Hochschulinformationssicherheits-programm – HISP

'Die Hochschulen kennen ihre Informationsrisiken und schaffen durch Informations-sicherheitsmanagement Vertrauen!'

Stabsstelle Informationssicherheit der bayerischen, staatlichen Hochschulen und Universitäten

Version 1.0 – Anhang A und B

Datum	**Kommentar**
	Freigabe CIO Runde Universitäten Bayern
	Freigabe RZ-Leiter/ CIO Runde Hochschulen Bayern
	Information an UniBayern e.V.
	Information an Hochschule Bayern e.V.
	Information an StMWK

Inhaltsverzeichnis

A. Anhang - kontinuierliches Informationssicherheitsmanagement

A.1. Einführung

Die Einführung eines ISMS ist für eine Hochschule eine strategische Entscheidung. Erstellung und Umsetzung eines ISMS richten sich nach den Bedürfnissen und Zielen, den Informationssicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Hochschule. Es ist davon auszugehen, dass sich alle diese Einflussgrößen im Laufe der Zeit ändern.

Das ISMS wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Information unter Anwendung eines Risikomanagementprozesses und erlaubt Partnern und Hochschulangehörigen auf eine angemessene Steuerung von Risiken der Hochschule vertrauen zu können.

Es ist wichtig, dass das ISMS als Teil der Abläufe der Organisation in deren übergreifende Steuerungsstruktur integriert ist und die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt wird. Es wird erwartet, dass die Umsetzung eines ISMS entsprechend den Bedürfnissen der Hochschule skaliert wird. Die Phasen eines sich kontinuierlich verbessernden ISMS werden in der ISO27003 wie folgt beschrieben (siehe Abbildung 1: Regelkreis eines ISMS):

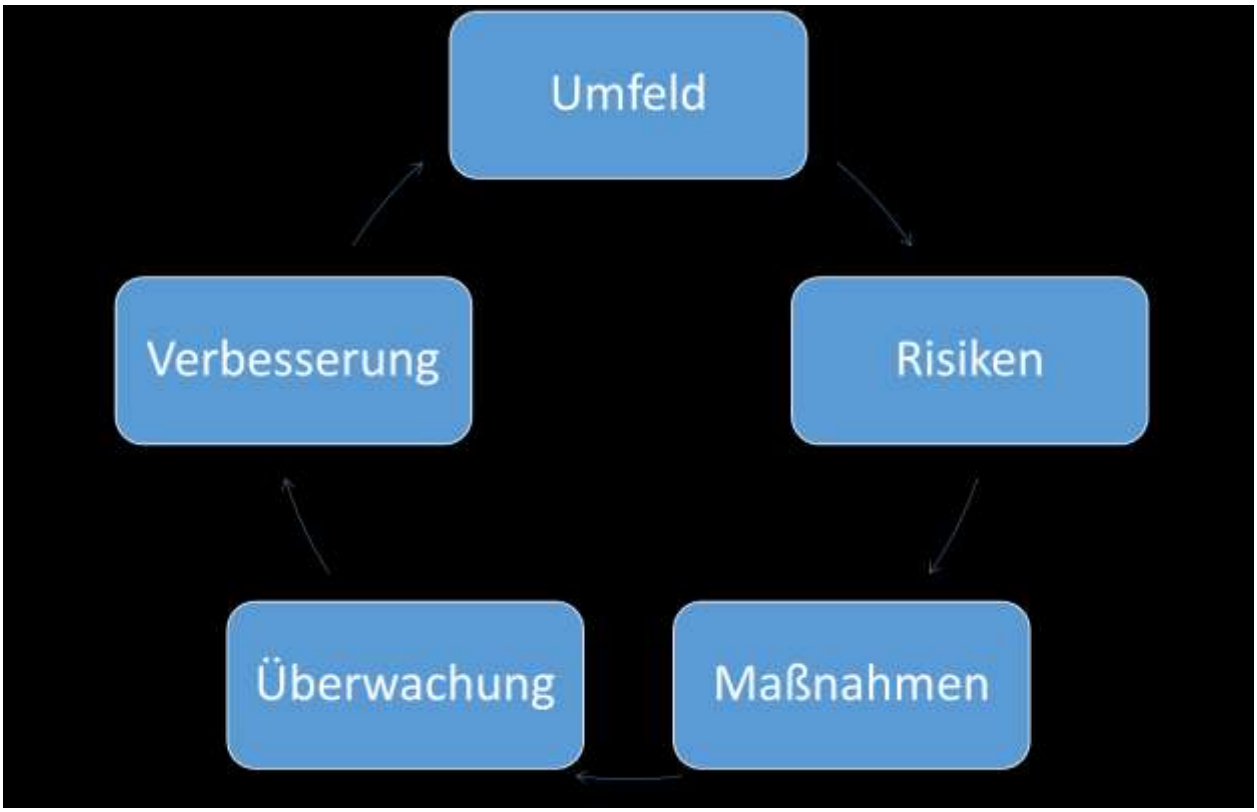

Abbildung 1: Regelkreis eines ISMS

A.2. Vorgehensweise und Aufbau eines ISMS

Die abstrakten Schritte lassen sich wie folgt den Schritten des ISO27003 Standards („Information security management systems — Guidance“) zuordnen.

Regelkreis	Kapitel ISO27003	HISP Arbeitspakte
Umfeld dokumentieren – Verständnis für die Bedürfnisse der Hochschule und der Notwendigkeit eine Informationssicherheitsleitlinie und -ziele und Rahmen zu etablieren.	**Umfeld der Organisation** • Org. Zusammenhang • Beteiligtes Umfeld • Umfang des ISMS • Betrieb des ISMS **Führungsverhalten** • Verhalten u. Verpflichtung • Richtlinien • Rollen, Verantwortung	• Leitlinie, Umfang • Organisation • Kommunikation, Schulung

Risiken (planen) – Erfassung der Informationssicherheitsrisiken der Hochschule über eine einheitliche hochschulweite Klassifikation der zu schützenden Informationen.	**Planung**
	• Umgang mit Risiken
	  ○ Rahmenbedingungen
	  ○ Risikoappetit
	• Pläne und Ziele
		• Risikomanagement

Maßnahmen(umsetzung) – Einführung und Betrieb von Informationssicherheitsprozessen, Steuerungsmaßnahmen und anderen Maßnahmen um die Risiken zu behandeln. *Anm.: Hier finden sich die Verbesserungen der um die Informationssicherheit erweiterten täglichen Abläufe im Betrieb eines Rechenzentrums bzw. einer Hochschule.*	**Unterstützung** • Ressourcen • Kompetenzen • Sensibilisierung • Kommunikation • Dokumente **Arbeitsablauf** • Risikoprozesse • Risikoerfassung • Risikobehandlung	• Risikomanagement
Überwachung durchführen – Überwachung und Prüfung der Performance und Effektivität des ISMS.	**Leistungsbeurteilung** • Überwachen, Messen, Beurteilen der Informationssicherheitskonzepte • Internes Audit • Berichte an die Leitung	• Berichte • Audit
Verbesserungen entscheiden – Ausüben der kontinuierlichen Verbesserung.	**Verbesserung** • Abweichungen korrigieren • Kontinuierliche Verbesserung	keine eigene Stufe aus HISP, da hier Entscheidungen zur Verbesserung getroffen werden.

Tabelle 1: Zuordnung der Schritte zum ISO27003

Da der ISO27003 Standard mit seinen Schritten nur den Regelkreis beschreibt und die Zertifizierung nach anderen Standards erfolgen kann, werden in der Folge die erforderlichen Schritte im Hochschulumfeld beschrieben. Beispiele und Formblätter werden im Anhang B zur Verfügung gestellt.

A.3. Schritte an Hochschulen (Kurzfassung)

A.3.1. Umfeld

Die Hochschulleitung verabschiedet eine Leitlinie zur Informationssicherheit und etabliert eine Organisation, die sich mit der Umsetzung und Verbesserung der Informationssicherheit beschäftigt. Die Rolle des/der Informationssicherheitsbeauftragten wurde einer Person zugewiesen und entsprechende Kompetenzen erteilt.

Der Auftrag zu einem Einführungsprojekt wurde an diese Person vergeben und ein Komitee prüft den Umsetzungsgrad und die Ergebnisse.

Es müssen zum Teil verpflichtende Informationsangebote entwickelt werden, um frühzeitig alle Angehörigen der Einrichtung und betroffenen Personen in das ISMS einzubeziehen. Dazu können die zentral zur Verfügung gestellten Unterlagen des Datenschutz- und Schulungskonzepts verwendet werden.

A.3.2. Risiken/Planung

Ein entscheidender Schritt ist Anpassung des verfügbaren Musterklassifikation-, und Umsetzungsdokuments an die eigene Institution. Dies kann ebenso in Form einer Schutzbedarfsanalyse erfolgen. Die Erkenntnis über die kritischsten Informationen wird Basis (Bestimmung der Informationswerte) für alle weiteren Schritte und die Priorität bei der Umsetzung sein und den Rahmen für den Beginn eines Informationssicherheitsmanagementsystems festlegen.

Die Rollen eines Risikomanagers und Entscheidungsgremiums sind zu definieren und Personen zuzuweisen. Diese müssen Prozesse zur Erfassung, Bewertung und Behandlung von Risiken etablieren. Nur die kontinuierliche Betrachtung der neuen und bestehenden Risiken kann zur kontinuierlichen Verbesserung führen.

A.3.3. Maßnahmen

Die Integration des Risikomanagements in den Betrieb der Hochschule wird unabhängig vom gewählten Standard Maßnahmen zur Verbesserung der Informationssicherheit dokumentieren.

Ein Teil dieser Maßnahmen wird der Aufbau des ISMS mit Erstellung notwendiger Konzepte, Dokumente, Integration in bestehende IT-Prozesse und die Organisation der Hochschule sein.

Es sollte ein Audit durch einen Auditor der Hochschulen Bayerns durchgeführt werden, um bestehende Maßnahmen auf Wirksamkeit und Entsprechung gegenüber einem ISMS Standard zu überprüfen und Prioritäten für die neuen Maßnahmen festzulegen.

A.3.4. Überwachung

Ein regelmäßiger Bericht ist der Leitung vorzulegen und für Abweichungen, geänderte oder neue Anforderungen müssen Maßnahmen geplant werden.

Ein kontinuierlicher Auditplan mit internen und externen Audits, Schwachstellenprüfungen und Penetrationstest ist zu erstellen. Abweichungen sind formal an das Risikomanagement zur Bewertung weiterzuleiten.

A.3.5. Verbesserung

Den Entscheidungsgremien werden Verbesserungsvorschläge unterbreitet und Projekte zur Korrektur von Abweichungen und notwendigen Erweiterung auf Fakultäten, Institute oder Forschungseinrichtungen werden gestartet.

B. Anhang - Umsetzungshinweise

Die folgenden Schritte beschreiben ein idealtypisches Vorgehen an einer Hochschule.

B.1. Umsetzung Schritt 0 - Bestandsaufnahme, Status

Die individuelle Bestandsaufnahme zeigt der Hochschule deutlich den Reifegrad der unterschiedlichen Prozesse zur Stärkung der Informationssicherheit. Außer bei den Hochschulen, die bereits an einer Zertifizierung arbeiten (wie die Universitäten Bamberg und Bayreuth) ist kein ISMS zu erwarten.

Wesentlich kann die Bestandsaufnahme dazu beitragen, die empfindlichsten Schwachpunkte zu präsentieren und helfen, parallel zum Aufbau eines ISMS diese zu beseitigen.

Allgemein ist dieses Audit für ein Verständnis zum weiteren Aufbau eines ISMS hilfreich, da die einzelnen Verbesserungsprozesse im Detail angesprochen werden.

B.1.1. Ziele

a) Klärung der Anforderungen eines ISMS an die Hochschule und Erkenntnis über den möglichen Umfang bzw. kritischen Punkte in relevanten Prozessen.

b) Der Auditbericht zeigt notwendige Maßnahmen auf und hilft bei der Priorisierung der Umsetzung.

c) Die Hochschulleitung wird für das Thema sensibilisiert.

d) Die Hochschule muss nachweisen, dass ein Informationssicherheitsmanagementsystem aufgebaut, verwirklicht, aufrechterhalten und fortlaufend verbessert wird.

Die Ergebnisse und Maßnahmenliste hilft der Hochschule die Aufmerksamkeit auf Zustände zu lenken, die mehr Aufmerksamkeit und Ressourcen benötigen. Oft werden Systeme kontinuierlich verbessert, die gut eingespielt sind und für die die Hochschule genügend Ressourcen und Know-How hat.

B.2. Umsetzung Schritt 1 - Umfeld des ISMS – Leitlinie und Organisation

B.2.1. Ziele

Details der Aufgaben, um die Ziele zu erreichen, entnehmen Sie dem Punkt B.2.4.ff.

a) Die Hochschule muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind. Im Falle einer Hochschule werden diese Themen die Verwaltung, Forschung und Lehre sein.

b) Die Hochschule muss die interessierten Parteien, die für ihr Informationssicherheitsmanagementsystem relevant sind, und die Anforderungen dieser interessierten Parteien (in alphabetischer Reihenfolge) mit Bezug zur Informationssicherheit bestimmen.

c) Die Hochschule muss die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen, und dabei Schnittstellen und Abhängigkeiten zwischen Tätigkeiten, die von der Hochschule selbst, und Tätigkeiten, die von anderen Organisationen durchgeführt werden, berücksichtigen. Daher müssen Sicherheitserwägungen in Hinblick auf den Datenschutz im Sinne eines Risikomanagements und an den Schnittstellen zu nicht kommerziellen Partnern, wie dem DFN, LRZ, RRZE, PRIMUSS Verbund und Dienstleistern, wie Bechtle, Sophos, HIS stattfinden. Bei der Integration in etablierte

Prozesse zur Förderung der Informationssicherheit bedürfen interne Schnittstellen wie zum Personal-, Qualitätsmanagement, Kommunikation oder zur Gebäudeleittechnik der besonderen Betrachtung.

d) Die Hochschulleitung muss in Bezug auf das Informationssicherheitsmanagement-system Führung und Verpflichtung zeigen.

e) Die Hochschulleitung muss eine Leitlinie zur Informationssicherheit verabschieden.

f) Die Hochschulleitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekannt gemacht werden.

B.2.2. Reifegradstufen Leitlinie

Stufe	Reifegrad	Ausprägung
0	**Nicht vorhanden**	Keine Leitlinie oder IT-Ordnungen sind vorhanden.
1	**Informell vorhanden**	Es gibt eine IT-Ordnung oder ähnliche Regelungen zum Umgang mit IT-Geräten bzw. zur Nutzung von zentralen Diensten und/oder dem Betrieb von IT-Systemen. De-facto Standards haben sich eingebürgert.
2	**Geplant**	Einheitliche Regelungen, wie Virenschutz, IDM (logischer Zugang), Netzwerksegmente, Zutrittskontrollen (physischer Zugang), etc. sind vorhanden.
3	**Dokumentiert**	Diese Regelungen und der Geltungsbereich sind von der Leitung und relevanten Führungskräften bestätigt, gut dokumentiert und freigegeben. Sie werden in unregelmäßigen Abständen überarbeitet und sind für den Geltungsbereich verpflichtend.
4	**Quantitativ überwacht**	Die Regelungen wurden von unabhängiger Stelle überprüft oder beruhen auf einer zentralen Vorlage und bilden einen vollständigen Satz an Informationssicherheitskonzepten.
5	**Kontinuierlich verbessert**	Die Regelungen und der Geltungsbereich werden **regelmäßig überprüft** und **angepasst**. Bei geänderten Umständen (neue Aufgaben wie Uniklinik oder neuartige Bedrohungen) werden die Dokumente überarbeitet und adaptiert.

Tabelle 2: Reifegradstufen zu Umfeldanalyse und Führungsverhalten

B.2.3. Reifegradstufen Organisation

Stufe	Reifegrad	Ausprägung
0	**Nicht vorhanden**	Keine Organisation für Informationssicherheit ist vorhanden bzw. keine Verantwortung zugewiesen.
1	**Informell vorhanden**	Die Aufgaben werden von einer oder verschiedenen Personen wahrgenommen. Es gibt keine Hinweise auf diese Tätigkeiten in der Aufgabenbeschreibung dieser Personen. Informationssicherheit wird als allgemeine Aufgabe verstanden.
2	**Geplant**	Die Aufgaben der Informationssicherheit werden einer Person informell übertragen.
3	**Dokumentiert**	Die verantwortliche Person ist von der Leitung und relevanten Führungskräften bestätigt, Aufgaben dokumentiert und Ressourcen freigegeben. Diese werden von einem Gremium, das in Entscheidungsprozesse involviert ist, priorisiert. Die Person ist hochschulweit bekannt gemacht und Ansprechpartner für Informationssicherheit.
4	**Quantitativ überwacht**	Berichte über den aktuellen Stand der Informationssicherheit werden regelmäßig an das verantwortliche Gremium erstellt.
5	**Kontinuierlich verbessert**	Die Aufgaben und Ressourcen der Informationssicherheit werden **regelmäßig überprüft** und **angepasst**. Bei geänderten Umständen (neue Aufgaben oder neuartige Bedrohungen) werden die Prioritäten überarbeitet und adaptiert.

Tabelle 3: Reifegradstufen zur Organisation

B.2.4. Details zu Umfeld des ISMS

			Reifegrad	Maßnahmen		
Ziele	**Inhalte**	**Muster/Vorlagen/Vorschläge**	**0-5**	**ISO**	**BSI 200-1 GS-Profil (Baustein)**	**ISIS12**
Relevante Themen	• Forschungsdaten • Forschungsprojekte • Prüfungen, und Prüfungsergebnisse, sowie Noten • Studierendendaten und andere personenbezogene Daten • Haushalts-, Personaldaten und andere Informationen der Verwaltung	• Forschungsdaten • Forschungsprojekte • Patientendaten (Unikliniken und Psychotherapeutische Beratungsstellen) • Prüfungen, und Prüfungsergebnisse, sowie Noten • Studierendendaten und andere personenbezogene Daten • Unterstützung f. kritische Infrastruktur (HPC) • etc		Kap. 4.1	Kap. 4.1 1. (ISMS.1)	
Interessierten Parteien und deren Anforderungen	• Dienststellen der Verwaltung • Bibliothek • Studierende	• Andere (externe) Wissenschaftler • Dienststellen der Verwaltung • Fakultäten • Forschungspartner • Ministerium • Studierende		Kap. 4.2	Kap. 4.1 1. (ISMS.1)	
Grenzen und die Anwendbarkeit des ISMS bestimmen	• Statement of Applicability • Liste mit externen Dienstleistern	Statement of Applicability ISO27k_SOA.xlsx		Kap. 4.3	Kap. 4.1 1. (ISMS.1)	

Führung und Verpflichtung Leitlinie	• strategischen Ausrichtung • in die Prozesse der Hochschule integriert • erforderlichen Ressourcen zur Verfügung stellt • die Bedeutung sowie die Wichtigkeit des Informations-sicherheitsmanagement-systems vermittelt; • beabsichtigte Ergebnisse erzielt • Personen anleitet und unterstützt • fortlaufende Verbesserung fördert • relevante Führungskräfte unterstützt	Leitlinie SicherheitsLL_template_ISO27K.docx SicherheitsLL_template_BSI.docx		Kap. 5.1 und 5.2	Kap. 4.1 2. und 3. (ISMS.1)	Schritt 1 B1.1 M 1.1 M 1.2 M 1.3 M 1.4
Befugnisse für Rollen im ISMS zuweisen und bekannt machen	• Organigramm • Organisationsrichtlinie • Aufgabenbeschreibung	SK_Sicherheitsorganisation_Vx.docx		A 6.1 Kap. 5.3	Kap. 4.1 2. U. 7.2 (ORP.1)	Schritt 1 B 1.1, B1.2 M 2.1 M 2.2 M 1.9 M 1.10

B.2.5. Arbeitspakete

Mögliche Prozesse	mögliche Projekte	Unterstützende Tools/Software	Betroffene Rollen/Funktionen

• Freigabe- und Überprüfungs-prozess der Regelungen
• Abstimmprozess mit
  ○ Justiziariat, Datenschutz
  ○ Einkauf
  ○ F&E
  ○ Verwaltung
  ○ Fakultäten
	• Leitlinie erstellen und verab-schieden
	• Organisationskonzept erstellen und verabschieden
	• Funktionen zuweisen, ernennen
	• Aufgabenbeschreibung f. ISB erstellen
	• Klärung der interessierten Parteien und mögliche Anknüpfungspunkte in bestehenden Prozessen
	• Statement of Applicability erstellen
	• Relevante Informationen bestimmen
		• Dokumentenmanagement
		• Projektmanagement
		• ISMS Tool
		• Inventarverzeichnis
			• Hochschulleitung
			• ISB
			• beauftragter Projektleiter (möglicherweise der ISB)
			• technische und wirtschaftliche, strategische Leitung des Rechenzentrums
			• interessierte Parteien
			• Datenschutzbeauftragter

B.2.6. Überprüfung, Auditfragen, Mindestanforderungen

ISO 2700x	BSI Grundschutz	ISIS12
A 5 - Informationssicherheitsrichtlinien A 6.1 - Interne Organisation	Übergeordnete Maßnahmen Relevante Bausteine aus dem IT-Grundschutz-profil für Hochschulen: Priorität 1: - ISMS.1 - ORP.1 - ORP.2 Priorität 3: - ORP.5	**Kontrollfragen zu Schritt 1** 1.8.1 Wurde die Leitlinie für Informations-sicherheit fertiggestellt? 1.8.2 Hat die komplette Organisationsleitung die Leitlinie abgezeichnet? 1.8.3 Wurde der Stellenwert der Informations-sicherheit bezogen auf die spezifischen Organisationsziele dargestellt? 1.8.4 Wurde der Geltungsbereich der Leitlinie festgelegt? 1.8.5 Wurde ein (neuer) Revisionstermin gesetzt und eine verantwortliche Person benannt? **Kontrollfragen zu Schritt 3** 3.4.1 Ist eine Person auf der Grundlage einer Rollenbeschreibung von der Organisationsleitung als ISB benannt worden? 3.4.2 Sind der benannten Person ihre Aufgaben als ISB in der Organisation bekannt? 3.4.3 Sind die Rolle des ISB und die aktuelle Besetzung in der Organisation ausreichend bekannt? 3.4.4 Existiert ein Informationssicherheitsteam und sind Aufgaben, Regeln, Berichtswesen und Häufigkeit der Treffen festgelegt? 3.4.5 Ist im aktuell gültigen Organigramm die Stelle des ISB eingetragen? 3.4.6 Wurde ein (neuer) Revisionstermin gesetzt und eine verantwortliche Person benannt?

B.2.7. Berichte und Verbesserung

Kennzahlen, KPIs	Berichtspunkte und Periodizität
• Anzahl der überprüften und überarbeiteten, freigegebenen Dokumente • Anzahl veröffentlichter Dokumente • Prozentualer Anteil der IT-Systeme im Geltungsbereich • ISMS Überprüfungsprozess • Tragweite der Informationssicherheitsorganisation • Aktualität der Personenliste	• Status der Regelungen • Reifegrad des ISMS • Laufende Projekte zur Entwicklung von Regelungen • Interessierte Parteien (neue Forschungsprojekte, Partner, etc) • Treffen (mit Statusbericht) 2-4x im Jahr • Gesamtbericht 1x Jahr

B.2.7.1. Performance Indikator (Beispiele):

Engagement der Hochschulleitung

Beschreibung	Bedeutung oder Zweck
Zweck	Erhebung des Engagements und der Überprüfungsaktivitäten bezüglich der Informationssicherheit durch die Hochschulleitung
Maßzahl	Durchschnittliche Teilnehmerrate an Informationssicherheitstreffen
Formel	PI=Anzahl der stattgefundenen Treffen/Anzahl der geplanten Treffen*100
Zielwerte	Grün: PI>= 70%, Gelb:70%<PI>=50%, Rot: PI<50% • Grün: keine Aktion erforderlich • Gelb: Überwachung des Indikators auf Tendenzen und prüfen von Korrekturmaßnahmen • Rot: Intervention erforderlich; Klärung der Umstände und festlegen von Korrekturmaßnahmen
Erhebungsunterlagen und Datenquelle	• Anzahl der geplanten Überprüfungstreffen • Anzahl der geplant und ungeplant abgehaltenen und verschobenen Treffen • Terminplan und Inhalte der Überprüfungstreffen; Protokolle derartiger Treffen
Erhebungsfrequenz	Sammlung: quartalsweise Analyse und Bericht: je Semester Maßnahmenüberprüfung: alle 2 Jahre
Verantwortlich	• ISMS Verantwortlicher

Überprüfung der Regelungen zur Informationssicherheit

Beschreibung	Bedeutung oder Zweck
Zweck	Bewertung ob Regelungen wie geplant oder bei signifikanten Veränderungen der Umwelt überprüft werden.
Maßzahl	Prozentsatz der Regelungen die überprüft wurden
Formel	PI=Anzahl der geänderten Regelungen/Anzahl der freigegebenen Regelungen*100
Zielwerte	Grün: PI>= 80%, Gelb:80%<PI>=40%, Rot: PI<40% • Grün: keine Aktion erforderlich • Gelb: Überwachung des Indikators auf Tendenzen und prüfen von Korrekturmaßnahmen • Rot: Intervention erforderlich; Klärung der Umstände und festlegen von Korrekturmaßnahmen
Erhebungsunterlagen und Datenquelle	• Überarbeitungshistorie in den Regelungen • Liste der Regelungen mit Hinweisen auf Änderungen • Überarbeitungsplan für Regelungen, DMS Wiedervorlageplan
Erhebungsfrequenz	• Jährlich
Verantwortlich	• Informationseigentümer der Regelungen • ISMS Verantwortlicher

Überprüfung des ISMS Prozesses

Beschreibung	Bedeutung oder Zweck
Zweck	Bewertung des Grads der Durchführung einer unabhängigen Überprüfung der Informationssicherheit
Maßzahl	Fortschrittsrate der durchgeführten unabhängigen Überprüfungen
Formel	PI=Anzahl der durchgeführten Überprüfungen/Anzahl geplanten Überprüfungen
Zielwerte	0,8<=PI<=1,1 Bei einem Wert unter 0,6 ist dringende Intervention erforderlich
Erhebungsunterlagen und Datenquelle	• Überprüfungsplan (Anzahl) • Prüfungsberichte (Anzahl)
Erhebungsfrequenz	• Jährlich
Verantwortlich	• Interner Auditor • ISMS Verantwortlicher

B.2.7.2. Effizienz Indikator (Beispiel):

Engagement der Hochschulleitung

Beschreibung	**Bedeutung oder Zweck**
Zweck	Erhebung des Engagements und der Überprüfungsaktivitäten bezüglich der Informationssicherheit durch die Hochschulleitung
Maßzahl	Durchschnittliche Teilnehmerrate an Informationssicherheitstreffen
Formel	EI=Mittelwert und Standardabweichung der Teilnehmerrate an Überprüfungsmeetings
Zielwerte	Berechnete Konfidenzintervalle basierend auf der Standardabweichung geben die Wahrscheinlichkeit an, dass ein tatsächliches Ergebnis nahe der durchschnittlichen Beteiligungsrate erzielt wird. Sehr große Intervalle lassen eine potential große Abweichung vermuten und müssen näher betrachtet werden.
Erhebungsunterlagen und Datenquelle	• Anzahl der geplanten Überprüfungstreffen • Anzahl der geplant und ungeplant abgehaltenen und verschobenen Treffen • Anzahl der geplanten und ungeplanten Teilnehmer pro Treffen • Terminplan und Inhalte der Überprüfungstreffen; Protokolle derartiger Treffen
Erhebungsfrequenz	Sammlung: quartalsweise Analyse und Bericht: je Semester Maßnahmenüberprüfung: alle 2 Jahre
Verantwortlich	• ISMS Verantwortlicher

B.3. Umsetzung Schritt 1 - Umfeld des ISMS – Kommunikation/Schulung

B.3.1. Ziele

Details der Aufgaben, um die Ziele zu erreichen, entnehmen Sie dem Punkt 3.3.ff.

Alle Beschäftigten der Hochschule, sollten ein angemessenes Bewusstsein bekommen durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Regelungen und Verfahren im Bereich der Informationssicherheit, die für ihr berufliches Arbeitsgebiet relevant sind.

Ein Sensibilisierungsprogramm für Informationssicherheit sollte in Einklang mit Informationssicherheitsrichtlinien und relevanten Verfahren der Hochschule, unter Berücksichtigung der zu schützenden Informationswerte der Hochschule und der schon bestehenden Maßnahmen zum Schutz dieser festgelegt werden. Das Sensibilisierungsprogramm sollte eine Reihe von Sensibilisierungsmaßnahmen enthalten, wie Kampagnen (z.B. „Tag der Informationssicherheit“) und das Herausgeben von Broschüren und Rundschreiben. Aus- und Weiterbildung in Informationssicherheit sollte generelle Aspekte enthalten wie:

a) Darlegung der Verpflichtung der Leitung zu Informationssicherheit in der gesamten Hochschule;

b) die Notwendigkeit, mit geltenden Regeln und Verpflichtungen der Informationssicherheit vertraut zu werden und sie zu beachten, wie in Richtlinien, Normen, Gesetzen, Verordnungen, Verträgen und Vereinbarungen festgelegt;

c) persönliche Verantwortung für eigene Handlungen und Unterlassungen sowie allgemeine Verantwortlichkeiten zur Sicherung oder zum Schutz von Informationen, die der Hochschule und externen Parteien gehören;

d) grundsätzliche Verfahren zur Informationssicherheit und grundlegende Sicherheitsmaßnahmen;

e) Anlaufstellen und Ressourcen für zusätzliche Informationen und Empfehlungen zu Fragen der Informationssicherheit, einschließlich weiterer Aus- und Weiterbildungsunterlagen zur Informationssicherheit.

B.3.2. Reifegradstufen

Stufe	Reifegrad	Ausprägung
0	**Nicht vorhanden**	Keine Schulungs- oder Kommunikationsverfahren zur Informationssicherheit sind vorhanden.
1	**Informell vorhanden**	Schulungen werden individuell angefordert und genehmigt. Vereinzelt werden Hochschulangehörige allgemein bei Vorkommnissen (z.B.: Phishing-Attacken) informiert.
2	**Geplant**	Es gibt Informationssicherheitsveranstaltungsangebote und entsprechende Hinweise auf den Seiten der Hochschule. Hochschulangehörige werden in unregelmäßigen Abständen unterwiesen.
3	**Dokumentiert**	Es gibt Regelungen zur Teilnahme an Schulungsveranstaltungen für Hochschulangehörigen. Schulungsangebote sind nach relevanten Bereichen getrennt und von Führungskräften bestätigt. Sie werden in unregelmäßigen Abständen überarbeitet und sind für die Hochschule verpflichtend.
4	**Quantitativ überwacht**	Die Teilnahme an den Schulungen wird kontrolliert und es gibt eine regelmäßige Überprüfung und Aufforderung bei fehlender Teilnahme.
5	**Kontinuierlich verbessert**	Die Schulungen werden **regelmäßig überprüft** und **angepasst**. Bei geänderten Umständen werden die Dokumente überarbeitet und adaptiert.

Tabelle 4: Reifegradstufen zu Kommunikation und Schulung

B.3.3. Details zu Kommunikation/Schulung

			Reifegrad	Kapitel/Bausteine/Maßnahmen		
Ziele	**Inhalte**	**Muster/Vorlagen/Vorschläge**	**0-5**	**ISO**	**BSI 200-1 GS-Profil**	**ISIS12**
• Verpflichtung der Leitung • Wissen über Regeln • persönliche Verantwortung • grundlegende Verfahrung und Maßnahmen • Ansprechpartner • Sensibilisierungs-programm	Inhalte für • Mitarbeiter (neue, bestehende) • Lehrende • Leitung • Administratoren (fachspezifische Trainings) • ‚Sicherheitstage' • Newsletter • Info-Webseiten • Benutzerordnung	• Moodle-Kurse • BITS • Kommunikationskonzept FHWS (auf Anfrage)		Kap. 7.2.2	ORP.3	Schritt 2; B1.2 tw. 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. Arbeitspakete

Mögliche Prozesse	mögliche Projekte	Unterstützende Tools/Software	Betroffene Rollen/Funktionen
• Schulungseinladungen • Kontrolle der Teilnahme/Eskalation • Integration in HS Aus- und Weiterbildungsprozesse • Datenschutzschulungen • Updates in geeigneter Form (Newsletter, Webseite) • Ansprechpartner aktualisieren	• Schulungsprogramm entwickeln und aktuell halten (bei Regeländerungen) • Sicherheitstage organisieren • Schulungsauswahl • Spezialisiertes Training für Administratoren/Entwickler planen	• eLearning • Wissensmanagement	• Kommunikationsabteilung • Personalabteilung (für interne Schulungen) • Personalrat • ISB • beauftragter Projektleiter (möglicherweise der ISB) • Datenschutzbeauftragter

B.3.5. Überprüfung, Auditfragen, Mindestanforderungen

ISO 2700x	BSI Grundschutz	ISIS12
A 7.2.2 - Informationssicherheitsbewusstsein, -ausbildung und -schulung	Anforderungen ORP.3	**Kontrollfragen zu Schritt 2** • 2.3.1 Wurden alle Mitarbeiter über ISIS12 informiert und für das Thema Informationssicherheit sensibilisiert? • 2.3.2 Wurde sichergestellt, dass die Mitarbeiter zukünftig regelmäßig über Informationssicherheit informiert werden? • 2.3.3 Wurde auf mögliche Sanktionen bei Verstößen gegen die Leitlinie, gegen zukünftige Sicherheitsrichtlinien oder generell bei Verletzung der Informationssicherheit hingewiesen? • 2.3.4 Wenn eine Arbeitgebervertretung vorhanden ist, wurde dann die Arbeitnehmervertretung beteiligt? • 2.3.5 Wurde ein (neuer) Revisionstermin gesetzt und eine verantwortliche Person benannt?

B.3.6. Berichte und Verbesserung

Kennzahlen, KPIs	Berichtspunkte und Periodizität
• Verfügbarkeit und Aktualität eines Sensibilisierungsprogramms/-prozesses • Anzahl geschulter Personen • Anzahl geplanter und gehaltener Trainings • Anzahl in Trainings integrierter Regelungen • Aktualität der Kontaktlisten (interne und externe Ansprechpartner für Informationssicherheit)	• Status der Teilnahmen • Aktualität der Kurse • Planung eines ‚Sicherheitstags', Beteiligung am Cyber Security Month • Durchführung von Kampagnen • Lfd. Bericht im Sicherheitsgremium

B.3.6.1. Performance Indikator (Beispiel):

ISMS und Informationssicherheitssensibilisierungsschulung

Beschreibung	**Bedeutung oder Zweck**
Zweck	Bewertung der Übereinstimmung der Anforderungen des ISMS mit den Trainingsinhalten
Maßzahl	Prozentsatz der Personen die eine entsprechende Schulung erhalten haben
Formel	PI=Anzahl der Personen die ein Training erhalten haben/Anzahl der Personen die ein Training erhalten müssen*100
Zielwerte	Grün: PI>= 90%, Gelb:90%<PI>=60%, Rot: PI<60% • Grün: keine Aktion erforderlich • Gelb: Überwachung des Indikators auf Tendenzen und prüfen von Korrekturmaßnahmen • Rot: Intervention erforderlich; Klärung der Umstände und festlegen von Korrekturmaßnahmen
Erhebungsunterlagen und Datenquelle	• Teilnehmerliste • Personalstand nach Gruppen • VIVA
Erhebungsfrequenz	• Jährlich oder halbjährlich
Verantwortlich	• Schulungsverantwortlicher • ISMS Verantwortlicher

B.3.6.2. Effizienz Indikator (Beispiel):

ISMS und Informationssicherheitssensibilisierungsschulung

Beschreibung	**Bedeutung oder Zweck**
Zweck	Bewertung des Verständnisses über das ISMS und Informationssicherheit
Maßzahl	Prozentsatz der Personen die einen abschließenden Verständnistest bestanden haben
Formel	EI=Anzahl der Personen die den Test bestanden haben/Anzahl der Personen die den Test durchgeführt haben*100
Zielwerte	Grün: EI>= 90%, Gelb:90%<EI>=60%, Rot: EI<60% • Grün: keine Aktion erforderlich • Gelb: Überwachung des Indikators auf Tendenzen und prüfen von Korrekturmaßnahmen • Rot: Intervention erforderlich; Klärung der Umstände und festlegen von Korrekturmaßnahmen
Erhebungsunterlagen und Datenquelle	• Teilnehmerliste • Testergebnisse/Zertifikate/Badges
Erhebungsfrequenz	• Aufzeichnung nach dem Test • Monatlich, quartalsweise
Verantwortlich	• Schulungsverantwortlicher • ISMS Verantwortlicher

B.4. Umsetzung Schritt 2 - Risikomanagement

B.4.1. Ziele

Details der Aufgaben, um die Ziele zu erreichen, entnehmen Sie dem Punkt B.4.3.ff.

Die Hochschule muss planen:

a) Ein Klassifikationsschema zur Einordnung der Informationswerte;

b) Maßnahmen zum Umgang mit diesen Risiken und Chancen;

c) wie die Maßnahmen in die ISMS Prozesse integriert und dort umgesetzt werden;

d) und die Wirksamkeit dieser Maßnahmen bewertet wird.

e) Einen Prozess zur Risikobeurteilung;

f) Kriterien zur Risikoakzeptanz;

g) dokumentierte Informationen über den Beurteilungsprozess aufbewahren;

h) einen Prozess und Optionen zur Risikobehandlung.

B.4.2. Reifegradstufen

Stufe	Reifegrad	Ausprägung
0	**Nicht vorhanden**	Kein Verfahren zur Risikobeurteilung oder –einschätzung ist vorhanden. Informationen sind keiner Klasse zugeordnet.
1	**Informell vorhanden**	Informationsklassen und Risiken werden ad-hoc im Verantwortungsbereich zuständiger Informationseigentümer oder Systembetreuer eingeschätzt. Maßnahmen im Team evaluiert, es gibt aber kein einheitliches Schema zur Klassifizierung und Integration.
2	**Geplant**	Eine Trennung in personenbezogene und nicht personen-bezogene Daten ist nachvollziehbar dokumentiert. Eine Übereinkunft für Kritikalitätsklassen und Sicherheitsmaßnahmen existiert. Diese werden im Verantwortungsbereich als de-facto Standards kommuniziert.
3	**Dokumentiert**	Rahmen zur Informationsklassifizierung für alle Schutzziele sind von der Leitung bestätigt, gut dokumentiert und freigegeben. Ein Prozess zur Risikosammlung, -bewertung und -behebung ist dokumentiert. Verantwortliche und Beteiligte für den Prozess sind bestimmt. Maßnahmen werden strukturiert in den Betrieb integriert.
4	**Quantitativ überwacht**	Eine Liste der Risiken und resultierender Maßnahmen wird von einer Person oder einem Gremium verfolgt. Maßnahmen zur Datenklassifikation werden von Informationseigentümern kontrolliert.
5	**Kontinuierlich verbessert**	Der Bewertungsprozess und die akzeptieren Risiken, einschließlich der Kriterien zur Beurteilung werden regelmäßig, bei großen Änderungen des Umfelds oder erkannten Schwachstellen einer Prüfung unterzogen und angepasst. Die Wirksamkeit (Risikobeurteilung) von Maßnahmen wird regelmäßig überprüft und Maßnahmen werden an geänderte Umstände angepasst (Restrisikobewertung).

Tabelle 5: Reifegradstufen zu Risikomanagement

B.4.3. Details zu Risikomanagement

			Reifegrad	Maßnahmen		
Ziele	**Inhalte**	**Muster/Vorlagen/Vorschläge**	**0-5**	**ISO 27001**	**BSI 200-x GS-Profil**	**ISIS12**
Risikomanagement-organisation	• Handelnde Personen • Grenzwerte • Risikoappetit • Berichtsperioden	ISO27005 (Kap. 7.4) BSI 200-1 (Kap.8.1)				
Klassifikationsschema	Schutzziele: • Vertraulichkeit • Integrität • Verfügbarkeit	Klassifikationsschema der Stabsstelle Informationssicherheit bayerischer staatlicher Hochschulen		Kap. A.8.2 Kap. 6.2	200-1: Kap. 4.2 200-2: Kap. 5.1.	Schritt 4 B 1.11 M 1.39
Maßnahmen zum Umgang Risiken und Chancen	• Risikoakzeptanzkriterien und -behandlungsoptionen definieren • Risikomanagementprozess • Integration in ISMS Prozesse und Wirksamkeitsbetrachtung	ISO 27005 Schutzbedarfsfeststellung nach BSI Standard 200-2 mit anschließender Risikobetrachtung nach BSI Standard 200-3 (Risikoanalyse) Projektarbeit - *„IT-Risikoanalyse für IT-Sicherheitsmanagement“* Farruh Djumayev – „*Vorgehensweise bei der Einführung eines IT-Risikomanagements an Hochschulen“* Firuza Muhamadova – *„Analyse und Ausarbeitung der in den ISO-Standards 27001-27005 geforderten Prozesse zum Betrieb eines ISMS“*		Kap. 6.1 Kap. 8.2 u. 8.3	200-2: Kap. 6/7/8 Schutzbedarfs-feststellung Kap. 7.5 Risikoanalyse Kap. 7.8 200-3 (Risiko-analyse)	Schritt 6 (Schutz-bedarfs-festellung)

B.4.4. Arbeitspakete

Mögliche Prozesse	mögliche Projekte	Unterstützende Tools/Software	Betroffene Rollen/Funktionen
• Risikoidentifikation • Risikobeurteilung • Risikodokumentation • Risikoakzeptanz • Risikobehandlung • Berichtsprozesse • Aktualisierung der Rahmenbedingungen	• Aufbau eines Risikomanagementprozesses • Berichtswesen • Erhebung der Rahmenbedingungen	• Dokumentenmanagement • Risikomanagement/ISMS Tool • Projektmanagement • Changemanagement (Integration) • Ticketsystem (Integration)	• Hochschulleitung • ISB • beauftragter Projektleiter (möglicherweise der ISB) • technische und wirtschaftliche, strategische Leitung des Rechenzentrums (f. IT-Risiken) • interessierte Parteien • Datenschutzbeauftragter • Qualitätsmanagement

B.4.5. Überprüfung, Auditfragen, Mindestanforderungen

ISO 2700x	BSI Grundschutz	ISIS12
Kap. 6 - Planung Kap. 8 - Betrieb Kap. 9 - Bewertung der Leistung A 5 - Informationssicherheitsrichtlinien A 6.1 - Interne Organisation A 8.2 - Klassifizierung von Informationen	BSI Standard 200-2 Kap. 7.5 u. 8.2 BSI Standard 200-3 Anforderungen • ISMS.1 • ORP.1 • CON.2 (Datenschutz)	**Kontrollfragen zu Schritt 6** 6.5.1 Wurden die aktuell kritischen Anwendungen und IT-Services identifiziert? Wurde eine Liste der kritischen Anwendungen und kritischen IT-Services erstellt? 6.5.2 Sind die Schutzbedarfskategorien an die eigene Organisation angepasst und hat die Organisationsleitung die Freigabeerteilt? 6.5.3 Ist der Schutzbedarf für alle kritischen Anwendungen von den Fachverantwortlichen mit Begründung festgestellt und dokumentiert? 6.5.4 Ist jeder kritischen Anwendung eine MTA zugeordnet?

B.4.6. Berichte und Verbesserung

Kennzahlen, KPIs	Berichtspunkte und Periodizität
• Anzahl der neu identifizierten Risiken • Anzahl der behandelten Risiken • Anzahl berichteter und akzeptierter Restrisiken • Risikopotential/Risikostatus	• Status der Risiken • Je Semester für mittlere Risiken • Quartalsweise für hohe Risiken • Bei Bedarf bei sehr hohen Risiken

B.4.6.1. Effizienz Indikator (Beispiel):

Risikopotenzial

Beschreibung	Bedeutung oder Zweck
Zweck	Einschätzung des Potentials/Gefahr der Universität für Informationssicherheitsrisiken. Der akzeptierte Schwellwert für mittlere und hohe Risiken sollte definiert werden und die verantwortlichen Personen über eine Überschreitung des Schwellwerts zeitgerecht informiert werden.
Maßzahl	• Anzahl der Risiken die über dem Risikoschwellwert liegen und behandelt werden müssen • Anzahl der Risiken die zeitgerecht berichtet wurden • Zeitraum für den Bericht von Risiken über dem Risikoschwellwert
Formel	PI=Anzahl der berichteten Risiken über dem Schwellwert/Anzahl der Risiken über dem Schwellwert EI=Anzahl der nicht zeitgerecht berichteten Risiken über dem Schwellwert
Zielwerte	PI = 1 EI=0
Erhebungsunterlagen und Datenquelle	• Risikoregister/-liste
Erhebungsfrequenz	• Je Semester
Verantwortlich	• Risiko-/Informationseigentümer • Risikobearbeiter

B.5. Umsetzung Schritt 3 – Maßnahmenumsetzung

B.5.1. Ziele

Details der Aufgaben, um die Ziele zu erreichen, entnehmen Sie dem Punkt B.5.3.ff.

Die in Schritt 2 definierten Prozesse gilt es jetzt anzuwenden und im Betrieb zu integrieren. Der Betrieb der Prozesse hilft Ihnen dabei die richtigen Maßnahmen zur Risikominimierung auszuwählen, das Restrisiko abzuschätzen, den Einsatz zu planen und die Wirksamkeit zu überprüfen. So wird für die gewählten Maßnahmen jeweils ein Verbesserungszyklus (PDCA) geschaffen, um das Niveau der Informationssicherheit für diese aufrechtzuerhalten.

Die Leitung stellt Ressourcen für eine kompetente Umsetzung notwendiger Maßnahmen im ausreichenden Maß zur Verfügung.

In regelmäßigen Abständen sollte ein Audit durch einen Auditor der Hochschulen Bayerns durchgeführt werden.

Technische Maßnahmen zur Absicherung der IT Infrastruktur und des Betriebs sind den jeweiligen Standards zu entnehmen. Hier werden nur Prozesse oder Konzepte erwähnt die zur Steigerung der Informationssicherheit integriert werden müssen.

B.5.2. Reifegradstufen

Stufe	Reifegrad	Ausprägung
0	**Nicht vorhanden**	Keine Prozesse zur Erfüllung der Informationssicherheitsanforderungen sind vorhanden. Es erfolgt keine risikobasierte Steuerung der Maßnahmen. Es gibt keine Behandlungspläne.
1	**Informell vorhanden**	Maßnahmen werden im Team besprochen und ad-hoc im Verantwortungsbereich zuständiger Informationseigentümer oder Systembetreuer eigenverantwortlich implementiert.
2	**Geplant**	Es gibt eine interne Übereinkunft über Maßnahmen zur Erfüllung der Informationssicherheitsanforderungen. Diese werden im Verantwortungsbereich als de-facto Standards kommuniziert. Die Umsetzungsverantwortlichen sind entsprechen geschult und ein Budget für die Umsetzung ist von der Leitung genehmigt.
3	**Dokumentiert**	Das Sicherheitskonzept zur Erfüllung der Anforderungen (des Schutzbedarfs) ist dokumentiert und freigegeben. Ein Prozess zur Risikobehandlung ist dokumentiert und Maßnahmen werden strukturiert wie geplant im Betrieb integriert. Ein definiertes IT-Sicherheitsbudget ist zugesichert.
4	**Quantitativ überwacht**	Geplante Änderungen werden von einer Person oder einem Gremium verfolgt, sowie die Folgen unbeabsichtigter Änderungen beurteilt und, falls notwendig, Maßnahmen ergriffen, um negativen Auswirkungen zu vermindern. Ausgelagerte Prozesse sind dokumentiert, kontrolliert und gesteuert. Die Ergebnisse der Risikobehandlung werden dokumentiert.
5	**Kontinuierlich verbessert**	In geplanten Abständen oder immer dann, wenn erhebliche Änderungen vorgeschlagen werden oder auftreten, werden Informationssicherheitsrisikobeurteilungen vorgenommen. Dokumentierte Informationen über die Ergebnisse der Informationssicherheitsrisikobeurteilungen werden aufbewahrt. Die Wirksamkeit bereits implementierter Maßnahmen wird regelmäßig überprüft und gegebenenfalls neu geplant.

Tabelle 6: Reifegradstufen zu Maßnahmenumsetzung

B.5.3. Details zu Maßnahmenumsetzung

			Reifegrad	Maßnahmen		
Ziele	**Inhalte**	**Muster/Vorlagen/Vorschläge**	**0-5**	**ISO 27001**	**BSI 200-x GS-Profil**	**ISIS12**
Einführung oder Verbesserung der Prozesse um die Informationssicherheits-anforderungen zu erreichen.	Planung und Integration von Betriebsprozesse für: • Dokumente • Änderungen, Projekte ○ aufbauen, warten, entfernen • Beschaffung • Identitäten & Rechte, Zutritt • Sicherheitsvorfälle • Schutz vor Schadsoftware • Schwachstellen • Systementwicklung • Notfall/Kontinuität • Schulung • Inventar • Kapazitätsplanung • Protokollierung • Überprüfung	Kataloge für diverse Service-managementprozesse: • ITIL • FitSM Firuza Muhamadova – *„Analyse und Ausarbeitung der in den ISO-Standards 27001-27005 geforderten Prozesse zum Betrieb eines ISMS“* Thomas Kietreiber - *„Integration von Schwachstellenmanagement“*		Kap.8 Kap. 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: Kap. 9 Priorität 1: ISMS.1.A9 ORP.3.A4 ORP.4 CON.3 CON.6 OPS.1.1 DER.4 Priorität 2: CON.2 CON.4 OPS.2.2 DER.2.1 Priorität 3: ORP.5 CON.1 CON.4 CON.7 OPS.1.2 OPS.2.2	Schritt 5 Schritt 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	Planung eines definierten IT-Sicherheitsbugets	5-10% des IT-Budget		Kap. 7.1, 7.2	ISMS.1.A15	Schritt 10.3
Wirksamkeitsprüfung	Prüfpläne, Audits Intrinsische Kontrollen der Maßnahmen	Matthias Mödinger - „Metrics and KPIs for Information Security Reports”		Kap. 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. Arbeitspakete

Mögliche Prozesse	mögliche Projekte	Unterstützende Tools/Software	Betroffene Rollen/Funktionen

Planung und Integration von Betriebsprozesse für:
• Dokumente
• Änderungen, Projekte
  ○ aufbauen, warten, entfernen
• Beschaffung
• Identitäten & Rechte, Zutritt
• Sicherheitsvorfälle
• Schutz vor Schadsoftware
• Schwachstellen
• Systementwicklung
• Notfall/Kontinuität
• Schulung
• Inventar
• Kapazitätsplanung
• Protokollierung
• Überprüfung
	• Einführung eines Servicemanagements und Kontroll- und Berichtswesen	• Monitoring SW:
		  ○ Ansible
		  ○ Zabbix
		  ○ Nagios
		  ○ etc
		• Netzwerkmanagement
		• SIEM
		• Logserver
		• Softwareverteilung
		• Servicemanagement
		• Identity & Access Management
		• Zentrale AV-Lösung und Monitoring
		• Betriebliches Kontinuitäts-management
		• Datenschutzmanagement
		• Business Intelligence
			• Hochschulleitung (Budget)
			• ISB
			• Projektleiter
			• technische und wirtschaftliche, strategische Leitung des Rechenzentrums
			• Datenschutzbeauftragter
			• Service Desk
			• IT-Administratoren

B.5.5. Überprüfung, Auditfragen, Mindestanforderungen

ISO 2700x	BSI Grundschutz	ISIS12
Spezifische Informationssicherheitsausbildung für technische Angestellte im RZ Betrieb und Entwicklung. Effektivität verschiedener IT-Betriebsprozesse mit intrinsischen Kontrollen und Verbesserungsschritten (A 12.1.1). Ist ein Informationssicherheitsbudget zugewiesen? Vergabe, Änderung, Löschung und Prüfung von Zugangsrechten durch Informationseigentümern. (A 9.2.5) Physische Sicherheit (A 11) Audits von Informationssystemen (A 12.7.1) Informationsübertragung (A 13.2) Anschaffung, Entwicklung und Instandhaltung von Systemen (A 14.1, A14.2.3, 14.2.8, A 14.2.9) Lieferantenbeziehungen (A 15.1.1, A 15.2.1) Sicherheitsvorfälle (A 16.1.6) Compliance (A 18)	Basisanforderungen zu den relevanten Maßnahmen (s.o.) des BSI HS Grundschutzprofils. Prozessbaustein DER (Detektion und Reaktion)	**Kontrollfragen zu Schritt 5** • 5.5.1 Sind die drei Basis-ISIS12-IT-Service-managementprozesse angepasst und modelliert? • 5.5.2 Sind die IT-Mitarbeiter mit den IT-Servicemanagementprozessen vertraut? • 5.5.3 Sind andere erforderliche Abteilungen beim Änderungsprozess beteiligt worden? • 5.5.4 Wurde den Mitarbeitern die ent-sprechende Information über die Bereiche Änderungswünsche und Störungsmeldungen vermittelt? **Kontrollfragen zu Schritt 10** • 10.9.1 Wurden die Maßnahmen gemäß Kapitel 10.1 konsolidiert? • 10.9.2 Wurden die Maßnahmen gemäß Schutzbedarfsklasse, Breitenwirkung und Abhängigkeiten priorisiert? • 10.9.3 Hat die Geschäftsleitung über die Umsetzung der Maßnahmen entschieden? • 10.9.4 Wurden die Rollen des Initiators, des Umsetzers und des Verantwortlichen für die Überwachung für alle offenen Maßnahmen festgelegt? • 10.9.5 Sind konkrete Umsetzungstermine und ggf. Schulungstermine festgelegt und den zuständigen Personen mitgeteilt worden? • 10.9.6 Wurde ein (neuer) Revisionstermin gesetzt und eine verantwortliche Person genannt?

B.5.6. Berichte und Verbesserung

Kennzahlen, KPIs	Berichtspunkte und Periodizität
• Anzahl der Verbesserungsmaßnahmen interner Prozesse • Budget; Ressourcenverwendung • Anzahl der Nachbesprechungen von Sicherheitsvorfällen • Anzahl durchgeführter Überprüfungen von Zugangsrechten • Anzahl der durchgeführten (geplanten) Wartungen von IT-Systemen • Anzahl von Änderungen relevanter IT-Systeme • Performance des Schutzes gegen Schadsoftware • Anzahl durchgeführter Überprüfungen der Protokolldateien • Anzahl und Kritikalität der Verwundbarkeiten von IT-Systemen • Anzahl, Erledigungszeitraum und Trend von Sicherheitsvorfällen • Anzahl der Vorfälle, Bericht und Erhebungen von Sicherheitsvorfällen	• Zustandskennzahlen und kritische Zustände monatlich • Überprüfungen je Semester • Quartalsweise für Trends und geplante Vorgänge • Bei Bedarf Sicherheitsvorfälle • Jahresgesamtbericht

B.5.6.1. Effizienz Indikator (Beispiele):

Budget, Ressourcenverwendung

Beschreibung	Bedeutung oder Zweck
Zweck	Angabe der Ressourcen die für Informationssicherheit zur Verfügung gestellt werden im Bezug zum Hochschulbudget oder IT-Budget.
Maßzahl	Anzahl der Ressourcen (internes und externes Personal, Hardware, Softwarelizenzen, eingekaufte Dienste, etc) des aktuellen Budgets (Semester/Jahr/2 Jahre) im Vergleich zur Verwendung monetär ausgedrückt.
Formel	EI=Im Zeitraum angefallene Kosten/budgetierte Kosten
Zielwerte	EI=1
Erhebungsunterlagen und Datenquelle	Haushalt; Kostenstelle oder andere Kostenverfolgung Budgetposten, Kostenverwendungen
Erhebungsfrequenz	Sammlung: Semester; Bericht: jährlich
Verantwortlich	• Kostenstellenverantwortlicher • Informationssicherheitsbeauftragter • Budgetverantwortlicher

Verbesserungsmaßnahmen zu internen Prozessen

Beschreibung	Bedeutung oder Zweck
Zweck	Den Status von Maßnahmen zur Verbesserung der Informationssicherheit und deren Verwaltung gemäß den geplanten Maßnahmen überprüfen.
Maßzahl	Anzahl der Verbesserungsmaßnahmen (im Zeitrahmen, Kosten und Qualität/Persistenz) im Verhältnis zu geplanten Maßnahmen. Die Maßnahmen sollen über einen geplanten Status (begonnen, in Arbeit, fertig) evaluiert werden. Eine Gewichtung nach Kritikalität kann die Messung verbessern.
Formel	EI=laufende oder abgeschlossene Maßnahmen/geplante Maßnahmen*100
Zielwerte	EI>=90%
Erhebungsunterlagen und Datenquelle	Statusverfolgung von Verbesserungsmaßnahmen (Ticketsystem) Projektpläne
Erhebungsfrequenz	Sammlung: Semester; Bericht: Semester
Verantwortlich	• Informationseigentümer, Projektmanager • Informationssicherheitsbeauftragter

Lernen aus Vorfällen

Beschreibung	Bedeutung oder Zweck
Zweck	Prüfen ob Sicherheitsvorfälle Verbesserungsmaßnahmen auslösen.
Maßzahl	Anzahl der Sicherheitsvorfälle die eine Verbesserungsmaßnahme auslösen.
Formel	EI= Anzahl der Sicherheitsvorfälle die eine Verbesserungsmaßnahme auslösen/ Anzahl der Sicherheitsvorfälle*100
Zielwerte	EI>=80% oder durch das Sicherheitsgremium oder Hochschulleitung bestimmt
Erhebungsunterlagen und Datenquelle	Verbesserungsmaßnahmen die auf einen Sicherheitsvorfall zurückgeführt werden können Berichte, Listen der Sicherheitsvorfälle (Ticketsystem)
Erhebungsfrequenz	Sammlung: Semester; Bericht: Semester
Verantwortlich	• Informationseigentümer, • CSIRT • Informationssicherheitsbeauftragter

Effektivität der Zutrittskontrolle

Beschreibung	Bedeutung oder Zweck
Zweck	Sicherstellen eines Umfelds umfassender Sicherheit und Rechenschaftspflicht für Personal, Einrichtungen und Informationswerten. Einsatz von physischen Schutzmechanismen um angemessenen Schutz der Informationswerten sicherzustellen.
Maßzahl	Anzahl der unberechtigten Zutritte zu Räumen mit informationsverarbeitender Technologie.
Formel	EI= Aktuelle Zahl der unberechtigten Zutritte
Zielwerte	EI=0
Erhebungsunterlagen und Datenquelle	Systematische Analyse der Zutrittsprotokolle, Alarme von unberechtigten Zutritten Sicherheitsberichte der physischen Sicherheit
Erhebungsfrequenz	Sammlung: je Semester; Bericht: Semester
Verantwortlich	• Facility Management, Gebäude und Technik, • CSIRT (wenn Alarme dort aufschlagen) • Informationssicherheitsbeauftragter, CIO

Effektivität bei der Behandlung von Sicherheitsvorfällen

Beschreibung	Bedeutung oder Zweck
Zweck	Prüfen der Effektivität bei der Behandlung von Sicherheitsvorfällen
Maßzahl	Anzahl der Sicherheitsvorfälle die nicht im vorgesehenen Zeitraum erledigt wurden
Formel	• Bestimmen Sie die Kategorien für Sicherheitsvorfälle und ihre Erledigungszeiträume • Bestimmen Sie die Schwellwerte für Vorfälle die diese Zeiträume überschreiten • Vergleichen Sie Anzahl jener Vorfälle pro Kategorie und Schwellwert
Zielwerte	EI=Anzahl der Vorfälle deren überfällige Erledigungszeit den Schwellwert für den Zeitrahmen der zugewiesenen Kategorie nicht übersteigen
Erhebungsunterlagen und Datenquelle	Die monatlich berichteten Schwellwertüberschreitungen
Erhebungsfrequenz	Sammlung: monatlich; Bericht und Überprüfung der Schwellwerte und Zeiträume: je Semester
Verantwortlich	• Verantwortlicher für die Behandlung von Sicherheitsvorfällen • Informationssicherheitsbeauftragter • CIO, Berichtsempfänger

Trend der Sicherheitsvorfälle

Beschreibung	Bedeutung oder Zweck
Zweck	• Trends der Sicherheitsvorfälle • Trends der Kategorien von Sicherheitsvorfällen
Maßzahl	Anzahl der Sicherheitsvorfälle im Berichtszeitraum Anzahl der Sicherheitsvorfälle je Kategorie im Berichtszeitraum
Formel	EI= durchschnittliche Anzahl der Sicherheitsvorfälle einer Kategorie der letzten beiden Zeiträume/ durchschnittliche Anzahl der Sicherheitsvorfälle einer Kategorie der letzten 6 Zeiträume • Analyse aller Vorfälle • Analyse der Vorfälle je Kategorie
Zielwerte	Beispiel für Grenzwerte: Grün: EI<1 Gelb: 1 <=EI<=1.3 Rot: EI >1.3

Erhebungsunterlagen und Datenquelle	Anzahl der monatlich berichteten Sicherheitsvorfälle aus den Sicherheitsberichten oder Ticketsystem
Erhebungsfrequenz	Sammlung: monatlich; Bericht: je Semester
Verantwortlich	• CSIRT • Informationssicherheitsbeauftragter, CIO, CISO

B.5.6.2. Performance Indikator (Beispiele):

Überprüfung der Benutzerrechte

Beschreibung	**Bedeutung oder Zweck**
Zweck	Anzahl der Überprüfungen von Benutzerrechten für kritische/sensible Systeme der Hochschule
Maßzahl	Prozentsatz der kritischen System die regelmäßig überprüft werden
Formel	PI=Anzahl der überprüften kritischen Systeme/Gesamtzahl der kritischen Systeme*100
Zielwerte	Grün: PI>= 90%, Gelb:90%<PI>=70%, Rot: PI<70% • Grün: keine Aktion erforderlich • Gelb: Überwachung des Indikators auf Tendenzen und prüfen von Korrekturmaßnahmen • Rot: Intervention erforderlich; Klärung der Umstände und festlegen von Korrekturmaßnahmen
Erhebungsunterlagen und Datenquelle	Bestätigte Prüfungen (email, Ticketsystem) Informationsinventar, Verfahrensverzeichnis,
Erhebungsfrequenz	Sammlung: monatlich oder bei Veränderungen (Aufnahme/Austritt) ; Bericht: jährlich
Verantwortlich	• Informationseigentümer • ISMS Verantwortlicher • Systemverantwortliche

Zutrittskontrolle

Beschreibung	**Bedeutung oder Zweck**
Zweck	Zeigt die Existenz, den Umfang und die Qualität des Zutrittskontrollsystems
Maßzahl	Stärke des Zutrittskontrollsystems

Formel	PI Reifegrad auf einer Skala von 0-5 0 = Kein System 1 = PIN Code (oder anderes mechanisches 1 Faktorsystem wie Schlüssel) 2 = elektronisches Zutrittskontrollsystem (Campus Card) als einzigen Faktor 3 = Kartensystem mit PIN Code (für gewählte Bereiche) 4 = Kartensystem mit PIN Code und aktivierter Protokollierung 5 = Kartensystem mit biometrischem 2. Faktor und aktivierter Protokollierung
Zielwerte	PI>=3
Erhebungsunterlagen und Datenquelle	Überprüfung des Zutrittskontrollsystems auf folgende Merkmale: • Zutrittskarten • PIN Code • Protokollierung • Verwendung von Biometrie
Erhebungsfrequenz	Sammlung: jährlich; Bericht: jährlich
Verantwortlich	• Gebäudetechnik, Facility Manager • Hochschulleitung

Wartung von Informationssystemen

Beschreibung	**Bedeutung oder Zweck**
Zweck	Bewerten der zeitgerechten Wartungen gemäß eines Wartungsplans
Maßzahl	Wartungsverzögerungen pro erledigter Wartung
Formel	PI=Differenz in Tagen zwischen Datum der Planung und Datum der tatsächlichen Erledigung
Zielwerte	PI=0 oder von der Hochschule akzeptierte Verzögerungen (z.B. 3 Tage) Trend soll stabil oder gegen 0 gehen
Erhebungsunterlagen und Datenquelle	Erledigungsdatum der geplanten Wartungen, geplantes Datum der Wartungen, Gesamtzahl der geplanten Wartungen, Gesamtzahl der erledigten Wartungen Wartungsplan, Ticketsystem (Wartungstickets)
Erhebungsfrequenz	Sammlung: je Semester; Bericht: jährlich
Verantwortlich	• Systemadministratoren • Service Desk • Informationssicherheitsbeauftragter

Änderungsmanagement

Beschreibung	Bedeutung oder Zweck
Zweck	Bewertung ob best practices für Änderungsmanagement und Hardening Regelungen eingehalten werden
Maßzahl	Prozentsatz der neuen Systeme die gemäß dem Änderungsmanagement und Hardening Regelungen installiert wurden
Formel	PI=Anzahl der ordnungsgemäß installierten Systeme/Anzahl installierter Systeme*100
Zielwerte	• Grün: PI>= 90%, Gelb:90%<PI>=70%, Rot: PI<70% • Grün: keine Aktion erforderlich • Gelb: Überwachung des Indikators auf Tendenzen und prüfen von Korrekturmaßnahmen • Rot: Intervention erforderlich; Klärung der Umstände und festlegen von Korrekturmaßnahmen
Erhebungsunterlagen und Datenquelle	Ticketsystem (Änderungstickets), Abnahmeberichte, Konfigurationschecklisten, Fertigstellungsberichte Emails, Post Implementation Review
Erhebungsfrequenz	Sammlung: je Semester; Bericht: jährlich
Verantwortlich	• Change Manager, RZ-Leitung • System Administratoren • Informationssicherheitsbeauftragter

Schutz vor Schadsoftware

Beschreibung	Bedeutung oder Zweck
Zweck	Wurde auf IT-Systemen (im Hochschulnetz) mit veraltetem Schutz vor Schadsoftware diese installiert
Maßzahl	Anzahl befallener IT-Systeme mit veraltetem Schutz (mehr als 3/5/7 Tage alt)
Formel	PI = Anzahl der befallenen IT-Systeme mit veraltetem Schutz
Zielwerte	PI = 0
Erhebungsunterlagen und Datenquelle	Befall von Schadsoftware, Konsole für Schutz vor Schadsoftware (Bericht) Listen der Sicherheitsvorfälle (Ticketsystem), Überwachungstools, Systemprotokolle
Erhebungsfrequenz	Sammlung: bei Auftreten; Bericht: monatlich
Verantwortlich	• IT-Betrieb/Service Desk • Informationssicherheitsbeauftragter • RZ-Leitung

Überprüfung der Protokolle

Beschreibung	Bedeutung oder Zweck
Zweck	Prüfung ob kritische Systemprotokolle gemäß der Anforderungen überprüft wurden
Maßzahl	Prozentsatz der im Prüfzeitraum kontrollierten kritischen Systemprotokolle
Formel	PI=Anzahl der geprüften kritischen Systemprotokolle/Anzahl der kritischen Systemprotokolle/100
Zielwerte	PI>=20%, liegt der PI unter 20% sollte eine Überprüfung der Kontrollen durchgeführt werden
Erhebungsunterlagen und Datenquelle	Anzahl der Systemprotokolle Logdateien, Tickets oder andere Beweise der Protokollprüfungen
Erhebungsfrequenz	Sammlung: monatlich; Bericht: je Semester
Verantwortlich	• Sicherheitsmitarbeiter, Protokollverantwortlicher • ISMS Verantwortlicher • Informationssicherheitsbeauftragter

Verwundbarkeit von Informationssystemen

Beschreibung	Bedeutung oder Zweck
Zweck	Bewertung der Verwundbarkeit von IT-Systemen mit sensiblen Informationen
Maßzahl	Prozentsatz kritischer IT-Systeme, die bei einer Schwachstellenanalyse oder einem Penetrationstest als verwundbar erkannt wurden.
Formel	PI=Anzahl der als verwundbar erkannten kritischen IT-Systeme/Anzahl der kritischen IT-Systeme*100
Zielwerte	Grün: PI>= 100%, Gelb:99%>PI>=75%, Rot: PI<75% • Grün: keine Aktion erforderlich • Gelb: Überwachung des Indikators auf Tendenzen und prüfen von Korrekturmaßnahmen • Rot: Intervention erforderlich; Klärung der Umstände und festlegen von Korrekturmaßnahmen
Erhebungsunterlagen und Datenquelle	Liste der kritischen IT-Systeme, Berichte der Schwachstellenprüfungen und Penetrationstests, IT-System Inventar,
Erhebungsfrequenz	Sammlung: nach Schwachstellenscans oder Penetrationstests; Bericht: jährlich
Verantwortlich	• Risikomanager, • RZ-Leitung • Informationssicherheitsbeauftragter

Sicherheitsereignisse- und Schwachstellenerhebung und -berichte

Beschreibung	**Bedeutung oder Zweck**
Zweck	Prüfen ob Sicherheitsereignisse und Schwachstellen berichtet und korrekt behandelt werden
Maßzahl	Anzahl der Sicherheitsereignisse die an das CSIRT gemeldet wurden und als solche klassifiziert und behandelt wurden
Formel	PI= Anzahl der gemeldeten Sicherheitsereignisse/ Anzahl der behandelten Sicherheitsereignisse
Zielwerte	PI=1
Erhebungsunterlagen und Datenquelle	Liste der Sicherheitsereignisse (Ticketsystem) und/oder –berichte Schwachstellenscans
Erhebungsfrequenz	Sammlung: jährlich; Bericht: jährlich
Verantwortlich	• Hochschulleitung, RZ-Leitung • CSIRT (Computer Security Incident Response Team) • Informationssicherheitsbeauftragter

B.6. Umsetzung Schritt 4 – Überwachung

Ein regelmäßiger Bericht ist der Leitung vorzulegen und für Abweichungen, geänderte oder neue Anforderungen müssen Maßnahmen geplant werden.

Ein kontinuierlicher Auditplan mit internen und externen Audits, Schwachstellenprüfungen und Penetrationstest ist zu erstellen. Abweichungen sind formal an das Risikomanagement zur Bewertung weiterzuleiten.

B.6.1. Ziele

Details der Aufgaben, um die Ziele zu erreichen, entnehmen Sie dem Punkt B.6.3.ff.

Zur umfassenden Bewertung der Wirksamkeit des ISMS muss die Hochschule die folgenden Rahmenbedingungen bestimmen:

- Zu messende Prozesse und Maßnahmen
- Methoden zur Messung
- Durchführungs- und Berichtszeiträume
- Verantwortlichkeiten für Überwachung, Messung, Sammlung, Analyse und Berichte

Es empfiehlt sich, in einer Regelung diese Rahmenbedingungen zu dokumentieren. Diese Regelung kann den hochschulweiten ISMS-Auditplan enthalten. Dieser Plan enthält den Umfang und die Zeiträume der internen und externen Audits, die prüfen, ob die Anforderungen an ein ISMS erfüllt, aufrechterhalten bzw. verbessert werden. Idealerweise werden diese Audits von hochschulinternen Auditoren (Kollegen anderer Hochschulen) durchgeführt.

In regelmäßigen Abständen sind Bewertungssitzungen der Sicherheitsgremien zu planen, damit die fortdauernde Eignung, Angemessenheit und Wirksamkeit des ISMS sichergestellt ist. Die Berichte als Grundlage der Bewertung muss folgende Aspekte behandeln:

a) den Status von Maßnahmen vorheriger Bewertungssitzungen;
b) Veränderungen bei externen und internen Themen, die das Informationssicherheits-managementsystem betreffen;
c) Rückmeldung über die Informationssicherheitsleistung, einschließlich Entwicklungen bei:
    a. Nichtkonformitäten und Korrekturmaßnahmen;
    b. Ergebnissen von Überwachungen und Messungen;
    c. Auditergebnissen; und
    d. Erreichung von Informationssicherheitszielen;
d) Rückmeldung von interessierten Parteien;
e) Ergebnisse der Risikobeurteilung und Status des Plans für die Risikobehandlung; und
f) Möglichkeiten zur fortlaufenden Verbesserung

Im Protokoll zu den Bewertungssitzungen sind Entscheidungen zur kontinuierlichen Verbesserung und Änderungsbedarf am ISMS zu dokumentieren.

B.6.2. Reifegradstufen

Stufe	Reifegrad	Ausprägung
0	**Nicht vorhanden**	Keine Berichte, Audits oder Bewertungssitzungen zum ISMS sind vorhanden oder geplant.
1	**Informell vorhanden**	In unregelmäßigen Abständen werden Audits oder andere Tests der Informationssicherheitsprozesse durchgeführt. Die Ergebnisse werden im Team besprochen und ad-hoc im Verantwortungsbereich projekthaft implementiert.
2	**Geplant**	Informationssicherheitsprozesse die einem ISMS dienen sind implementiert und werden im Verantwortungsbereich als de-facto Standards eingehalten. Externe Prüfungen werden durchgeführt und Ergebnisse an Gremien oder die Hochschulleitung rückgemeldet.
3	**Dokumentiert**	Informationssicherheitsprozesse die einem ISMS dienen sind in unterschiedlichen Regelungen dokumentiert und sind verpflichtend. Schwachstellenscans und/oder Penetrationstests werden geplant und regelmäßig durchgeführt. Ein Bericht zeigt Schwächen und die Wirksamkeit des ISMS auf und wird einem definierten Gremium vorgelegt.
4	**Quantitativ überwacht**	KPIs zum ISMS sind definiert und werden in regelmäßigen Berichten dem Gremium zur Bewertung vorgelegt. Interne und externe Audits prüfen das ISMS und die Ergebnisse sind Teil des regelmäßigen Berichts. Protokolle zu Entscheidungen des Gremiums sind vorhanden.
5	**Kontinuierlich verbessert**	Regelmäßige Überwachungsaudits und Änderungen des ISMS werden im Sicherheitsgremium oder von der Hochschulleitung entschieden, geplant und sind mit ausreichend Ressourcen ausgestattet um eine fristgerechte Umsetzung sicherzustellen. Die Anwendbarkeit und Aussagekraft der KPIs wird regelmäßig (mind. Alle 2 Jahre) überprüft.

Tabelle 7: Reifegradstufen zu Überwachung

B.6.3. Details zu Überwachung

			Reifegrad	Maßnahmen		
Ziele	**Inhalte**	**Muster/Vorlagen/Vorschläge**	**0-5**	**ISO 27001**	**BSI 200-x GS-Profil**	**ISIS12**
Bewertung des ISMS	• Planung und Definition von Messgrößen und Key Performance Indikatoren (KPI) • Berichtszeiträume und Verant-wortlichkeiten •	ISO27004 - 'Information security management - Monitoring, measurement, analysis and evaluation' Matthias Mödinger - „Metrics and KPIs for Information Security Reports" Matthias_Mödinger - 'Information-Security-Report-Template_(deutsch).doc' Matthias_Mödinger – 'Bestimmung KPIs_Value Benefit Analysis.xlsx' KPIs aus den Umsetzungsdetailkapiteln dieses Dokuments.		Kap. 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: Kap. 4 Kap. 7.5 BSI 200-2: Kap. 10 Priorität 1: ORP.1.A1 ORP.1.A14 Priorität 3: ORP.5.A4 ORP.5.A7	Schritt 11 und 12 M 1.4
Audits	• Auswahl des Standards • Auditplan,	ISO27001 BSI 200-1 ISIS12 TISAX SOC-2 …		Kap. 9.2	Kap. 7.4 DER.3.1.A13	Schritt 11
Gremiensitzungen	• ISMS Bericht • Entscheidungs-vorlagen • Gremienprotokolle	Matthias Mödinger - „Metrics and KPIs for Information Security Reports" Anhang_Master_Thesis__Matthias_Mödinger__Information-Security-Report-Template_(deutsch)		Kap. 9.3	BSI 200-1: Kap. 4.3 und Kap. 8.3 ORP.5.A8	Schritt 11.5

B.6.4. Arbeitspakete

Mögliche Prozesse	mögliche Projekte	Unterstützende Tools/Software	Betroffene Rollen/Funktionen
• Analyse der notwendigen Kennzahlen und Messmethoden • Auditdurchführung • Berichterstellung • Bewertungssitzung halten	• Einführung eines Kontroll- und Berichtswesens (für das ISMS selbst) • Zusammenarbeit mit dem Qualitätsmanagement	• Monitoring SW (Messgrößen) • Auswertetools für Protokolle • Business Intelligence • Ticketsystem	• Hochschulleitung • ISB • Sicherheitsgremium • Datenschutzbeauftragter • Qualitätsmanagement

B.6.5. Überprüfung, Auditfragen, Mindestanforderungen

ISO 2700x	BSI Grundschutz	ISIS12
• Audits von Informationssystemen (A 12.7.1) • Compliance (A 18)	• Prozessbaustein ORP.5 Complianceanforderungen • • BSI 200-2 Kap. 10	Revisionsfragen zu den einzelnen Schritten **Kontrollfragen zu Schritt 11 (optional)** • 11.6.1 Gibt es einen Auditplan und sind in diesem Plan alle wichtigen Informationen hinterlegt? • 11.6.2 Gibt es einen Audit-Bericht? • 11.6.3 Wurden Maßnahmen aus dem Audit abgeleitet? • 11.6.4 Wurden die Änderungen dokumentiert? • 11.6.5 Wurden ein neuer Termin und ein Verantwortlicher festgelegt? **Kontrollfragen zu Schritt 12** • 12.4.1 Wurden den Revisionsterminen verantwortliche Personen zugeordnet? • 12.4.2 Liegen die festgelegten Revisions-termine innerhalb von 12 Monaten? • 12.4.3 Ist aus dem Revisionsplan ersichtlich, was zum nächsten Revisionstermin geprüft werden muss? • 12.4.4 Wurden besondere offene Maß-nahmen identifiziert und wenn ja, ist sichergestellt, dass die Maßnahmen innerhalb von 12 Monaten umgesetzt werden können? • 12.4.5 Hat die Organisationsleitung den Jahresbericht des ISB zur Kenntnis genommen?

B.6.6. Berichte und Verbesserung

Kennzahlen, KPIs
• Anzahl der Verbesserungsmaßnahmen der ISMS Prozesse • Auditprogramm • Überprüfung des ISMS

Berichtspunkte und Periodizität
• Überprüfungen je Semester • Semesterweise für Trends • Jahresgesamtbericht • Interne Audits jährlich • Externe Audits alle 2 Jahre

B.6.6.1. Effizienz Indikator (Beispiel):

Verbesserungsmaßnahmen zu ISMS Prozessen

Beschreibung	**Bedeutung oder Zweck**
Zweck	Den Status von Maßnahmen zur Verbesserung der Informationssicherheit und deren Verwaltung gemäß den geplanten Maßnahmen überprüfen.
Maßzahl	Anzahl der Verbesserungsmaßnahmen (im zeitrahmen, Kosten und Qualität/Persistenz) im Verhältnis zu geplanten Maßnahmen. Die Maßnahmen sollen über einen geplanten Status (begonnen, in Arbeit, fertig) evaluiert werden. Eine Gewichtung nach Kritikalität kann die Messung verbessern.
Formel	EI=laufende oder abgeschlossene Maßnahmen/geplante Maßnahmen*100
Zielwerte	EI>=90%
Erhebungsunterlagen und Datenquelle	Statusverfolgung von Verbesserungsmaßnahmen (Ticketsystem) Projektpläne
Erhebungsfrequenz	Sammlung: Semester; Bericht: jährlich
Verantwortlich	• Informationseigentümer, Projektmanager • Informationssicherheitsbeauftragter

B.6.6.2. Performance Indikator (Beispiele):

Auditprogramm

Beschreibung	Bedeutung oder Zweck
Zweck	Einhaltung des Prüfplans/Auditplans
Maßzahl	Anzahl der durchgeführten geplanten Prüfmaßnahmen (z.B. Audits, Penetrationtests, Schwachstellenscans) Anzahl der geplanten Prüfmaßnahmen
Formel	PI=Anzahl der abgeschlossenen Prüfmaßnahmen/Anzahl der geplanten Prüfmaßnahmen*100
Zielwerte	PI>= 90%
Erhebungsunterlagen und Datenquelle	Auditplan, Ergebnisse von Prüfmaßnahmen
Erhebungsfrequenz	Sammlung: nach jeder Prüfmaßnahme; Bericht: jährlich
Verantwortlich	• Auditor, Informationssicherheitsbeauftragter • Sicherheitsgremium, Hochschulleitung

Überprüfung des ISMS (Audits)

Beschreibung	Bedeutung oder Zweck
Zweck	Einhaltung durchgeführter und geplanter Audits zur Wirksamkeit des ISMS
Maßzahl	Anzahl der durchgeführten geplanten Audits Anzahl der geplanten Audits
Formel	PI=Anzahl der abgeschlossenen Audits/Anzahl der geplanten Audits
Zielwerte	PI=1, wegen der geringen Anzahl der zu erwartenden Audits darf es hier keine Abweichung geben
Erhebungsunterlagen und Datenquelle	Auditplan, Auditberichte
Erhebungsfrequenz	Sammlung: nach jedem Audit; Bericht: jährlich
Verantwortlich	• ISMS Verantwortlicher, Auditor • Sicherheitsgremium, Hochschulleitung

B.7. Umsetzung Schritt 5 – Verbesserung

B.7.1. Ziele

Details der Aufgaben, um die Ziele zu erreichen, entnehmen Sie dem Punkt B.7.3.ff.

Die Hochschule muss auf Abweichungen von den Sicherheitsanforderungen reagieren, indem sie Maßnahmen zur Überwachung und/oder Korrektur ergreift. Die angemessenen Maßnahmen müssen durch Analyse der Ursachen und des Ausmaßes bewertet, eingeleitet und auf Wirksamkeit überprüft werden. Gegebenenfalls muss das ISMS angepasst werden.

Die Entscheidungen der Hochschulleitung oder des bestimmten Entscheidungsgremiums sind im Risikomanagement zu dokumentieren und an die Umsetzungsverantwortlichen zu kommunizieren. Im Protokoll zu den Entscheidungssitzungen sind diese zu dokumentieren.

B.7.2. Reifegradstufen

Stufe	Reifegrad	Ausprägung
0	**Nicht vorhanden**	Abweichungen werden nicht festgestellt oder nicht durch ein Entscheidungsgremium bewertet und keine Maßnahmen vorgeschlagen.
1	**Informell vorhanden**	RZ-Leiter und CIOs sind im Rahmen der Gesamtverantwortung für die IT mit den Entscheidungen zur Verbesserung der Informationssicherheit beauftragt. Investitionen we rden über Großanträge abgewickelt.
2	**Geplant**	Entscheidungsvorlagen für Verbesserungen werden in einem Sicherheitsgremium bewertet und entschieden.
3	**Dokumentiert**	Die Verbesserung der Informationssicherheit ist regelmäßiger Tagesordnungspunkt in Entscheidungsgremien und Ergebnisse dieser Sitzungen werden protokolliert.
4	**Quantitativ überwacht**	Das Sicherheitsgremium fordert regelmäßig Bericht über den Status des ISMS und Abweichungen. Es bewertet das Ausmaß, berät über angemessene Korrekturmaßnahmen und stellt ausreichend Ressourcen zur Korrektur zur Verfügung. Protokolle zu Entscheidungen des Gremiums sind vorhanden.
5	**Kontinuierlich verbessert**	Berichtszeiträume und –umfang wird regelmäßig (mind. alle 2 Jahre) überprüft. Bei ungenügender Aussagekraft oder geändertem Umfeld werden die Berichte angepasst und die Berichts- und Entscheidungsprozesse verbessert.

Tabelle 8: Reifegradstufen zu Verbesserung

B.7.3. Details zu Verbesserung

			Reifegrad	Maßnahmen		
Ziele	**Inhalte**	**Muster/Vorlagen/Vorschläge**	**0-5**	**ISO 27001**	**BSI 200-x GS-Profil**	**ISIS12**
Reaktion auf Abweichungen	• ISMS Bericht (Kapitel mit Abweichungen) • Entscheidungs-vorlagen, • Gremienprotokolle	Anhang_Master_Thesis__Matthias_Mödinger__Information-Security-Report-Template_(deutsch) Risikobewertung		Kap. 10.1 A 6.1.1	BSI 200-1: Kap. 4.4 und Kap. 8.4 BSI 200-1: Kap. 5.2.4 Kap. 10.3 ORP.5.A8	Schritt 11.5
Verbesserung des ISMS	• Entscheidungs-protokolle • Projekte, Großanträge			Kap. 10.2	Kap. 7.5	Schritt 11.5

B.7.4. Arbeitspakete

Mögliche Prozesse	mögliche Projekte	Unterstützende Tools/Software	Betroffene Rollen/Funktionen
• Vorbereitung von Entscheidungsgrundlagen • Berichterstellung über Abweichungen des ISMS	• Einführung eines Kontroll- und Berichtswesens (für das ISMS selbst) • Zusammenarbeit mit dem Qualitätsmanagement	• Monitoring SW (Messgrößen) • Auswertetools für Protokolle • Business Intelligence • Ticketsystem	• Hochschulleitung • Sicherheitsgremium • ISB • Datenschutzbeauftragter • Qualitätsmanagement

B.7.5. Überprüfung, Auditfragen, Mindestanforderungen

ISO 2700x	BSI Grundschutz	ISIS12
ISO27001 Kap.10 Compliance (A 18.2.2)	BSI 200-1 Kap. 4.4, 7.5 BSI 200-2 Kap. 10.3	**Kontrollfragen zu Schritt 11 (teilweise)** • 11.6.3 Wurden Maßnahmen aus dem Audit abgeleitet? • 11.6.4 Wurden die Änderungen dokumentiert? • 11.6.5 Wurden ein neuer Termin und ein Verantwortlicher festgelegt?

B.7.6. Berichte und Verbesserung

Kennzahlen, KPIs	Berichtspunkte und Periodizität
• Anzahl der Verbesserungsmaßnahmen der ISMS Prozesse • Überprüfung des ISMS	• Überprüfungen je Semester • Semesterweise für Trends • Jahresgesamtbericht • Entscheidungsprotokolle

B.7.6.1. Effizienz Indikator (Beispiel):

Verbesserungsmaßnahmen zu ISMS Prozessen

Beschreibung	**Bedeutung oder Zweck**
Zweck	Den Status von Maßnahmen zur Verbesserung der Informationssicherheit und deren Verwaltung gemäß den geplanten Maßnahmen überprüfen.
Maßzahl	Anzahl der Verbesserungsmaßnahmen (im zeitrahmen, Kosten und Qualität/Persistenz) im Verhältnis zu geplanten Maßnahmen. Die Maßnahmen sollen über einen geplanten Status (begonnen, in Arbeit, fertig) evaluiert werden. Eine Gewichtung nach Kritikalität kann die Messung verbessern.
Formel	EI=laufende oder abgeschlossene Maßnahmen/geplante Maßnahmen*100
Zielwerte	EI>=90%
Erhebungsunterlagen und Datenquelle	Statusverfolgung von Verbesserungsmaßnahmen (Ticketsystem) Projektpläne
Erhebungsfrequenz	Sammlung: Semester; Bericht: jährlich
Verantwortlich	• Informationseigentümer, Projektmanager • Informationssicherheitsbeauftragter

B.7.6.2. Performance Indikator (Beispiel):

Überprüfung des ISMS (Verbesserungen)

Beschreibung	**Bedeutung oder Zweck**
Zweck	Einhaltung durchgeführter Verbesserungen und Entscheidungen zur Wirksamkeit des ISMS
Maßzahl	Anzahl der durchgeführten Verbesserungen Anzahl der Entscheidungen
Formel	PI=Anzahl der Verbesserungen/Anzahl der Entscheidungen*100
Zielwerte	PI=80%
Erhebungsunterlagen und Datenquelle	Protokolle der Entscheidungsgremien Umsetzungsaufträge, Großanträge
Erhebungsfrequenz	Sammlung: nach jeder Gremiensitzung; Bericht: jährlich
Verantwortlich	• ISMS Verantwortlicher, Auditor • Sicherheitsgremium, Hochschulleitung