Higher Education Information Security Programme – HISP

“The universities know their information security risks and create trust through information security management!”

Information Security Unit of the Bavarian State Universities

Version 1.0 – Appendices A and B

Date	**Comment**
	Approval by CIOs of Bavarian research universities (*Universitäten*)
	Approval by computer centre managers/CIOs of Bavarian universities of applied sciences (*Hochschulen*)
	Association *UniBayern e.V.* informed
	Association *Hochschule Bayern e.V.* informed
	Bavarian State Ministry of Science and the Arts (*StMWK*) informed

Table of contents

A. Appendix – continual information security management

A.1. Introduction

The introduction of an ISMS is a strategic decision for a university. The creation and implementation of an ISMS are dependent on the needs and goals, the information security requirements, the administrative procedures and the size and structure of the university. It is to be assumed that all these factors will change over time.

The ISMS maintains confidentiality, integrity and accessibility of information by implementing a risk management procedure and enables partners and members of the university to trust in an appropriate management of risk at the university.

It is important to integrate the ISMS, which forms part of the organisational processes, into the overall steering structure of the organisation and to already take information security into consideration when planning processes, information systems and measures. It is expected that the implementation of an ISMS be scaled to fit the requirements of the university. The phases of a continuously improving ISMS are described as follows in ISO 27003 (see Figure 1: Regulatory cycle of an ISMS):

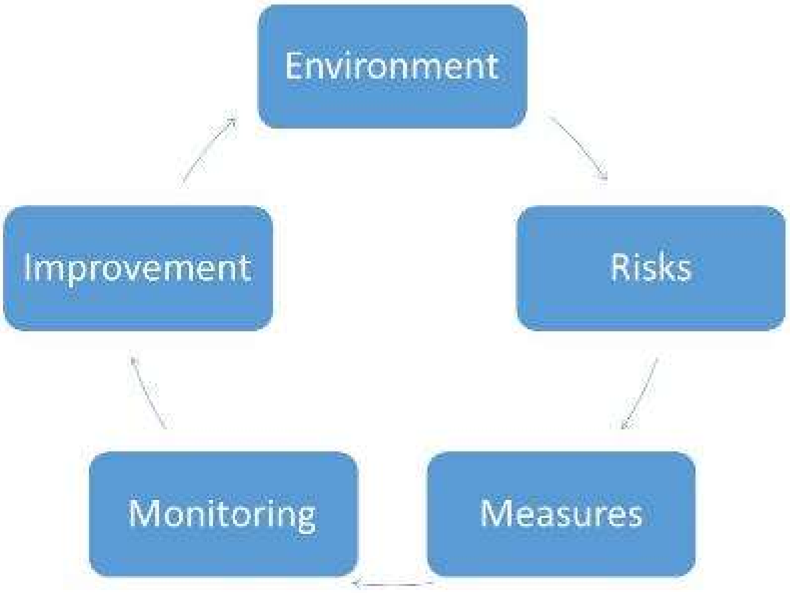

Figure 1: Regulatory cycle of an ISMS

A.2. Implementation and structure of an ISMS

The abstract steps can be matched to the steps of the ISO 27003 standard ("Information security management systems — Guidance") as follows.

Regulatory cycle	Chapter in ISO27003	HISP levels
Document the environment – Understanding of the university's needs and the necessity for establishing an information security policy, information security objectives and an information security framework.	**Environment of the organisation** • Org. context • Involved environment • Scope of the ISMS • Operation of the ISMS **Leadership** • Leadership and commitment • Policy • Roles and responsibilities	• Guidance, scope • Organisation • Communication, Training
Risks (planning) – Identification of the university's information security risks using a uniform university-wide classification of the information assets to be protected.	**Planning** • Dealing with risks ○ General conditions ○ Risk appetite • Plans and objectives	• Risk management
Measures (implementation) – Introduction and operation of information security processes, steering measures ('controls') and other measures for treating risks. *Note: This includes the improvements of the daily routines in operating a computer centre or a university that have been expanded to include information security*	**Support** • Resources • Competences • Awareness • Communication • Documents **Work processes** • Risk processes • Risk identification • Risk treatment	• Risk management
Implementing monitoring – Monitoring and reviewing performance and effectiveness of the ISMS.	**Performance assessment** • Monitoring, measuring and assessing the information security approach • Internal audit • Reports to executive management	• Evaluations • Audit
Deciding on improvements – Implementation of continual improvement.	**Improvement** • Correcting deviations • Continual improvement	This is not a separate HISP level as this is where decisions for improvement are made.

Table 1: Correlation of the steps to the ISO 27003 standard

Since the ISO 27003 standard only describes the steps in the regulatory cycle and other standards may be used for certification, the following describes the necessary steps in the higher education environment. Examples and forms are available in appendix B.

A.3. Steps to be undertaken by the universities (short version)

A.3.1. Environment

The university adopts a policy on information security and establishes an administrative unit that is responsible for implementation and improvement of information security. The role of Information Security Officer (ISO) has been assigned and appropriate competences have been authorised.

The ISO has been tasked with a project to introduce an ISMS and a committee monitors the degree of implementation and the results.

Information and training events need to be provided, some of which should be obligatory, so that all members of the institution and stakeholders can be involved with the ISMS at an early stage. For this purpose, the documents from the data protection and training plans provided centrally can be used.

A.3.2. Risks/planning

An essential step is adapting the available model classification and implementation document to the individual organisation. This may also be done in the form of a protection needs analysis. Insight into which information is most critical (identifying the information assets) will be the basis for all further steps and will therefore be the first implementation priority; it will also define the framework for setting up the information management system.

The roles of a risk manager and a decision-making body need to be defined and assigned. They then need to establish processes for identifying, assessing and treating risks. Only a continual review of new and existing risks can lead to continual improvement.

A.3.3. Measures

The integration of risk management into university operations will document measures to improve information security, regardless of the standard chosen.

An important part of these measures will be to set up an ISMS, including the creation of necessary plans and documents, and integrating the ISMS into existing IT processes and university administration.

An audit should be performed by a Bavarian university auditor, to monitor the effectiveness of existing measures and their conformity with an ISMS standard and to set priorities for the new measures.

A.3.4. Monitoring

A regular report needs to be submitted to executive management and measures for dealing with deviations and changed or new requirements need to be planned.

A continual audit plan including internal and external audits, testing for vulnerable areas and penetration tests needs to be created. Deviations need to be formally reported to risk management for assessment.

A.3.5. Improvement

Suggestions for improvements are presented to the decision-making bodies.
Projects to correct deviations are started.
Projects are started for the necessary expansion to the faculties, institutes or research facilities.

B. Appendix – notes on implementation

The following steps describe model procedures at a university.

B.1. Implementation of step 0 – survey of the status quo

An individual survey of the status quo will show the university clearly which processes to strengthen information security are at what capability level. Except for universities that are already working on certification (like the University of Bamberg and the University of Bayreuth), the existence of an ISMS is not to be expected.

The survey of the status quo can make a considerable contribution to presenting the most vulnerable areas and to eliminating these weaknesses these whilst setting up an ISMS.

In general, this audit is helpful in understanding the next steps in building an ISMS, as it addresses the individual improvement processes in detail.

B.1.1. Objectives

a) Clarifying the requirements for an ISMS and gaining insight into its potential scope and security issues within relevant processes.

b) The audit report highlights necessary measures and helps to set priorities for implementation.

c) Awareness is raised at board level.

d) The university needs to demonstrate that an information security management system is being developed, implemented, maintained and continually improved.

The results and the list of measures help the university to focus on issues that require more attention and resources. Often, systems that are well established and for which the university has sufficient resources and know-how are continuously improved.

B.2. Implementation of step 1 – ISMS environment – guidance and organisation

B.2.1. Objectives

Details of the tasks to be completed to achieve the goals are listed in point B.2.4 et seq.

a) The university needs to determine internal and external topic areas that are relevant to its purpose. In the case of universities, these topic areas will be administration, research and teaching.

b) The university needs to identify (and list in alphabetical order) the stakeholders that are relevant for the information security management system and their requirements with regard to information security.

c) The university needs to define the limits and the applicability of the information security management system in order to determine its scope, taking into consideration interfaces and dependencies between activities performed by the university itself and activities performed by other organisations. Therefore, security issues must be considered that concern data protection in the sense of risk management and at the interfaces with non-commercial partners, such as the German National Research and Education Network (*DFN*), the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities (*LRZ*), the Erlangen Regional Computing Centre (*RRZE*) or the *PRIMUSS* association as well as with service providers, such as *Bechtle*, *Sophos* and *HIS*. Special attention needs to be paid to internal interfaces, such as with

Human Resource Management, Quality Management, Marketing or Facility Management.

d) The executive management of the university needs to show leadership and commitment with regard to the information security management system.

e) University management must adopt an information security policy.

f) University management must ensure that the responsibilities and rights for roles connected to information security are assigned and communicated.

B.2.2. Capability levels guidance

Level	Capability level	Characteristics
0	**Non-existent**	There is no guideline and there are no IT regulations.
1	**Existent but informal**	There are IT regulations or similar rules for handling IT devices or for using central services and/or IT systems. De-facto standards have become established practice.
2	**Planned and tracked**	Uniform rules, such as virus protection, identity management (IDM – logical access), network segments, access control (physical access), etc. are in place.
3	**Well-defined**	These rules and regulations and their scope have been confirmed by executive management and relevant executive staff; they are well documented and approved. They are revised at irregular intervals and are binding within the area(s) to which they apply.
4	**Quantitatively controlled**	The rules and regulations have been reviewed by an independent party or are based on a central model and represent a complete set of information security guidelines.
5	**Continuously improving**	The rules and regulations as well as the scope are **regularly reviewed** and **adapted**. If the situation changes (new tasks such as university clinic or new types of risks), the documents are revised and adapted.

Table 2: Capability levels for environmental analysis and leadership

B.2.3. Capability levels organisation

Level	Capability level	Characteristics
0	**Non-existent**	No organisation for information security exists or no responsibility has been assigned.
1	**Existent but informal**	The tasks are performed by one or more people. These tasks are not mentioned in this person's/these people's job description(s). Information security is understood as a general task.
2	**Planned and tracked**	The tasks of information security are informally assigned to a person.
3	**Well-defined**	The responsible person has been endorsed by the relevant manager, tasks are documented and resources have been made available. These are prioritised by a committee that is involved in decision-making processes. The person responsible has been made known throughout the university and is the contact person for information security.
4	**Quantitatively controlled**	Reports on the current status of information security are drawn up and sent to the responsible committee on a regular basis.
5	**Continuously improving**	The rules and tasks as well as resources for information security are **regularly reviewed** and **adapted**. If the situation changes (new tasks or new types of risks), the priorities are revised and adapted.

Table 3: Capability levels organisation

B.2.4. Details on ISMS environment

			Capability level	**Measures**		
Objectives	**Content**	**Models/Templates/Suggestions**	**0-5**	**ISO**	**BSI 200-1** ***BSI Grundschutz-Profil***[1] (component)	**ISIS12**[2]
Relevant topics	• Research data • Research projects • Examinations, examination results and grades • Student data and other personal data • Budget, personnel and other administrative information	• Research data • Research projects • Patient data (university clinics and psychotherapeutic counselling services) • Examinations, examination results and grades • Student data and other personal data • Support for critical infrastructure (high performance computing – HPC) • etc.		Chapter 4.1	Chapter 4.1 1. (ISMS.1)	
Stakeholders and their requirements	• Administrative departments • Library • Students	• Other (external) researchers • Administrative departments • Faculties • Research partners • Ministry • Students		Chapter 4.2	Chapter 4.1 1. (ISMS.1)	

[1] basic IT security profile

[2] ISIS12 is a German information security management system in 12 steps that was specifically developed for use in municipal administration and small and medium-sized enterprises (SMEs).

Determine applicability and limits of the ISMS	• Statement of Applicability • List of external service providers	Statement of Applicability ISO27k_SOA.xlsx		Chapter 4.3	Chapter 4.1 1. (ISMS.1)	
Leadership and commitment guidance	• Strategic orientation • Integrates into university processes • Makes necessary resources available • Communicates the importance and meaning of the information security management system; • Achieves intended results • Instructs and supports employees • Supports continual improvement • Supports relevant management staff	Guidance SicherheitsLL_template_ISO27K.docx SicherheitsLL_template_BSI.docx		Chapter 5.1 and 5.2	Chapter 4.1 2. and 3. (ISMS.1)	Step 1 B1.1 M 1.1 M 1.2 M 1.3 M 1.4
Assign and communicate rights for roles within ISMS	• Organisation chart • Organisation guideline • Specification of tasks	SK_Sicherheitsorganisation_Vx.docx		A 6.1 Chapter 5.3	Chapter 4.1 2. U. 7.2 (ORP.1)	Step 1 B 1.1, B1.2 M 2.1 M 2.2 M 1.9 M 1.10

B.2.5. Work packages

Possible processes

- Approval and review process for regulations
- Agreement process with
    - legal department, data protection
    - purchasing
    - R&D
    - administration
    - faculties

possible projects

- Create and adopt policy
- Create and adopt administrative guideline
- Assign, nominate functions
- Create description of tasks for Information Security Officer (ISO)
- Clarify who the stakeholders are and possible connections to existing processes
- Create statement of applicability
- Determine relevant information

Supporting tools/software

- Document management
- Project management
- ISMS tool
- Inventory

Affected roles/positions

- University Management
- ISO
- Responsible project manager (possibly the ISO)
- Technical and business as well as strategic management of the computer centre
- Stakeholders
- Data Protection Officer

B.2.6. Review, audit questions, minimum requirements

ISO 2700x	***BSI Grundschutz*** (Federal Office for Information Security's (*BSI*) basic IT security recommendations)	**ISIS12**
A5 – information security guidance A 6.1 – internal organisation	General measures Relevant components from the basic IT security profile for universities: Priority 1: - ISMS.1 - ORP.1 - ORP.2 Priority 3: - ORP.5	**Checklist for step 1** 1.8.1 Has the information security guidance been completed? 1.8.2 Has the information security guidance been signed off by all the members of the board? 1.8.3 Has the significance of information security with regard to specific company objectives been portrayed? 1.8.4 Has the scope of the policy been determined? 1.8.5 Has a (new) review date been set and has responsibility been assigned? **Checklist for step 3** 3.4.1 Has executive management designated someone as Information Security Officer based on a role description? 3.4.2 Is this person familiar with their tasks within the organisation as ISO? 3.4.3 Are the role of the ISO and who the current ISO is sufficiently known within the organisation? 3.4.4 Is there an information security team and have their tasks, rules, reporting structures and frequency of meetings been clarified? 3.4.5 Has the position of ISO been entered into the organisation chart? 3.4.6 Has a (new) review date been set and has responsibility for this review been assigned?

B.2.7. Reports and improvement

Key figures, KPIs
• Number of documents reviewed, edited and released • Number of documents published • Percentage of IT systems within the scope • ISMS review process • Scope of activity of the information security organisation • How up-to-date is the list of people involved?

Items to report and frequency
• Status of the regulations • Capability level of the ISMS • Projects in progress to develop regulations • Stakeholders (new research projects, partners etc.) • Meeting (with status report) 2-4 x per year • Overall report 1 x per year

B.2.7.1. Performance indicator (PI – examples):

Involvement of university management

Description	Significance or purpose
Purpose	Recording university management's involvement and review activities concerning information security
Indicator	Average participation ratio for information security meetings
Formula	PI = number of meetings held / number of planned meetings * 100
Desired results	Green: PI >= 70 %, Yellow: 70 % < PI >= 50 %, Red: PI < 50 % • Green: no action necessary • Yellow: monitor trends in the indicator and check corrective measures • Red: intervention necessary; clarify circumstances and decide on corrective measures
Records and data source	• Number of planned review meetings • Number of planed or unplanned meetings actually held or postponed • Schedule and contents of review meetings; minutes of these meetings
Frequency of review	Collection: quarterly Analysis and report: once a semester Review of measures: every 2 years
Responsible	• Person responsible for ISMS

Review of information security regulations

Description	Significance or purpose
Purpose	Assessment of whether regulations are in fact reviewed as scheduled or in the case of significant changes in the environment
Indicator	Percentage of regulations reviewed
Formula	PI = number of amended regulations / number of approved regulations * 100
Desired results	Green: PI >= 80%, Yellow: 80 % < PI >= 40 %, Red: PI < 40 % • Green: no action necessary • Yellow: monitor the indicator, observe trends and review corrective measures • Red: intervention necessary; clarify circumstances and determine corrective measures
Records and data source	• History of amendments to the regulations • List of regulations with mention of amendments • Schedule for reviewing regulations, Document Management System resubmission/follow-up schedule
Frequency of survey	• Annually
Responsible	• Information owner of the regulations • Person responsible for ISMS

Review of the ISMS process

Description	Significance or purpose
Purpose	Assessment of the degree to which an independent review of information security levels is conducted
Indicator	Progress rate of the conducted independent reviews
Formula	PI = number of reviews conducted / number of planned reviews
Desired results	0.8 <= PI <= 1.1 If the resulting figure is below 0.6, intervention is needed urgently.
Records and data source	• Review schedule (number of planned reviews) • Review reports (number of reviews conducted)
Frequency of review	• Annual
Responsible	• Internal auditor • Person responsible for ISMS

B.2.7.2. Efficiency indicator (EI – example):

Involvement of university management

Description	**Significance or purpose**
Purpose	Recording university management's involvement and supervisory activities concerning information security
Indicator	Average participation rate for information security meetings
Formula	EI = mean and standard deviation of participation rate in review meetings
Desired results	Confidence intervals calculated on the basis of the standard deviation give the probability that an actual result lies close to the mean participation rate. Very large intervals point to a potentially large deviation and should be investigated further.
Records and data source	• Number of planned supervision meetings • Number of planed or unplanned meetings actually held or postponed • Number of planned and unplanned participants per meeting • Schedule and contents of review meetings; minutes of these meetings
Frequency of survey	Collection: quarterly Analysis and report: once a semester Review of measures: every 2 years
Responsible	• Person responsible for ISMS

B.3. Implementation of step 1 – ISMS environment – communication/training courses

B.3.1. Objectives

Details of the tasks to be completed to achieve the goals are listed in point 3.3. et seq.

All employees of the university should gain an appropriate level of awareness through training and regular updates of the regulations and procedures in the area of information security that are relevant to their area of work.

An awareness-raising programme for information security should be created that takes into account the information security policy, relevant procedures at the university as well as which information at the university needs protecting and the existing measures to protect it. This awareness-raising programme should comprise a range of measures, like campaigns (e.g. Information Security Day) or publishing brochures and memoranda. Training and further training in information security should cover general aspects, such as:

a) demonstrating executive management's commitment to information security throughout the university;

b) the necessity to familiarise oneself and comply with the regulations and responsibilities in place, as specified in guidelines, norms, legal provisions, contracts and agreements;

c) personal responsibility for actions or inaction as well as general responsibilities for securing and protecting information that is owned by the university or third parties;

d) general procedures to ensure information security and basic security measures;

e) contact people and resources for additional information and recommendations concerning information security, including further training documents.

B.3.2. Capability levels

Level	Capability level	Characteristics
0	**Non-existent**	No training or communication procedures concerning information security exist.
1	**Existent but informal**	Training measures are requested and approved individually. Occasionally, university members are informed of general events (such as phishing attacks).
2	**Planned and tracked**	There are training measures on information security and information on these is available on the university website. University members are trained at irregular intervals.
3	**Well-defined**	There are regulations on participation in training measures for university members. Training measures are tailored to different work areas within the organisation and are approved by supervisors. They are revised at irregular intervals and are binding within the university.
4	**Quantitatively controlled**	Participation in training measures is monitored and regularly checked; participants who have not participated are reminded to do so.
5	**Continuously improving**	Training courses are **regularly reviewed** and **adapted**. Whenever circumstances change, the documents are reviewed and amended.

Table 4: Capability levels – communication and training

B.3.3. Details on communication/training

			Capability level	**Chapter/modules/measures**		
Objectives	**Content**	**Models/Templates/Suggestions**	**0-5**	**ISO**	**BSI 200-1** ***BSI Grundschutz-Profil***	**ISIS12**
• Management commitment • Knowledge of rules • Personal responsibility • Basic procedures and measures • Contact person • Awareness-raising programme	Content for • Employees (new, existing) • Teaching staff • Executive management • Administrators (specialised training courses) • ‘Security Days’ • Newsletters • Information pages on website • User Regulations	• Moodle courses • *BITS* (*Behörden IT-Sicherheitstraining* – an IT security training programme for public authorities) • Communication guidelines of the University of Applied Sciences Würzburg-Schweinfurt (*FHWS* – available on request)		Chapter 7.2.2	ORP.3	Step 2; parts of B1.2 M 1.81 M 2.13 M 2.16 M 2.46 M 2.78 M 2.91 M 2.176 M 2.180 M 2.184 M 2.188 M 2.196 M 2.224 M 3.1

B.3.4. Work packages

Possible processes	possible projects	Supporting tools/software	Affected roles/positions
• Invitations to training courses • Monitoring participation/escalation • Integration into university further training processes • Data protection training courses • Updates in appropriate format (newsletter, website) • Update contact person(s)	• Develop set of courses and keep it up-to-date (if regulations change) • Organise Security Days • Selection of training courses • Plan specialised training course for administrators/developers	• eLearning • Knowledge management	• Marketing department • Personnel department (for internal training courses) • Staff council • ISO • Responsible project manager (possibly the ISO) • Data Protection Officer

B.3.5. Review, audit questions, minimum requirements

ISO 2700x	***BSI Grundschutz*** (Federal Office for Information Security's (*BSI*) basic IT security recommendations)	**ISIS12**
A 7.2.2 – Information security awareness and training	ORP.3 requirements	**Checklist for step 2** • 2.3.1 Have all employees been informed about ISIS12 and has awareness of information security been raised? • 2.3.2 Has it been ensured that employees will be informed about information security regularly in the future? • 2.3.3 Have employees been informed of possible sanctions in the case of violations of the guidance, of future security guidelines or generally in the case of security breaches? • 2.3.4 If there is an employer representation, was employee representation also involved? • 2.3.5 Has a (new) review date been set and has the responsibility for this next review been allocated?

B.3.6. Reports and improvement

Key figures, KPIs	Items to report and frequency
• Availability and up-to-dateness of awareness-raising programme/procedure • Number of people trained • Number of courses planned and that took place • Number of regulations covered in training courses • Up-to-dateness of contact lists (internal and external contact persons for information security)	• Participation status • Topicality of courses • Planning a Security Day, participation in Cyber Security Month • Conducting campaigns • Regular reporting in the security committee

B.3.6.1. Performance indicator (PI – example):

ISMS and information security awareness training

Description	Significance or purpose
Purpose	Assessment of the extent to which the ISMS requirements are communicated in the training courses.
Indicator	Percentage of people who have received training in IT security
Formula	PI = number of people who have received training / number of people who need to receive training * 100
Desired results	Green: PI >= 90 %, Yellow: 90 % < PI >= 60 %, Red: PI < 60 % • Green: no action necessary • Yellow: monitor the indicator, observe trends and review corrective measures • Red: intervention necessary; clarify circumstances and determine corrective measures
Records and data source	• Attendance list • Number of employees by groups • VIVA
Frequency of survey	• Annual or every six months
Responsible	• Person responsible for training courses • Person responsible for ISMS

B.3.6.2. Efficiency indicator (EI – example):

ISMS and information security awareness training

Description	**Significance or purpose**
Purpose	Assessment of the understanding of the ISMS and information security
Indicator	Percentage of people who have passed an end-of-training test
Formula	EI = number of people who have passed the test / number of people who sat the test * 100
Desired results	Green EI >= 90 %, Yellow: 90 % < EI >= 60 %, Red: EI < 60 % • Green: no action necessary • Yellow: monitor the indicator, observe trends and review corrective measures • Red: intervention necessary; clarify circumstances and determine corrective measures
Records and data source	• Attendance list • Test results/certificates/badges
Frequency of survey	• Collection: after test completion • Quarterly
Responsible	• Person responsible for training courses • Person responsible for ISMS

B.4. Implementation of step 2 – risk management

B.4.1. Objectives

Details of the tasks to be completed to achieve the goals are listed in point B.4.3 et seq.

The university needs to plan:

a) a classification plan for classifying the value of information assets;

b) measures for dealing with these risks and opportunities;

c) how the measures are integrated into and implemented within ISMS processes;

d) how the effectiveness of these measures is assessed.

e) A process for risk assessment;

f) criteria for risk acceptance;

g) storage of documented information on the assessment process;

h) a process and options for risk treatment.

B.4.2. Capability levels

Level	Capability level	Characteristics
0	**Non-existent**	There is no procedure for risk assessment. No classification of information assets has been conducted.
1	**Existent but informal**	Information classes and risks are assessed ad hoc by the responsible information owners or system administrators. Measures are evaluated in the team, but there is no uniform classification and integration plan.
2	**Planned and tracked**	A division into personal and non-personal data is documented and can be traced. Agreement on criticality classes of information and security measures has been reached. These are communicated as de-facto standards within the area of responsibility.
3	**Well-defined**	Frameworks for classifying information for all protection goals have been confirmed by management, well documented and approved. There is a documented procedure for recording, assessing and treating risks. The people responsible for and involved in this procedure have been designated. Measures are integrated into operations in a structured manner.
4	**Quantitatively controlled**	A list of risks and resulting measures is monitored by an individual or committee. Information owners check the measures to classify data.
5	**Continuously improving**	The assessment process and the accepted risks, including assessment criteria, are checked and amended regularly, in the case of important changes to the environment or when weaknesses have been identified. The effectiveness (risk assessment) of measures is regularly checked and measures are adapted to changed circumstances (assessment of residual risk).

Table 5: Capability levels for risk management

B.4.3. Details of risk management

			Capability level	**Measures**		
Objectives	**Content**	**Models/Templates/Suggestions**	**0-5**	**ISO 27001**	**BSI 200-x** ***BSI Grundschutz-Profil***	**ISIS12**
Risk management organisation	• People involved • Threshold values • Risk appetite • Reporting periods	ISO27005 (chapter 7.4) BSI 200-1 (chapter 8.1)				
Classification system	Protection goals: • Confidentiality • Integrity • Availability	Classification system provided by the Information Security Unit of the Bavarian State Universities		Chapter A.8.2 chapter 6.2	200-1: Chapter 4.2 200–2: chapter 5.1	Step 4 B 1.11 M 1.39
Measures for dealing with risks and opportunities	• Define risk acceptance criteria and risk treatment options • Risk management process • Integration into ISMS procedures and review of effectiveness	ISO 27005 Determination of need for protection according to *BSI* standard 200-2 followed by risk review according to *BSI* standard 200-3 (risk analysis) Project paper – *„IT-Risikoanalyse für IT-Sicherheitsmanagement“* (IT risk analysis for IT security management) Farruh Djumayev – *„Vorgehensweise bei der Einführung eines IT-Risikomanagements an Hochschulen“* (How to introduce an IT risk management system at a university)		Chapter 6.1 chapters 8.2 & 8.3	200-2: Chapters 6/7/8 determination of need for protection chapter 7.5 risk analysis chapter 7.8 200-3 (risk analysis)	Step 6 (determination of need for protection)

		Firuza Muhamadova – *„Analyse und Ausarbeitung der in den ISO-Standards 27001-27005 geforderten Prozesse zum Betrieb eines ISMS“ (Analysis and report on the processes for operating an ISMS that are required by the ISO standards 27001-27005)*				

B.4.4. Work packages

Possible processes	**possible projects**	**Supporting tools/software**	**Affected roles/positions**
• Risk identification • Risk assessment • Risk documentation • Risk acceptance • Risk treatment • Reporting procedures • Update of framework conditions	• Setting up a risk management process • Reporting • Survey of framework conditions	• Document management • Risk management/ISMS tool • Project management • Change management (integration) • Ticketing system (integration)	• University Management • ISO • Responsible project manager (possibly the ISO) • Technical, business and strategic management of the computer centre (for IT risks) • Stakeholders • Data Protection Officer • Quality management

B.4.5. Review, audit questions, minimum requirements

ISO 2700x	***BSI Grundschutz*** (Federal Office for Information Security’s *(BSI)* basic IT security recommendations)	**ISIS12**
Chapter 6 - Planning chapter 8 - Operation chapter 9 - Evaluation of Achievements A 5 - Information security guidance A 6.1 - Internal organisation A 8.2 - Classification of information assets	BSI standard 200-2 chapters 7.5 & 8.2 BSI standard 200-3 requirements • ISMS.1 • ORP.1 • CON.2 (data protection)	**Checklist for step 6** 6.5.1 Have currently critical applications and IT services been identified? Has a list of critical applications and IT services been created? 6.5.2 Have the categories of need for protection been adapted to the organisation and has management approved them? 6.5.3 Has the need for protection been determined, justified and documented by the responsible members of staff for all critical applications? 6.5.4 Has an MTPD been allocated to each critical application?

B.4.6. Reports and improvement

Key figures, KPIs
• Number of newly identified risks • Number of risks treated • Number of residual risks reported and accepted • Risk potential/risk status

Items to report and frequency
• Status of risks • Per semester for medium risks • Quarterly for high risks • As needed for very high risks

B.4.6.1. Efficiency indicator (EI – example):

Risk potential

Description	Significance or purpose
Purpose	Assessment of potential/danger of information security risks for the university. The accepted threshold value for medium and high risks should be defined and the staff responsible should be informed promptly if this threshold is exceeded.
Indicator	• Number of risks that are above the threshold value and need to be treated • Number of risks that were reported promptly • Period for reporting risks above the threshold value
Formula	PI = number of reported risks above the threshold value / number of risks above the threshold value EI = Number of risks above the threshold value not reported promptly

Desired results	PI = 1
	EI = 0

Records and data source	• Register/list of risks
Frequency of survey	• Per semester
Responsible	• Risk owner/information owner • Risk processor

B.5. Implementation of step 3 – implementation of measures

B.5.1. Objectives

Details of the tasks to be completed to achieve the goals are listed in point B.5.3 et seq.

Now it is time to implement the procedures defined in step 2 and integrate them into operations. Operating these procedures will help you to select appropriate measures for minimising risks, assess the residual risk, plan the implementation and check the effectiveness of the measures. This creates an improvement cycle (Plan-Do-Check-Act, PDCA) for the selected measures in order to maintain the level of information security for these.

Management provides resources to implement necessary measures competently and to the extent that they are necessary.

Audits should be performed by Bavarian university auditors at regular intervals.

Technical measures for protecting IT infrastructure and operations are described in the respective standards. In this document, the focus is on processes and concepts that need to be integrated in order to improve information security.

B.5.2. Capability levels

Level	Capability level	Characteristics
0	**Non-existent**	There are no procedures for fulfilling the information security requirements. Measures are not steered based on risk. There are no treatment plans.
1	**Existent but informal**	Measures are discussed in the team and implemented on an ad-hoc basis within the area of responsibility of the information owner or system administrator.
2	**Planned and tracked**	There is an internal agreement on measures to fulfil information security requirements. These are communicated as de-facto standards within the area of responsibility. Those responsible for implementing them have received appropriate training and a budget for implementing them has been approved by management.
3	**Well-defined**	The security guidelines for fulfilling the requirements (need for protection) are documented and have been approved. A procedure for risk treatment is documented and the measures are integrated into operations in a structured manner and as planned. A defined IT security budget has been agreed.
4	**Quantitatively controlled**	Planned changes are monitored by an individual or committee; the consequences of unintentional changes are assessed and, if necessary, measures are taken to reduce negative consequences. Outsourced processes are documented, checked and steered. The results of risk treatment are documented.
5	**Continuously improving**	Information security risk assessments are carried out at planned intervals, or when substantial changes are suggested or occur. Documented information on the results of information security risk assessments is stored. The effectiveness of measures already implemented is checked regularly and new measures are planned as necessary.

Table 6: Capability levels for implementing measures

B.5.3. Details of implementing measures

			Capability level	**Measures**		
Objectives	**Content**	**Models/Templates/Suggestions**	**0-5**	**ISO 27001**	**BSI 200-x *BSI Grundschutz-Profil*)**	**ISIS12**
Introduction or improvement of procedures to achieve the information security goals.	Planning and integration of operational processes for: • Documents • Changes, projects ○ Set-up, maintenance, removal • Purchasing • Identities & rights, access • Security incidents • Protection from malware • Weak spots • System development • Emergencies/continuity • Training courses • Inventory • Capacity planning • Logging • Review	Catalogues for various service management procedures: • ITIL • FitSM Firuza Muhamadova – *„Analyse und Ausarbeitung der in den ISO-Standards 27001-27005 geforderten Prozesse zum Betrieb eines ISMS“ (Analysis and report on the processes for operating an ISMS that are required by the ISO standards 27001-27005)* Thomas Kietreiber – *„Integration von Schwachstellenmanagement“ (Integration of weak spot management)*		Chapter 8 chapters A 6.1.5 A 7.2.2 A 7.2.3 A 7.3 A 8.1.1 A 8.3 A 9.2, A 9.4 A 10.1.2 A 11.1.2 A 11.2.7 A 12.1.2 A 12.1.3 A 12.2.1 A 12.4 A 12.5 A 12.6 A 13.1 A 14.2.2 A 14.2.5 A 15.2 A 16 A 17 A 18.2.1	BSI 200-2: Chapter 9 priority 1: ISMS.1.A9 ORP.3.A4 ORP.4 CON.3 CON.6 OPS.1.1 DER.4 priority 2: CON.2 CON.4 OPS.2.2 DER.2.1 priority 3: ORP.5 CON.1 CON.4 CON.7 OPS.1.2 OPS.2.2	Step 5 step 10 M 1.11 M 2.14 M 2.17 M 4.1 B 1.3 B 1.5 B 1.6 B 1.7 B 1.8 B 1.9 B 1.10 B 1.12 B 1.13 M 1.53 M 1.124 M 1.126
Budget	Planning a defined IT budget	5-10 % of the IT budget		Chapters 7.1 and 7.2	ISMS.1.A15	Step 10.3

Review of effectiveness	Test schedules, audits Intrinsic tests of measures taken	Matthias Mödinger – „Metrics and KPIs for Information Security Reports”		Chapters 8.2 A 18.2.2 A 18.2.3	DER.1 DER.3.2	M 2.84 M 2.85 M 2.87

B.5.4. Work packages

Possible processes	possible projects	Supporting tools/software	Affected roles/positions
Planning and integration of operational processes for: • Documents • Changes, projects ○ Set up, maintain, remove • Purchasing • Identities & rights, access • Security incidents • Protection from malware • Weak spots • System development • Emergencies/continuity • Training courses • Inventory • Capacity planning • Logging • Review	Introduction of service management, monitoring/auditing and reporting	• Monitoring software: ○ Ansible ○ Zabbix ○ Nagios ○ etc. • Network management • Security Information & Event Management • Logserver • Software distribution • Service management • Identity & access management • Central anti-virus solution and monitoring • Organisational continuity management • Data protection management • Business intelligence	• University management (budget) • ISO • Project manager • Technical and business as well as strategic management of the computer centre • Data Protection Officer • Service desk • IT administrators

B.5.5. Review, audit questions, minimum requirements

ISO 2700x	***BSI Grundschutz*** (Federal Office for Information Security's *(BSI)* basic IT security recommendations)	**ISIS12**
Specific information security training for technical staff in computer centre operations and development. Effectiveness of various IT operational procedures with intrinsic checks and improvement steps (A 12.1.1). Has an information security budget been allocated? Assigning, changing, deleting and checking access rights by the information owners. (A 9.2.5). Physical safety (A 11). Audits of information systems (A 12.7.1). Information transfer (A 13.2). Systems purchasing, development and maintenance (A 14.1, A 14.2.3, A 14.2.8, A 14.2.9). Supplier relations (A 15.1.1, A 15.2.1). Security incidents (A 16.1.6). Compliance (A 18).	Basic requirements for the relevant measures (see above) of the *BSI* basic security profile for universities. Procedure module DER (detection and reaction).	**Checklist for step 5** • 5.5.1 Have the three basic ISIS12 IT service management procedures been adapted and modelled? • 5.5.2 Is the IT staff familiar with the IT service management procedures? • 5.5.3 Were other necessary departments involved in the change process? • 5.5.4 Have the staff been appropriately informed about the areas of change requests and reporting faults and errors? **Checklist for step 10** • 10.9.1 Were the measures consolidated in accordance with chapter 10.1? • 10.9.2 Have the measures been prioritised according to their classification by need for protection, scope and dependencies? • 10.9.3 Has executive management decided on the implementation of the measures? • 10.9.4 Have the roles of initiator, implementer and person responsible for monitoring been assigned for all pending measures? • 10.9.5 Have specific implementation dates and, if necessary, training dates been set and communicated to those responsible? • 10.9.6 Has a (new) review date been set and has responsibility for it been assigned?

B.5.6. Reports and improvement

Key figures, KPIs

- Number of improvement measures for internal processes
- Budget; use of resources
- Number of debriefings held after security incidents
- Number of checks performed on access rights
- Number of times maintenance on IT systems is performed (planned)
- Number of changes of relevant IT systems
- Performance of protection against malware
- Number of checks of log files
- Number and criticality of weak spots in IT systems
- Number of, time needed to deal with, and trend in security incidents
- Number of incidents, report and surveys of security incidents

Items to report and frequency

- Status indicators and critical situations monthly
- Reviews per semester
- Trends and planned actions quarterly
- Security incidents as needed
- Overall annual report

B.5.6.1. Efficiency indicator (EI – examples):

Budget, use of resources

Description	**Significance or purpose**
Purpose	Resources allocated to information security in relation to the university budget or IT budget.
Indicator	Numbers/amounts for resources (internal and external staff, hardware, software licenses, outsourced services, etc.) in the current budget (semester/year/two years) compared to use expressed in monetary terms.
Formula	EI = cost incurred/costs budgeted for period
Desired results	EI = 1
Records and data source	Budget; cost centre or other cost tracking Budget items, use of funds
Frequency of review	Collection: semester; report: annual
Responsible	• Cost centre owner • Information Security Officer • Budget owner

Improvement measures for internal processes

Description	**Significance or purpose**
Purpose	Check the status of measures for improving information security as well as the administration in accordance with planned measures.
Indicator	Number of improvement measures (in period) in relation to planned measures (or actual cost and quality/persistence of planned measures in relation to planned values). Measures should also be evaluated as to whether the status (started, in progress, completed) originally planned for a given time is reached at that time. A weighting by criticality can improve measurement.
Formula	EI = ongoing or completed measures / planned measures * 100
Desired results	EI >= 90 %
Records and data source	Status tracing of improvement measures (ticketing system) Project planning
Frequency of review	Collection: semester; report: semester
Responsible	• Information owner, project manager • Information Security Officer

Learning from incidents

Description	Significance or purpose
Purpose	Check whether security incidents trigger improvement measures
Indicator	Number of security incidents that trigger improvement measures.
Formula	EI = Number of security incidents that trigger improvement measures / number of security incidents * 100
Desired results	EI >= 80 % or determined by security committee or university management
Records and data source	Improvement measures that can be traced back to a security incident Reports, lists of security incidents (ticketing system)
Frequency of review	Collection: semester; report: semester
Responsible	• Information owner, • CSIRT (computer security incident response team) • Information Security Officer

Effectiveness of access control

Description	Significance or purpose
Purpose	Ensuring an environment of comprehensive security and accountability for staff, institutions and information assets. Use of physical protection mechanisms to ensure appropriate protection of information.
Indicator	Number of instances of unauthorised access to rooms with information processing technology.
Formula	EI = current number of instances of unauthorised access
Desired results	EI = 0
Records and data source	Systematic analysis of access logs & alarms concerning unauthorised access Security reports on physical safety
Frequency of review	Collection: once a semester; report: semester
Responsible	• Facility management • CSIRT (if they are the recipient of alarms) • Information Security Officer, CIO

Effectiveness of security incident treatment

Description	Significance or purpose
Purpose	To check how effective security incident treatment is
Indicator	Number of security incidents that were not treated within the planned time period
Formula	• Determine the categories for security incidents and periods within which they must be treated • Set a limit to the duration by which the period for dealing with incidents may be exceeded (threshold value) • Compare the number of those incidents by category and threshold value
Desired results	EI = number of incidents that were not treated within the planned time period but did not exceed this time period beyond the threshold value that has been set for the applicable category
Records and data source	Instances of the threshold value being exceeded that are reported per month
Frequency of review	Collection: monthly; report and review of threshold values and planned time periods: once a semester
Responsible	• Person responsible for treating security incidents • Information Security Officer • CIO, recipient of report

Security incident trend

Description	Significance or purpose
Purpose	• To identify trends in security incidents • To identify trends in categories of security incidents
Indicator	Number of incidents in reporting period Number of incidents per category in reporting period
Formula	EI = average number of security incidents in one category in the last two periods / average number of security incidents in one category in the last 6 periods • Analysis of incidents • Analysis of incidents per category
Desired results	Example for limits (threshold values): Green: EI < 1 Yellow: 1 <= EI <= 1.3 Red: EI > 1.3

Records and data source	Number of reported security incidents per month from security reports or ticketing system
Frequency of review	Collection: monthly; report: once a semester
Responsible	• CSIRT • Information Security Officer, CIO, CISO

B.5.6.2. Performance indicator (PI – examples):

Checking user rights

Description	**Significance or purpose**
Purpose	Number of checks on user rights for critical/sensitive systems at the university
Indicator	Percentage of critical systems that need to be checked regularly
Formula	PI = number of checked critical systems / total number of critical systems * 100
Desired results	Green: PI >= 90 %, Yellow: 90 % < PI >= 70 %, Red: PI < 70 % • Green: no action necessary • Yellow: monitor trends in the indicator and review corrective measures • Red: intervention necessary; clarify circumstances and determine corrective measures
Records and data source	Confirmed reviews (email, ticketing system) Inventory of information, list of procedures
Frequency of review	Collection: monthly or when there are changes (new user/user leaves); report: annual
Responsible	• Information owner • Person responsible for ISMS • Staff responsible for systems

Access control

Description	**Significance or purpose**
Purpose	Shows the existence, scope and quality of the access control system
Indicator	Strength of access control system

Formula	PI capability level on a scale from 0 to 5 0 = no system 1 = PIN Code (or other mechanical 1-factor system such as keys) 2 = electronic access control system (Campus Card) as only factor 3 = card system with PIN Code (for selected areas) 4 = card system with PIN Code and activated logging 5 = card system with biometric second factor and activated logging
Desired results	PI >= 3
Records and data source	Checks for the following features in the access control system: • Access cards • PIN codes • Logging • Use of biometric data
Frequency of review	Collection: annual; report: annual
Responsible	• Facility management • University Management

Maintenance of information systems

Description	**Significance or purpose**
Purpose	Check timely maintenance according to a maintenance schedule
Indicator	Delays in maintenance per instance of maintenance performed
Formula	PI = difference in days between planned date and date when actually completed
Desired results	PI = 0 or delay that is accepted by the university (for example 3 days) Trend should be stable or approach zero
Records and data source	Completion date of planned maintenance, planned date of maintenance, total number of times maintenance was planned, total number of times maintenance was completed Maintenance schedule, ticketing system (maintenance tickets)
Frequency of review	Collection: once a semester; report: annual
Responsible	• System administrators • Service desk • Information Security Officer

Change management

Description	Significance or purpose
Purpose	Assessment whether best practices for change management and hardening rules are adhered to
Indicator	Percentage of new systems that were installed in accordance with change management and hardening rules
Formula	PI = number of correctly installed systems / total number of installed systems * 100
Desired results	Green: PI >= 90 %, Yellow: 90 % < PI >= 70 %, Red: PI < 70% • Green: no action necessary • Yellow: monitor trends in the indicator and review corrective measures • Red: intervention necessary; clarify circumstances and determine corrective measures
Records and data source	Ticketing system (change request tickets), inspection and approval reports, configuration check lists, completion reports Emails, post implementation review
Frequency of review	Collection: per semester; report: annual
Responsible	• Change manager, head of computer centre • System administrators • Information Security Officer

Protection from malware

Description	Significance or purpose
Purpose	Was malware installed on IT systems (in the university network) with out-of-date protection?
Indicator	Number of infected IT systems with out-of-date protection (more than 3/5/7 days old)
Formula	PI = number of infected IT system with out-of-date protection
Desired results	PI = 0
Records and data source	Infection with malware, console for protection from malware (report) Lists of security incidents (ticketing system), monitoring tools, system log files
Frequency of review	Collection: as they occur; report: monthly
Responsible	• IT operations/service desk • Information Security Officer • Management of computer centre

Checking logs

Description	Significance or purpose
Purpose	Check whether critical system logs were checked according to the requirements
Indicator	Percentage of critical system logs checked in the relevant period
Formula	PI = number of critical system logs checked / number of critical system logs * 100
Desired results	PI >= 20 %, if the PI is under 20 %, log file checking should be reviewed
Records and data source	Number of system logs Log files, tickets or other evidence that logs have been checked
Frequency of review	Collection: monthly; report: once a semester
Responsible	• Staff responsible for security, staff responsible for logging • Person responsible for ISMS • Information Security Officer

Vulnerability of information systems

Description	Significance or purpose
Purpose	Vulnerability assessment for IT systems containing sensitive data
Indicator	Percentage of critical IT systems that were identified as being vulnerable in a weak spot analysis or a penetration test
Formula	PI = number of critical IT systems that were identified as being vulnerable / number of critical IT systems * 100
Desired results	Green: PI >= 100 %, Yellow: 99 % > PI >= 75 %, Red: PI < 75 % • Green: no action necessary • Yellow: monitor trends in the indicator and review corrective measures • Red: intervention necessary; clarify circumstances and determine corrective measures
Records and data source	List of critical IT systems, reports on weak spot analyses and penetration tests, IT system inventory,
Frequency of review	Collection: after scans for weak spots or penetration tests; reporting: annual
Responsible	• Risk manager • Computer centre management • Information Security Officer

Data collection and reporting on security incidents and weak spots

Description	**Significance or purpose**
Purpose	To check whether security incidents and weak spots are reported and treated correctly
Indicator	Number of security incidents that are reported to the CSIRT and classified and treated as such
Formula	PI = number of reported security incidents / number of treated security incidents
Desired results	PI = 1
Records and data source	List of security incidents (ticketing system) and/or security incident reports Scans for weak spots
Frequency of review	Collection: annual; report: annual
Responsible	• University management, computer centre management • CSIRT • Information Security Officer

B.6. Implementation of step 4 – monitoring and review

A regular report needs to be submitted to executive management and measures for dealing with deviations and changed or new requirements need to be planned.

A continual audit plan including internal and external audits, testing for vulnerable areas and penetration tests needs to be created. Deviations need to be formally reported to risk management for assessment.

B.6.1. Objectives

Details of the tasks to be completed to achieve the goals are listed in point B.6.3 et seq.

To enable a comprehensive assessment of the effectiveness of the ISMS, the university needs to determine the following general conditions:

- Processes to be measured and measures to be taken
- Measurement methods
- Frequency of measurement and reporting periods
- Responsibilities for monitoring and review, measurement, collection, analysis and reporting

We recommend documenting these general conditions in a regulation. This regulation may also contain the university-wide ISMS audit schedule. This schedule covers the scope and frequency of internal and external audits that check whether the ISMS requirements are met, maintained or improved. Ideally, these audits are conducted by university auditors (colleagues from other universities).

Regular assessment meetings of the security committees need to be planned, so that the continuous suitability, appropriacy and effectiveness of the ISMS can be ensured. The report that the assessment is based on must contain the following points:

a) Status of measures decided on in previous assessment meetings;
b) Changes concerning internal and external issues that affect the information security management system;
c) Feedback on information security performance, including developments in:
    a. Non-conformities or correction measures;
    b. Results of reviews and measurements;
    c. Audit results; and
    d. Achievement of information security goals;
d) Feedback from interested parties;
e) Results of risk assessments and status of the plan for risk treatment; and
f) Possibilities for continual improvement

Decisions on continual improvement and the need for changes to the ISMS need to be documented in the minutes of the assessment meetings.

B.6.2. Capability levels

Level	Bis morgen	Characteristics
0	**Non-existent**	No existing or planned reports, audits or assessment meetings concerning the ISMS.
1	**Existent but informal**	Audits or other tests of the information security procedures are conducted at irregular intervals. The results are discussed in the team and implemented on an ad-hoc basis, like a project.
2	**Planned and tracked**	Information security procedures that serve an ISMS have been implemented and are complied with in the area of responsibility as a de-facto standard. External audits are conducted and the results are reported to committees or university management.
3	**Well-defined**	Information security procedures that serve an ISMS are documented in a number of regulations and are binding. Scans for weak spots and/or penetration tests are planned and regularly implemented. A report shows weak spots and the effectiveness of the ISMS and is submitted to a defined committee.
4	**Quantitatively controlled**	KPIs concerning the ISMS have been defined and are submitted to the committee in regular reports. Internal and external audits check the ISMS and the results are part of the regular report. Committee decisions are documented in meeting minutes.
5	**Continuously improving**	The security committee or university management decides on and plans regular supervisory audits and amendments to the ISMS; sufficient resources are provided to ensure implementation within the planned time frame. The KPIs are checked regularly (min. once every two years) for being usable and meaningful.

Table 7: Capability levels for monitoring

B.6.3. Details of monitoring

			Capability level	**Measures**		
Objectives	**Content**	**Models/Templates/Suggestions**	**0-5**	**ISO 27001**	**BSI 200-x** ***BSI Grundschutz-Profil***	**ISIS12**
Assessment of the ISMS	• Planning and definition of measured values and Key Performance Indicators (KPIs) • reporting periods and responsibilities	ISO27004 – ‘Information security management - Monitoring, measurement, analysis and evaluation’ Matthias Mödinger – „Metrics and KPIs for Information Security Reports” Matthias_Mödinger – ‘Information-Security-Report-Template_(english).doc’ Matthias_Mödinger – ‘Bestimmung KPIs_Value Benefit Analysis.xlsx‘ KPIs from the implementation chapters of this document.		Chapters 9.1 A 6.1.1 A 12.6.1 A 12.7.1 A 14.2.8 A 16.1.6 A 18.2	BSI 200-1: chapter 4 chapter 7.5 BSI 200-2: chapter 10 priority 1: ORP.1.A1 ORP.1.A14 priority 3: ORP.5.A4 ORP.5.A7	Steps 11 and 12 M 1.4
Audits	• Selection of standard • Audit schedule	ISO27001 BSI 200-1 ISIS12 TISAX SOC-2 …		Chapter 9.2	Chapter 7.4 DER.3.1.A13	Step 11
Committee meetings	• ISMS report • decision proposals • committee meeting minutes	Matthias Mödinger – „Metrics and KPIs for Information Security Reports” Anhang_Master_Thesis__Matthias_Mödinger__Information-Security-Report-Template_(english)		Chapter 9.3	BSI 200-1: chapter. 4.3 and chapter 8.3 ORP.5.A8	Step 11.5

B.6.4. Work packages

Possible processes	possible projects	Supporting tools/software	Affected roles/positions
• Analysis of the necessary performance indicators and measurement methods • Conducting audits • Reporting • Conducting assessment meetings	Introduction of a monitoring and reporting system (for the ISMS itself) Collaboration with quality management	• Monitoring software (measured values) • Security Information and Event Management tools (SIEM) • Business intelligence • Ticketing system	• University Management • ISO • Security committee • Data Protection Officer • Quality management

B.6.5. Review, audit questions, minimum requirements

ISO 2700x	***BSI Grundschutz*** (Federal Office for Information Security's *(BSI)* basic IT security recommendations)	**ISIS12**
Audits of information systems (A 12.7.1) Compliance (A 18)	Procedure component ORP.5 compliance requirements BSI 200-2 chapter 10	Review questions for the individual steps **Checklist for step 11 (optional)** • 11.6.1 Is there an audit schedule and does it contain all the important information? • 11.6.2 Is there an audit report? • 11.6.3 Have measures been developed as a result of the audit? • 11.6.4 Have the changes been documented? • 11.6.5 Has a new date been set and has responsibility for it been allocated? **Checklist for step 12** • 12.4.1 Has responsibility for the review dates been allocated to specific members of staff? • 12.4.2 Are the planned review dates within 12 months? • 12.4.3 Does the review schedule show what needs to reviewed in the next audit? • 12.4.4 Have any specific measures been identified that are still pending? If so, has it been ensured that these measures can be implemented within 12 months? • 12.4.5 Has management taken note of the annual report of the ISO?

B.6.6. Reports and improvement

Key figures, KPIs

- Number of improvement measures for the ISMS processes
- Audit programme
- Review of the ISMS

Items to report and frequency

- Reviews per semester
- Trends per semester
- Overall annual report
- Annual internal audits
- External audits once every two years

B.6.6.1. Efficiency indicator (EI – example):

Improvement measures for ISMS processes

Description	**Significance or purpose**
Purpose	Check the status of measures for improving information security as well as their administration in accordance with planned measures
Indicator	Number of improvement measures (in period) in relation to planned measures (or actual cost and quality/persistence of planned measures in relation to planned values). Measures should also be evaluated as to whether the status (started, in progress, completed) originally planned for a given time is reached at that time. A weighting by criticality can improve measurement.
Formula	EI = ongoing or completed measures / planned measures * 100
Desired results	EI >= 90 %
Records and data source	Status tracing of improvement measures (ticketing system) Project planning
Frequency of review	Collection: semester; report: annual
Responsible	• Information owner, project manager • Information Security Officer

B.6.6.2. Performance indicator (PI – examples):

Audit programme

Description	**Significance or purpose**
Purpose	To adhere to the review plan and the audit plan
Indicator	Number of planned review measures (e.g. audits, penetration tests, scans for weak spots) that were completed Number of planned review measures
Formula	PI = number of completed review measures / number of planned review measures * 100
Desired results	PI >= 90 %
Records and data source	Audit schedule, Results of review measures
Frequency of review	Collection: after every review measure; report: annual
Responsible	• Auditor, information security officer • Security committee, university management

Review of the ISMS (Audits)

Description	**Significance or purpose**
Purpose	To adhere to implemented and planned improvements concerning the effectiveness of the ISMS
Indicator	Number of planned audits that were conducted Number of planned audits
Formula	PI = Number of completed audits / Number of planned audits
Desired results	PI = 1, due to the small number of expected audits, no deviation can be tolerated
Records and data source	Audit schedule, Audit reports
Frequency of review	Collection: after every audit; report: annual
Responsible	• Person responsible for ISMS, auditor • Security committee, university management

B.7. Implementation of step 5 – improvement

B.7.1. Objectives

Details of the tasks to be completed to achieve the goals are listed in point B.7.3 et seq.

The university needs to react to deviations from the security requirements by using monitoring and/or correction measures. Appropriate measures need to be assessed (analysis of cause and extent), introduced and checked for effectiveness. The ISMS may need to be amended.

The decisions taken by university management or the defined decision-making body need to be documented as part of risk management and communicated to those responsible for implementing them. They need to be documented in the minutes of the decision-making meetings.

B.7.2. Capability levels

Level	Capability level	Characteristics
0	**Non-existent**	Deviations are not discovered or not assessed by a decision-making body and no measures are suggested.
1	**Existent but informal**	The head of the computer centre and the CIO are responsible for decisions concerning improvements to information security within the scope of their overall responsibility for information technology. Investments are processed as bulk orders.
2	**Planned and tracked**	Decision proposals for improvements are assessed and decided on by a security committee.
3	**Well-defined**	The improvement of information security is a regular topic in meetings of decision-making bodies and the results of these meetings are documented.
4	**Quantitatively controlled**	The security committee regularly requests reports on the status of the ISMS and deviations. It assess the severity, consults on appropriate corrective measures and provides sufficient resources for the necessary correction. Committee decisions are documented in meeting minutes.
5	**Continuously improving**	Reporting periods and scope of reporting are reviewed regularly (min. once every two years). If the reports are not sufficiently meaningful or if the environment changes, the reports are amended and the reporting and decision-making procedures are improved.

Table 8: Capability levels for Improvement

B.7.3. Details on improvement

			Capability level	**Measures**		
Objectives	**Content**	**Models/Templates/Suggestions**	**0-5**	**ISO 27001**	**BSI 200-x** ***BSI Grundschutz-Profil***	**ISIS12**
Reaction to deviations	- ISMS report (chapter on deviations) - Decision proposals, - Committee meeting minutes	Anhang_Master_Thesis__Matthias_Mödinger__Information-Security-Report-Template_(english) Risk assessment		Chapter 10.1 A 6.1.1	BSI 200-1: chapter. 4.4 and chapter 8.4 BSI 200-1: chapter 5.2.4 chapter 10.3 ORP.5.A8	Step 11.5
Improvement of the ISMS	- Records of decisions - Projects, bulk orders			Chapter 10.2	Chapter 7.5	Step 11.5

B.7.4. Work packages

Possible processes	**possible projects**	**Supporting tools/software**	**Affected roles/positions**
• Preparing the basis of decisions • Reporting on deviations from the ISMS	Introduction of a monitoring and reporting system (for the ISMS itself) Collaboration with quality management	• Monitoring software (measured values) • Security Information and Event Management tools (SIEM) • Business intelligence • Ticketing system	• University Management • Security committee • ISO • Data Protection Officer • Quality management

B.7.5. Review, audit questions, minimum requirements

ISO 2700x	***BSI Grundschutz*** (Federal Office for Information Security's (*BSI*) basic IT security recommendations)	**ISIS12**
ISO27001, chapter 10 Compliance (A 18.2.2)	BSI 200-1 chapter 4.4, 7.5 BSI 200-2 chapter 10.3	**Checklist for (parts of) step 11** • 11.6.3 Have measures been developed as a result of the audit? • 11.6.4 Have the changes been documented? • 11.6.5 Has a new date been set and has responsibility for it been allocated?

B.7.6. Reports and improvement

Key figures, KPIs	**Items to report and frequency**
• Number of improvement measures for the ISMS processes • Review of the ISMS	• Reviews per semester • Trends per semester • Overall annual report • Records of decisions

B.7.6.1. Efficiency indicator (EI – example):

Improvement measures for ISMS processes

Description	**Significance or purpose**
Purpose	Check the status of measures for improving information security as well as the administration in accordance with planned measures
Indicator	Number of improvement measures (in period) in relation to planned measures (or actual cost and quality/persistence of planned measures in relation to planned values). Measures should also be evaluated as to whether the status (started, in process, completed) originally planned for a given time is reached at that time. A weighting by criticality can improve measurement.
Formula	EI = ongoing or completed measures / planned measures * 100
Desired results	EI >= 90 %
Records and data source	Status tracing of improvement measures (ticketing system) Project planning
Frequency of review	Collection: semester; report: annual
Responsible	• Information owner, project manager • Information Security Officer

B.7.6.2. Performance indicator (PI – example):

Review of the ISMS (improvements)

Description	**Significance or purpose**
Purpose	To adhere to implemented improvements and decisions concerning the effectiveness of the ISMS
Indicator	Number of improvements implemented Number of decisions
Formula	PI = number of improvements / number of decisions * 100
Desired results	PI = 80 %
Records and data source	Minutes of decision committee meetings Implementation orders; bulk orders
Frequency of review	Collection: after every committee meeting; report: annual
Responsible	• Person responsible for ISMS, auditor • Security committee, university management