005 [58].

- context establishment
- risk assessment
  - risk identification
  - risk estimation
  - risk evaluation
- risk treatment
- risk acceptance
- Risk communication
- risk monitoring and review

The following graphic provides an overview of the whole information security risk management process. A fundamental understanding of the risk management process is to be provided.

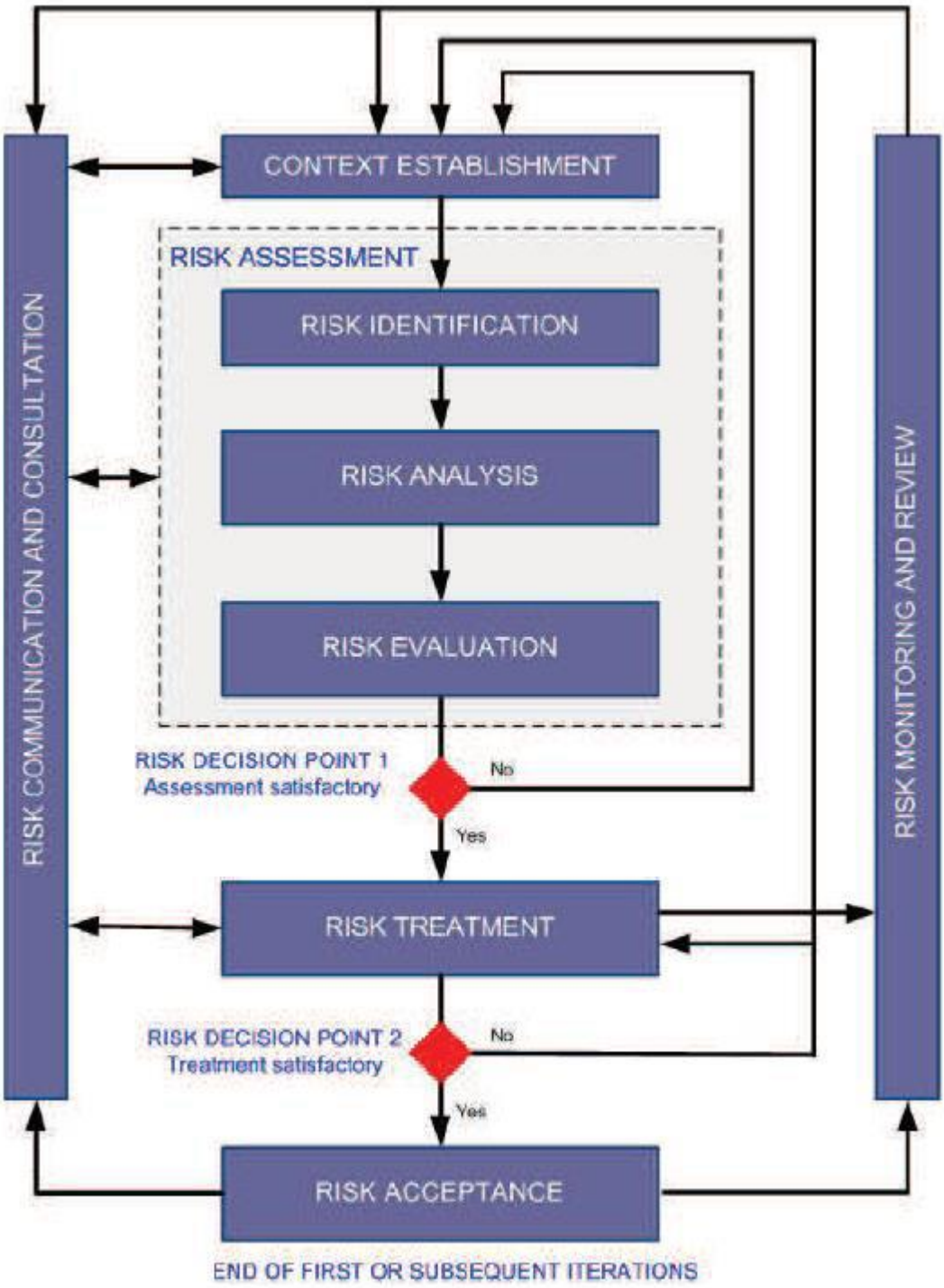


Figure 12: Information security risk management process [58]

5.7.1 Planning risk assessment

- **Context establishment**

As illustrated in figure 12, the starting point is the framework conditions with the internal and external context of an organization. Criteria for assessing and accepting risks, the scope and limits of application and the establishment of a risk management organization are defined. Risk acceptance criteria can be based on cost-value aspects, consequences for the university or on the maximum of acceptable risks. See also chapter 5.2 and following chapters.

- **Risk assessment**

Once the framework conditions have been defined with the basic criteria, the next step is to carry out a risk assessment. An effective risk assessment involves the identification of risks, risk analysis with risk estimation and the evaluation of risks. Since a risk, as described in ISO/IEC 27000, is a combination of the probability of occurrence of an unexpected event and its consequences, a risk assessment quantifies or qualifies the risk and makes it possible to prioritize the risks according to their seriousness.

With the help of a risk assessment, it is possible to determine the goodwill of the information assets, to identify the relevant existing or possible threats and vulnerabilities, to analyze and assess the existing countermeasures and their effect on the existing risks, to determine the potential consequences and finally to prioritize the derived risks and to classify them on the basis of the assessment criteria. A risk assessment is usually carried out in two or more iterative runs to achieve meaningful results. The first iteration is the highest-level assessment to identify potential high-level risks that justify the next iteration. The following iteration allows a detailed analysis of the identified risks. If this flow of information is insufficient to carry out a meaningful risk assessment, a more in-depth analysis may need to be carried out using a different method, where appropriate, for the whole framework.

As soon as the risk assessment produces sufficient useful information to provide a basis for decision-making on the selection of effective risk management measures, this process step is completed. Thus, the risk decision point 1 can be answered positively and the subsequent process step can be carried out. Otherwise, the current process status will be run again and iteratively until adequate information is available. The framework conditions are being redefined and the internal process of risk assessment with its sub-elements is being retraced in order to obtain suitable information.

Risk assessment must identify, among other things, risks with regard to confidentiality, integrity, availability and risk owners and their consequences, as well as assess risks using risk criteria[68].

- Identification of risks

The purpose of identifying risks is to determine how potential damage may have occurred. Risks should also be recorded, regardless of whether or not they originate from the organization. In order to fully identify the risks, it is necessary to define values, identify threats and vulnerabilities, identify existing countermeasures and determine the consequences. When determining assets, everything relevant to the organization should be taken into account. For more details see chapter 5.6.

The level of detail of the value identification should be high enough to ensure that sufficient information is available for risk assessment. The level of detail determines the overall scope of the risk assessment.

In order to fully identify and analyze risks, **threats** must be identified. It should be noted that threats of both natural or human origin, accidental or deliberate, can occur within or outside the organization. Generally speaking, threats should always be identified and categorized generically, according to their type and source, to avoid overlooking any unexpected threats and to limit the search for them. It should be noted that a threat can affect several assets and therefore the impact may vary depending on which asset has been affected. In addition, experience from previous incidents or risk assessments should be included in the current risk assessment.

However, when using standardized threat catalogs or using the results of old risk assessments, it should be noted that threats are constantly changing, especially when the external circumstances of the organization change. Threats can be classified by type, origin, and manner (intentional, accidental, natural, environmental or non-human). After this sub step has been performed, a list of possible threats should be available, categorized according to their type and source.

Possible **weaknesses** are identified as the next sub-process step in risk identification. According to ISO/IEC 27001, vulnerabilities exploited by threats can cause damage to the assets of the organization or the organization itself. Vulnerabilities can exist throughout the entire organizational process. Weaknesses can occur in the areas of business processes, management level, HR department, physical environment, or organizational structure, as well as in the configuration of an information system, in the hardware and software area, or as a result of dependence on external third parties. Since the mere existence of a vulnerability without a corresponding threat does not cause any damage, and is therefore not understood as a risk, no countermeasure must be developed. However, this vulnerability should be monitored as changes create a corresponding threat and can be exploited and therefore pose a risk.

It should be noted that an incorrectly implemented, a wrongly functioning security measure or the improper use of this countermeasure can itself be a weakness.

Vulnerabilities can be categorized into different areas (hardware, software, network, human resources, location and organizational structure) with associated potential threats. Once this sub-step has been completed, the result should be a list of vulnerabilities with reference to the assets of a university, the threats and the existing control measures, as well as a list of vulnerabilities without corresponding threats.

Furthermore, one has to identify the **consequences** of a loss of confidentiality, integrity and availability of values. This measure identifies the effects of an incident scenario using the impact criteria set in the definition of the framework conditions. The effects may affect an asset, part of it, or several assets. For this reason, assets should be assigned both a financial value and goodwill. (See chapter 5.2) Effects may be of short duration or permanent in case of destruction. The classification of impacts should be carried out from the following points of view.

- Discovery and recovery time,
- loss of working time,
- loss of opportunities,
- health and safety,
- financial costs related to damage repair expertise
- and damage to reputation and reputation

As a result, a structured list of incident scenarios, the affected values and the consequences should be available once this sub step has been completed.

- Risk analysis

Once the previous process step of risk identification has been completed in the risk management process, the risk analysis with its sub-areas assessment of the impact and the probability is completed, as well as a risk estimation.

The first step is to choose a suitable method for carrying out the risk analysis. The level of detail of a risk analysis can vary greatly, depending on the criticality of assets, the extent of known vulnerabilities or the number of previous incidents. Depending on the situation, risk analysis can be carried out using qualitative, quantitative methods or a combination of both. Often, a qualitative method is used initially to determine the general indication of risk levels and identify the main risks. A quantitative method is then used to further examine the main risks. Quantitative methods are often more expensive and complex than qualitative methods. The design of the analysis should be consistent with the risk assessment criteria defined in the definition of framework conditions.

Qualitative risk methods use a framework of qualifying attributes (such as low, medium, and high) to describe the extent of potential impacts and their likelihood of occurrence. Depending on the given circumstances, the framework of the qualitative method can be adapted or extended as required. Advantageous in the use of a qualitative method of risk analysis is the simple and understandable readability of the results. Whereas the dependency of the subjective frame selection can be regarded as a disadvantage.

In quantitative risk analysis methods, the frame is provided with numerical values from a large number of sources. The quality of this method depends on the precision, accuracy, completeness of numerical values and validity of the models used. In quantitative methods, historical data from previous incidents are usually used. This has the advantage that the protection goals and concerns of the organization can be

deduced directly from it. However, the disadvantage is the lack of data on new risks or new vulnerabilities. The way in which the effects and likelihood of expressing the risk measure vary widely and depends on the nature of the risk and the purpose of the assessment result. The fluctuations and uncertainty of the impact and probability analysis must be taken into account when considering the analysis and communicated accordingly. A disadvantage of the quantitative risk analysis method is that there are no verifiable data available. Therefore, Chapter 7 deals with a qualitative risk management method.

In order to carry out a meaningful risk analysis, the effects must be assessed. First, a monetary value is assigned to the identified values of the university by classifying them according to their criticality and importance.

The determination of the values can be carried out by two different measures. On the one hand, by determining the cost of the replacement value when the value is restored and, on the other hand, by determining the costs incurred as a result of the effects on the operating procedure in the event of loss or endangerment of the values. This includes, for example, regulatory or legal consequences resulting from the disclosure, modification, unavailability or destruction of information or other assets. In most cases, the value that arises as a result of the impact on the business process is higher than the simple replacement value. Asset valuation is a key factor in assessing the impact of an incident scenario, as more than one asset is usually affected. Different vulnerabilities and threats have different impacts on values such as loss of confidentiality, integrity or availability. The consequences can be illustrated with monetary, technical or human impact criteria. In some cases, it may be necessary to express the consequences for different groupings, periods or situations with more than one value in order to provide a meaningful basis for the of decision making. In the first iteration of the impact assessment, the simple replacement value is usually determined in the first iteration of the impact assessment, whereas in the next iteration, the immediate damage value is determined, which was caused by the effects of an incident scenario. See also chapter 5.6.

As a result of this sub step, a list of evaluated consequences of an incident scenario that are reflected by values and impact criteria should be available**.**

Once the incident scenarios have been identified, it is necessary to determine the probability of occurrence of each individual scenario using qualitative or quantitative analysis methods. Depending on the frequency of threats and how easy it is to exploit the vulnerabilities, the following points of view should be taken into account in the probability assessment:

- empirical values and appropriate statistics for the probability of a threat
- deliberate sources of danger:
  - Motivation of the offender
  - Ability of the offender
  - Available resources of the offender
  - Attractiveness of the assets concerned as perceived

- Random, unintentional sources of danger:
  - Geographical location
  - Extreme weather conditions
  - Other factors that can cause human error
- individual or clustered vulnerabilities
- effectiveness of existing countermeasures

It should be noted that intentional and unintentional sources of danger can change continuously. After the probability assessment has been carried out, a list of accident scenarios should be available with their probability of occurrence.

Finally, the risk level must be determined in a meaningful risk analysis. The probability value is combined with the value of the consequences. In addition, other variables such as costs or concerns of interest groups can also be used to determine the level of risk. As a result of the analysis, risk assessment methods discussed in ISO/IEC TR 13335-3 (Information technology - Guidelines for the management of IT security -Part 3: Techniques for the managing of IT security) are used to determine the level of risk.

To assess the information security risk, the "High Level Information Security Risk Assessment" method and the "Detailed Information Security Risk Assessment" method are used.

- "High Level Information Security Risk Assessment" method

The high-level risk assessment method is often used at the beginning of a risk assessment to obtain an overview of the existing risks. If a simultaneous implementation of all security measures is not possible for cost reasons and therefore only the risks classified as critical are addressed, this method is used for risk assessment. The "high-level" risk assessment method addresses the global perspective of the organization, in which the technical aspects are considered independently of the business processes. In addition, a limited list of threats and vulnerabilities that have already been grouped together by domain will be analyzed to speed up the process.

In this approach, the focus is on the entire risk scenario rather than the individual elements. Since in this procedure the measures are prioritized and organizational, non-technical or management aspects of the technical security measures are focused, a comprehensible presentation of the risk situation is possible.

The advantage of this method is that it determines the need for direct protection and prioritizes the resources needed to carry out security measures. Due to the high level of risk assessment, it may be necessary to carry out a second detailed risk assessment iteration in order to obtain a meaningful result. If the lack of information security causes disastrous consequences for the organization, its business processes or assets, a second detailed iteration of the risk assessment is required to identify potential risks.

- "Detailed Information Security Risk Assessment" method

The "Detailed" risk assessment method includes a detailed identification and determination of the assets, their threat and vulnerability assessment. The consequences are assessed using quantitative, qualitative analysis methods or a combination of both. The likelihood of occurrence depends on the attractiveness of the value concerned, the extent to which a weak point is exploited, the abilities of the offender and the vulnerability of the weak point.

As this method is very time-consuming and requires a high degree of work and expertise, it is usually used in high-risk information systems. Often subjective and empirical measures are used in this type of valuation method and the results are presented in tabular form. It should be noted that each university should use the most appropriate measure for its individual needs, which provides reliable and reproducible results.

The following are examples of table-related methods. These examples are of course not conclusive.

- matrix with predefined values

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Figure 13: Matrix with predefined values [58]

This example creates a matrix with predefined values. In this type of risk assessment method, the value of each asset is grouped into categories 0-4 in relation to the associated replacement or reconstruction costs.

Next, for each type of threat, the matrix is filled from 0-8 for both probability of occurrence and vulnerability level.

As a result, the threat or vulnerability level of each asset can be determined using this matrix. For example, an asset with a value of 3 is quantified, the probability of

occurrence is classified as "high" and the exploitation of weak points is regarded as "low", the extent of the risk is shown as 5. Once all risks have been assessed, they can be treated according to their rankings. In order to be able to classify assets, probabilities of occurrence and vulnerability levels appropriately, it is necessary to collect information in advance from the relevant authorities (see also chapter 5.6).

A similar procedure is illustrated in figure 14.

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Figure 14: Risk Assessment matrix variant with predefined values [58]

A risk assessment is carried out by combining the probability of an incident scenario with the estimated effects. If the probability of an accident scenario is very high, this is categorized as 4, whereas the impact of the damage is only moderate, the overall risk is nevertheless very high and is quantified at 6. After the resulting risk is categorized on a scale of 0-8, the result is measured according to the acceptance criteria. This matrix also allows an overall risk assessment.

- Threat ranking based on risk measures

Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

Figure 15: Risk Assessment Matrix: Threat Ranking [58]

As shown in figure 15, the first step in this procedure is to list various threats (column a). In a second step, the effects on the assets (column b) are evaluated in a predefined scale of 0-5. In the next step, the probability of occurrence (column c) is also evaluated in a predefined scale of 0-5. After these steps have been carried out, the risk measures Product are calculated in column d from columns b and c. Finally, the threats can be prioritized in the final step, depending on the risk measures (column d).

This approach allows you to compare and prioritize different threats with their impact on assets and probabilities. In addition to these methods for assessing the information security risk, there are other guidelines and assessment methods which are described in more detail in the ISO/IEC 31010 standard.

For a risk assessment of the highly sensitive processes "Access Control with the Campus Card" and "Recording of marks" a similar matrix as in figure 14 illustrated is used in chapter 7. This matrix makes it possible to prioritize risks in a simple but meaningful way. Other presentation and calculation methods are also possible.

- risk evaluation

On the basis of a meaningful risk analysis, the next step in the risk assessment process is the sub-process step of the risk evaluation. The risk level is compared with the risk acceptance and risk evaluation criteria. These criteria, which were already set in the initial stage of defining the framework conditions (see chapter 5.2), should be checked for actuality or redefined in this sub process step.

The risk assessment should take into account that an accumulation of several small risks may constitute a high overall risk.

Similarly, the information security characteristics that are important for the university must also be examined. For example, if the criterion of confidentiality is irrelevant to the university, all risks that are influenced by this criterion are also meaningless. In order to carry out a correct risk evaluation, the importance of a business process must be examined. In the event of minor importance, the associated risks should be considered to be lower. The risk evaluation is used for future decision-making on the basis of the risk analysis. Adequate risk evaluation is the basis for prioritizing and dealing with risks. During the risk assessment phase, contractual, legal and regulatory requirements should also be considered as factors. At the end of this phase, a list of prioritized risks should be available, in accordance with the above-mentioned criteria, assigned to the relevant incident scenarios.

Risks are assessed by comparing the results of the risk analysis with the defined criteria. The identified risks are prioritized for the next step in the process, namely risk management.

In order to obtain comparable reproducible results, the risk assessment must be carried out systematically under the same conditions. It is necessary to repeat the risk assessment process on a regular basis as changes in organizational objectives and strategies, values and safety requirements affect both the results of risk analysis and risk assessment and the associated countermeasures.

5.7.2 Conducting risk treatment

- Risk treatment

Taking into account the results of the risk assessment, appropriate options for dealing with the identified risks are selected in this process step. The effectiveness of risk management depends on the results of the risk assessment. Risk management involves a cyclical process with the following elements.

  - Assessment of risk treatment
  - Decision on the acceptance of the remaining residual risk
  - Introduction of a new risk treatment in the event of an unacceptable residual risk
  - Assessment of the effectiveness of this risk treatment

It must be borne in mind that the cost of the measures is proportionate to the extent of the damage, i.e. the costs for risk treatment measures must be lower than those for the threats caused by the risks.

The risk management options consist of risk reduction, risk retention, risk avoidance and risk transfer. The choice of risk management options should be based on the outcome of the risk assessment, the expected cost of establishing the corresponding option and the expected success of the respective option.

These four options should not be considered independently of each other. Often, a combination of these options is the most effective approach to risk management. For example, the likelihood of occurrence and impact can be reduced while the residual risk is transferred to several parties.

A risk management plan should be defined to effectively manage the risks. In order to save costs, existing countermeasures must be examined for effectiveness. Often it can make sense to maintain redundant security measures rather than remove some of them at the expense of the security of the overall process. It is the responsibility of management to maintain a balance between the implementation costs of security measures and the damage caused by the risks.

After the risk management plan has been defined the remaining residual risks must be determined. The determination of residual risks involves a renewed iteration of the risk assessment, taking into account the expected effects of the defined risk treatment options. If a residual risk does not meet the requirements of the risk acceptance criteria, a new iteration of the risk treatment prior to the risk acceptance procedure is necessary.

The **risk treatment plan** includes the priority of the assessed risks and their management, including the treatment periods set, to ensure compliance with the acceptance criteria. In some cases, residual risks do not correspond to the defined acceptance criteria, since the time circumstances were not taken into account when defining these criteria. For example, risks were accepted because the benefits of the risks were very attractive, or because the costs of risk reduction were too high. Under these circumstances, the acceptance criteria are not adequate and should be redefined. If these criteria cannot be changed within a reasonable period of time, risks must be accepted even though they do not meet the regular acceptance criteria. In such a case, there must be a substantiated documentation.

In order to reduce risk, security measures should be selected to meet the requirements of risk assessment and risk management. Generally speaking, security measures include one or more types of safeguards, such as corrective measures, deletions, preventive measures, minimization of impact, recovery, monitoring and awareness.

When selecting the protection measures, it is of great importance to keep the acquisition costs, implementation costs, administration costs, maintenance costs and monitoring costs in proportion to the value of the property to be protected.

It should also be borne in mind that special skills and expertise may be required to develop new security measures or adapt existing ones. There are several factors that influence the choice of security measures, such as technical, cultural, legal, time, financial, environmental, human resources, or the simplicity of application. When selecting the appropriate security measure, the balance between the performance of the measure and the effectiveness of information security should be maintained. As a result of this risk management method, a list of possible security measures should be available, including costing, benefits and priorities. If risks meet the acceptance criteria, they can remain untreated. In this case, there is no need to establish security measures.

Risk avoidance as a risk management option is used when identified risks are considered to be too high or the implementation costs of a security measure are not proportionate to the resulting benefits. In this case, all activities that cause the risks will be withdrawn or their basic conditions changed.

The last option of the risk management method, risk transfer, reallocates the risks to third parties. However, it should be noted that this method may give rise to new risks or that the existing risks are changed. In this case, additional risk treatment is required.

Redistribution can mean, for example, that insurance companies bear the financial damage effects or that third parties are responsible for monitoring an information system and for intervening in the event of a malfunction, or that they have been shown to have done so (outsourcing).

- risk acceptance

The risk acceptance measure must ensure that the residual risk is explicitly borne by the university´s management level, particularly in situations where the introduction of control measures is omitted or postponed. If the level of residual risk is unacceptable, a new iteration of the risk assessment with any changed context parameters, such as criteria for risk acceptance or impact, must be carried out. If necessary, this is illustrated by a renewed risk treatment such as decision point two (Risk decision point 2).

- risk communication

Throughout the entire information security risk management process, communication of risks and their treatment measures within the organization is critical. Raising awareness of the risks and effectiveness of control measures among the people concerned is the most effective way of dealing with unforeseeable incidents.

Effective bi-directional communication between decision-makers and stakeholders is of paramount importance to ensure that all those involved in the risk management process understand the basis on which decisions are made and that certain measures are implemented. The exchange of information in the risk management process involves the existence of risks, their manifestation, the way in which they appear, the likelihood of their occurrence, the severity, the treatment options and the acceptance of the risks. In addition, risk communication plans should be drawn up regularly for both normal operations and emergencies. By setting up a committee, risks, their prioritization and treatment can be debated between the decision-makers and the interested parties.

The aim of risk communication is to

  - to provide confidence in the risk management results,
  - Collect risk information,

- to communicate the results of the risk assessment and present the risk management plan,
- to support decision-making,
- coordinate with other third parties, assigning responsibilities to reduce the impact of the damage,
- to give decision-makers and third parties a sense of responsibility for risks
- and to improve awareness.

Particularly in crisis communication, it is crucial to cooperate with the appropriate press office or communication unit within the university in order to ensure the coordination of all measures relating to risk communication.

- Risk monitoring and improvement

This part of the risk management process can be found in the "Check" or "Act" phase of the "PDCA cycle", as illustrated in figure 11. For this reason, more details are described in chapter 5.8.

Generally speaking, both the risks and the overall risk management process must be continuously monitored and improved. These monitoring and improvement measures concern all levels, from the university management to simple staff. There are many different approaches to effective risk management, so that each university or university of applied sciences has to choose the most appropriate approach for it, depending on the circumstances [58]. More details can be found in chapter 5.8.

Challenge:

One of the most difficult tasks in dealing with an ISMS is to plan the risk assessment and to address the risk. Because planning includes the actions to address risks, their integration and implementation into the ISMS process. In addition, the evaluation of the effectiveness of these measures must also be taken into account in the planning process.

The risk assessment itself is also carried out according to the rules of the "PDCA cycle", so that the context has to be defined at the beginning of the "planning phase", a risk assessment with identification of all threats, weak points and consequences and a risk treatment plan has to be prepared, as well as an acceptance plan for risks has to be carried out. However, the planning phase can only be completed effectively if the preparatory work on how to determine correct and complete values has been carried out. It is also important that the area to be analyzed is precisely defined and that the areas not considered are also documented with justification.

It should also be borne in mind that small individual risks can represent a very high risk. However, the level of detail of a risk assessment should not be too detailed, at least not in the first run. It is better to create a meaningful result at a high level than to make a too detailed assessment without a statement.

In the risk assessment process, the information security officer or his or her team should be in constant contact with all persons involved, from top management at the university to the individual persons responsible for the values. In order to avoid misunderstandings, the criteria for risk assessment and its acceptance should be confirmed by the university's top management.

In addition, it is of great importance that the risk owner is also aware of the respective risks so that attention is paid to them and that the risks can be dealt with in the appropriate form and that the risk management system can be improved in the next step.

In addition, the results of the risk analysis should be compared with the acceptance criteria, so that priority can be given to further risk management. This is often difficult if you have a certain budget for risk management and therefore need to decide which risks to deal with first or not at all. Since this decision can entail far-reaching consequences, the reasons for the decision should be documented in the most precise way. Finally, when performing the risk assessment it is of great importance that the results are valid, comparable, reproducible and repeatable.

The identification of risks, their analysis and evaluation by a third party should be traceable and their results should be the same when different people assess the risks in the same context. Possible inconsistencies may indicate an inappropriate method and should be reviewed in this case.

This is the only way to be able to react quickly to changes in time and reflect the meaning of iterative, effective risk management. Only through effective sophisticated risk management can an effective HS-UNI-ISMS be introduced, implemented, maintained and improved.

5.8 Designing the ISMS

This is the last step in managing a HS-UNI-ISMS project. Here, the activities planned in advance are converted and verified into functioning and controlling processes.

The final ISMS project implementation plan is the result of this step [69]. In order to gain confidence in an effective implementation of the planning, all previously carried out activities in each phase of the HS-UNI-ISMS process should be documented.

During this period, the HS-UNI-ISMS-project can be started at the university as part of the "DO" phase of the PDCA cycle. Based on the planning, implementation, management and control of the university's information security officer, the university implements and controls the processes in order to satisfy the information security requirements and achieve the university's information security goals.

If processes have been outsourced, it is the university's responsibility to check and control them in order to meet the requirements of information security.

Once the implementation has been successfully completed, the processes are controlled, monitored and reviewed to ensure that the requirements arising from the framework conditions and needs of all parties involved are met.

If the HS-UNI-ISMS is changed (intentionally or unintentionally) during operation, its consequences must be assessed in order to monitor any negative effects.

In particular, the following processes should be reviewed and implemented throughout the university:

- specific information security management processes (e.g. risk management, incident management, continuity management, internal audits, management reviews
- processes regarding the risk management plan
- reporting structures within the information security area regarding contents, frequency, format, responsibilities, and so on, (for example incident reports, reports on measuring the fulfilment of information security objectives, reports on performed activities)
- meeting structures (frequency, participants, purpose and authorization) within the information security area. Representatives from different areas with relevant roles in terms of information security should participate in this process.

If changes (planned) are subsequently made to the HS-UNI-ISMS in this process step, the following points should be taken into account:

- planning the implementation of the change and assigning tasks, responsibilities, deadlines and resources to it
- Implement changes as planned
- Monitor its implementation
- Collecting documented information on the implementation of the changes (with responsibilities, deadlines, efficacy evaluations)

If unintentional changes have already occurred, the following points should be taken into account.

- Check the consequences
- determine whether adverse effects have already occurred or may occur in the future
- plan and implement measures to eliminate negative consequences
- Collecting documented information on negative changes and measures to eliminate them

5.8.1 Risk treatment

The university conducts the process defined in 5.7 for risk assessments of information security. This should be done either after a serious change of the HS-UNI-ISMS, its context or after information security incidents, but at least once a year.

Consequently, the risk management plan will be implemented or updated either in accordance with a pre-defined timetable or in response to significant changes or incidents related to information security. It is helpful if the following points are present for each individual risk in the risk management plan

- selected treatment option(s)
- necessary control(s)
- implementation status
- risk owner(s)
- expected residual risk after the implementation of measures.

In addition, authorization should be obtained from the risk owners on the basis of defined risk acceptance criteria or, in the event of a deviation, on justified arguments.

It is important that the acceptance of the risk owner for the remaining residual risk is recorded and approved by the university management. If the implementation of the risk management plan or parts of it fail, a new iteration of the process for dealing with information security risks must be carried out.

5.8.2 Performance Evaluation

Correct, meaningful monitoring, measurement, analysis and evaluation is crucial for the success of an effective ISMS. For monitoring and measurement, the university defines

- what to monitor and measure
- who monitors and measures
- when to monitor and measure
- what methods to produce valid results

With the help of the monitoring and measurement, the university can achieve the high-level-security statement or question – the defined information need.

For evaluation, the university analysis on the one hand the security performance and on the other hand the effectiveness of the ISMS. Evaluate the performance means, determining whether the university is doing as expected, which includes determining how well the processes within the ISMS meet their specifications

Performance evaluation means whether the university works as expected and how well the processes within the ISMS correspond to its specifications.

Evaluation of effectiveness means determining whether the organization is doing the right thing, including determining the extent to which the objectives of information security are met.

For analysis and evaluation, the university defines

- who analyses and evaluates the results from monitoring and measurement
- when to analyze and evaluate
- what methods to produce valid results

Be careful when defining the attributes to be measured.

It is impracticable, expensive and counterproductive to gauge too many or wrong attributes. In addition to the costs of measuring, analyzing and evaluating numerous attributes, there is also the possibility that important questions are hidden or even missing.

It may be useful to identify the people involved in monitoring, measurement, analysis and evaluation and assign different roles to them. This is because the appropriate expertise is required in each case.

In addition, the university should conduct **internal audits** to provide information on ISMS compliance with the previously defined requirements. The evaluation of an ISMS at planned intervals by means of internal audits gives top management the assurance that the ISMS has the desired status. An internal audit can detect deviations, risks and opportunities.

The scope and frequency of internal audits should be tailored to the size and nature of the university as well as the type, functionality, complexity and maturity of the ISMS (risk-based audit).

The effectiveness of the controls implemented should be reviewed within the framework of internal audits. An audit programme should be designed to cover all necessary controls and to assess the effectiveness of selected controls over a period of time. Key controls should be part of each audit.

An audit programme should include documented information about:

- audit criteria
- audit methods
- selection of audit teams
- processes for handling confidentiality, information security and other similar matters

When carrying out an audit, it should be taken into account that procedures and controls should have been in operation for some time to enable appropriate evidence to be assessed. In order to obtain a meaningful result of the audit, the selection of

auditors should take into account their competence, independence and appropriate training.

The selection of internal auditors can be challenging for smaller universities. If the required resources and competencies are not provided within the university, external auditors should be employed. When universities employ external auditors, they should verify that they have acquired sufficient knowledge of the university context. This information should be provided by internal staff.

However, it should be borne in mind that internal staff acting as internal auditors can carry out detailed audits taking into account the business context, but may not have sufficient knowledge of how to carry out audits.

If this is the case, an appropriate audit team of internal and external auditors with the necessary knowledge and skills should be formed. A central internal audit team, who is too permanent for all Bavarian universities and universities of applied sciences, would also be possible.

When performing the audit, the head of the audit team should prepare an audit plan, taking into account the results of previous audits and the need to respond to reported deviations and unacceptable risks.

The audit plan should be kept as documented information and should contain criteria, scope and methods of testing.

The following points should be included in an audit:

- Appropriateness and effectiveness of the processes and established controls;
- Compliance of the objectives of information security;
- Compliance with the requirements of ISO/IEC 27001:2013, paragraphs 4 to 10;
- Adherence to the university´s own information security requirements
- Consistency of the declaration of applicability with the outcome of the information security risk management process;
- Compliance of the real plan for dealing with information security risks with the identified assessed risks and the criteria for risk acceptance;
- relevance (taking into account the size and complexity of the university) of the management review of inputs and outputs
- Impact of the results of management assessments (including the need for improvement) on the university

If the result of the audit contains any discrepancies, the auditor should draw up an action plan for each discrepancy, which normally includes the following:

- description of the lack of conformity found;
- Description of the reason (s) of the lack of conformity
- description of the short-term and longer-term corrective measures taken to correct a discrepancy within a specified period
- the people responsible for executing the plan

Audit reports with audit results should be allocated to the university´s top management.

Finally, the university´s top **management reviews** the ISMS at planned intervals (daily, weekly, or monthly) ensuring the continuing appropriateness, adequacy and effectiveness of the ISMS

Generally speaking, management review is an important process carried out at various levels of the university to determine the current status of the ISMS and, if necessary, to initiate improvements.

There are many ways in which management can verify the ISMS, such as checking measurements and reports, electronic communication or verbal updates.

Important key factors such as the results of the performance evaluation of information security measures (described above) and the results of the internal audits (described above) as well as the results of the risk assessment and the status of the risk treatment plan play a decisive role.

In verifying the results of information security risk assessment and status of the information security risk treatment plan, management should affirm that the remaining risks meet the risk acceptance criteria and that the Risk Management Plan takes into account all relevant risks and their options for risk management. Therefore, all aspects of the ISMS should be reviewed by management at scheduled intervals, at least once a year, by setting appropriate schedules and agenda items at management meetings.

When carrying out a management review, the focus should be on the following:

- Status of measures taken from previous management reviews
- Changes in external and internal context (see 5.2)
- feedback on information security performance accordingly
    - non-conformities and corrective action
    - monitoring and measurement results
    - audit findings
    - compliance with information security objectives
- feedback from stakeholders, including proposal for improvement, change requests and complaints
- Results of the evaluation of information security risk assessment and the status of the treatment plan for dealing with information security risk
- Possibilities for continuous improvement, including efficiency gains in both ISMS and information security controls.

The level of detail should be according to its use. The results of the management review should be documented for reasons of traceability.

As a result of the management review process, decisions on continuous improvement opportunities and the need for changes to the ISMS such as changes in the information

security policy and objectives, changes of the risk acceptance criteria, changes of resources or budget for the ISMS, should emerge.

5.8.3 Improvement

Both the complete HS-UNI-ISMS and risk management must be continuously improved in iterative cycles to ensure an effective HS-UNI-ISMS.

Universities or universities of applied sciences and their framework conditions are not statically self-contained components. This changes both the vulnerabilities and threats as well as the risks rapidly and new ones arise.

Moreover, there exists no 100 percent perfect HS-UNI-ISMS. There is always room for improvement, even if it is only an increase in the efficiency of the HS-UNI-ISMS.

In order to have an effective HS-UNI-ISMS that is always up to date, it must be checked regularly for its suitability, effectiveness and alignment with the university´s goals. The HS-UNI-ISMS can be seen as an evolving, learning, living part of the university's business operations

By means of a systematic and continuous iterative improvement process, the information security of each university can be increased.

With the help of a continuous iterative improvement process, the university top management can set goals for continuous improvement, e.g. by measuring effectiveness, cost or process maturity. A continuous improvement of the HS-UNI-ISMS means that the ISMS itself and all its elements are evaluated taking into account the scope see 5.2, and the results of the performance evaluation see 5.8.2.

The following points must be observed:

- Suitability of the ISMS: Are the context, the requirements of interested parties, the objectives of information security and the identified risks of information security adequately addressed by planning and implementing the ISMS?
- Adequacy of the ISMS: Are ISMS processes and information security controls compatible with the general objectives, activities and processes of the organization?
- Effectiveness of the ISMS: Are the resources required to set up, implement, maintain and continuously improve the ISMS appropriate to the results?

In particular, improvements should be made if nonconformity such as failure to fulfil a requirement in the ISMS or its correct implementation or failure to comply with legal, contractual or agreed customer requirements.

If discrepancies such as those who do not behave as expected by procedures and guidelines, projects that do not deliver the expected results, or controls that do not

function according to the design, it is imperative that an improvement be made to the whole HS-UNI-ISMS or to the affected part.

If nonconformity is detected, e.g. through analysis of information security incidents, alerts from users, monitoring and measurement results not meeting acceptance criteria and the objectives are not achieved, a predefined plan for improvement or correction should be used.

The following aspects should be addressed:

- Determination of the extent and impact of non-conformity
- what kind of corrections are made to limit the impact of non-conformity? After all, wrong corrections can have worse consequences.
- communication with all persons concerned to ensure that corrections are carried out as agreed
- monitor the situation to ensure that corrections have the envisaged effect and do not cause undesired side effects

The following questions should be asked:

- is a corrective action according to defined criteria (e. g. effects of non-conformity, repeatability) required?
- has non-conformity been verified? (e. g. similar non-conformities, consequences of non-conformity and their corrections)
- has a thorough root cause analysis of non-conformity been carried out taking into account the errors? What was the trigger that caused the deviation? (e. g. persons, methods, processes or procedures, hardware or software tools, incorrect measurements, environment)
- Can patterns or criteria be derived from this in order to identify similar situations in the future?
- has an analysis of the possible impact on the ISMS been carried out? Are there similar problems in other areas? See previous point!
- are the corrective measures taken in a balanced relationship between the effects of non-conformity and their costs?
- are the improvement measures taken effective? Have there been no side-effects that could lead to new, significant information security risks?
- have priority corrective actions (including deadline and person responsible) been planned?
- have corrective actions been carried out in accordance with the plan?
- have corrective measures been assessed to determine their effectiveness?

Overall, the handling process should achieve to a managed status regarding non-conformity and the associated consequences. However, it should be noted that corrections alone do not necessarily prevent the recurrence of non-conformity. The evaluation should be impartial, evidence-based, documented and communicated to

the relevant roles and interested parties. All non-conformity management and corrective action management measures (e.g. root cause analysis, audit, decision to implement measures, review and change decisions for the ISMS itself, efficacy assessment) should be kept in a documented form in order to achieve further improvement.

5.8.4 Documentation and communication

In every phase of the HS-UNI-ISMS process important information is generated, which has to be documented. Proper documentation increases the effectiveness of the HS-UNI-ISMS. The documented output of a phase is the basis and input for the subsequent phases within the HS-UNI-ISMS process and for the subsequent iterations of the entire HS-UNI-ISMS process. Only complete and proper documentation can be used to verify the results of the previous phases and, if necessary, to improve them.

Furthermore, documented information is essential to identify and communicate information security goals, policies, guidelines, instructions, directives, controls, processes, procedures for information security and audits and to determine which people are involved and how they should behave.

In particular, important decisions for the implementation or omission of a certain action for reasons of comprehensibility and liability should be documented without fail.

It is especially important to note that when people in key roles leave the university without documented information, the maintenance of an effective HS-UNI-ISMS is at risk.

Depending on the size and protection requirements of the university or the university of applied sciences, the main results should be documented. Each university or university of applied sciences can decide for itself how the documentation is to be done.

Each university should define a documentation approach that includes a clear structure that allows for quick, easy and unambiguous identification. The documentation should of course always be up to date.

At least, however, documentation should be provided on the following aspects:

- the results of the context establishment, the definition of the scope and boundaries (see 5.2);
- the resources (financial, personal, infrastructural) determined and provided and the expected competence

- the roles, responsibilities and authorities (see 5.1)
- policies, rules and directives for directing and operating information security activities (see 5.3)

- processes and procedures used to implement, maintain and improve the ISMS (see chapter 5)
- plans and results of awareness activities (see 5.5);
- reports of the risk management (see 5.7);
- reports of communication activities (see 5.8);
- processes and procedures used to implement, maintain and improve the ISMS and the overall information security status (see 5.8);
- results of ISMS processes (e.g. incident management, access control, information security continuity, equipment maintenance, etc.).

Once the documented information has been verified and approved, it should be communicated to the target audience. The documented information should be available everywhere and at all times, while maintaining integrity, confidentiality and relevance.

The continuous **communication** is a key role not only in the risk management process, but also in the entire HS-UNI-ISMS process. In order to introduce, implement, maintain and improve an effective HS-UNI-ISMS, the focus is on continuous communication.

Communication should take place regularly between all persons involved at all levels of the university or with external interested parties.

In order to be able to operate an effective HS-UNI-ISMS, not only the communications processes, communication channels, the communications point in time, the communications structure, the content of communication, but also the way e. g.. orally, in writing analogously, in writing digitally, etc.) as communicated, defined and protected accordingly. It should be regulated, among other things,

- which process for everyday communication?
- who is allowed to communicate externally and internally (e. g. in special cases such as data abuse, security incidents)?
- when and how often communication takes place?
- what content is communicated to whom?
- which pre-defined emergency communication plans are used in the event of a crisis?
- what means and channels of communication?
- what classification of communication according to the requirements of the university?

A way must be found to ensure that the necessary information can be communicated to all parties involved at any time and that the protection of sensitive data (e.g. personal data, research data, and examination data) can be assured.

Especially in the event of incidents or crises, a fast, transparent communication channel is often the key to maintaining and strengthening confidence in the university's ability to ensure information security and to cope with unexpected situations.

- **Challenge:**

The design of the HS-UNI-ISMS is a challenging task. Because in this final process step of the HS-UNI-ISMS project, the activities that have to be planned in advance are converted into functioning and controlling processes. However, this can only be done if activities such as determining the scope and boundaries of the information security management system, adopting an ISMS policy, obtaining resources for handling an HS-UNI-ISMS project, conducting an information security requirement analysis or the whole planning process of the HS-UNI-ISMS project handling, from the previous project phases were carried out correctly and completely. For example, there may be major difficulties in risk management if no proper, correct, iterative and above all change-sensitive risk planning has been carried out. A sophisticated risk planning, however, can only be based on a correct prior information security requirements analysis and an exact definition of the scope and boundaries often he HS-UNI-ISMS. If, for example, information security requirements analysis does not completely and correctly determine and classify the values, effective risk planning and risk treatment is not possible, since this was then carried out on the basis of incorrect results. With an incorrect or incomplete risk treatment, an effective HS-UNI-ISMS cannot be carried out and therefore information security at the Bavarian universities and universities of applied sciences cannot be guaranteed.

From this it can be seen that this last step of the HS-UNI-ISMS project handling can only be carried out successfully if all previous project phases are carried out correctly. The entire HS-UNI-ISMS process is an iterative cycle according to the Plan-Do-Check-Act cycle according to Deming, which is based on the previous phases. If a phase is not carried out completely and correctly, the subsequent phases cannot provide meaningful results.

In order to be able to carry out continuous improvements throughout the entire process and thus ensure an effective HS-UNI-ISMS, performance evaluation is of great importance. A challenge can be to define the correct attributes for the measurement.

It is helpful to decide on this definition with the help of all involved knowledge carriers. This can, of course, take longer to reach agreement on the definition of performance criteria. However, a meaningful performance evaluation of the HS-UNI-ISMS can only be carried out with the help of correctly defined criteria.

If performance evaluation is carried out by internal auditors, two important factors should be taken into account. On the one hand, the auditor should be familiar with the internal processes of the respective university or university of applied sciences, but on the other hand, he or she should also be independent and not professionally blind and possess sufficient skills to be able to carry out a sophisticated audit. A central auditor for all Bavarian universities of applied sciences and universities with sufficient audit

expertise and knowledge within the university sector would certainly be a suitable solution.

Furthermore, management reviews should take place on a regular basis in order to assess all processes, identify opportunities for continuous improvement, and highlight the need for changes to the ISMS, such as changes in information security policy and objectives, changes to risk acceptance criteria, changes in resources or the ISMS budget.

A management review can be problematic if there is too much detailed, unstructured and unprocessed information. Often the university's top management does not have detailed expert knowledge of the individual areas, but must nevertheless be able to form a comprehensive picture in order to initiate all improvements and changes. For the entire performance evaluation process, it is therefore of decisive importance that the results from all phases are prepared appropriately and that the degree of detail is classified according to the necessity. Thus, with a continuous impartial evidence-based performance evaluation, iterative improvements can be implemented both in the risk assessment process and in the entire HS-UNI-ISMS process. Even if avoidable improvements are made, it is important to check if they are real improvements or if there are any weaknesses. All phases of the entire HS-UNI-ISMS process must be documented in detail according to their importance. As mentioned above, each phase with its individual steps and results is input for the next phase. For this reason, it is of great importance that all results are well structured and documented and communicated to the people involved. It is also important that the reasons for not taking certain actions are documented.

In order to be able to retrieve information not only in the event of a crisis, it is essential to have a well-structured procedure for documenting information and results.

Documented information is a key component in the entire HS-UNI-ISMS process and is therefore necessary, for example, to uniquely identify information security goals, policies, guidelines, instructions, directives, controls and processes and to communicate with the relevant target group.

Documented information must always be up to date and accessible to all persons involved at all times. A problem can arise if no prior definition of the communications process, communication channels, and the communications point in time, the communications structure or the content of communication is specified.

A central distribution list for all authorized users, a digital notice board with different authorizations, and weekly or daily short update meetings might prove helpful. It is also essential that an emergency communication plan in the event of a crisis is defined in advance and communicated to all persons involved from the outset. Since sensitive data such as research data, personal data and examination data are handled in the higher education sector, it is vital to find a way of preserving the confidentiality and integration of sensitive data, while at the same time ensuring that all important data is available at all times. Transparent communication is the key component to maintain and strengthen trust in the university's information security, not only in times of crisis.

6 Checklists for implementation the “HS-UNI-ISMS”

In this chapter, universal checklists are created for each phase of the newly developed HS-UNI-ISMS. Based on these checklists, this master thesis enables all Bavarian universities and universities of applied sciences to create, implement, maintain and improve their own HS-UNI-ISMS, which is tailored to the local characteristics of each individual university or universities of applied sciences.

With the help of these checklists, an important step has been taken towards guaranteeing information security in the Bavarian higher education sector.

Action	In progress	Done / is available	Not finished /is not available
1. Obtaining management approval			
Before the management approval is obtained: Is there a rough concept with a rough milestone plan, including financial, personal and functional planning to establish the ISMS?			
Has top management allocated resources with financial means, facilities, technical infrastructure and appropriately qualified staff by assigning security roles with decision-making authority?			
Has an information security officer been appointed by the top management?			
Has the university's management demonstrated leadership and commitment of the university by assigning information security responsibilities to appropriately qualified manpower?			
Has the university ensured that the objectives of information security are compatible with the strategic orientation of the university and the integration of			

Action	In progress	Done / is available	Not finished /is not available
requirements and controls into the university's processes?			
Which decision-makers have a positive attitude towards an ISMS ?			
2. Determining the scope and boundaries of the information security management system			
Have all the external topics been analyzed? (E.g. social and cultural, political, legal, normative and regulatory, financial and macroeconomic, technological, natural, competitive)			
Have all internal issues been analyzed? (E.g. the university´s culture, policies, objectives, governance, organizational structure, roles and responsibilities, standards, guidelines and models adopted by the university, contractual relationships, resources and knowledge, physical infrastructure and environment, information systems, information flows and decision making processes)			
Are all interested external and internal third parties identified?			
Are all internal and external issues and their dependencies exactly described?			
Is there a uniform conceptual hygiene in the ISMS environment?			
Are the boundaries exactly defined?			
Are the out-of-scope areas exactly defined?			
Has any exclusion from the scope of the ISMS been justified?			

Action	In progress	Done / is available	Not finished /is not available
Has every exclusion from the application area been documented?			
Are there gaps in knowledge between the processes or between the knowledge carriers of the individual areas of responsibility? If so, have they been documented?			
Have you constantly checked the scope and requirements of the ISMS?			
3. Determining an ISMS policy			
Are the objectives of information security identified and defined?			
Are the requirements and objectives of information security always kept up to date?			
Does the policy contain short, comprehensible directional and orientation statements at a high level with regard to the university's information security?			
Has an overarching policy been created on which other thematic policies are based?			
Have the following aspects been taken into account when developing the policy? • aims and objectives of the university • strategies adopted to achieve the university´s objectives • the structure and processes, • aims and objectives associated with the topic of the policy • the requirements of related higher level policies • the target group of the policy			

Action	In progress	Done / is available	Not finished /is not available
Does the structure of the ISMS policy include the following issues? • Administrative issues • Policy summary/ Introduction • Scope • Objectives/ Key outcomes • Principles • Responsibilities • Related policies • Policy requirements			
Did the top management of university sign off the policy?			
Did an announcement of the ISMS policy to all university's employees, professors, students and third parties involved, take place?			
4. Obtaining resources			
Has the university management or the Bavarian state administration made sufficient resources available for dealing with the ISMS?			
Was a rough resource calculation and planning executed?			
Are there sufficient human resources available to handle an ISMS?			
Is there a sophisticated information security organization in which everyone involved can communicate with each other?			
Is there a clear task definition for the Information Security Officer and his or her team?			

Action	In progress	Done / is available	Not finished /is not available
Is the Information Security Officer's Office an independent body? (instead of being an IT administrator who receives instructions from other sources at the same time)			
Does the Information Security Officer and his or her team have appropriate professional knowledge, empathy and a high level of communication skills?			
Does the Information Security Officer have leadership and trainer qualities?			
Does the Information Security Officer regularly attend training courses and conferences?			
Is there a sufficient time frame for the execution of the project?			
Are there enough financial resources to acquire, develop and implement all necessary tools and infrastructure?			
Are there adequate information resources to support decision-making, measure the performance of actions and improve knowledge?			
Is an infrastructure and other means of evaluating, acquiring, maintaining or improving information security (e.g. license for advanced tools) available?			
Were technical security measures embedded in a suitable organizational framework with appropriate personnel, time and financial resources?			
Is the design of the security strategy consistent with the University's economic aspects? Does each security measure meet the cost-benefit ratio?			

Action	In progress	Done / is available	Not finished /is not available
5. Awareness of all university's members			
Has an awareness concept been developed for different target groups (e.g. management, administrator, users and students)?			
Has awareness training been carried out for all members of the university?			
Have the negative consequences of non-compliance with ISMS requirements been identified and communicated?			
Do all parties involved know that there is a HS-ISMS policy? Do the persons involved accept the derived goals and requirements of the HS-ISMS Policy and implement them?			
Are reporting ways defined and communicated in the event of an incident?			
Are individuals encouraged to be responsible for their own conduct to protect the assets of the university?			
Were people asked to notify the contact person of any identified vulnerabilities?			
Has a plan been established to communicate important topics at regular intervals or at any change in the university's general policy or information security policy?			
Has the knowledge and understanding of information been tested during and after awareness training?			
Has the works council's right of co-determination been respected in awareness-raising programs?			

Action	In progress	Done / is available	Not finished /is not available
6. Conducting information security requirements analysis			
Are all assets (primary and supported) identified ?			
Are all dependencies between the assets identified?			
Are all assets, their dependencies and their context exactly described?			
Have criteria been defined for the asset classification?			
Have all assets and their dependencies been classified?			
Are the criteria for asset classification clear and unambiguous?			
Have all non-documented ways of working been transferred into documented processes?			
Were the lived processes documented retrospectively?			
Has each asset a responsible person assigned to it?			
Is the inventory up-to-date?			
7. Planning Risk Assessment - Identification-Estimation-Evaluation			
Has a case distinction been made to determine the requirement for protection?			
Has the context (internal, external) been established?			

Action	In progress	Done / is available	Not finished /is not available
Have the criteria for impact, probability and risk been clearly and unambiguously defined?			
Are the criteria for assessing and accepting risks defined?			
Are the scope and limits of applications and the establishment of a risk management organization specified?			
Have all risks been fully identified?			
Have all vulnerabilities been completely identified?			
Have all threats been fully detected?			
Have all impacts been fully identified?			
Have experiences from previous incidents or risk assessments been included in the current risk assessment?			
Has a suitable risk analysis method been selected and applied?			
Has the risk level been compared with the criteria of risk acceptance and risk evaluation?			
Have these criteria been updated or redefined?			
Has it taken in consideration that the aggregate of many weak risks can represent a very high overall risk?			
Has the risk assessment been carried out systematically and under the same conditions as previously defined in order to obtain comparable, reproducible results?			
Has the risk assessment process been repeated regularly?			

Action	In progress	Done / is available	Not finished /is not available
Have the risks been priorised?			
Has a suitable option (risk reduction, risk retention, risk avoidance and risk transfer) been selected for risk management?			
Has the balance between the cost of security measures to the value of the property to be protected been maintained?			
Has an effective risk treatment plan been developed?			
In the case of a risk acceptance measure, has it been ensured that the residual risk is explicitly borne by the management level of the university?			
Have the risks been communicated to all participants in the appropriate form and in the appropriate depth of detail?			
Is the entire risk management process regularly iteratively reviewed and improved?			
8. Designing the ISMS			
Has a final HS-UNI-ISMS-project implementation plan been created?			
Were changes (intentional or unintentional) during operation of the ISMS evaluated and integrated into the current process?			
Has the risk management plan been implemented or updated according to a predefined timetable or in response to significant changes or incidents related to information security?			

Action	In progress	Done / is available	Not finished /is not available
Has a performance evaluation (e.g. internal audit) of the ISMS been performed regularly?			
Has a management review been conducted at least once a year?			
Has a transparent, fast communication channel been established to transmit information to all parties involved, not only in the event of a crisis?			
Has the ISMS been regularly reviewed in an iterative process for its suitability, effectiveness and compliance with the university's goals?			
Has the ISMS been regularly improved in terms of suitability, appropriateness and effectiveness?			
Has every phase of the HS-UNI-ISMS been documented in a suitable form?			
Was a documentation approach defined that includes a clear structure that allows quick, easy and unambiguous identification?			
Is the documentation up-to-date?			

Figure 16: Checklist HS-UNI-ISMS

7 Exemplary handling of a HS-UNI-ISMS with the processes “Recording of marks” and “Access control with the campus card” at the University of Applied Sciences Augsburg

In this chapter, this master thesis describes the handling of the HS-UNI-ISMS in an exemplary way. Based on the results of a rough risk tolerance table, the processes "Recording of marks" and "Access control with the campus card" were classified as very critical. Thus, the newly developed HS-UNI-ISMS from Chapter 5 is applied in a model-like manner to these critical processes.

In order to implement, maintain and improve an effective HS-UNI-ISMS, all aspects of information security must be considered. For this reason, the process was conducted according to the criteria of hardware, software, organization and personnel. This makes it possible to gain a complete overview of the entire critical process. This is the basis for a correct scope and boundaries definition. The output of this step is a very important input for the following steps.

This master thesis focuses on the HS-UNI-ISMS process steps scope and boundaries definition, conducting the information security requirements analysis and the planning of the risk assessment and the risk treatment for the critical processes "Access Control with the campus card" and "Recording of marks".

The process steps "obtaining management approval for initiating an ISMS project, obtaining resources, determining an ISMS policy and all awareness measures" are dealt with centrally. The final process step designing the HS-UNI-ISMS is also carried out on a centralized basis.

7.1 General central steps in dealing with the HS-UNI-ISMS

In this chapter, the general steps in handling the HS-UNI-ISMS are performed centrally for effective reasons. The process steps "obtaining management approval for initiating an ISMS project, obtaining resources, determining an ISMS policy and all awareness measures” are strategic tasks that have to be defined and determined, regardless of which sub-areas are considered in detail. Thus, these steps are carried out independently of the exemplary processes "Access Control with the Campus Card" and "Recording of Marks".

For reasons of scope, however, these general steps are only briefly explained. For detailed information please read chapter five.

7.1.1 Obtaining management approval for initiating an ISMS project

In order to be able to introduce an ISMS, the first step is always the approval of the top management of the University of Applied Sciences Augsburg. This is done by order of the Bavarian State Ministry.

Top management of the University of Applied Sciences Augsburg bears overall responsibility for the ISMS by allocating competencies to the university or by providing resources for the actual work. Before the management's approval was obtained, a rough concept with a rough milestone plan, including financial, personal and functional planning to establish the ISMS, was elaborated. This first step is considered given in this exemplary consideration. For further detailed information, please refer to item 5.1.

7.1.2 Determining the scope and boundaries of the information security management system

This process step is of great importance, as the result of this step has a strong influence on the subsequent process steps. Without a correct and complete scope and boundaries definition no meaningful information requirement analysis is possible, therefore no risk assessment and consequently no effective HS-UNI-ISMS.

In order to be able to carry out a significant scope and boundaries definition, an exact process survey of the processes to be considered must first be carried out in addition to the aspects mentioned in chapter 5.2.

With the help of a rough risk tolerance table (see chapter 5.2), the highly critical processes can be identified at the beginning. The table is not exhaustive and is only used as a model here.

Problem or Risk	Level 1 not significant	Level 2 serious	Level 3 very serious	Level 4 seriously critical
Student data or stored documents have been manipulated. (Marks, ECTS points, certificates)		Approval certificates or individual marks, ECTS points have been manipulated	Exam results or ECTS points were manipulated several times	Complete diplomas and certificates have been manipulated or reprinted
Information (notes, certificates) were published without authorization		Information about a single non-public student has been published	Information about a group of unknown graduates has been published	Information is freely available. Information about one or more prominent persons is available or has been published
Personal data of HSA staff or confidential information of the HSA has been published	Individual internal documents related to university members have been published	Individual confidential information or contact details of university members have been published	Personal data of university staff or large amounts of internal or confidential information have been published	Personal data that threaten the well-being of university members or' secret' information has been published
unauthorized access to the HSA campus or building	unauthorized access to the HSA campus	unauthorized access to HSA buildings	unauthorized access to confidential buildings	unauthorized access to strictly confidential buildings
Failure of the IT infrastructure	Failure shorter than 4h	>=4h to <24h	>=24h to <4 days	>4 days
…				

Figure 17: Risk tolerance table

The associated scope and boundaries definition, based on the asset identification, assessment and classification of the critical processes "Access Control with the Campus Card" and "Recording of marks" is described in chapter 7.2.1 and chapter 7.2.2 respectively.

7.1.3 Determining an ISMS policy

This process step of the HS-UNI-ISMS is not discussed here for reasons of volume. Since the setting of an ISMS policy is a strategic issue, the ISMS policy is set once for the entire University of Applied Sciences Augsburg, regardless of whether the process access control with the campus card or recording of marks is considered as an example in this master thesis. Derived from the high-level ISMS policy, special detailed guidelines for the considered processes could be established. For further information please read chapter 5.3. or Annex A.

7.1.4 Obtaining resources

This process step includes build an information security organization, build an information security team and provide resources for the infrastructure, the equipment and the organization. Resources include human resources, time resources, financial resources, information resources and infrastructure resources.

In chapter 5.4, a human resource analysis was carried out for the entire HS-UNI-ISMS-project at the University of Applied Sciences Augsburg. For the processes access control with the campus card or recording of marks, an explicate resource analysis is neglected in this master thesis for reasons of size and complexity.

7.1.5 Awareness of all university’s ‘employees and staff

This process step is only briefly dealt with in this master thesis for reasons of size. As described in chapter 5.5, awareness measures should affect all hierarchies, from top management of the university to the students. Possible awareness measures in the area of access control would be, for example, hints on the correct use of the Campus Card, such as the safe custody of the Campus Card against theft or loss, or awareness of locking the doors to sensitive research laboratories or awareness measures in the area of social engineering. Possible negative consequences could also be identified. In addition, a declaration of consent could be signed for safe use of the Campus Card, which describes liability for possible negative consequences from all the owners of the Campus Card for signature. It is important for these awareness measures that the members of the university understand, accept and above all want to apply awareness measures. It is also important that an emergency plan exists in the event of a crisis

and is communicated to the members of the university. A comprehensive awareness concept containing the contents described in chapter 5.5 should be worked out in this step.

7.2 Conducting information security requirements analysis

In this process step, the assets of the universities are determined, valued and categorized based on a comprehensive process description. This process step is very essential because it is the basis for a comprehensive risk management and hence for an effective HS-UNI-ISMS. According to the scope of the information security requirement analysis, the following risk management is performed.

In an effort to achieve a meaningful result, the inventory has to be precise, up-to-date and comprehensive. As already discussed in chapter 5.6, an inventory of all university information resources needs to be managed and controlled by a responsible person. In addition, the specific owner of the asset ought to specify that all assets are inventoried, classified and hedged.

At present, however, there is no systematic inventory of the values at University of Applied Sciences Augsburg. Consequently, either the values are recognized or the corresponding owners of the identification asset are identified, so that no classification of the values could be made.

In the ensuing, this master's thesis will provide an exemplary inventory of the values with the appropriate asset owner for the processes “Access control with the campus card” and "Recording of marks".

This classifies the values identified as examples. It should be considered that the value identification and classification is only model-based due to the scope of the model and does not guarantee completeness.

7.2.1 Access control with the campus card

In this subchapter, this master thesis illustrates the sub process step conducting an information security requirements analysis using the critical process "Access control with the campus card" as an example. Starting with a comprehensive process description, an asset identification, assessment and classification is carried out within information requirement analysis.

7.2.1.1 Process description

An exact and complete process description is the basis for all subsequent steps.

For this reason, a process survey of the infrastructural component access control with the campus card is carried out in the areas of software, hardware, organization and personnel. So far, there is no comprehensive process documentation of this. In some cases, lived processes exist; in others, individual process fragments exist without an overarching connection. Without a comprehensive process context, no serious scope and boundaries definition is possible; consequently, no useful information requirement analysis is realizable. For this reason, the following is a comprehensive process overview of the infrastructural component access control with the campus card in the areas of software, hardware, organization and personnel. The following information is based on interviews and information from the computing center staff.

- Hardware:

An RS485-based RFID card reader is attached to each door of the University of Applied Sciences Augsburg buildings, which manages access control on the campus. In addition, there are also RS485-based RFID card readers at all barriers that regulate access control at University of Applied Sciences Augsburg. In order to gain access to the campus area or to certain rooms within the university, the Campus Card must be held in front of the card reader with appropriate rights. Each card reader is marked with an individual number, so that it can be clearly traced which card was used at which card reader at which point in time.

The card reader " VOXIO-A-1200-A-advant RS485 " is connected to an additional device via an I^2C-Bus interface with an I/O box.
The front module of the reader is equipped with three LED fields in green, yellow and red as well as a piezo buzzer (as horn) for optical and acoustic user information. A control mechanism is also integrated, which is activated when the transparent cover is removed. A host computer via an RS485 communication interface controls the readers.

The readers have two operating modes offline and online. In offline mode, no cards or inputs are read out. In this offline mode, the yellow LED flashes as a circular circle symbol. After switching on the devices, they first go into offline mode. They automatically switch to online mode when they receive messages from their host system. The reader is only active in online mode and reads the cards held in front of it. The readers automatically switch back to offline mode if they have not received any messages from the master for more than 10 seconds. The readers handle all communication with the campus cards, „legic advant card“, independently.

Figure 18: Card reader [own picture]

The card reader is connected to the accessory device, the I/O box, for door monitoring and door control. The connection is made via an I²C bus interface. The I/O box has two digital inputs and outputs each with two relays. This enables the status of the door contacts in the doors to be determined. However, the I/O box cannot be addressed directly, but always receives its commands from the reader via the I²CBus.

The exchange of messages between the host and the reading devices takes place with the protocol "phg_crypt", via RS485 busses in the master-slave procedure with the host. Communication takes place via a polling procedure. Certain commands are sent to the readers, e.g. open doors and switch on the corresponding LED. Messages are encrypted using the AES encryption method, in which all devices of the same system use the same secret key. Each time the system is rebooted, it is recreated and saved to a file on the host.

All settings of the card reader are permanently stored in the reader's EEPROM. However, there are no specific security settings, such as login security settings, upload of AES encryption parameters, upload of MIFARE parameters, which could prevent unauthorized modification of the parameter settings of the readers.

Figure 19: I/O-Box [67]

The Campus Card has been a legic advant card since 2013. It contains a contactless chip for storing the data. Read and write access to the card is provided by a rotating antenna, which also serves to power the chip. Communication takes place using the AES-256 standard for data encryption.

The Campus Card Augsburg contains several independent data segments for storing information. The individual segments on the card are each protected with their own cryptographic keys according to their respective application (payment, library, badge, access control). The use of different cryptographically protected segments for the various applications is intended to ensure that the different applications can only access their own segments.

Figure 20: Campus Card [own picture]

If the Campus Card is held in front of the card reader, a decision is made as to whether or not access is denied. Various feedback messages appear on the card reader

- Green hook symbol→ access guaranteed, the door relay is open, the door opener is switched on so that the door can be opened;
- round yellow symbol→"ready" status or flashing yellow symbol→"offline" status;
- Red cross symbol→ access denied

If the access is blocked, the door opener remains open for a maximum of 4 seconds. When attempting to sabotage the card reader, the red cross symbol illuminates.

Cameras are installed on the entire campus, especially at critical locations such as the computer center, the library in front of some research laboratories, to further secure access control. Please note that the card reader is only splash-proof, but not waterproof.

The clients are stored in locked electrical rooms. These rooms can only be opened by authorized persons with a special key. The doors themselves, which can be opened by the Campus Card, only have a snap lock. There is neither an airlock here, nor a real verification of who actually gains access..

HP switches exist at the network level, but routing is not possible here. The card readers on OSI layer two communicate with each other via IP. As shown in the following figure, the clients and the application server are located within the CCA-

VLAN. The Sever application is located next to the LDAP database, the SQL database and the web server in the server-VLAN. An 802.1x protocol does not exist [70].

The following graphic shows the schematic structure of the Access control.

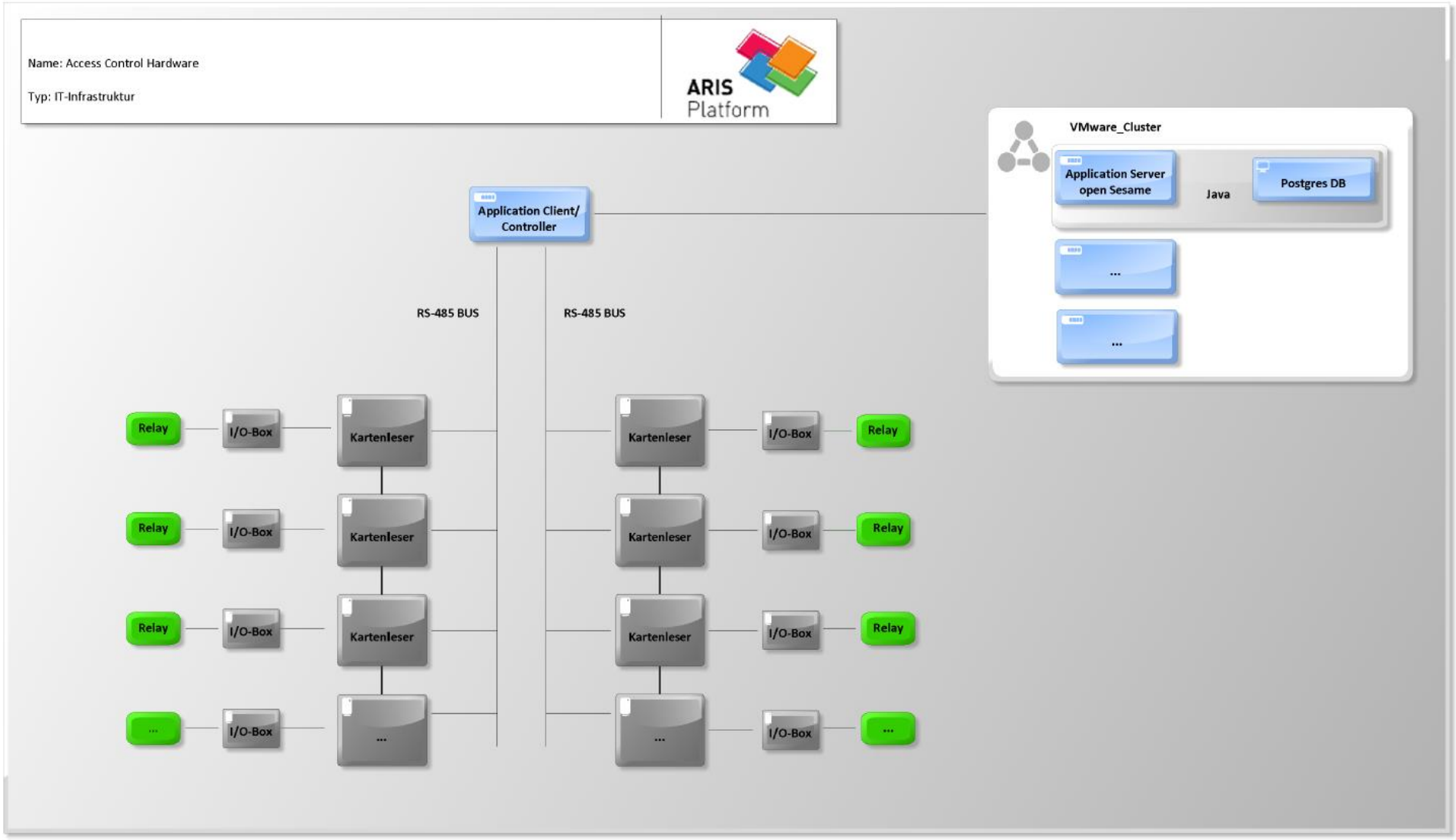


Figure 21: schematic structure of the access control [own preparation]

The Application Server Opensesame is connected to the Postgres database within a VMware cluster. The Application Server is connected to the Application Client. The client program controls two RS485 busses to which the card readers are connected, which are connected via their own I²C bus to the I/O box. At each I/O box, the door opener and the door contacts connected.

- Software

There is a client program for controlling the access control, which is connected to a server program via RMI interface over the network. The server program controls the client program. The client program controls the RS485 bus connected to the readers. Both programs are implemented in JAVA. The RMI encryption between server and client takes place via an RSA cipher. (SSL_RSA_WITH_RC4_128_MD5).

Additionally, the server and client are password-protected. These passwords are stored in a safe. Only three people in the data center have access to this safe.
The following code section shows an example of an access.

2017-07-06 20:21:51,570 [RMI TCP Connection(423291)-192.168.0.101] DEBUG phg.PHG_SERVER - Request received: RS485_Interface_Number(13), Reader_Number(7), LEGIC_Cardnumber(xxx)

2017-07-06 20:21:51,571 [Thread-11] DEBUG phg.PHG_WorkerThread - Room enter request: RS485_Interface_Number(13), Reader_Number(7), LEGIC_Cardnumber(xxx)

2017-07-06 20:21:51,641 [Thread-11] DEBUG phg.RMI_Client - Open door : RS485_Interface_Number (13), Reader_Number(7)

2017-07-06 20:21:55,647 [Thread-11] DEBUG phg.RMI_Client - Close door: RS485_Interface_Number (13), Reader_Number(7)

A Campus Card is held at card reader 7. Using the RMI interface and TCP connection, a room enter request is started in system 13 on card reader 7.

There are different states of access control. The server program decides which of the states has occurred on the basis of the determined data from the database. To do this, the client program must send the card number read out to the server program.

The server program is connected to the Postgres database and checks whether access is granted by means of data received from the client program. If access is permitted, the door opener is switched on for four seconds. The server program controls the client program by informing the client program of the states it has to take with regard to the optical, acoustic display elements and the door release relay.

The communication between the client program and the reading devices takes place via an RS485 bus, which is carried out with the JAVA interface as an RXTX implementation.

The Application client is connected to the application Sever as described above.

The application server with the Web server and the SQL database is located within the VMWare cluster. Both the Sever application and the web server are powered by the SQL database. The LDAP database contains an IDM, which in turn fills the SQL database with important data such as personal data. The Postgres database contains the corresponding rights. The entire server architecture of access control can only be accessed in the university network.

The graphic below shows the system landscape of the Access Control. As you can see from the graphic, there is no three-tier architecture.

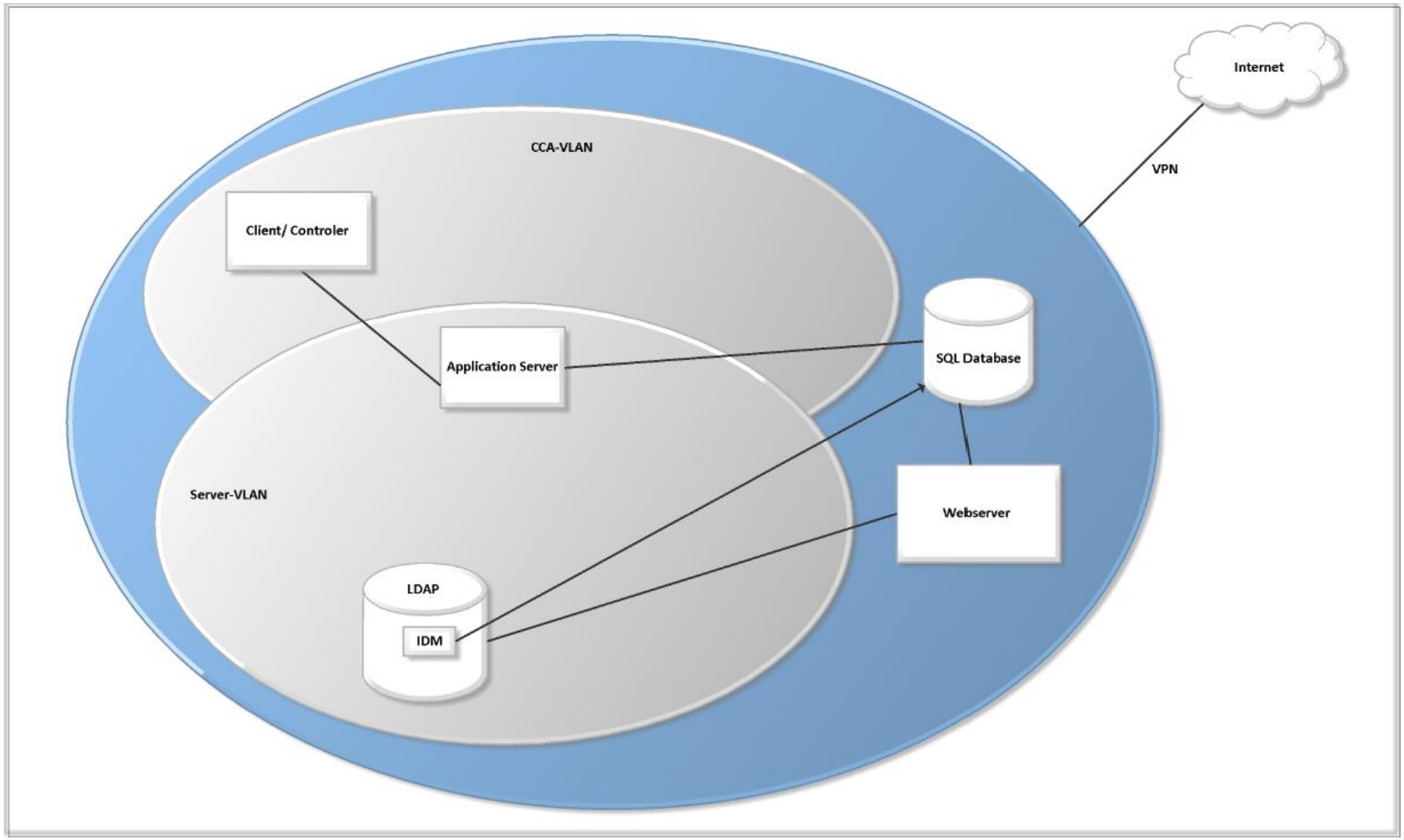


Figure 22: System landscape Access Control [own preparation]

- Organisation/Persons

Access control is organized as follows. There are blanket, default and special rights. The blanket rights depend on the faculty and course of study. According to the faculty and the course of study, special rooms are activated with time and day. Attributes, lecture time or semester break including holidays are also set.

The default rights are the same for each student and include the attributes evening and Saturday opening hours of the library, the opening hours of the data center rooms, the outside area of the campus and the opening hours of the barriers for the student car park. Employees or professors have extended default rights, such as access to all rooms of their faculty and access to the employee parking space. If, in addition to the blanket and default rights, a university member wishes to have additional access to certain areas or at certain times, special rights are required.

If special rights are required, the respective student or employee must submit a request to the professor or dean of the respective faculty.

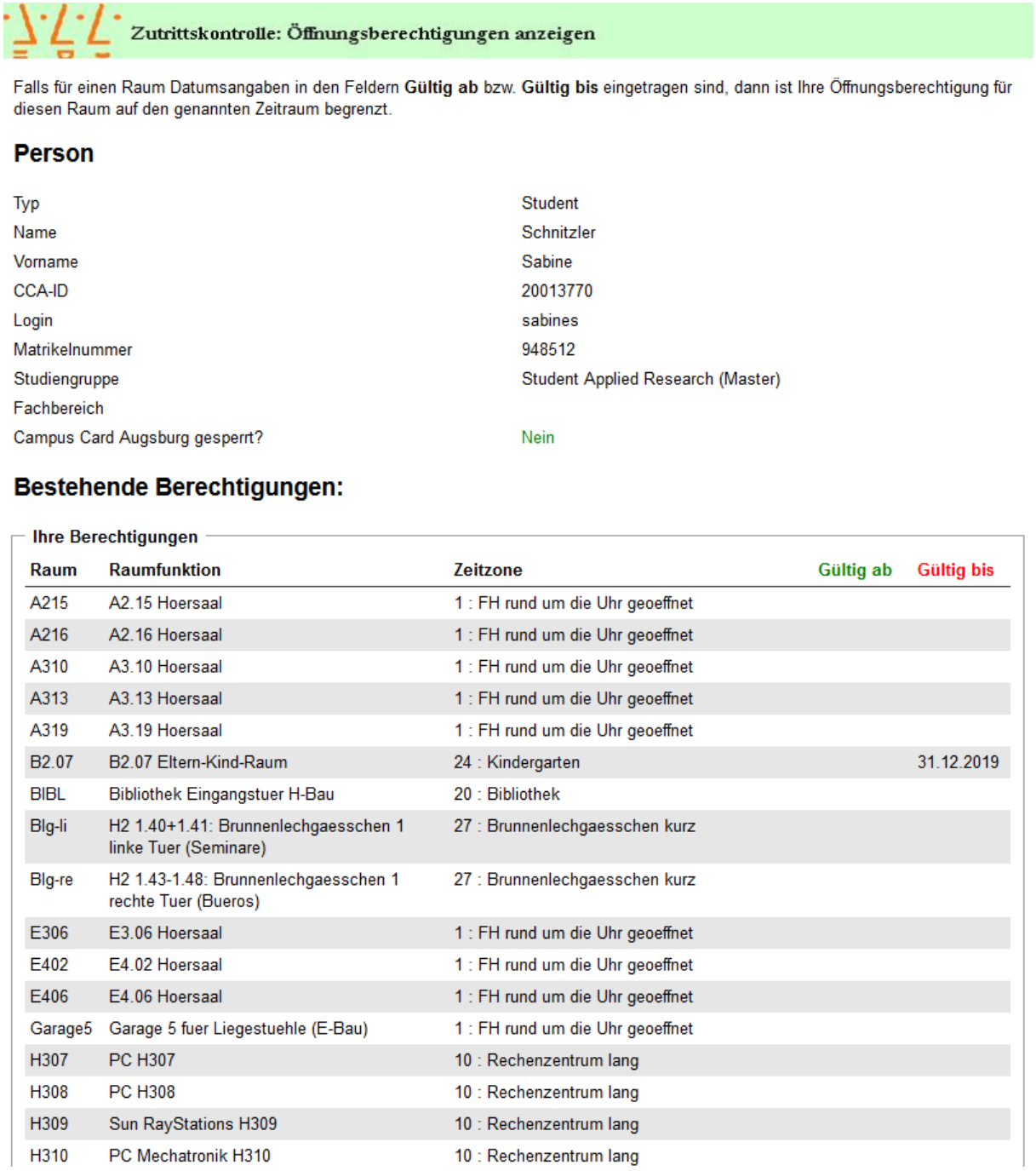
The professor or the dean must approve it and have it activated by the secretariat of the respective faculty. Authorized persons within the Secretariat are secretarial staff and faculty assistants. The activation is then done via a website. There, the authorized persons must enter their user ID and password in order to activate the system.

All special rights have a certain predefined validity date, such as the end of the semester or the end of an employee's contract.

However, default and blanket rights do not have a preset validity date. For example, if a student is de-registered, his or her access rights are only blocked after the HR department has notified the data center. It can take several days or weeks between de-registration and actual blocking of access rights, so that access is still possible during this time.

It is also possible to gain access to the network of authorities. This requires an employee campus card with a separate application. This part is not considered in this master thesis.

The following figure shows an example of a section of the author's access rights:



Zutrittskontrolle: Öffnungsberechtigungen anzeigen

Falls für einen Raum Datumsangaben in den Feldern **Gültig ab** bzw. **Gültig bis** eingetragen sind, dann ist Ihre Öffnungsberechtigung für diesen Raum auf den genannten Zeitraum begrenzt.

Person

Typ	Student
Name	Schnitzler
Vorname	Sabine
CCA-ID	20013770
Login	sabines
Matrikelnummer	948512
Studiengruppe	Student Applied Research (Master)
Fachbereich	
Campus Card Augsburg gesperrt?	Nein

Bestehende Berechtigungen:

Ihre Berechtigungen

Raum	Raumfunktion	Zeitzone	Gültig ab	Gültig bis
A215	A2.15 Hoersaal	1 : FH rund um die Uhr geoeffnet		
A216	A2.16 Hoersaal	1 : FH rund um die Uhr geoeffnet		
A310	A3.10 Hoersaal	1 : FH rund um die Uhr geoeffnet		
A313	A3.13 Hoersaal	1 : FH rund um die Uhr geoeffnet		
A319	A3.19 Hoersaal	1 : FH rund um die Uhr geoeffnet		
B2.07	B2.07 Eltern-Kind-Raum	24 : Kindergarten		31.12.2019
BIBL	Bibliothek Eingangstuer H-Bau	20 : Bibliothek		
Blg-li	H2 1.40+1.41: Brunnenlechgaesschen 1 linke Tuer (Seminare)	27 : Brunnenlechgaesschen kurz		
Blg-re	H2 1.43-1.48: Brunnenlechgaesschen 1 rechte Tuer (Bueros)	27 : Brunnenlechgaesschen kurz		
E306	E3.06 Hoersaal	1 : FH rund um die Uhr geoeffnet		
E402	E4.02 Hoersaal	1 : FH rund um die Uhr geoeffnet		
E406	E4.06 Hoersaal	1 : FH rund um die Uhr geoeffnet		
Garage5	Garage 5 fuer Liegestuehle (E-Bau)	1 : FH rund um die Uhr geoeffnet		
H307	PC H307	10 : Rechenzentrum lang		
H308	PC H308	10 : Rechenzentrum lang		
H309	Sun RayStations H309	10 : Rechenzentrum lang		
H310	PC Mechatronik H310	10 : Rechenzentrum lang		

Figure 23: Existing permissions for access control [own preparation]

After the process description of the Access control has been completed, the asset identification, assessment and classification must be performed. In the area of access control, all areas of hardware, software, organization and personnel are examined. However, for reasons of scope, only an exemplary consideration is given in this master thesis, so that only a few aspects are described in detail in the subsequent process steps of ISMS handling.

7.2.1.2 Asset identification – assessment – classification

In this process step the universities assets are identified, evaluated and then classified. This process step is very important because it forms the basis for a comprehensive risk management and thus for an effective HS-UNI-ISMS. The following risk management is carried out in accordance with the scope of the information security requirements analysis.

As already described in chapter 5.6, an inventory of all university information assets should be collected, managed and controlled by a responsible person. In order to obtain a significant result, the university of applied sciences' inventory must be accurate, up to date and complete. Furthermore, the respective owner of the asset should determine that all assets are inventoried, classified and secured.

However, there is currently no structured inventory of the values at the University of Applied Sciences Augsburg. Thus, neither the values are known nor the respective owner of the asset identified, so that no classification of the values could be carried out.

In the following, this master thesis will carry out an exemplary inventory of the values with the corresponding asset owner regarding the process "access control with the campus card".

As a result, the values identified as examples are classified. It should be noted that the value identification and classification is only carried out as a model for reasons of scope and does not claim to be complete.

- Primary assets:

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Business processes and activities	Guaranteeing access to the Members of the HSA to the respective rooms in order to impart or maintain teaching				x	Mrs. Example
Business processes and activities	Students can use the respective resources and facilities for research and teaching purposes			x		Mr. Xy

Information

Information	access logs			x		Mrs. Example
Information	authorization groups				x	Mrs. Example
Information	admin accounts				x	Mrs. Example
…	…					Mrs. Example

- Supporting Assets:

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Hardware	Campus card				x	Mrs. Example
Hardware	Card reader				x	Mrs. Example
Hardware	Application Client /Controller				x	Mr. Xy
Hardware	Application Server open Sesame				x	
Hardware	PC			x		Mrs. Example
Hardware	…					Mrs. Example
Software	software for card reader operation				x	Mr. Xy
Software	LDAP database with IDM				x	Mr. Xy
Software	SQL data base				x	Mr. Xy
Software	…					
Network	Communication (IP, IPSec, ..)				x	Mrs. Example
Network	Medium and supports (e.g. Wireless-Protokoll-Spezifikationen (z.B. WiFi 802.11)				x	Mrs. Example
Network	VLAN				x	Mrs. Example
Network	…					
Personnel	Authorized person who				x	Mr. Xy

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
	register the special rights (Card administrator)					
Personnel	Users (students)				x	Mr. Xy
Personnel	Users (staff)			x		Mr. Xy
Personnel	LDAP administrator				x	Mr. Xy
Personnel	…					
Site	examination office rooms				x	Mr. Xy
Site	Rooms in the computing center				x	Mr. Xy
Site	services for cooling the air, heating			x		Mr. Xy
Site	Door				x	Mr. Xy
Site	…					
Organization	Structure of the computing center				x	Mr. Xy
Organization	Process organization				x	Mr. Xy
	…					

Figure 24: Asset identification und classification - Access Control

7.2.2 Recording of marks

In this subchapter, the handling of the sub process step conducting an information security requirement analysis is described exemplarily by means of the sensitive process "Recording of marks".

7.2.2.1 Process description

In order to be performed an information security requirement analysis an exact process evaluation of the processes to be considered must first be performed in addition to the aspects specified in chapter 5.6.

For this reason, a process analysis of the process of recording marks is carried out and described in the areas of software, hardware, organization and personnel. So far, there is no comprehensive process documentation. In some cases, lived processes exist; in others, individual process fragments exist without an overall association. Without a comprehensive process context, no serious scope and boundaries definition is achievable. For this reason, the following is a comprehensive process overview of note recording in the areas of software, hardware, organization and personnel. The following information is based on interviews and information from the computing center staff.

- Organization/Personal

With the HIS Online Portal, students can register their exams and view exam results. At the same time, examiners can enter the examination results, the marks, via this web interface. The following figure shows the HIS Online Portal.

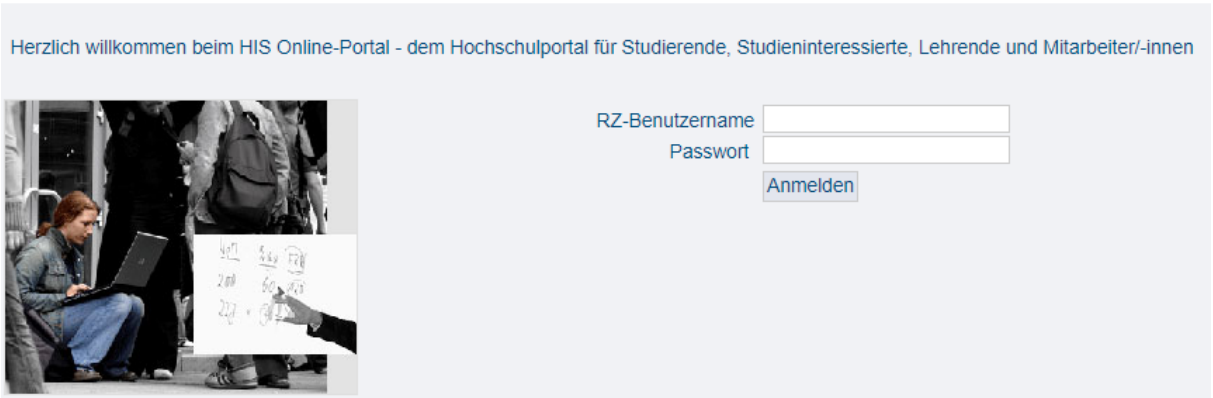


Figure 25: HIS Online Portal

The Recording of marks process starts by the student registering for one or more exams at the beginning via the HIS-online portal. For this purpose, the student logs into the HIS Portal with a user name and password. Using the data from the HIS Database and the LDAP Database, excel lists of all the data required for planning examinations at the faculties, such as the name of the student, the faculty, the course of study, the exam, etc. are generated.

These excel lists are emailed to the respective faculty using an encrypted AES algorithm and password, sent to the respective faculty, refused and reported back to the respective examiner. The HIS-admin checks whether the respective examiner has an authorized account for the respective exam and is therefore authorized to enter grades in the HIS portal. The examination committee appoints persons to record grades. As a rule, this is the first and second examiner.

If this is not the case, the process is stopped, the status is determined and corrected if necessary. Otherwise, a confirmation will be issued so that the examiner can enter the grades. The entry of the marks can only be made within a period fixed by the examination committee. It is not possible to enter the grades outside the deadline. In this case, the process is stopped. If the grades are entered within this period, the examiner presses on "Finish" so that the entry of the examination results is completed. The examiner must print out and sign the entered marks so that they can be filed in the examination office and stored in a paper form for possible disputes. The HIS administrator maintains the HIS portal including the HIS database. The student can view his or her grades via the HIS portal in time for review by logging in again with his or her user name and password. The examination office stores both the student's grades and the student's diploma for a certain period of time in paper form for reasons of monitoring. The following figure illustrates the described process.

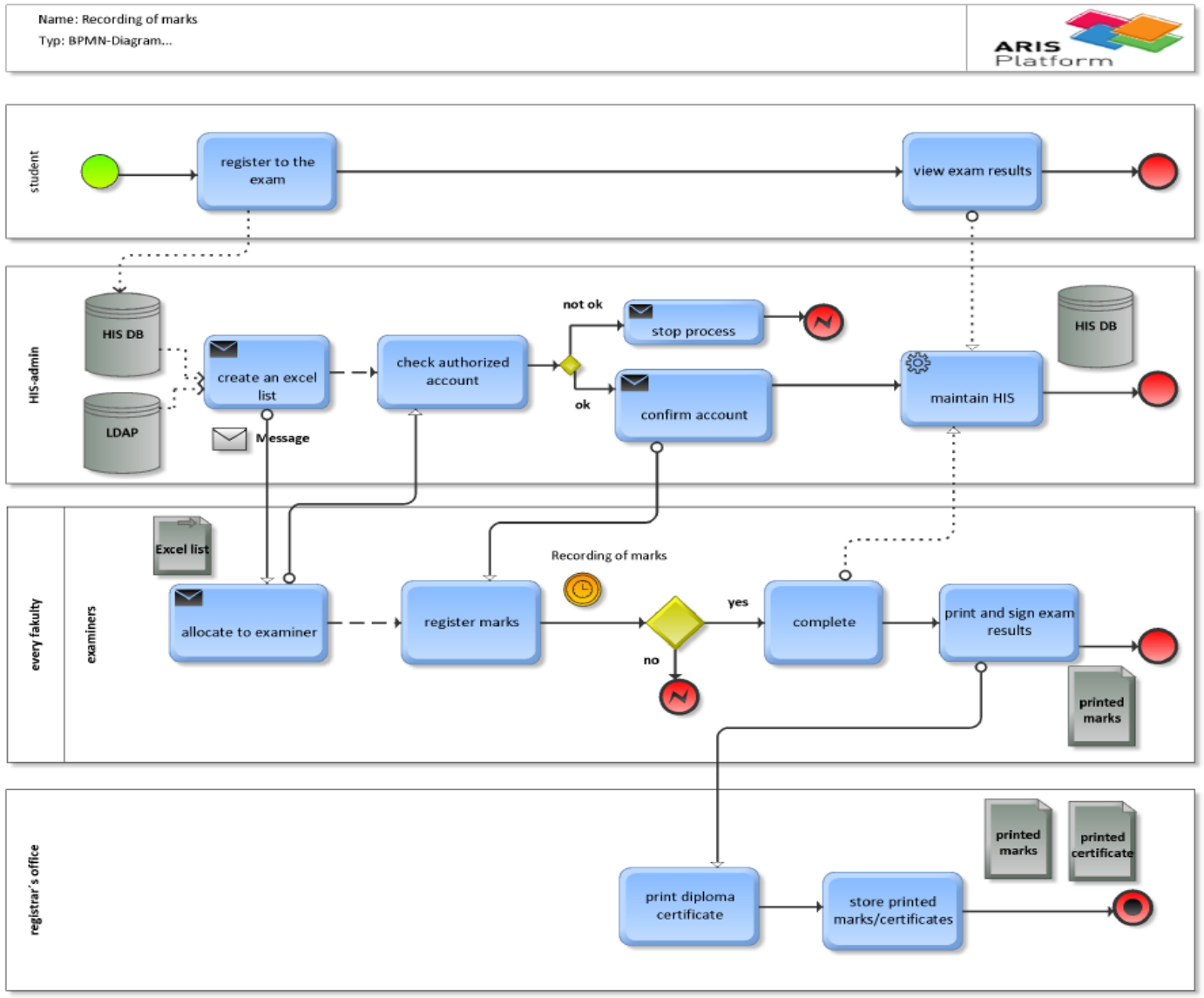


Figure 26: Recording of marks - BPMN [own preparation]

There are different roles with different rights, such as the student, the examiner, the administrative person in the examination office or the system administrator.

- Hardware/Software

The HIS Online Portal is a Java-based Tomcat Apache application that communicates with the database server. The application server accesses the production database of the examination administration directly.

The HIS application consists of the components HIS database, HIS application server for web applications (based on Apache Tomcat with a dedicated web server (forwarding requests to the application server) in the DMZ, user clients (users submit requests via browser to the web server) and HIS-GX programs of the student administration staff.

The HIS application was developed by HIS eG. The HIS administrator of the HSA can adapt the pre-defined templates and the Java classes according to your needs.

Because guidelines of the Bavarian State Administration apply to the higher education institutions' administrative network, [70] such as "BayITSiLL" [72] to an IT Security Policy for the Bavarian public administration or the "BayITSiR-02"[34] to special policy for the "Operation of a Transition to the Internet" must be implemented accordingly. As figure 29 shows, the web server is located in a DMZ, and the application server is located in the protected administrative network.

External access to the web server is only possible via an external packet filter as a pre-filter and via the Application Level Gateway (ALG). The ALG is the second protection component.

The third level of protection is the internal packet filter (PFL) between ALG and the administration network. This internal packet filter finally protects the internal administration area.

These levels are implemented by three physically separated machines. The ALG has network interfaces to the PFLs and coordinates the data traffic to the DMZ and the PFLs. This allows IP traffic between network segments to be controlled and sensitive zones to be protected. Communication takes place via IP.

The administrative network contains the components for handling highly sensitive data such as the Application Server, the HIS-database or the HIS-GX programs, administration staff PCs and others.

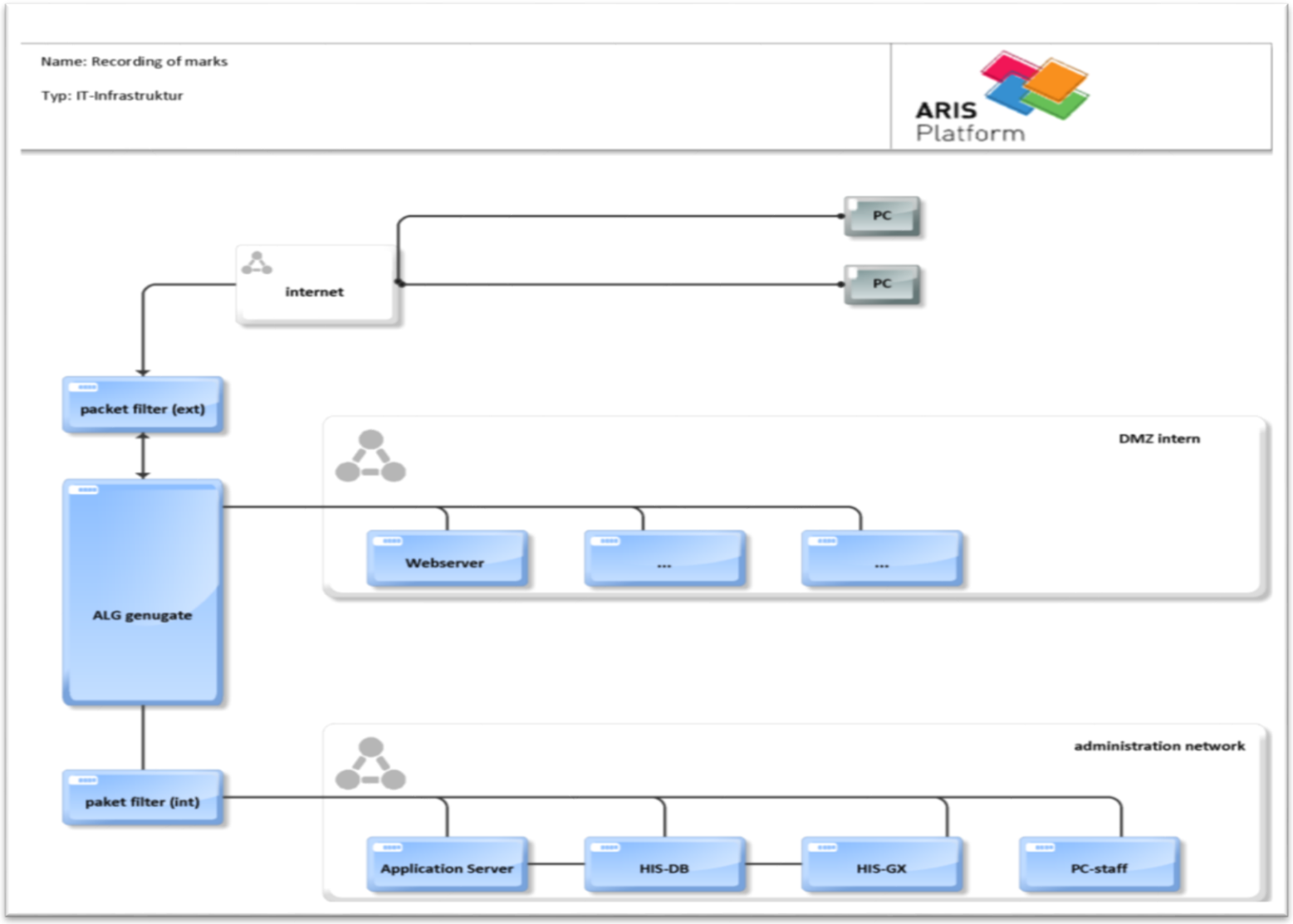


Figure 27: Recording of marks-three tier-architecture [own preparation]

The following communication protocols are used in the note acquisition process. The clients of the students and examiners access the web server via HTTPS, the web server and the application server communicate via AJP13 protocol [73]. To check the user passwords, the application server requires access to the separate authentication server LDAP.

The user (student or examiner) registers via the HIS portal. The LDAP is authentication. There is a bidirectional exchange of information between the HIS application and the HIS portal. The HIS database fills the IDM of the LDAP.

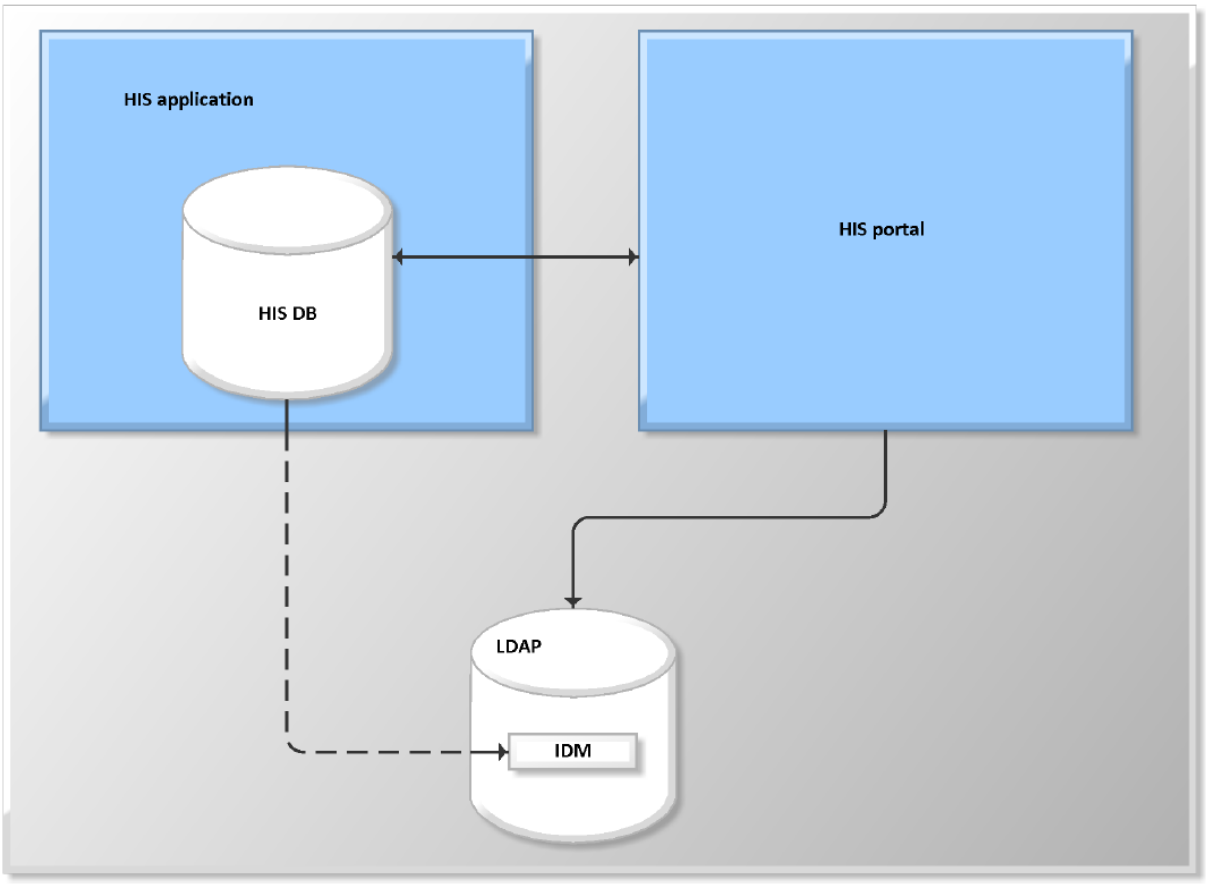


Figure 28: Information exchange [own preparation]

7.2.2.2 Asset identification – assessment – classification

In this process step, the assets of the universities are determined, valued and categorized. This process step is very essential because it is the basis for a comprehensive risk management and hence for an effective HS-UNI-ISMS. According to the scope of the information security requirement analysis, the following risk management is performed.

.

At present, however, there is no systematic inventory of the values at University of Applied Sciences Augsburg. Consequently, either the values are recognized or the corresponding owners of the identification asset are identified, so that no classification of the values could be made.

In the following, this master's thesis will present an exemplary inventory of the values with the appropriate asset owner for the process "recording of marks".

This classifies the values identified as examples. It should be noted that the value identification and classification is only model-based due to the scope of the model and does not guarantee completeness.

- Primary assets:

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Business processes and activities	Students can register for the exam				x	Mrs. Example
Business processes and activities	Examiners can enter marks				x	Mr. Xy
Business processes and activities	Examination office keeps the grades				x	Mrs. Example
Business processes and activities	Examination office prints the diploma certificate				x	Mrs. Example
Business processes and activities	Students can view their exam results		x			Mrs. Example

- Information:

Information	data about grades				x	Mrs. Example
Information	personal data				x	Mrs. Example
Information	overview of marks				x	Mrs. Example
…	…					Mrs. Example

- Supporting Assets:

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Hardware	Application Server				x	Mrs. Example
Hardware	Web Server				x	Mrs. Example
Hardware	ALG genugate				x	Mr. Xy
Hardware	user clients			x		Mrs. Example
Hardware	Laptop examiners				x	
Hardware	examination office clients				x	
Hardware	diploma certificate in paper form				x	Mrs. Example
Hardware	printed and signed marks verifications in paper form				x	Mr. Xy
Hardware	…					
Software	Software for HIS Portal (Java)				x	Mr. Xy, HIS eG
Software	LDAP database with IDM				x	Mr. Xy

Type of assets	Assets	Degree of negative consequences				Asset owner
		Negligible	Low	Medium	High	
Software	HIS data base				x	Mr. Xy
Software	…					
Network	Communication (IP)				x	Mrs. Example
Network	AJP13				x	
Network	…					
Personnel	Users (students)		x			
Personnel	Users (staff)				x	Mr. Xy
Personnel	Users (examiners)				x	
Personnel	Employees in the computing center				x	
Personnel	…					
Site	examination office rooms				x	
Site	office of the professor/examiners		x			
Site	Rooms in the computing center				x	
Site	services for cooling the air, heating			x		
Site	…					
Organization	Structure of the computing center			x		
Organization	Structure of the “recording of marks”			x		
	…					

Figure 29: Asset identification and classification - Recording of Marks [own preparation]

7.3 Planning risk assessment – Identification- Estimation- Evaluation

As already described in chapter 5.7, the Augsburg University of Applied Sciences' need for protection was classified as high, so that the ISO/IEC 27005 standard with its iterative risk management process is used.

In order to carry out effective risk management, the context is first of all determined. In this case, the context is the access control with the campus card respectively the recording of marks in which the risk management is carried out.

As described in chapter 5.2, defining the risk acceptance criteria is part of the context definition.

The risk acceptance criteria are defined as follows.

- 1 - 3: risk is accepted
- 4 – 9: risk is accepted with conditions
- >= 10: risk is not accepted

The next step is to start with risk assessment. Risks with regard to confidentiality, integrity, availability and risk owners and their consequences are identified and risks are assessed on the basis of risk criteria. The previously defined values are essential for risk identification. Furthermore, it is necessary to identify threats, vulnerabilities and their impacts as well as to identify the existing countermeasures.[71], [64].

Subsequently, a high-level risk assessment method is used for risk assessment in order to obtain an overview of the existing risks. A limited list of threats and vulnerabilities that have already been grouped by domain is analyzed to speed up the process. The focus is not on the individual element, but on the entire risk scenario.

For this purpose, an Impact-Likelihood-Matrix, similar to the figure 14, can be used for illustration (see figure 32).

Impact Likelihood	1	2	3	4
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4

Figure 30: Impact-Likelihood-Matrix [own preparation]

By multiplying the impact (I) with likelihood (L), the result is the existing risk value (R). The risks can then be categorized and prioritized according to their seriousness as described in chapter 5.7. The prioritization provides a high-level overview. The high level of abstraction of the risk assessment may, however, make it required to perform a further detailed iteration of the risk assessment in order to obtain a complete result.

Depending on the acceptance criteria previously set, a decision is made as to how to proceed in dealing with the risks. The prioritization of risks is already included in the risk treatment plan in this master thesis. As already described in the previous chapter, care must be taken to ensure that the trade-off between the costs of security measures and the values of the goods to be protected is in the right relationship. In addition, the chosen security measures should also be realizable [60].

In this procedure, the measures are prioritized so that a comprehensible overview of the risk situation is possible. However, due to the high abstraction level of the risk assessment, it may be necessary to carry out a second detailed iteration of the risk assessment in order to obtain a meaningful result.

7.3.1 Access control with the campus card

In this subchapter, a risk assessment for the critical process access control with the campus card is performed. The first step is to describe the context in which the following risk management is carried out.

All members (students, staff and professors) of the University of Applied Sciences Augsburg have a Campus Card to gain access to the campus and buildings. In addition, Campus Cards are also issued for non-members of the University of Applied Sciences Augsburg, e.g. for visitors to the library, for members of the kindergarten Kindernest. Suppliers generally do not have a Campus Card, but by registering in advance, they also have access to the HSA campus.

The following matrix illustrates a high-level risk assessment.

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
01	access logs in database	medium	information disclosure	authorized access, strong passwords	information disclosure with reduced likelihood	2	1	2	computing centre	Awareness, guidelines for handling with access logs, separated networks, authorized access, strong passwords
02	access logs in database	medium	tampering	authorized access, strong passwords	tampering with reduced likelihood	3	2	6	computing centre	Awareness, guidelines for handling with access logs, separated networks,
03	access logs in database	medium	non-availability	authorized access, strong passwords	non-availability	3	1	3	computing centre	Awareness, guidelines for handling with access logs, separated networks,
04	authorizatio n groups	high	Tampering	authorized access, strong passwords	Tampering	4	2	8	computing centre, human resources dep.	Awareness, guidelines, separated networks,

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
04	Authori-zation groups	high	information disclosure	authorized access, strong passwords	information disclosure	3	1	3	computing centre, human resources departmen t	Awareness, guidelines, separated networks
05	Authori-zation groups	high	non-availability	authorized access, strong passwords, back-up		2	1	2	computing centre, human resources dep.	Awareness, guidelines, separated networks,
06	admin password	high	information disclosure	strong passwords, password encryption	social engineering, shoulder surfing, phishing	4	2	8	computing centre	Awareness, guidelines, separated networks, two factor authentication
07	admin accounts	high	non-availability, tampering	reduced numbers of administrato rs, patches, updates	non-availability	4	1	4	computing centre	Awareness, guidelines, , additional security mechanism
08	Campus Card	High	theft	blocking card by computing centre, notice on website		4	2	8	Owner of the campus card	Awareness, self-service blocking of the card in case of theft by the owner

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
09	Campus Card	High	loss	notice on website	loss	4	3	12	Owner of the campus card	Awareness, self-service blocking of the card in case of loss by the owner
10	Campus Card	High	Spoofing, Skimming	No controls	Spoofing, Skimming	4	2	8	computing centre	regular control for skimming
11	Card reader	High	theft	No controls	theft	3	1	3	Card reader supplier, computing centre	additional security mechanism, cameras on each card reader, alarm function
12	Card reader	High	Destruction (human, nature etc.)	installed under the roof	destruction	3	1	3	Card reader supplier, computing centre	material for fire and water protection, protection against misuse, cameras on each card reader, alarm function

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities/ weaknesses	Impact	Likeli - hood	Risk	Risk owner	Actions
13	Card reader	High	tampering	no ones	tampering	4	3	12	Card reader supplier, computing centre	protection against misuse, additional security mechanism (secure login), cameras on each card reader, alarm function
14	software for card reader operation	High	Tampering, exploita-tion	patching	Tampering	4	3	12	Developer computing centre	Secure coding with additional security mechanism, penetration tests
15	software for card reader operation	High	Information Disclosure Denial of Service	No Controls	Information Disclosure	4	2	8	Developer computing centre	Secure coding with additional security mechanism, penetration tests

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
16	software for card reader operation	High	Denial of Service	No Controls	Information Disclosure	4	1	4	Developer computing centre	Secure coding with additional security mechanism, penetration tests
17	Application Client /Controller	High	Tampering	RSA Cipher. (SSL_RSA_ WITH_RC4 _128_MD5), physical protection	Tampering	4	2	8	computing centre	three tier architecture, separated network
18	Door	High	Information Disclosure	no control, only a snap lock	reduced Information Disclosure, Piggy Packing	4	3	12	university	additional security mechanism, airlock, ID check
19	Application Client /Controller	High	Spoofing	RSA Cipher. (SSL_RSA_ WITH_RC4 _128_MD5) physical protection, password protection	Man-in-the-middle	4	2	8	computing centre	three tier architecture, separated network, authentication

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
20	Application Client /Controller	High	Information Disclosure	RSA Cipher. (SSL_RSA_ WITH_RC4 _128_MD5) physical protection, password protection	Tampering	4	2	8	computing centre	three tier architecture, separated network, authentication
21	Application Server open Sesame	High	Spoofing, tampering	RSA Cipher. (SSL_RSA_ WITH_RC4 _128_MD5), password protection	Spoofing	4	2	8	computing centre	three tier architecture, separated network, authentication , compliance
22	SQL data base	High	Tampering	separate networks	Tampering	4	2	8	computing centre	three tier architecture, separated network, Access, Application Server has as minimum rights to the database

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
23	SQL data base	High	Information Disclosure	separate networks	Information Disclosure	4	2	8	computing centre	three tier architecture, separated network, Access, Application Server has as minimum rights to the database
24	SQL data base	High	Non-available	separate networks	Information Disclosure	4	2	8	computing centre	three tier architecture, separated network, Access, Application Server has as minimum rights to the database
25	LDAP database with IDM	High	tampering	Authorized access, separate networks	tampering	4	2	8	computing centre staff	awareness, additional security mechanism, three tier architecture

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
26	LDAP database with IDM	High	information disclosure	Authorized access, separate networks	information disclosure	4	2	8	computing centre staff	awareness, additional security mechanism, three tier architecture
27	LDAP database with IDM	High	Non-available	Authorized access, separate networks	information disclosure	4	2	8	computing centre staff	awareness, additional security mechanism, three tier architecture
28	CCA-VLAN/Server-VLAN	high	tampering	separate networks	tampering	4	2	8	computing centre staff	awareness, additional security mechanism, three tier architecture, 802.1x
29	CCA-VLAN/Server-VLAN	high	information disclosure	separate networks	information disclosure	4	2	8	computing centre staff	awareness, additional security mechanism, three tier architecture, 802.1x

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities/ weaknesses	Impact	Likeli - hood	Risk	Risk owner	Actions
30	Client Communication	medium	tampering		tampering	3	2	6	computing centre staff	awareness, 802.1x + IPSec additional security mechanism
31	Client Communication	medium	spoofing		spoofing	3	2	6	computing centre staff	awareness, 802.1x + IPSec additional security mechanism
32	Client Communication	medium	information disclosure		information disclosure	3	2	6	computing centre staff	awareness, 802.1x + IPSec additional security mechanism
33	Users (students)	high	spoofing	only authorized access, ID check	reduced spoofing, piggy packing, social engineering	4	3	12	university	awareness, ID control, guidelines with consequences
34	LDAP administrator	high	social engineering	only authorized access	social engineering	4	2	8	LDAP administrator	awareness, compliance

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities/ weaknesses	Impact	Likeli - hood	Risk	Risk owner	Actions
35	Users (staff)	high	social engineering	only authorized access	social engineering	3	2	6	staff	awareness
36	Rooms in the data center	high	tampering, information disclosure, destruction	Access only with a special key, physical protection	social engineering	4	2	8	computing centre	Awareness, additional security mechanism, alarm functions, cameras
37	services for cooling the air, heating	high	destruction	Access only with a special key	destruction	4	1	4	university	Awareness, additional security mechanism, alarm functions, cameras
38	services for cooling the air, heating	high	tampering	Access only with a special key	tampering	3	1	3	university	Awareness, additional security mechanism, alarm functions, cameras
39	structure of the process organization	high	tampering	no ones	tampering	4	2	8	university	awareness, regular controls, compliance

Risk ID	**Asset**	**Value**	**Threat**	**Existing Controls**	**Still existing vulnerabilities/ weaknesses**	**Impact**	**Likeli - hood**	**Risk**	**Risk owner**	**Actions**
40	structure of the process organization	high	elevation of privileges	no ones	elevation of privileges	4	2	8	university	awareness, regular controls, compliance

Figure 31: Risk Assessment - Access Control [own preparation]

- Definition of the impact:
    - 1: Negligible: no costs, no negative repudiation, no disruption of operations, no impairment of business performance, no breach of confidentiality, minor leak or loss of unessential data
    - 2: low: low costs, low negative repudiation local service disruption less than one week, low impairment of business performance, low breach of confidentiality, low loss or leak of significant data
    - 3: medium: medium costs, medium negative repudiation, serious interruption for several users for more than a week, medium impairment of business performance, medium breach of confidentiality, leak of significant data
    - 4: high: high costs, high negative repudiation, high disruption of operations, high impairment of business performance, high breach of confidentiality, severe impairments of serviceability, serious data loss or the leakage of essential data (personal, exams, scientific data)

- Definition of the likelihood:
    - 1: Negligible: unlikely
    - 2: low: happens less than once a year
    - 3: medium: happens every few months
    - 4: high: happens every month or more frequently

- Definition of the risk acceptance criteria:
    - 1 - 4: risk is accepted
    - 5 – 9: risk is accepted with conditions
    - >= 10: risk is not accepted

Irrespective of the depth of detail, you should always keep the "STRIDE"[33] approach in focus to obtain a meaningful result. After the risk evaluation has been carried out, one could carry out ranking of the risks or threats as described in chapter 5.7 for clarity. The prioritization of risks is already integrated into the risk treatment plan in this master thesis.

In the following risk treatment plan, only the high risks greater than or equal to ten are considered in model terms.

- Risk treatment plan:

Risk ID	Asset	Risk Value	Risk Treatment	Actions	approved residual risk- new likelihood ()	treatment periods
09	Campus Card	12	reduction	Awareness, self-service blocking of the card in case of loss by the owner	4 loss is not noticed new Likelihood: 1	March 2018 - September 2018, awareness continuously
13	Card reader	12	reduction	awareness, protection against misuse, additional security mechanism (secure login), cameras on each card reader, alarm function	4 tampering reduced new Likelihood: 1	February 2018- June 2018, awareness continuously
14	software for card reader operation	12	reduction	awareness, Secure coding with additional security mechanism, penetration tests	4 social engineering, information disclosure, theft new Likelihood: 1	awareness continuously
18	Door	12	reduction	Awareness, additional security	4 reduced Information Disclosure,	March 2018 - September 2018,

Risk ID	Asset	Risk Value	Risk Treatment	Actions	approved residual risk- new likelihood ()	treatment periods
				mechanism, airlock, ID check	Piggy Packing new Likelihood: 1	awareness continuously
33	Users (students)	12	reduction	awareness, ID control, guidelines with consequences	4 reduced piggy packing and spoofing social engineering, information disclosure new Likelihood: 1	February 2018- June 2018, awareness continuously
Place, Date, Signature						

Figure 32: Risk Treatment Plan - Access Control [own preparation]

When dealing with the risks, it is important to bear in mind that the costs of treatment are lower than the damage caused by the risks.

The choice of risk management method must be appropriate to the external circumstances. In particular, the interactions should be taken into account. In addition, it should also be possible to implement risk management methods in practice.[64] When determining the remaining residual risk, a new iteration of the risk assessment should be carried out.

Once the risk treatment plan has been drawn up, the risks should be communicated to all participants in an appropriate form as described in chapter 5.7. In this context, it is important that all levels of the risk management process are communicated to all those involved in the corresponding level of detail. The communication rules described in [64] should be observed.

7.3.2 Recording of marks

The first step in implementing sophisticated risk management is to define the context. So the recording of the notes is defined as context in this example.

Students register for the respective exams via the web interface (HIS Online Portal). The authorized examiners can register the test results (marks) via the web interface. The Examination Office stores the examination results in paper form and ultimately prints the final certificates on a special paper. The HIS-Online portal was developed and expanded by HIS eG. The HIS admin of the HSA can adapt and modify the predefined templates and the underlying Java code accordingly.

The following matrix shows the risk assessment for the process recording of marks.

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
01	personal data (digital, analog)	high	Tampering	https, authorized access, DMZ, email with AES	reduced Tampering, Phishing, Social Engineering	3	3	9	examination office, computing centre	Awareness, guidelines for handling with personal data, secure coding, authorized access, strong passwords, new process for sending excels lists, three tier architecture,
02	personal data (digital, analog)	high	information disclosure	https, authorized access, DMZ, email with AES	reduced information disclosure, Phishing, Social Engineering	3	3	9	examination office, computing centre	Awareness, guidelines for handling with personal data, secure coding, authorized access, strong passwords, new process for sending excels lists, three tier architecture
03	personal data (digital, analog)	high	Non-availability	https, authorized access, email with AES, back-up	Phishing, Social Engineering	2	2	4	examination office, computing centre	Awareness, guidelines for handling with personal data, authorized

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
										access, strong passwords, new process for sending excels lists, three tier architecture
04	data about grades (digital, analog)	high	Tampering during regular process flow	https, authorized access, DMZ, three tier architecture	reduced Tampering, social engineering	4	2	8	professor, computing centre, examina-tion office	Awareness, guidelines for handling with data about grades, strong passwords, Additional locking devices, defends in depth
05	data about grades (digital, analog)	high	Information Disclosure	https, authorized access, DMZ	reduced Information Disclosure, social engineering	3	2	6	professor, computing centre, examination office	Awareness, guidelines for handling with data about grades, strong passwords, Additional locking devices, defends in depth, three tier architecture
06	data about grades (digital, analog)	high	Non-availability	https, authorized access, DMZ, back-up	social engineering	2	2	4	professor, computing centre,	Awareness, guidelines for handling with data about

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
									examination office	grades, strong passwords, defends in depth, three tier architecture
07	data about grades (analog)	high	theft, destruction	no controls	theft, destruction	3	2	6	examination office	Awareness, guidelines for handling with data about grades, Additional locking devices, defends in depth
08	Application Server	High	Tampering server configuration	separated administration network, AJP13, Authenticat-ion	reduced Tampering	4	2	8	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth, improvements of AJP13, three tier architecture
09	Application Server	High	Information Disclosure	separated administration network, AJP13, Authenticat-ion	reduced Information Disclosure, only temporary data	2	2	4	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth, improvements of AJP13, three tier architecture

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
10	Application Server	High	Non-availability	separated administration network, AJP13, Authenticat-ion	restricted availability	1	2	2	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth, improvements of AJP13, three tier architecture
11	Web Server	High	Tampering server configuration	separated DMZ, firewall, Authenticat-ion	reduced Tampering	4	3	12	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth, improvements of AJP13 penetration tests, updates, patches, three tier architecture
12	Web Server	High	Information Disclosure, password capture	separated DMZ,	reduced Information Disclosure	4	3	12	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth, improvements of AJP13 penetration tests, updates,

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
										patches, three tier architecture
13	Web Server	High	Non-availability	DoS-basis service by DNF	restricted availability	1	2	2	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth, penetration tests, updates, patches
14	ALG genugate	high	Non-availability	DoS-basis service by DNF, physical protection	restricted availability	1	2	4	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth
15	ALG genugate	high	Tampering	EAL4-Certificate-Firewall, authorization, separated administrative network	reduced Tampering	4	1	4	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth
16	ALG genugate	high	Information Disclosure	HTTPS, SSL, separated administrative network	reduced Information Disclosure	2	1	2	computing centre	Awareness, continual monitoring, IDS, IPS, defends in Depth
17	user clients (students)	low	Tampering	logs of exam registration	Tampering	1	4	4	student	Awareness, strong password, regular updates

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
18	user clients (students)	low	Information Disclosure	logs of exam registration	No ones	1	4	4	student	Awareness, strong password, regular updates
19	workstation examiners	High	Tampering	authenticat-ion, VPN, virus protection	reduced Tampering, social engineering	4	2	8	examiners	Awareness, guidelines for laptop handling, session time out, regular updates
20	workstation examiners	High	Information disclosure	authenticat-ion, VPN, virus protection	reduced Information disclosure, social engineering	2	2	4	examiners	Awareness, guidelines for laptop handling, session time out, regular updates
21	workstation examiners	High	Non-availability	authenticat-ion	restricted availability	1	2	2	examiners	Awareness, guidelines for laptop handling, session time out, regular updates
22	examinat-ion office clients	High	Tampering	VDI (thin clients), dedicated network, virus scanner, authenticat-ion	reduced Tampering, Social Engineering, back-door, trojaner	4	2	8	examination office, computing centre	awareness, guidelines for dealing with information security, three tier architecture
23	examinat-ion office clients	High	Information Disclosure	VDI (thin clients), dedicated network, virus	reduced Information Disclosure,	2	2	4	examination office, computing center	awareness, guidelines for dealing with information

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
				scanner, authenticat-ion	Social Engineering					security, three tier architecture
24	examinat-ion office clients	High	Non-availability	VDI (thin clients), dedicated network, virus scanner, authenticat-ion	restricted availability	1	2	2	examination office, computing center	awareness, guidelines for dealing with information security, back-up, three tier architecture
25	printed and signed marks verificat-ions in paper form, diploma certificate	high	tampering	special paper for the diploma certificate, manual signed paper	falsify signature, manipulation of printed paper	4	1	4	examination office	awareness, additional security mechanism (additional locked cabinet)
26	printed and signed marks verificat-ions in paper form, diploma certificate	high	information disclosure	locked cabinet, sealed envelope	reduced information disclosure, social engineering	2	1	2	examination office	awareness, additional security mechanism (additional locked cabinet, archival backup copy)

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
27	printed and signed marks verificat-ions in paper form, diploma certificate	high	theft	no ones	reduced theft, social engineering	3	1	3	examination office	awareness, additional security mechanism (additional locked cabinet, archival backup copy)
28	Software for HIS Portal (Java)	high	tampering	regular updates, patches	reduced tampering	4	3	12	HIS EG, computing center staff	awareness, penetration tests, secure coding rules, security mechanism against SQL-Injections, Cross-Site Scripting
29	Software for HIS Portal (Java)	high	Non-availability	regular updates, patches, back up, DoS-basis service by DNF	restricted availability	1	2	2	HIS EG, computing center staff	awareness, penetration tests, secure coding rules, security mechanism against SQL-Injections, Cross-Site Scripting
30	LDAP database with IDM	high	tampering of user name and	Authorized access, Authenticat-	reduced tampering, weak	4	2	8	computing center	awareness, additional security mechanism,

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
			user groups	ion, physical protection	authenticatio n					two factor authentication
31	LDAP database with IDM	high	information disclosure	Authorized access, Authenticat-ion, physical protection	reduced information disclosure	2	2	4	computing center	awareness, additional security mechanism, two factor authentication
32	LDAP database with IDM	high	non-availability	Authorized access, Authenticat-ion, back up	restricted availability	1	2	2	computing center	awareness, additional security mechanism, two factor authentication, three tier architecture
33	HIS data base	high	tampering	Authenticat-ion, physical protection	reduced tampering	4	2	8	HIS eG, computing center	awareness, monitoring, improvements of AJP13, defends in Depth, penetration tests, three tier architecture
34	HIS data base	high	information disclosure	Authenticat-ion	reduced information disclosure	3	2	6	HIS eG, computing center	awareness, monitoring, improvements of AJP13, defends in Depth,

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
										penetration tests, three tier architecture
35	HIS data base	high	non-availability	Authenticat-ion, back-up	restricted availability	1	2	2	HIS eG, computing center	awareness, monitoring, improvements of AJP13, defends in Depth, penetration tests, three tier architecture
36	Communic ation (Network)	high	spoofing	filters, SSL, HTTPS	reduced spoofing, Man in the Middle	4	2	8	computing center staff	Awareness, continual monitoring, IDS, IPS, defends in Depth, IPSec, three tier architecture
37	Communic ation (Network)	high	tampering	filters, SSL, HTTPS	reduced tampering, Man in the Middle	4	2	8	computing center staff	Awareness, continual monitoring, IDS, IPS, defends in Depth, IPSec, three tier architecture
38	Communic ation (Network)	high	information disclosure	filters, SSL, HTTPS	reduced information disclosure,	2	2	4	computing center staff	Awareness, continual monitoring, IDS, IPS, defends in

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
					Man in the Middle					Depth, IPSec, three tier architecture
39	AJP13	high	tampering	AJP13	reduced tampering, Man in the Middle	3	3	9	computing center staff	Awareness, continual monitoring, IDS, IPS, defends in Depth, Improvements of AJP13 *, three tier architecture
40	AJP13	high	information disclosure	AJP13	reduced information disclosure, Man in the Middle	3	3	9	computing center staff	Awareness, continual monitoring, IDS, IPS, defends in Depth, Improvements of AJP13 *, three tier architecture
41	Users (staff, examiners)	high	social engineer-ing	authenticat-ion, authorization	reduced social engineering	4	2	8	staff	awareness, guidelines e.g. strong passwords, Locking the keyboard, locking the cabinet
42	Users (staff, examiners)	high	information disclosure	authenticati-on, authorization,	reduced information disclosure,	2	1	2	staff	awareness, guidelines e.g. strong

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
				official secret, NDA	social engineering					passwords, Locking the keyboard, locking the cabinet
43	Administrator HIS	high	social engineer-ing, information disclosure	none	social engineering, information disclosure	4	2	8	university, computing center staff	awareness, guidelines, four eyes principle
44	Administrator HIS	high	Non-availability (single personal resource)	none	Non-availability (single personal resource	4	2	8	university, computing center staff	back-up, additional personal resources
45	examinatio n office rooms	high	Access to the room	only access with a key	social engineering	3	1	3		awareness, guidelines, cameras, alarm functions
46	examinatio n office rooms	high	theft blank diploma certificate, marks verification in paper form	only access with a key, locked cabinet	social engineering	4	1	4		awareness, guidelines, cameras, alarm functions
47	Rooms in the data center	high	social engineer-ing, information	only access with a key, physical protection	social engineering, break the lock	4	2	8	computing center staff	awareness, guidelines, improved motor

Risk ID	Asset	Value	Threat	Existing Controls	Still existing vulnerabilities / weaknesses	Impact	Likeli-hood	Risk	Risk owner	Actions
			disclosure, theft, destruction							locks, cameras, alarm functions
48	services for cooling the air, heating	medi um	destruction	only access with a key	destruction	2	2	4	university	Awareness, additional security mechanism, alarm functions, cameras
47	Process of “recording of marks”	medi um	tampering	four eyes principle, limited data entry time	tampering	4	2	8	university	awareness, regular controls, compliance
48	Process of “recording of marks”	medi um	elevation of privileges	role concept	elevation of privileges, Administrator as weakness	4	2	8	university	awareness, regular controls, compliance
49	Process of “recording of marks”	medi um	information disclosure	four eyes principle, limited data entry time, Emails with AES encryption	information disclosure	2	2	4	university	awareness, regular controls, compliance, data classification

Figure 33: Risk Assessment - Recording of Marks [own preparation]

* such as advanced login features at connect time, basic authorization system with a shared secret key, basic protocol negotiation, clean handling of unknown packets, extra SSL information (like SSL_KEY_SIZE) [73]

- Definition of the impact:
    - 1: Negligible: no costs, no negative repudiation, no disruption of operations, no impairment of business performance, no breach of confidentiality, minor leak or loss of unessential data
    - 2: low: low costs, low negative repudiation local service disruption less than one week, low impairment of business performance, low breach of confidentiality, low loss or leak of significant data
    - 3: medium: medium costs, medium negative repudiation, serious interruption for several users for more than a week, medium impairment of business performance, medium breach of confidentiality, leak of significant data
    - 4: high: high costs, high negative repudiation, high disruption of operations, high impairment of business performance, high breach of confidentiality, severe impairments of serviceability, serious data loss or the leakage of essential data (personal, exams, scientific data)

- Definition of the likelihood:
    - 1: Negligible: unlikely
    - 2: low: happens less than once a year
    - 3: medium: happens every few months
    - 4: high: happens every month or more frequently

- Definition of the risk acceptance criteria:
    - 1 - 4: risk is accepted
    - 5 – 9: risk is accepted with conditions
    - >= 10: risk is not accepted

- Risk treatment plan:

In the following risk treatment plan, only those risks that are greater than or equal to ten are dealt with here as models.

Risk ID	Asset	Risk Value	Risk Treatment	Actions	approved residual risk-new likelihood ()	treatment periods
11/12	Web Server	12	reduction	Awareness, continual monitoring, IDS, IPS, defends in Depth, improvements of AJP13, penetration tests, updates, patches	4 reduced tampering, information disclosure new Likelihood: 1	March 2018 - September 2018, awareness continuously
28	Software for HIS Portal (Java)	12	reduction/ transfer	awareness, penetration tests, secure coding rules, security mechanism against SQL-Injections, Cross-Site Scripting	4 tampering reduced new Likelihood: 1	February 2018- June 2018, awareness continuously
Place, Date, Signature						

Figure 34: Risk Treatment Plan - Recording of Marks [own preparation]

The risk treatment plan in this master thesis is at a high level. It can be realized in different depths of detail.

The supported assets can be found in the risk treatment plan, as they support primary assets. In order to ensure confidentiality, integrity and availability for primary assets, security measures must be established for the supported assets. In this way, the risks of the supported assets can be reduced, transferred or avoided as required. If the risks are retained under certain circumstances, a justification should be given.

Regardless of the level of detail, the "STRIDE" [71] approach should be considered. The remaining residual risks are measured on the basis of risk acceptance criteria and,

if necessary, a new iteration of the risk assessment is executed. Generally speaking, care must be taken to ensure that the multi-layered "defense in depth" principle is applied. If a security mechanism is breached, the asset requiring protection is still protected by the other security measures.[74]

Finally, the risks are communicated to all persons involved in varying degrees of detail according to their functionality. The usual communication rules should be adhered to [18]

7.4 Designing the ISMS as a central terminal step

Finally, in this last process step, all previous centrally executed process steps as well as the decentralized preceding process steps from chapter 7.2 respectively 7.3 are actual implemented. In particular, the risk treatment plans developed in Chapters 7.2.3 and 7.3.3 are summarized and implemented centrally at this point. For reasons of scope, this final step is only briefly described in this master thesis.

At the latest in this process step, all changes (intentionally or unintentionally) that have occurred during the ISMS process must be integrated into the existing processes or, if necessary, the processes must be renewed. In particular, the risk treatment plan drawn up previously must be implemented here. It is of great importance that the remaining residual risk is borne and documented by the risk owner and, above all, approved by university management. In particular, the university's management with a justification must sign the accepted risks or the risks that have not been dealt with. Furthermore, a performance evaluation of the previous steps takes place here. In this way an effective HS-UNI-ISMS should be guaranteed. This performance evaluation may include an internal audit and a management review. Therefore, it is possible to achieve a continuous improvement of the HS-UNI-ISMS. In addition, all activities must be documented in the appropriate form and communicated to all participants in different levels of detail in an appropriate form. Detailed information on this step can be found in chapter 5.8.

8 Conclusion

Information security has become a serious, cross-sectoral issue due to various factors such as the disappearance of network boundaries and the simultaneous rapid increase in cyber-crime attacks in recent years.

Particularly in the knowledge-intensive higher education sector, where data are the most valuable asset, a trade-off must be found in which the fundamental values of confidentiality, integrity and availability of data are guaranteed on the one hand, and the freedom of research and teaching on the other.

In this master thesis, a special ISMS was developed, tailored to the requirements of the higher education sector, in order to take an important step towards guaranteeing information security at all Bavarian universities of applied sciences and universities.

Until now, there is no ISMS specifically designed for the knowledge-intensive university sector.

In a first step, general requirements of the public administration, in particular of the higher education sector, were defined. It was found that a Bavarian-wide view of all universities and universities of applied sciences could no longer be based on the definition of a standard authority (up to approx. 500 employees, a homogeneous IT basic infrastructure, no dislocated subsidiaries linked through unprotected public networks, normal protection requirements, no high level availability requirements regarding the IT-Systems, no critical applications in terms of KRITIS in the sense of the BSI.

Based on this understanding, the existing concepts for the creation, implementation, maintenance and improvement of an ISMS in the higher education sector were investigated. It was established that, on the one hand, there are old guidelines that do not yet differentiate between information security and IT security and, on the other hand, that the IT Planning Council (IT-PLR) has established minimum requirements for an ISMS for public administration.

In a next step, the contents of the existing standards, norms and concepts in the field of information security were examined and analyzed in detail. It turned out that the methods of the ISO/IEC 2700x standard family, the basic IT protection of the BSI and the ISIS 12 procedure are suitable to create, implement, maintain and improve an ISMS. Whereas the method of the Bavarian Innovation Foundation's work aid (AKDB) is not suitable for this purpose.

As a result, the next step compared the three prioritized approaches. Based on this, these procedural models in the ISMS environment were evaluated on the basis of criteria relevant to the u higher education sector, such as target group, resource efficiency, scalability, risk management, international significance, tool support, pre-defined process steps and the minimum requirements of the IT Planning Council with the help of a utility value analysis. As a result, the ISO/IEC 2700x family of standards has the highest utility value with 4.80 %, the second highest utility value of 3.10 % is

achieved by the ISIS 12 method, followed by the basic IT protection procedure with a utility value of 3.08 %. However, all three approaches have serious weaknesses in addition to their strengths.

As a result, the necessity of an individual solution especially for the knowledge-intensive higher education sector is emphasized, since no alternative solution studied covers all the necessary requirements completely alone.

In a next step, based on the case distinction to determine the requirement for protection, an individually sophisticated HS-UNI-ISMS for all Bavarian universities and universities of applied sciences will be developed by gradually combining the presented alternative solutions with their respective strengths.

This HS-UNI-ISMS, specially designed for the knowledge-intensive higher education sector, aims to be general and abstract on the one hand, so that it can be applied in the entire Bavarian higher education sector and on the other hand, to be individually scalable so that it can be adapted to the local requirements of each Bavarian higher education institution. The HS-UNI-ISMS is composed of eight consecutive steps. The output of each previous step is the necessary input of the next step.

With the help of checklists in every phase of the HS-UNI-ISMS, every Bavarian university and university of applied sciences can create, implement, maintain and improve an ISMS that is individually tailored to the specific local requirements of the respective universities.

In addition, the challenges that have already arisen at the University of Applied Sciences Augsburg are described in each ISMS phase in order to facilitate the handling of the HS-UNI-ISMS.

Based on the researched findings, the newly developed HS-UNI-ISMS as a prototype was applied as an example to the critical processes "Access control with the Campus Card" and "Recording of marks" at the University of Applied Sciences Augsburg.

Based on the preceding scope and boundary determination, the values of these critical processes were identified and classified in the information requirement analysis. Consequently, a sophisticated risk assessment was carried out on the basis of this. This master thesis shows how the risks were identified, evaluated and treated.

Thus, with the help of these master’s thesis, a very essential step was taken to ensure information security in the Bavarian higher education sector.

An ISMS is a very complex and rapidly developing topic, especially in the knowledge-intensive higher education sector. For this reason, the complete implementation of a HS-UNI-ISMS (not only in the area of Access control and Recording of marks) at the University of Applied Sciences Augsburg is the subject of further scientific work.

V. Annex A

A. 1 Information Security Policy at the University of Applied Sciences Augsburg

Preamble

The operation of a university depends to a large extent on the quality of its IT services. The trust of users in information technology forms the basis for successful use. To justify this trust, the integrity, confidentiality and availability of IT services and data must be ensured. In order for the university to fulfil this responsibility, all institutions must support the protection of information technology. These tasks are to be mastered on the basis of this guideline in a continuous information security management. This methodological approach is based on necessary rules and requires appropriate measures to protect information and data in such a way that

(1) their confidentiality is adequately preserved and knowledge can only be obtained from authorized persons,

(2) their integrity is ensured by their accuracy and completeness,

(3) their availability is guaranteed so that they can be used by authorized persons at the desired time,

(4) legal obligations (e. g. Bavarian Data Protection Act) can be fulfilled.

§1 Objective of the Policy

This document defines basic rules for the following information security objectives:

(1) Protection of the network infrastructure and IT systems, including the data processed with them, against misuse or sabotage from inside and outside.

(2) Ensuring information security for a robust, reliable and secure teaching, research and administrative operation.

(3) Realization of secure and trustworthy online services for users inside and outside the university.

(4) Ensure compliance with the data protection requirements resulting from the legal requirements.

(5) Damage caused by security incidents shall be prevented or minimized.

§ 2 Scope

This guideline covers the entire information technology and all university members and external users who use or provide it. It is binding for all faculties and central institutions of the university. It must also be observed by external service providers of the information technologies used at the University of Applied Sciences Augsburg.

3 § Information Security Management

The information security management system comprises all necessary organizational and technical measures to achieve and maintain a defined degree of information security (security level) in the long term. In order to achieve an adequate level of security, additional measures are defined for information requiring increased protection on the basis of a risk analysis.

The necessary and specific rules for achieving an adequate security level and implementation of the principles are included in a security concept. There, the requirements of this policy and the required security level are sufficiently detailed in the form of security policies. These are then the basis for the necessary security measures. These measures are documented in implementation requirements and service-specific security concepts.

The security policies cover at least the following areas:

(1) Organization of IT security

(2) Determination of information values (classification)

(3) Access control, network and operational security

(4) IT systems (such as servers, storage systems, workstations)

(5) Vulnerability detection and malware protection

(6) Handling of security incidents

(7) Backup and emergency planning

(8) Risk management, compliance and data protection

(9) Physical security

(10) Communication

The central IT security officer is responsible for the flow of the information security management system. He/she advises the IT committee and the IT representatives of the faculties as well as the computing center. With regular reviews of the implementation of the security concept and further development of the measures, he/she ensures adequate information security. He/she may gain an overview of information security in all areas of the university. Services offered by the university that can be reached from outside the university network require an examination by the IT security and data protection officer.

4 § Information security responsibility

The IT Committee is responsible for steering the information security management system. The Information Security Officer acts on behalf of the IT committee and methodically coordinates the information security management system. The final decision on risk acceptance and degree of implementation is the responsibility of the Presidium, which is ultimately responsible for the proper operation and information security of the university.

For the continuous further development of the policy and dependent documents (e.g. security concept), information security is an integral part of the agenda of the regular IT committee meetings. The Information Security Officer reports on the current status and receives his/her tasks based on the decisions of the IT Committee. The Senate is to be consulted before the adoption of information security policies.

Every university employee is responsible for maintaining the level of information security as an information owner or administrator in his or her field of activity.

5 § Information classification

Each type of information is classified by the information owner according to the information security policy - Information Classification. This is done in accordance with their value and sensitivity to developing an appropriate level of security.

6 § Access to information and data

Access to data and IT systems is adequately controlled by technical measures and processes, according to their value and significance.

All users of applications/IT systems are uniquely identifiable and are authorized and authenticated according to their function and task. The principle of minimum privileges is applied, i. e. authorizations are only granted to the extent necessary for the fulfillment of the respective tasks.

All changes to important information and decisions made must be traceable by appropriate logging and documentation. The information owner determines the need, type and manner of logging.

7 § Security awareness

The required level of information security can only be achieved if the people employed are aware of information security threats, know their own competencies and duties and behave responsibly.

Security related topics and rules are brought to the attention of the members of the higher education institution through appropriate training or information channels.

8 § Risk Intervention/Security Incidents

If there is a risk of violating the IT security of critical systems at the university, a service manager of the computing center can, together with the CIO, order the immediate temporary shutdown of the affected IT system and temporarily exclude the responsible users from using the information technology.

The handling of security incidents is carried out according to a documented process for the handling of IT security incidents.

The IT committee determines the IT services for which the central IT security officer collects and coordinates emergency plans. They contain instructions for dealing with critical situations and incidents.

9 § Entry into force

This constitution shall enter into force on the day following its publication. Issued on the basis of the Senate's decision of 11.07.2017 and the approval of the president of University of Applied Sciences Augsburg on 27.10.2017.

Augsburg, 27.10.2017

Prof. Dr. Gordon T. Rohrmair, governor

The constitution was laid down on 25.11.2017 at the University of Applied Sciences Augsburg; the resignation was announced on 25.11.2017 by notice board in the university.

The announcement date is 25.11.2017.according to the German version [75]

VI. Literaturverzeichnis:

[1] Heise Security, “WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm.”

[2] Heise Security, “Ransomware WannaCry befällt Rechner der Deutschen Bahn.”

[3] Heise Security, “WannaCry: Was wir bisher über die Ransomware-Attacke wissen.”

[4] T. Morsches, “Betreff: Whistleblowing und PRISM - Anhörung A09 - 06.02.2014 _Landtag Nordrhein-Westfalen.”

[5] W. Denkhaus and K. Geiger, “Landesrecht Freistaat Bayern Bayerisches E-Government-Gesetz.”

[6] Bayerische Staatskanzlei, “BayEGovG: Art. 8 Informationssicherheit und Datenschutz - Bürgerservice.” [Online]. Available: http://www.gesetze-bayern.de/Content/Document/BayEGovG-8. [Accessed: 17-Jan-2017].

[7] J. N. and X. Dai, “On the Information Security Issue in the Information Construction Process of Colleges and Universities,” *2016 12th Int. Conf. Comput. Intell. Secur.*, pp. 582–585, 2016.

[8] S. Hina and D. D. Dominic, “Information security policies: Investigation of compliance in universities,” in *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, 2016, pp. 564–569.

[9] B. Sussy, C. Wilber, L. Milagros, and M. Carlos, “ISO/IEC 27001 implementation in public organizations: A case study,” in *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, 2015, pp. 1–6.

[10] N. F. Doherty, L. Anastasakis, and H. Fulford, “The information security policy unpacked: A critical study of the content of university policies,” *Int. J. Inf. Manage.*, vol. 29, no. 6, pp. 449–457, 2009.

[11] Bayerische Staatsverwaltung, *IT-Sicherheitsrichtlinien für die bayerische Staatsverwaltung – Leitlinie zur Informationssicherheit (IT Security Policy) für die bayerische Staatsverwaltung (BayITSiLL)*. 2016, pp. 1–5.

[12] Bayerische Staatsverwaltung, *IT-Sicherheitsrichtlinien für die bayerische Staatsverwaltung - Betrieb eines Übergangs in das Internet (BayITSiR- 02)*. 2016, pp. 2–7.

[13] S. Schnitzler, “Analyse und Evaluation von Methoden und Modellen zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) an bayerischen Hochschulen und Universitäten,” 2017.

[14] Deutsches Institut für Normen e.V. DIN, “Informationssicherheits-Managementsysteme-Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014).”

[15] Bundesamt für Sicherheit in der Informationstechnik, “BSI-Standard 100-1 -

Managementsysteme für Informationssicherheit (ISMS)."

[16] K.-R. Müller, *IT-Sicherheit mit System*. .

[17] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of ISMS," in *7th International Conference on e-Commerce in Developing Countries:with focus on e-Security*, 2013, pp. 1–17.

[18] H.-P. Königs, *It-Risikomanagement mit System*. .

[19] S. Klipper, *Information Security Risk Management*. 2015.

[20] Deutsches Institut für Normen e.V. DIN, "Informationssicherheits-Managementsysteme - Überblick und Terminologie (E DIN ISO/IEC 27000:2015)," 2016.

[21] Bundesamt für Sicherheit in der Informationstechnologie, "BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschutz - Community Draft."

[22] Fraunhofer Institut, "Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung."

[23] Bundesamt für Sicherheit in der Informationstechnologie, "Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams in der öffentlichen Verwaltung."

[24] Bundesamt für Sicherheit in der Informationstechnologie, "Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz," *Stand 15. Ergänzungslieferung*. .

[25] Bundesministerium der Justiz und Verbraucherschutz, "91b/1 GG." [Online]. Available: https://www.gesetze-im-internet.de/gg/art_91b.html. [Accessed: 27-Feb-2017].

[26] IT-Planungsrat Kooperationsgruppe „Informationssicherheit des, "Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung- Hauptdokument-," vol. 8, pp. 1–13, 2013.

[27] Kooperationsgruppe „Informationssicherheit des IT-PLR, "Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung- Umsetzungsplan-," vol. 6, 2013.

[28] M. Stemmer and G. Goldacker, "IT-STANDARDISIERUNG IN DER ÖFFENTLICHEN VERWALTUNG – EIN DISKUSSIONSPAPIER."

[29] K. I. Alshitri and A. N. Abanumy, "Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia," in *2014 International Conference on Information Science & Applications (ICISA)*, 2014, pp. 1–4.

[30] G. D.-I. Schulz, "Informationssicherheit in Kommunen," *Stellvertreter des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vor.*

[31] Bundesamt für Sicherheit in der Informationstechnologie, "Kritis - Glossar - K." [Online]. Available: http://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functio

ns/glossar.html?lv2=4968594. [Accessed: 23-Jan-2017].

[32] Bundesamt für Sicherheit in der Informationstechnologie, “IT-Grundschutz-Kataloge 15. Ergänzungslieferung.” .

[33] K. Beckers, S. Fa??bender, M. Heisel, and H. Schmidt, “Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation,” *Proc. - 2012 7th Int. Conf. Availability, Reliab. Secur. ARES 2012*, pp. 242–248, 2012.

[34] B. für Sicherheit in der Informationstechnik, “BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS).”

[35] Bundesamt für Sicherheit in der Informationstechnologie, “BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise.”

[36] B. für Sicherheit in der Informationstechnik, “Ergänzung zum BSI-Standard 100-3, Version 2.5,” 2011.

[37] B. für Sicherheit in der Informationstechnik, “BSI-Standard 100-4.”

[38] Bundesamt für Sicherheit in der Informationstechnologie, “Gefährdungskatalog.”

[39] Bayerischer IT-Sicherheitscluster e.V., “ISIS12 - Katalog,” vol. 49, no. 0, pp. 0–75.

[40] Bayerischer IT-Sicherheitscluster e.V., “Informationssicherheit im Mittelstand Impressum-Handbuch,” no. September, pp. 0–85, 2016.

[41] S. Kuhrau, “Erstellung von Informationssicherheitskonzepten für Kommunen, INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE.”

[42] Bundesamt für Sicherheit in der Informationstechnik, “Informationssicherheit Ein Vergleich von Standards und Rahmenwerken.”

[43] I. WINDHORST and B. PIRZER, “Managementsysteme für Informationssicherheit,” 2012.

[44] M. Falk, *Ableitung des Control-Frameworks für IT-Compliance*. .

[45] Ralf-T. Grünendahl • Andreas F. Steinbacher and Peter H.L. Will, *Das IT-Gesetz: Compliance in der IT-Sicherheit*. .

[46] G. Disterer, “Zertifizierung der IT nach ISO 20000.”

[47] Bundesministerium der Justiz und Verbraucherschutz- Vertrag zur Ausführung von Artikel 91c GG, *IT-Staatsvertrag, Art. 91c GG*. .

[48] Zentrum für Kommunikation und Informationsverarbeitung e.V. (ZKI) in Lehre und Forschung, “Ergänzendes Material zum Papier IT-Sicherheit an Hochschulen, Rechtlicher Rahmen,” *Ergänzendes Mater. zum Pap. IT-Sicherheit an Hochschulen, Rechtl. Rahmen*, vol. 110, no. 35–36, p. A1595, 2013.

[49] IT-Planungsrat, “Kooperationsgruppe „ Informationssicherheit des IT - PLR “ Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung

Inhaltsverzeichnis," vol. 8, pp. 1–13, 2013.

[50] Universität Berlin, "IT-Sicherheitsrahmenrichtlinie für die Freie Universität Berlin Gliederung," pp. 1–67, 2005.

[51] J. B. Kühnapfel, "Das Vorgehen bei der Nutzwertanalyse," no. 5.

[52] E. Tiemeyer and H. E. Zsifkovits, *Handbuch IT-Projektmanagement*. 2010.

[53] N. Müller-Prothmann, Tobias, Dörr, *Innovationsmanagement*. 2014.

[54] W. Johannsen, "Status der IT-Governance in der öffentlichen Verwaltung," 10AD.

[55] W. Hommel, S. Metzger, and M. Steinke, "Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization."

[56] I. V Anikin, "Information Security Risks Assessment in Telecommunication Network of the University."

[57] Bundesamt für Sicherheit in der Informationstechnologie, "BSI - IT-Grundschutz Tools - Startseite." [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/gstool_node.html. [Accessed: 15-Feb-2017].

[58] Deutsches Institut für Normen e.V. DIN, "Information security risk management - ISO/IEC 27005:2011(E)," vol. 25021, 2012.

[59] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of ISMS," in *7th International Conference on e-Commerce in Developing Countries:with focus on e-Security*, 2013, pp. 1–17.

[60] H.-P. Königs, *IT-Risikomanagement mit System*. Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

[61] ISO, "INTERNATIONAL STANDARD ISO / IEC Information technology- 27003 - Security techniques — Information security management systems — Overview and vocabulary," vol. 2016, 2016.

[62] B. für Sicherheit in der Informationstechnik, "BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise."

[63] Deutsches Institut für Normen e.V. DIN, "Leitfaden für das Informationssicherheits-Management:ISO/IEC 27002_2017," 2016.

[64] S. Klipper, *Information Security Risk Management*. .

[65] G. N. Samy, R. Ahmad, and Z. Ismail, "A framework for integrated risk management process using survival analysis approach in information security," *2010 Sixth Int. Conf. Inf. Assur. Secur.*, pp. 185–190, 2010.

[66] DIN/IEC ISO 9001, "DIN EN ISO 9001 - Qualitätsmanagementsysteme - Anforderungen." [Online]. Available: https://www.beuth.de/de/norm/din-en-iso-9001-2015-11/235671251. [Accessed: 05-Jan-2018].

[67] Deutsches Institut für Normen e.V. DIN, "Informationsicherheits-

Managementsysteme - Überblick und Terminologie (ISO/IEC 27000:2009).”

[68] K. Beckers, M. Heisel, B. Solhaug, and K. St?len, “ISMS-CORAS: A Structured Method for Establishing an ISO?27001 Compliant Information Security Management System,” Springer, Cham, 2014, pp. 315–344.

[69] A. Asosheh, P. Hajinazari, and H. Khodkari, “A practical implementation of ISMS,” in *7th International Conference on e-Commerce in Developing Countries:with focus on e-Security*, 2013, pp. 1–17.

[70] Heise.de, “WLAN und LAN sichern mit IEEE 802.1X und Radius | c’t Magazin.” [Online]. Available: https://www.heise.de/ct/artikel/WLAN-und-LAN-sichern-mit-IEEE-802-1X-und-Radius-979513.html. [Accessed: 05-Dec-2017].

[71] A. Shostack, *Threat modeling : designing for security*. .

[72] Bayerische Staatsverwaltung, “IT-Sicherheitsrichtlinien für die bayerische Staatsverwaltung – Leitlinie zur Informa... Seite 1 von 5,” 2016.

[73] Apache Software Foundation, “The Apache Tomcat Connectors - AJP Protocol Reference - AJPv13 extensions Proposal.” [Online]. Available: https://tomcat.apache.org/connectors-doc/ajp/ajpv13ext.html. [Accessed: 11-Dec-2017].

[74] M. K. Jayanthi, “Strategic Planning for Information Security -DID Mechanism to befriend the Cyber Criminals to assure Cyber Freedom,” in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, 2017, pp. 142–147.

[75] S. Christian Fötinger, “Leitlinie zur Informationssicherheit an der Hochschule Augsburg,” pp. 1–4, 2017.