Hochschule
Augsburg University of
Applied Sciences

Fakultät für
Informatik

Forschungsbericht 2

Studienrichtung
Master of Applied Science

Sabine Schnitzler

Analyse und Evaluation von Methoden und Modellen zur Einführung eines Informationssicherheits-managementsystems (ISMS) an bayerischen Hochschulen und Universitäten

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

Abgabe der Arbeit am: 09.03.2017

Hochschule für angewandte
Wissenschaften Augsburg
University of Applied Sciences

An der Hochschule 1
D-86161 Augsburg

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

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

Verfasser des
Forschungsberichtes 2:
Sabine Schnitzler
Armenhausgasse 11d
86150 Augsburg
Telefon:+49 176/21160798

I. KURZFASSUNG

Auf Grund des steigenden Vernetzungsgrades, der stark wachsenden Informationsverteilung, bei gleichzeitigem Verschwinden von Netzwerkgrenzen, sowie der dazu simultan rasant steigenden Anzahl an Cyber Crime Delikten im letzten Jahrzehnt, ist Informationssicherheit ein essentielles, Sektor übergreifendes Thema. Gerade in einem wissensintensiven Umfeld wie dem Universitäts-und Hochschulbereich, in dem Daten das wertvollste Gut sind, müssen auf der einen Seite die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der Daten gewährleistet, aber andererseits auch die Freiheit der Forschung und Lehre bewahrt werden. Zusätzlich wurde die Notwendigkeit eines Informationssicherheitssystems (ISMS) durch die Verabschiedung einiger Gesetzte, Normen und Vorschriften auf unterschiedlicher Ebene unterstrichen. Nicht nur auf Grund des Gesetzes über die elektronische Verwaltung in Bayern (BayEGovG) in Verbindung mit dem Bayerischen Datenschutzgesetz (BayDSG) ist es unerlässlich, ein adäquates ISMS an allen bayerischen Universitäten und Hochschulen bis zum 01.01.2018 einzuführen. Allerdings existieren sehr unterschiedliche Ansätze und Verfahrensweisen im Bereich Informationssicherheit, sowohl in sehr differenzierter Quantität, als auch Qualität. Speziell im wissensintensiven Universitäts-und Hochschulbereich existiert bisher noch keine individuell geeignete Lösungsvariante, um ein ISMS zu erstellen, zu implementieren, instand zu halten oder gar zu verbessern. Im Rahmen dieses Forschungsberichtes werden die unterschiedlichen existierenden Ansätze und Verfahrensweisen analysiert und gegenübergestellt. Darauf basierend bewertet dieser Forschungsbericht die priorisierten Vorgehensweisen unter Verwendung einer Nutzwertanalyse, anhand für den Universitäts-und Hochschulbereich relevanten Kriterien. Dadurch ist es möglich, sowohl die Stärken und Schwächen der priorisierten Lösungsalternativen anhand der Teilnutzwerten zu identifizieren, als auch eine Gesamtbeurteilung der Varianten durchzuführen. Schlussendlich wird hierdurch die Notwendigkeit einer speziell für den wissensintensiven Universitäts- und Hochschulbereich individuellen Lösung verdeutlicht, da von keiner der untersuchten Lösungsmöglichkeit alle notwendigen Anforderungen komplett alleine erfüllt werden.

II. INHALTSVERZEICHNIS

III. ABBILDUNGSVERZEICHNIS

IV. ABBKÜRZUNGSVERZEICHNIS

AKDB	Arbeitshilfe der Bayerische Innovationsstiftung der Anstalt für Kommunale Datenverarbeitung in Bayern
BSI	Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung e.V.
IEC	International Electrotechnical Commission (Internationale Elektrotechnische Kommission)
ISB	Informationssicherheitsbeauftragte
ISIS 12	Informationssicherheitsmanagementsystem in 12 Schritten
ISM	Informationssicherheitsmanagement
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IT	Informationstechnik
PDCA	Plan-Do-Check-Act
PT	Personentage

1 Einleitung

Die Bedeutung der Informationssicherheit hat sich in den letzten Jahren sowohl in der Wirtschaft als auch im öffentlichen Bereich sehr stark verändert. Auf Grund des rasanten Wandels zur steigenden IT-Abhängigkeit in Form eines wachsenden Vernetzungsgrads, einer ansteigenden globalen IT-Verbreitung, einer wachsenden Interaktivität von Anwendungen mit gleichzeitigem Verschwinden der Netzgrenzen, erhöht sich die Anzahl an Bedrohungen und Angriffen und somit auch der potentielle, durch den Ausfall von Informationstechnik, entstehende Schaden. Gerade der mobile Zugriff auf interne Informationen durch eine wachsende Anzahl an Benutzern stellt eine große Gefahrenquelle für mögliche Angriffe dar. Da Informationssicherheit als ganzheitlicher Ansatz zu betrachten ist, muss nicht nur die technische, sondern auch die personelle, organisatorische und infrastrukturelle Komponente berücksichtigt werden. Jedoch wird gerade in der öffentlichen Verwaltung die Lage der Informationssicherheit als kritisch eingestuft, da notwendige Standardsicherheitsmaßnahmen, wie regelmäßige Updates, starke Passwörter oder Datensparsamkeit im Sinne des § 3a Bayerischen Datenschutzgesetzes (BDSG), oftmals nicht vorhanden sind [1]. Da in der öffentlichen Verwaltung, insbesondere im Hochschulbereich, Verwaltungsabläufe mittlerweile durch Informationstechnik unterstützt werden, sind Informationen das wertvollste Gut und müssen somit entsprechend geschützt werden. Um die Sicherstellung der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten, ist es notwendig, eine strukturelle Methodik zum Schutz der Informationssicherheit einzuführen. Mit Hilfe eines geeigneten Modells zur Etablierung eines sogenannten Informationsmanagementsystems (ISMS) ist möglich, die Informationssicherheit einer Organisation oder Behörde ganzheitlich zu garantieren. Um der Notwendigkeit eines wirksamen ISMS Nachdruck zu verleihen, wurden in letzter Zeit einige Gesetze, Vorschriften und Beschlüsse auf unterschiedlichen hierarchischen Ebenen verabschiedet. So wurde beispielsweise, neben der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), das Gesetz über die elektronische Verwaltung in Bayern (BayEGovG) in Verbindung mit dem Bayerischen Datenschutzgesetz (BayDSG) verabschiedet, welches die Etablierung eines Informationssicherheitskonzeptes bis 01.01.2018 in der öffentlichen Verwaltung vorschreibt[2],[3].

Besondere Herausforderungen stellt die Einführung eines ISMS in wissensintensiven Organisationen, wie in Universitäten und Hochschulen dar. Es muss auf der einen Seite den Anforderungen an die Freiheit der Forschung und Lehre gerecht werden, und auf der anderen Seite muss der hohe Schutzbedarf der sensiblen Daten, wie beispielsweise personenbezogene Verwaltungsdaten, Prüfungsergebnisse oder Forschungsdaten, beachtet werden. Daneben sollte bei den Hochschul-und Universitätsangehörigen ein Bewusstsein für die Wichtigkeit der Informationssicherheit vorhanden sein. Auf Grund dessen muss somit ein speziell auf die im Hochschul-und Universitätsbereich abgestimmten Anforderungen, ein ISMS etabliert werden [4], [5], [6], [7].

Zur Etablierung eines wirkungsvollen ISMS existieren unterschiedliche Ansätze und Vorgehensmodelle, wie beispielsweise die ISO/IEC 2700x Normenfamilie, das Informationssicherheitsmanagementsystem in 12 Schritten (ISIS 12) oder der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Daneben wurden vom IT-Planungsrat, der basierend auf dem IT-Staatsvertrag für die Vereinbarung gemeinsamer Mindestanforderungen zwischen Bund und Länder

verantwortlich ist, umzusetzende Mindestanforderung für die Informationssicherheit erstellt. Die Notwendigkeit ein ISMS zu erstellen, wurde kürzlich auch von der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) erkannt, so dass die Innovationsstiftung Bayerische Kommune im Dezember 2016 für Kommunen eine Arbeitshilfe zur Erstellung eines Informationssicherheitskonzeptes hervorbrachte.

Ziel dieses Forschungsberichtes ist es, die unterschiedlichen Ansätze und Verfahrensweisen mit ihren jeweiligen Stärken und Schwächen zu analysieren, gegenüberzustellen und zu bewerten. Mit speziell auf den Universitäts-und Hochschulbereich abgestimmten Anforderungen werden zur Bewertung der unterschiedlichen Verfahrensweisen bestimmte Kriterien definiert. Auf dieser Basis werden mit Hilfe einer Bewertungsmatrix die unterschiedlichen Ansätze zur Erstellung, Implementierung, Aufrechterhaltung und Verbesserung eines Informationsmanagementsystems im Universitäts-und Hochschulbereich bewertet. Durch diese Vorgehensweise bietet dieser Forschungsbericht eine fundierte Analyse und Bewertung der verschiedenen Modelle zur Etablierung eines ISMS an allen bayerischen Hochschulen und Universitäten. Als Ergebnis werden sowohl die Stärken und Schwächen jeder Lösungsalternative anhand der Teilnutzwerte aufgezeigt, als auch eine Gesamtbewertung anhand des Nutzwertes durchgeführt. Schlussendlich wird die Notwendigkeit einer individuellen speziell auf den Universitäts-und Hochschulbereich ausgerichteten Lösung aufgezeigt, da keine der untersuchten Lösungen alle Anforderungen gänzlich erfüllt.

Dieser Forschungsbericht ist folgendermaßen strukturiert. Im Kapitel zwei werden neben den für das Verständnis relevanten Definitionen die Anforderungen der öffentlichen Verwaltung, insbesondere im Universitäts-und Hochschulbereich beschrieben. Im nächsten Kapitel werden die bereits existierenden Konzepte im Umfeld der Informationssicherheit im Universitäts-und Hochschulbereich erläutert. Darüber hinaus werden relevante Normen, Standards und Rahmenbedingungen, die sich als Einflussfaktoren auf Managementsysteme für Informationssicherheit darstellen, beschrieben. Darauf aufbauend werden im Kapitel vier die unterschiedlichen Vorgehensweisen dieser jeweiligen Standards und Normen analysiert. Im Kapitel fünf werden die drei priorisierten Vorgehensmodelle zu Erstellung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS gegenübergestellt und erläutert. Darauf aufbauend werden im Kapitel sechs die verschiedenen Ansätze mit Hilfe einer Nutzwertanalyse bewertet. Abschließend werden im letzten Kapitel Anregungen für weitere wissenschaftliche Arbeiten gegeben.

2 Definition, Untersuchungsgegenstand und Anforderungen

2.1 Definition

In diesem Unterkapitel werden für eine grundlegende gemeinsame Basis notwendige Begriffe definiert, da unterschiedliche Definitionen existieren.

Öffentliche Verwaltung ist der Oberbegriff für Verwaltungen, die Aufgaben des Staates einschließlich Einrichtungen des öffentlichen Rechtes wahrnehmen. Träger der öffentlichen Verwaltung sind der Bund, die Länder und die Kommunen. Der Hochschulbereich fällt somit auch unter diesen Begriff.

Staatliche bzw. öffentliche IT bezeichnet die öffentlichen und die nicht-öffentlichen Bestandteile von Informationstechnologien, die in der Verantwortung der öffentlichen Hand betrieben werden. Dies umfasst IT auf allen staatlichen und überstaatlichen Ebenen, d.h. auf internationaler, europäischer, Bundes-, Landes- und kommunaler Ebene sowie im Rahmen von Bündnissen.

Informationssicherheit erweitert den Begriff IT-Sicherheit um die personelle, organisatorische, prozessuale und infrastrukturelle Komponente, in der die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität sichergestellt werden.

Unter Informationssicherheitsmanagement (ISM) wird die Planungs-, Lenkungs- und Kontrollaufgabe verstanden, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.[8]

Unter einem Informationssicherheitsmanagementsystem (ISMS) versteht man gemäß dem ISO/IEC Standard 27001 [9] sowie den BSI-Standard 100-1 [10] und den Aspekte nach Müller [11] die Gesamtheit aller Prozesse, Verantwortlichkeiten, Verfahren, Methoden sowie Ressourcen und Hilfsmittel, um der Leitungsebene mit einer effizienten Aufbauorganisation zu ermöglichen, alle auf Informationssicherheit ausgerichteten Aktivitäten und Aufgaben nachvollziehbar zu lenken und zu dokumentieren. Daneben enthält ein wirksames ISMS iterative Sicherheits-, Kontinuitäts- und Risikomanagementprozesse. Mit Hilfe eines ISMS wird Informationssicherheit in den Lebenszyklus von Prozessen, Ressourcen, Organisation, Produkten und Leistungen integriert. Einige Vorgehensweisen enthalten unterschiedliche Teilbereiche bzw. Kernelemente eines ISMS in unterschiedlicher Vollständigkeit, Detaillierung, Konkretisierung und Qualität [12].

Als Informationssicherheitsrisiko wird das Potential bezeichnet, indem die Bedrohung einer Schwachstelle ausgenutzt werden kann und somit Schaden verursacht wird. Das Risiko setzt sich aus der Kombination der Wahrscheinlichkeit eines Ereignisses und dessen Konsequenzen zusammen[13].

Unter Risikomanagement wird die Erhebung, Analyse, Bewertung, Justierung bzw. Behandlung, Überwachung, Früherkennung von Risiken sowie die zielgerichtete und anforderungskonforme Steuerung, das Reporting und die Kommunikation von Risiken verstanden [11],[14].

Der Risikomanagement-Prozess umfasst die systematische iterative Vorgehensweise wie Managementrichtlinien, -verfahren und -praktiken, um alle potentiellen Risiken zu identifizieren und zu bewerten, den Kontext festzulegen, sowie hierauf aufbauend entsprechende Maßnahmen zur Risikohandhabung, wie die Behandlung, Überwachung und Überprüfung von Risiken, auszuwählen und

umzusetzen, sowohl auf strategischer als auch auf operativer Ebene. Daneben unterliegt der Risikomanagement-Prozess ständigen Verbesserungsmaßnahmen [15], [14].

Die Risikoanalyse ist ein Prozess, um die Beschaffenheit des Risikos zu verstehen und das Risikoniveau zu bestimmen. Dabei liefert die Risikoanalyse die Grundlage für die Risikobewertung, Risikoabschätzung und die Entscheidungen auf Grund der Risikobehandlung [14].

2.2 Untersuchungsgegenstand und Abgrenzung

Der vorliegende Forschungsbericht enthält einen Überblick über die verschiedenen bereits vorhandenen Modelle zur Erstellung eines ISMS. Daneben wird eine Analyse über die Inhalte, Unterschiede und Überschneidungspunkte der verschiedenen Vorgehensmodelle durchgeführt. Anhand für die öffentliche Verwaltung, im Besonderen für den Universitäts-und Hochschulbereich definierten Anforderungen, werden die unterschiedlichen Ansätze evaluiert und bewertet.

Im Rahmen dieses Forschungsberichtes soll eine unabhängige Bewertung erfolgen, welches Vorgehensmodell sich am besten für die Erstellung eines ISMS im Hochschulbereich eignet. Darüber hinaus sollen die Stärken und Schwächen der unterschiedlichen Ansätze bewertet werden.

Die Planung und Umsetzung des geeigneten Modells ist nicht Bestandteil dieses Forschungsberichts. Ebenso ist die Analyse und Bewertung der einzusetzenden Tools nicht Inhalt dieser Arbeit. Der Forschungsbericht ist eine Momentaufnahme und gilt zum Zeitpunkt des Dokuments als abschließend.

2.3 Vorgehensweise

In einem ersten Schritt werden die allgemeinen Anforderungen und Rahmenbedingungen in der öffentlichen Verwaltung, im Besonderen im Universitäts-und Hochschulbereich definiert. Als nächstes werden die bereits vorhanden auf die Informationssicherheit bezogenen Dokumente beschrieben. Zudem analysiert dieser Forschungsbericht die unterschiedlichen Standards und Normen im Bereich der Informationssicherheit und stellt die unterschiedlichen Vorgehensmodelle vor. Die für den Hochschulbereich relevanten Vorgehensmodelle werden gegenübergestellt und anhand definierten Kriterien mit Hilfe einer Nutzwertanalyse bewertet. Als Ergebnis dieser Arbeit wird ein Vorgehensmodell aufgezeigt, mit diesem ein ISMS an allen bayerischen Hochschulen und Universitäten eingeführt werden kann.

Die Ergebnisse des Forschungsberichts basieren unter anderem auf Informationen des Bayerischen IT-Sicherheitscluster e.V., auf der Analyse der ISO/IEC 2700x Normenfamilie, des BSI-Grundschutzes und der Arbeitshilfe der Bayerischen Innovationsstiftung. In die Bewertung fließen die Ergebnisse von [16], [17], [18], [7], [6] mit ein. Daneben werden die Rahmenbedingungen und Anforderungen öffentlicher Verwaltungen, insbesondere im Universitäts-und Hochschulbereich, berücksichtigt.

2.4 Allgemeine Anforderungen der öffentlichen Verwaltung

Die Förderung von Wissenschaft, Forschung und Lehre ist eine gemeinsame zentrale Aufgabe von Staat und Gesellschaft und verfassungsrechtlich in Artikel 91b Absatz 1 GG [19] geregelt.

Da mittlerweile der überwiegende Anteil aller Verwaltungsprozesse in öffentlichen Verwaltungen, insbesondere im Universitäts-und Hochschulbereich, durch Informationstechnik unterstützt wird, ist die Arbeitsfähigkeit in der öffentlichen Verwaltung essentiell von der Verfügbarkeit, Vertraulichkeit und Integrität der Daten abhängig. Ein wesentliches Ziel des am 01.08.2013 in Kraft getretenen E-Gouvernement-Gesetz des Bundes ist es, auf allen staatlichen Ebenen nutzerfreundliche, effiziente und medienbruchfreie elektronische Verwaltungsverfahren bereitzustellen. Der IT-Planungsrat (IT-PLR) ist, basierend auf dem IT-Staatsvertrag [20], zuständig für die Vereinbarung gemeinsamer Mindestanforderungen zwischen Bund und Ländern. Somit gilt die verabschiedete „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ [21] für alle Behörden und Einrichtungen der Verwaltungen des Bundes und Länder. In dieser Leitlinie werden die Mindestanforderungen für IT-Sicherheit für Bund und Länder festgelegt. Allerdings sind die Vorgaben der Leitlinie von Bund und Ländern im jeweiligen Zuständigkeitsbereich in eigener Verantwortung umzusetzen [21],[22]. Die Festlegung des Mindestsicherheitsniveaus orientiert sich am IT-Grundschutz des BSI.

Es existieren besondere Herausforderungen für die IT in der öffentlichen Verwaltung, wie beispielsweise ein hierarchisches Umfeld, eine große Ansammlung an Regulierungen (Gesetzte, Verordnungen, Dienstvorschriften), Haushaltsregeln und sehr traditionell verankerte Vorgaben zu einzelnen Geschäftsabläufen. Daneben werden IT-Standards in der öffentlichen Verwaltung auf Grund ihrer dezentralen Organisation, der föderalen Gliederung des Staates und des Ressortprinzipes größtenteils dezentral entwickelt. Allerdings führt dieser Ansatz zu unterschiedlichen Ergebnissen.[23] Sinnvoll erscheint hier eine zentrale Stelle zur Erreichung einheitlicher IT-Sicherheitsstandards.

Anlehnend an [24], [25] ist die Grundvoraussetzung für eine erfolgreiche Einführung eines ISMS im öffentlichen Sektor ein gesundes Human Ressources Management, wie beispielsweise Investitionen in hochqualifizierte Fachexperten im Bereich Informationssicherheit, Trainings- und Sensibilisierungsmaßnahmen.

Besonders im universitären Bereich muss auf der einen Seite die Freiheit der Forschung und Lehre gewahrt werden und auf der anderen Seite müssen die sensiblen Daten, wie beispielsweise personenbezogenen Angestellten und Studentendaten, Prüfungen, Zeugnisse oder Forschungserbnisse geschützt werden. Die Gewährleistung von Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit ist eine elementare Voraussetzung jedes IT-Verfahrens. Bei einer bayernweiten Betrachtung aller Universitäten und Fachhochschulen kann nicht mehr von der Definition einer Standardbehörde (bis zu ca. 500 Mitarbeiter, eine möglichst homogene IT-Basisinfrastruktur, keine über öffentliche Netze ungeschützt angebundene Außenstellen, einen überwiegend normalen Schutzbedarf, keine Hochverfügbarkeitsanforderungen an IT-Systeme und keine kritischen Anwendungen (d.h. keine kritischen Infrastrukturen)) im Sinne des BSI ausgegangen werden. Selbst wenn jede Universität und Hochschule unabhängig voneinander betrachtet wird, sind dort jeweils mehr als 500 Personen angehörig. Daneben existieren über öffentliche Netze ungeschützt angebundene Außenstellen und der Schutzbedarf kann gerade im Bereich von Forschungsergebnissen oder Prüfungen als nicht mehr normal hoch eingestuft werden. Meist existiert im Hochschulbereich auch keine homogene IT-Basisinfrastruktur, da die einzelnen Fakultäten oftmals unabhängig voneinander agieren. Greifen tausende Studenten auf eine Anwendung (z.B. Webserver für Emailverkehr, E-Learning) zu, bestehen Hochverfügbarkeitsanforderungen an IT-Systeme. Daneben lässt sich diskutieren, ob Universitäten und Hochschulen unter den Begriff KRITIS (kritische Infrastrukturen) fallen können. Falls Rechenzentrum eine Jahresdurchschnittsleistung von 5 Megawatt enthalten oder etwa Universitäten mit einer medizinischer Fakultät das Notfall-und Rettungswesen unterstützen, ließe sich der Begriff bejahen [26],[27].

3 Vorhandene Standards, Normen und Konzepte

3.1 Bereits existierende Konzepte hinsichtlich Informationssicherheit an Hochschulen und Universitäten

In diesem Kapitel beschreibt dieser Forschungsbericht die bereits existierenden Konzepte im Umfeld der Informationssicherheit an Hochschulen und Universitäten. Diese wurden zum einen von den Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.(ZKI) des Arbeitskreises IT-Sicherheit und zum anderen von der Kooperationsgruppe „Informationssicherheit des IT-Planungsrates“ eruiert. Allerdings stützen sich diese Konzepte sowohl auf die ISO/IEC 27001, als auch auf den BSI Grundschutz. Daneben existiert bereits seit 2005 ein von der Freien Universität Berlin etabliertes Sicherheitskonzept. Jedoch berücksichtigt dieses Konzept keinen prozessorientierten Ansatz mit kontinuierlichen Verbesserungsmaßnahmen. Nachfolgend werden die Bestandteile der unterschiedlichen Sichtweisen beschrieben.

3.1.1 Kooperationsgruppe „Informationssicherheit des IT-Planungsrates (IT-PLR)“

Der IT-PLR ist, basierend auf dem IT-Staatsvertrag [20], zuständig für die Vereinbarung gemeinsamer Mindestsicherheitsanforderungen zwischen Bund und Ländern mit ihren Behörden und Einrichtungen der Verwaltung. Somit ist er für die Erarbeitung, Verabschiedung, Weiterentwicklung und Erfolgskontrolle der Informationssicherheitsleitlinie verantwortlich. Eines der wichtigsten Ziele dieser Leitlinie ist, der Aufbau und die Etablierung des Informationssicherheitsmanagements in den öffentlichen Verwaltungen, welches auf Basis des IT-Grundschutz des BSI oder ISO 27001 in den Behörden bis 01.01. 2018 einzuführen ist. Die im Jahr 2013 definierten Mindestanforderungen, die fünf Säulen der der Informationssicherheit, basieren auf dem IT-Grundschutz des BSI. Nachfolgend werden die Bestandteile dieser fünf Säulen beschrieben.

- Informationssicherheitsmanagement
    - Definition von Verantwortlichkeiten (z.B. Benennung IT-Sicherheitsbeauftragte)
    - Erstellung und Umsetzung von Sicherheitskonzepten für Behörden und Einrichtungen.
    - Definition von verbindlichen Leitlinien für die Informationssicherheit
    - Definition und Dokumentation der Abläufe bei IT-Sicherheitsvorfällen
    - Etablierung von Prozessen zur regelmäßigen Kontrolle der Umsetzung, Einhaltung und Wirksamkeit der Informationssicherheitsmaßnahmen (z.B. Fortschreibung Sicherheitskonzepte)
    - Durchführung regelmäßiger Sensibilisierungsmaßnahmen aller Beschäftigter
    - Regelmäßige Fortbildung aller IT-Sicherheitsbeauftragten → wünschenswerte Zertifizierung der IT-Sicherheitsbeauftragten
    - Regelmäßiger Erfahrungsaustauch der IT-Sicherheitsbeauftragten

- Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung gemäß §4 IT-NetzG
    - Errichtung eines ISMS

    - direkt angeschlossene Netze gemäß den BSI-Standards 100-1, 100-2, 100-3 und 100-4
    - Festlegen des Schutzbedarfs für Netzwerkverbindungen, über die kritische IT-gestützte Ebenen-Übergreifende Geschäftsprozesse
    - gegenseitige Auditierung

- Einheitliche Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren
    - Anwendung des BSI Grundschutzes
- Gemeinsame Abwehr von IT-Angriffen
    - Aufbau entsprechender LandesCERTs mit Festlegung übergreifender Prozesse
    - Etablierung eines Meldeverfahrens mit zentraler Sammelstelle im BSI
    - gegenseitige Unterstützung bei IT-Sicherheitsvorfällen
    - Erstellung eines übergreifenden IT-Sicherheitslageberichtes
- Standardisierung und Produktsicherheit
    - Gewährleistung der Mindestanforderungen [28]

3.1.2 Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.(ZKI) des Arbeitskreises IT-Sicherheit

Bei diesen Anforderungen an die Informationssicherheit, die bereits 2005 festgesetzt wurden, wurde noch kein Unterschied zwischen der IT-Sicherheit und der Informationssicherheit gemacht. Es sollten folgende Aspekte bei der Einführung von IT-Sicherheit berücksichtigt werden:

- Definition und Kommunikation des angestrebten Ziels
- Beschluss einer Sicherheitsordnung
- Festlegen der Zuständigkeiten und Verankerung in der Hochschulleitung
    - Definition der Beteiligten am Sicherheitsprozess
- Erarbeitung und Verabschiedung einer Rahmenrichtlinie für die Hochschule
    - Beschreibung der Ausgangsituation
    - Beschreibung der Grundschutzmaßnahmen
    - Anleitung für eine Schutzbedarfsanalyse als Basis zur Beschreibung des IT-Einsatzes
    - Anleitung für eine Risikoanalyse zur Erfassung ganz besonders sensibler IT-Bereiche
    - Beschreibung der Umsetzung der IT-Sicherheit als Fortschreibungsprozess
- Beschreibung der IT-Infrastruktur als Basiskomponente des IT-Einsatzes
- Bestandsaufnahme der vorhandenen IT-Verfahren

Anschließend wird auf Grundlage dieser Aspekte eine kontinuierliche Risikoanalyse mit den notwendigen Sicherheitsmaßnahmen durchgeführt. Die Risikoanalyse wird jedoch hier nicht näher beschrieben. Daneben wird bezüglichen den technischen Punkten ein rechtlicher Rahmen beschrieben, in dem vor allem die Gesetzte TDG, TDDSG, MDStV, TKG Anwendung finden [29], [30].

3.1.3 Informationssicherheitsrahmenrechtlinie der Freien Universität Berlin

Die im Jahr 2005 entwickelte Informationssicherheitsrahmenrichtlinie der freien Universität Berlin orientiert sich sehr stark an den IT-Grundschutz des BSI. Aufgrund des Erstellungszeitpunktes basiert die erstellte Rahmenrichtlinie allerdings noch auf dem Sicherheitshandbuch des BSI von 1992 und dem Grundschutzhandbuch des BSI von 2002. Das Sicherheitshandbuch und das Grundschutzhandbuch wurden ab 2005 durch die BSI Standards 100-1bis 100-4 abgelöst. Der Aufbau dieser Richtlinie besteht aus folgenden Punkten:

- Definition der Ausgangssituation
- Definition des Grundschutzes
- Schutzbedarfsanalyse
- Risikoanalyse
- Umsetzung der IT-Sicherheitsrichtlinie

Dieses Konzept verfolgt auf Grund der verwendeten Quellen (Sicherheitshandbuch und Grundschutzhandbuch) noch keinen iterativen Prozess mit Verbesserungsmaßnahmen wie etwa dem PDCA-Zyklus, sondern stellt vielmehr eine Moment-bezogene Bestandsaufnahme dar [31].

3.2 Relevante Normen und Standards im Bereich der Informationssicherheit

In diesem Kapitel beschreibt dieser Forschungsbericht auf die Informationssicherheit bezogene, internationale DIN ISO Normen und strukturiert die Inhalte des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Daneben wird das Informationssicherheitsmanagementsystem in 12 Schritten (ISIS 12) des bayerischen Sicherheitscluster e.V. und die Inhalte der Arbeitshilfe der bayerischen Innovationsstiftung der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) analysiert. Zusätzliche werden weitere Standards, die die Informationssicherheit tangieren, vorgestellt.

3.2.1 ISO/IEC 2700x Normenfamilie

3.2.1.1 ISO 27000: Überblick/Terminologie/Definitionen

Die DIN ISO Norm 27000 (ISO/IEC DIS 27000:2015) gilt als wichtigste Norm im Bereich der Informationssicherheitsmanagementsysteme. Diese Norm verschafft einen grundlegenden Überblick über die gesamten Normen der DIN ISO 2700x-Normenfamilie der International Standards Organisation. Durch die Mitarbeit des Deutschen Institutes für Normung e.V. (DIN) mit seiner Arbeitsgruppe Normenausschuss Informationstechnik und Anwendungen (NIA) [32] wurden einige dieser internationalen Normen als deutsche DIN Normen übernommen. Basierend auf dem Britischen Standard BS 7799-1[33], der hauptsächlich von Prof. Edward Humphreys beeinflusst wurde, werden notwendige Fachbegriffe definiert, die in der ISMS-Normenfamilie verwendet werden und somit für ein grundlegendes Verständnis erforderlich sind.

Die DIN ISO/IEC Norm 27000 beschreibt ein, auf internationalen Standards ausgerichtetes Vorgehensmodel zur Einrichtung und Betreibung eines Informationssicherheitsmanagementsystems (ISMS). Dieses Vorgehensmodell, welches auf dem internationalen „Stand der Technik“ basiert, ermöglicht Organisationen, art-und größenunabhängig, ein Rahmenwerk zu entwickeln, um die Sicherheit ihrer zu schützenden Informationswerte aufrechtzuhalten und zu verwalten [34]. Dieses Vorgehensmodell wird als prozessorientierter Ansatz bezeichnet, der kontinuierliche Verbesserungsmaßnahmen enthält. In der vorherigen Version dieser Norm (DIN ISO/IEC 27000:2011) basiert der Gesamtprozess der Erstellung, Instandhaltung, Kontrolle und Verbesserung eines ISMS noch auf dem „Plan-Do-Check-Act-Prozess“ („Planen, Durchführen, Prüfen, Handeln“) bzw. „PDCA-Prozess“, wohingegen in der aktuellen Version dieser Prozess lediglich im Teilprozess des Informationssicherheitsrisikomanagements (siehe Kapitel 4.1) angewendet wird [34][14].

Allgemein betrachtet, besitzt die gesamte DIN ISO/IEC Normenfamilie im Vergleich zu anderen Rahmenwerken in Bezug auf die Informationssicherheit einen sehr abstrakten Charakter [35]. Die „family of standards“ umfasst neben Anforderungen an ISMS, auch detaillierten Leitlinien zur Erstellung, Umsetzung, Aufrechterhaltung oder zur Verbesserung eines ISMS aus gesamtprozessualer Sichtweise. Die ISMS „family of standards“ besteht aus Folgenden internationalen Standards:

- ISO/IEC 27000, Information security management systems Overview and vocabulary
- ISO/IEC 27001, Information security management systems Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management - Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC DIS 27009, Sector-specific application of ISO/IEC 27001 - Requirements
- ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014, Governance of information security
- ISO/IEC TR 27015, Information security management guidelines for financial services
- ISO/IEC TR 27016, Information security management - Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud Services
- ISO/IEC 27018, Code of practice for PII protection in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO 27799:2008, Health informatics - Information security management in health using ISO/IEC 27002

Die Normen der ISMS-Normenfamilie werden anhand ihres Typs bzw. ihrer Rolle klassifiziert. So existieren Normen,

- die einen Überblick verschaffen und die Terminologie festlegen,
- die Anforderungen festlegen,
- die Leitfäden beschreiben,
- die sektorspezifische Leitfäden beschreiben.

In der nachfolgenden Grafik wird der Zusammenhang der einzelnen Normen in ISMS-Normenfamilie und deren Beziehungen zueinander verdeutlicht.

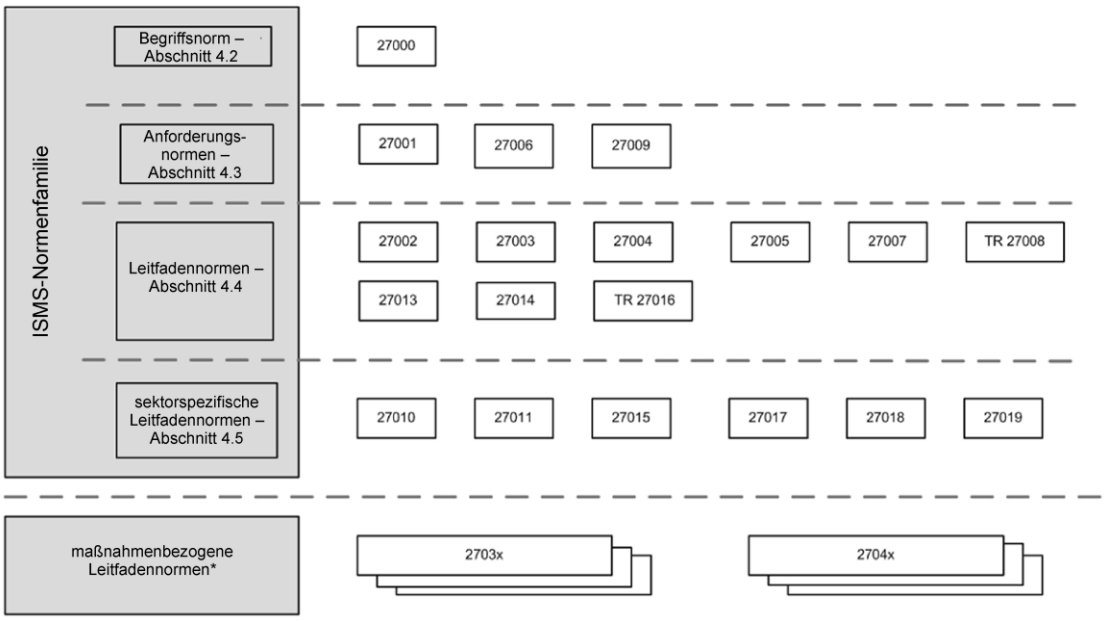

Abbildung 1: ISO/IEC 2700x Normenfamilie [34]

3.2.1.2 ISO 27001: Anforderungen

Einen zentralen Bestandteil der ISMS-Normenfamilie bildet die internationale Norm DIN ISO/IEC 27001:2015, die im Jahr 2005 aus dem zweiten Teil des britischen Standards BS 7799-2 [36] hervorgetreten ist. Dieser Standard wird, neben den Normen DIN ISO 27006 und DIN ISO 27009 in der Gruppe „Normen, die Anforderungen festlegen“ kategorisiert. Somit dient die internationale Norm zur Bestimmung und Definition von Anforderungen einer Institution bezüglich der Umsetzung, Pflege und kontinuierlichen Verbesserung eines Informationssicherheitsmanagementsystems. Ein weiterer Bestandteil dieser Norm sind Anforderungen für die Beurteilung und Behandlung von individuellen Sicherheitsrisiken einer Organisation. Die Einführung eines ISMS als strategische Entscheidung ist als ganzheitlicher Ansatz zu betrachten, indem es einen festen Bestandteil der übergreifenden Steuerungsstruktur darstellt. Somit ist die Informationssicherheit bereits in die Konzeption von Prozessen, Informationssystemen und Maßnahmen integriert. Die Erstellung und Umsetzung eines ISMS orientiert sich nach Einflussfaktoren wie den Organisationszielen-und Bedürfnissen, den Sicherheitsanforderungen und nach Größe und Art der Institution.

Durch die Einführung eines ISMS wird das CIA-Prinzip (Confidentily-Integrity-Availability) gewahrt. Mithilfe dieser Norm können sowohl interne, als auch externe Parteien die Einhaltung der Informationssicherheitsanforderungen einer Organisation beurteilen. Dieser Standard definiert die Anforderungen der Prozesse sehr exakt, wohingegen die Aspekte auf der technischen Ebene nicht konkretisiert werden. Somit bildet diese Norm ein Rahmenwerk, welches die anderen Standards der ISMS-Normenfamilie weiter konkretisieren. Basierend auf diesem Standard können zusätzlich Zertifizierungen nach den Kriterien der ISMS-Normenfamilie erfolgen [37], [38].

Nachfolgend werden die Anforderungen der DIN ISO 27001 um ein ISMS einzuführen, zu etablieren, zu kontrollieren und zu verbessern beschrieben.
Um den internen und externen Kontext einer Organisation festzulegen, müssen sowohl, mit Bezug auf die Informationssicherheit, interessierte Parteien bestimmt, als auch deren Anforderungen festgelegt werden. Dabei sind gesetzliche, regulatorische oder vertragliche Bedingungen zu prüfen.
Des Weiteren müssen die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems bestimmt werden. Der Anwendungsbereich, wie Schnittstellen bzw. Abhängigkeiten von internen bzw. externen Tätigkeiten, muss dokumentiert werden. Die nächste Anforderung betrifft den Punkt Führung und Verpflichtung. Dabei muss durch die oberste Leitung Folgendes sichergestellt werden:

- Bestimmung der Informationssicherheitspolitik und –ziele und deren gleichzeitige Vereinbarung mit der strategischen Organisationsausrichtung
- Integrierung der Informationssicherheitsmanagementanforderungen in die Geschäftsprozesse der Institution
- Bereitstellung von erforderlichen Ressourcen zur Errichtung, Pflege und Verbesserung eines ISMS
- Vermittlung der Wichtigkeit eines ISMS und Erfüllung von dessen Anforderungen
- Erreichung der Ziele des ISMS
- Anleitung und Unterstützung von Personen zur Wirksamkeit eines ISMS
- Förderung einer kontinuierlichen Verbesserung eines ISMS
- Unterstützung relevanter Führungskräfte in Verantwortungsbereichen des ISMS

Desweitern beinhaltet die DIN ISO 27001 die Anforderung zur Festsetzung einer Informationssicherheitspolitik durch die oberste Leitung. Die Informationssicherheitspolitik muss für den Organisationszweck angemessen sein, Informationssicherheitsziele und eine Verpflichtung zur Anforderungserfüllung und zur fortlaufenden Verbesserung des ISMS beinhalten. Sie muss in dokumentierter Form innerhalb der Institution bekannt und für interessierte Parteien zugänglich gemacht werden. Ein weiteres Element ist die Zuweisung und die Bekanntmachung von Verantwortlichkeiten und Befugnissen der Rollen bezüglich der Informationssicherheit durch die oberste Leitung. Durch die Zuweisung der Verantwortlichkeiten muss gewährleistet werden, dass das ISMS die Anforderungen dieser Norm erfüllt. Zusätzlich muss sichergestellt werden, dass über die Leistung des ISMS Bericht erstattet wird. Diese internationale Norm beinhaltet eine weitere entscheidende Anforderung: die Planung**.** Bei der Planung eines ISMS müssen der oben beschriebene Kontext einer Institution, die interessierten Parteien sowie die damit verbundenen Anforderungen beachtet und die Maßnahmen zum Umgang mit Risiken und Chancen definiert, in die Informationssicherheitsprozesse integriert und folglich die Wirksamkeit dieser Maßnahmen bewertet

werden. Zweck dieser Planung sind die Erreichung der gewünschten Ergebnisse des ISMS, die Verhinderung von unerwünschten Auswirkungen und die Erzielung einer kontinuierlichen Verbesserung. Zur Informationssicherheitsbeurteilung muss als erstes ein Prozess definiert werden, der folgendes festlegt:

- Risikokriterien für die Informationssicherheit
    - Risikoakzeptanz
    - Kriterien für die Durchführung der Risikobeurteilung
- Identifikation von Informationssicherheitsrisiken:
    - Prüfung im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit von Information
    - Eruierung der Risikoeigentümer
- Analyse der Informationssicherheitsrisiken
    - Abschätzen der realistischen Eintrittswahrscheinlichkeiten
    - Bestimmung des Risikoniveaus
    - Abschätzen der Folgen nach Eintritt der Risiken
- Bewertung der Risiken
    - Vergleich der Ergebnisse der Risikoanalyse mit festgelegten Kriterien
    - Priorisierung der analysierten Risiken für die Risikobehandlung

Dabei ist zu beachten, dass wiederholte Informationssicherheitsrisikobeurteilungen zu konsistenten, gültigen und vergleichbaren Ergebnissen führen müssen. Eine Beurteilung von Informationssicherheitsrisiken muss kontinuierlich wiederholt werden insbesondere dann, wenn erhebliche Änderungen auftreten. Dieser Prozess muss dokumentiert werden.

Der nachfolgende Prozessschritt ist die Informationssicherheitsrisikobehandlung. Dieser Prozessschritt besteht wiederum aus einzelnen Prozesselementen, die folgendermaßen festgelegt und chronologisch durchgeführt werden müssen.

- Auswahl geeigneter Optionen zur Behandlung der Risiken unter Berücksichtigung der Ergebnisse aus der Risikobewertung
- Festlegung aller Maßnahmen zur Durchführung der ausgewählten Optionen
- Erstellung einer Anwendbarkeitserklärung der erforderlichen Maßnahmen
- Begründete Dokumentation zur Auswahl und zur Nicht-Auswahl von Maßnahmen.
- Formulierung eines Risikobehandlungsplans
- Risikoeigentümer:
    - Einholung einer Genehmigung für den Risikobehandlungsplan
    - Prüfen der Akzeptanz der Informationssicherheitsrisiken

Die Prozesselemente Risikobeurteilung und Risikobehandlung stehen im Einklang mit den Grundsätzen der internationalen Norm ISO 31000 [39]. Basierend hierauf definiert der internationale Standard IEC/ISO 27005 den Prozess des Informationssicherheitsrisikomanagements in Kapitel 3.2.1.4. Ebenfalls besteht bei der Organisation eine dokumentierte Aufbewahrungspflicht über diesen Prozessschritt. Eine weitere wichtige Anforderung dieser internationalen Norm ist die Festlegung von Informationssicherheitszielen. Diese müssen mit der Informationssicherheitspolitik übereinstimmen und Faktoren wie die Informationssicherheitsanforderungen oder Ergebnisse, die Risikobeurteilung

und-behandlung berücksichtigen. Ebenfalls müssen diese Ziele messbar sein und bei Bedarf angepasst werden. Zur Erreichung der Informationssicherheitsziele muss im Vorfeld der Gegenstand (was getan wird), die zur Zielerfüllung erforderlichen Ressourcen, die Verantwortlichkeiten, der Zeitraum und schließlich die Methode zur Bewertung der Ergebnisse festgelegt werden. Um ein ISMS aufzubauen, umzusetzen, zu pflegen und kontinuierlich zu verbessern, muss die Institution sämtliche Ressourcen und Kompetenzen festsetzen und zur Verfügung stellen. Darüber hinaus stellt diese Norm Anforderungen an das Bewusstsein einer Informationssicherheitspolitik und die interne und externe Kommunikation in Bezug auf das ISMS. Alle Prozesse und Informationen in Bezug auf das ISMS müssen in dokumentierter Form vorliegen, situationsabhängig gestaltet und aufbewahrt werden. Eine bedeutsame Anforderung stellt die Leistungsbewertung dar. Diese umfasst die Überwachung, Messung, Analyse und Bewertung des ISMS. So muss die Organisation den Gegenstand der Messung, einschließlich der Informationssicherheitsprozesse und Maßnahmen, die verwendeten Methoden, den Zeitraum der Messung, den Verantwortlichen der Messung und den Zeitraum und Verantwortlichen der Analyse erfassen. Um eine vollständige Bewertung der Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems durchführen zu können, sind interne Audits und Managementbewertungen erforderlich. In regelmäßigen Abständen müssen interne Audits durchgeführt werden, um zu prüfen, ob die Anforderungen dieser Norm und der Organisation an ihr ISMS verwirklicht und umgesetzt werden. Dabei sind festgelegte Anforderungen an ein internes Audit zu beachten. Daneben muss das ISMS durch die oberste Leitung in regelmäßigen Abständen bewertet werden, um die Wirksamkeit des ISMS sicherzustellen und auf vorkommende Veränderungen situationsabhängig reagieren zu können. Inhalt dieser Bewertungen müssen Entscheidungsmöglichkeiten zur kontinuierlichen Verbesserung oder Änderungen des ISMS sein. Die gesamte Leistungsbewertung muss auch hier in dokumentierter Form aufbewahrt werden. Die letzte Anforderung dieser internationalen Norm betrifft die kontinuierliche Verbesserung. Die Organisation muss zum einen Nichtkonformitäten beheben und entsprechende Maßnahmen einleiten und zum anderen die Wirksamkeit, die Eignung und die Angemessenheit des ISMS kontinuierlich verbessern. Im Anhang A dieser Norm befinden sich Maßnahmen und Maßnahmenziele, die in der ISO/IEC 27002, Abschnitte 5 bis 18 auftreten. Diese sind direkt abgeleitet und müssen im Kontext der Informationssicherheitsrisikobehandlung angewendet werden. Allerdings sind diese Maßnahmen nicht abschließend und müssen situationsabhängig erweitert werden [9].

3.2.1.3 ISO/IEC 27002: Leitfaden

Die internationale Norm DIN ISO/IEC 27002:2016-11, die auf dem Britischen Standard BS 7799-1 basiert, wird in der ISMS-Normenfamilie als „Norm, die Leitlinien beschreiben“ kategorisiert. Zweck dieses Standards ist, Informationssicherheit als gesamtorientierten Ansatz zu betrachten, indem alle Bereiche einer Organisation, die an der Erhebung, Speicherung, Verarbeitung und Löschung beteiligt sind, in den Prozess der Informationssicherheit integriert werden. Diese Norm beinhaltet Leitlinien, allgemeine Managementgrundsätze von Informationssicherheit und Prinzipien zur Erstellung, Umsetzung, Aufrechterhaltung und Verbesserung eines ISMS. Ziel dieser Norm ist, die darin beschriebenen Maßnahmen und Maßnahmenziele umzusetzen, um die im Rahmen einer Risikoanalyse identifizierten Anforderungen zu realisieren.

Daneben soll dieser Standard als Ausgangspunkt dienen, um organisationsindividuelle und -spezifische Sicherheitsstandards zu erschaffen. Allerdings ist das Messen der Informationssicherheit außerhalb des Geltungsbereichs dieses Standards.
Diese Norm umfasst 14 Abschnitte mit Sicherheitsmaßnahmen, gegliedert in 35 Hauptsicherheitskategorien und 114 einzelnen Maßnahmen. Die Reihenfolge der Abschnitte ist unabhängig von ihrer Wichtigkeit. Jede Hauptmaßnahmenkategorie setzt sich zusammen aus einem Maßnahmenziel und einer oder mehreren Maßnahmen, die beschreiben wie das Maßnahmenziel erreicht werden sollen, zusammen.
Die Maßnahmen sind in drei Bereiche unterteilt. Als erstes wird darin die spezifische Maßnahme definiert und beschrieben wie das Maßnahmenziel erreicht werden kann. Als zweites wird eine detaillierte Anleitung zur Umsetzung der Maßnahmen beschrieben. Abschließend enthält die Maßnahme zusätzliche Informationen über rechtliche Aspekte oder andere tangierte Normen.
Diese internationale Norm lässt sich in folgende Schritte strukturieren:

- Identifikation und Festsetzung von Sicherheitsanforderungen
- Einschätzung von Sicherheitsrisiken
- Auswahl geeigneter Maßnahmen
- Entwicklung eigener Leitfäden

Dieser Forschungsbericht geht in Kapitel vier näher auf die Methode zur Einführung, Etablierung, Aufrechterhaltung und Verbesserung ISMS ein.
Die Auswahl der geeigneten Maßnahmen ist abhängig von den Informationssicherheitsanforderungen, der Risikoakzeptanzkriterien, Risikobehebungsmöglichkeiten und der allgemeinen Einstellung der obersten Leitung bezüglich des Risikomanagements.
Relevante internationale und nationale Gesetze bzw. Vorschriften und das Interagieren der Maßnahmen sind weitere Einflussfaktoren auf die Auswahl der Maßnahmen. Die meisten Maßnahmen können als Richtlinie für das ISMS, aber auch als Ausgangslage betrachtet werden, um neue auf die Organisation spezifische, situationsabhängige Maßnahmen zu entwickeln.
Diese Norm beschreibt folgende Maßnahmen bzw. Maßnahmenziele, die als Ausgangspunkt zur Erstellung, Umsetzung, Aufrechterhaltung und Verbesserung eines ISMS dienen.

- Informationssicherheitsrichtlinien
    - Vorgaben der Leitung für Informationssicherheit
- Organisation der Informationssicherheit
    - Interne Organisation
    - Mobilgeräte und Telearbeit
- Personalsicherheit
    - Vor der Beschäftigung
    - Während der Beschäftigung
    - Beendigung und Änderung der Beschäftigung
- Verwaltung der Werte
    - Verantwortlichkeit für Werte
    - Informationsklassifizierung
    - Handhabung von Datenträgern

- Zugangssteuerung
    - Geschäftsanforderungen an die Zugangssteuerung
    - Benutzerzugangsverwaltung
    - Benutzerverantwortlichkeiten
    - Zugangssteuerung für Systeme und Anwendungen
- Kryptographie
    - Kryptographische Maßnahmen
- Physische und umgebungsbezogene Sicherheit
    - Sicherheitsbereiche
    - Geräte und Betriebsmittel

- Betriebssicherheit
    - Betriebsabläufe und -verantwortlichkeiten
    - Schutz vor Schadsoftware
    - Datensicherung
    - Protokollierung und Überwachung
    - Steuerung von Software im Betrieb
    - Handhabung technischer Schwachstellen
    - Audits von Informationssystemen
- Kommunikationssicherheit
    - Netzwerksicherheitsmanagement
    - Informationsübertragung
- Anschaffung, Entwicklung und Instandhaltung von Systemen
    - Sicherheitsanforderungen an Informationssysteme
    - Sicherheit in Entwicklungs- und Unterstützungsprozessen
    - Testdaten
- Lieferantenbeziehungen
    - Informationssicherheit in Lieferantenbeziehungen
    - Steuerung der Dienstleistungserbringung von Lieferanten
- Handhabung von Informationssicherheitsvorfällen
    - Handhabung von Informationssicherheitsvorfällen und -verbesserungen
- Informationssicherheitsaspekte beim Business Continuity Management
    - Aufrechterhalten der Informationssicherheit
    - Redundanzen
- Compliance
    - Einhaltung gesetzlicher und vertraglicher Anforderungen
    - Überprüfungen der Informationssicherheit [40]

Allerdings ist zu beachten, dass diese Maßnahmen und Maßnahmenziele nicht abschließend sind und bei Bedarf situationsabhängig erweitert werden müssen. In Bezug auf die Erstellung eines Informationssicherheitskonzeptes an bayerischen Hochschulen und Universitäten muss geprüft werden, welche Sicherheitskategorien bzw. welche Maßnahmen in diesem Kontext sinnvoll erscheinen.

3.2.1.4 ISO/IEC 27005: Risikomanagement

Die internationale Norm ISO/IEC 27005:2011(E) wird innerhalb der Normenfamilie zu Normen, „die Leitlinien beschreiben“ gruppiert, da diese Norm Leitlinien für ein systematisches und prozessorientiertes Informationssicherheitsrisikomanagement enthält. Dieser internationale Standard basiert auf dem ISO/IEC TR 13335 [41] und unterstützt die Anforderungen aus der DIN ISO 27001 und setzt die Leitlinien aus der DIN ISO 27002 voraus. Die Norm ISO/IEC 27005 gibt keine spezifischen Methoden vor, sondern dient als Ausgangspunkt zur Erstellung eines Risikomanagements für die Informationssicherheit. Es ist Aufgabe der Organisation das Vorgehen für ein Risikomanagement zu definieren, abhängig beispielsweise von der Art des Industriesektors, der Größe der Organisation oder auch der allgemeinen Organisationshaltung gegenüber dem Risikomanagement. Dieser internationale Standard gibt als Rahmenwerk verschiedene Methoden vor, um ein organisationsspezifisches Risikomanagement zu gestalten. Um Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten, zu behandeln und zu überwachen beschreibt dieser internationale Standard den nachfolgenden Prozess des Risikomanagements.

- Definition der Rahmenbedingungen (Context establishment)
- Risikobeurteilung (Risk assessment)
    - Identifizierung von Risiken (Risk identification)
    - Abschätzung von Risiken (Risk estimation)
    - Auswertung von Risiken (Risk evaluation)
- Risikobehandlung (Risk treatment)
- Risikoakzeptanz (Risk acceptance)
- Risikokommunikation (Risk communication)
- Risikoüberwachung und Verbesserung (Risk monitoring and review)

Dieser Prozess muss iterativ durchgeführt werden, um auf Veränderungen zeitnah reagieren zu können. Dabei kann dieser systematische Prozess die ganze Organisation, einen Teilbereich davon oder lediglich eine Systemkomponente betreffen. Eine Risikoanalyse kann im Vorfeld vorgenommen werden, bevor eine Entscheidung über die Art und den Zeitpunkt der Maßnahmen getroffen wird. Nachfolgend werden die einzelnen Schritte des Informationssicherheitsrisikomanagementprozesses näher beschrieben.

- Rahmenbedingungen definieren

Zu Beginn eines Informationssicherheitsrisikomanagementprozesses müssen die Rahmenbedingungen eruiert werden. Dabei ist der externe und interne Kontext einer Organisation, welcher die Definition der grundlegenden Kriterien für ein Informationssicherheitsrisikomanagement, den Anwendungsbereich mit dessen Grenzen und die Etablierung einer wirksamen Risikomanagementorganisation beinhaltet, festzulegen. Es ist von großer Bedeutung den Zweck des Informationssicherheitsrisikomanagements und dessen Auswirkungen auf den Gesamtprozess zu ermitteln. Die Unterstützung eines ISMS, die gesetzesmäßige Compliance und dessen Beweis der Sorgfaltspflicht, die Vorbereitung eines Geschäftsablaufplans oder eines incident response Plans oder die Beschreibung der Informationssicherheitsanforderungen eines Produkts, einer Dienstleistung oder eines Mechanismus können beispielsweise darunterfallen. Eine adäquate Risikomanagementvorgehensweise beinhaltet grundlegende Kriterien, wie Risikoakzeptanzkriterien,

Risikobewertungskriterien und Auswirkungskriterien. Die Kriterien zur Risikobewertung sollten den strategischen Wert des Geschäftsinformationsprozesses, die Kritikalität der Informationswerte, die gesetzlichen, regulatorischen und vertraglichen Verpflichtungen, die Wichtigkeit von Verfügbarkeit, Vertraulichkeit und Integrität, die Erwartungen und Sichtweisen der Geschäftspartner und die negativen Konsequenzen einer Reputationsschädigung enthalten. Daneben können Risikobewertungskriterien zur Spezifikation von Prioritäten für die Risikobehandlung verwendet werden. Die Auswirkungskriterien sollten das Ausmaß des Schadens oder der Kosten, die durch ein Informationssicherheitsvorfall verursacht wurden, spezifizieren. Dabei ist das Klassifikationslevel der betroffenen Informationswerte, die Informationssicherheitsbrüche unter Verlust von Verfügbarkeit, Vertraulichkeit und Integrität, beeinträchtigte Arbeitsabläufe, Verlust des Geschäfts-und Finanzwertes, Unterbrechung von Zeitplänen und Deadlines oder die Rufschädigung zu berücksichtigen.

Die Kriterien der Risikoakzeptanz sind oftmals abhängig von Richtlinien der Organisation, deren Zielen und Grundsätzen und den Interessen der Stakeholder. Eine Organisation sollte ihren eigenen Rahmen zur Risikoakzeptanz unter Berücksichtigung von Geschäftskriterien, gesetzlichen und regulatorischen Aspekten, betriebswirtschaftlichen, technischen, sozialen und menschlichen Faktoren, definieren. Die Risikoakzeptanzkriterien sind abhängig von der Dauer eines vorhandenen Risikos und können zusätzlich zukünftige Anforderungen zur Risikobehandlung enthalten. Daneben sollte der Anwendungsbereich des Informationssicherheitsrisikomanagements und dessen Grenzen festgelegt werden, um sicherzustellen, dass alle relevanten Vermögenswerte im Gesamtprozess des Informationssicherheitsrisikomanagements in Betracht gezogen werden. Zusätzlich sind dessen Grenzen zu definieren, da Risiken durch die Definition der Grenzen entstehen können. Bei der Bestimmung des Anwendungsbereichs und dessen Grenzen sollten die Strategie und das Leitbild der Organisation, ihre Geschäftsbereiche, der Geschäftsprozess, die Funktion und Struktur der Organisation, die gesetzlichen, regulatorischen und vertraglichen Anforderungen, die Informationssicherheitsleitlinie, die Informationswerte, die geografische Standort der Organisation, Erwartungen der Stakeholder, das soziokulturelle Umfeld und sämtliche Schnittstellen in Betracht gezogen werden. Außerdem ist eine Nichteinbeziehung in den Anwendungsbereich schriftlich zu begründen. Der Anwendungsbereich eines Informationssicherheitsrisikomanagements kann beispielsweise eine IT-Anwendung, eine IT-Infrastruktur, ein Geschäftsprozess oder ein festgelegter Teil der Organisation sein. Die Einführung, der konzeptionelle Aufbau und die Instandhaltung eines Informationssicherheitsrisikomanagementprozesses mit dessen zugehörigen Verantwortlichkeiten ist ein weiterer Bestandteil der Rahmenbedingungen. So muss ein für die Organisation ein adäquater Informationssicherheitsrisikomanagementprozess entwickelt werden, die Stakeholder identifiziert und analysiert werden, die Rollen und Verantwortlichkeiten aller internen und externen Parteien definiert, sämtliche internen und externen Schnittstellen analysiert und ein Entscheidungseskalationsweg entwickelt werden. Die Festsetzung der Rahmenbedingungen sollte unter Zustimmung der relevanten Managementebene erfolgen.

- Risikobeurteilung

Nachdem die Rahmenbedingungen mit den Basiskriterien definiert wurden, kann als nächster Schritt die Risikobeurteilung durchgeführt werden. Eine wirksame Risikobeurteilung beinhaltet die Teilbereiche Identifizierung von Risiken (Risk identification), Risikoanalyse (Risk analysis) mit Risikoabschätzung (Risk estimation) und die Auswertung von Risiken (Risk evaluation). Da ein Risiko, wie in der ISO/IEC 27000 beschrieben, aus der Kombination der Wahrscheinlichkeit der Erscheinung

eines unerwarteten Ereignisses und deren Konsequenzen verursacht wird, quantifiziert oder qualifiziert eine Risikobeurteilung das Risiko und ermöglicht eine Priorisierung der Risiken entsprechend ihrer Ernsthaftigkeit. Mit Hilfe einer Risikobeurteilung ist es möglich den Geschäftswert der Informationswerte zu ermitteln, die maßgeblichen existenten oder möglichen Bedrohungen und Schwachstellen zu identifizieren, die bereits existierenden Gegenmaßnahmen und deren Wirkung auf die vorhandenen Risiken zu analysieren und zu beurteilen, die potentiellen Konsequenzen zu ermitteln und letztendlich die abgeleiteten Risiken zu priorisieren und sie anhand den Beurteilungskriterien zu klassifizieren. Eine Risikobeurteilung wird meist in zwei oder mehr iterativen Durchläufe durchgeführt, um aussagekräftige Ergebnisse zu erzielen. Bei der ersten Iteration wird die Beurteilung auf höchster Ebene durchgeführt, um potentiell hochrangige Risiken zu identifizieren, die die nächste Iteration rechtfertigen. Die nachfolgende Iteration erlaubt eine detaillierte Betrachtung der ermittelten Risiken. Falls dieser Durchlauf unzureichende Informationen ergibt, um eine aussagekräftige Risikobeurteilung durchzuführen, muss eine tiefgreifendere Analyse gegebenenfalls mit einer anderen Methode, in Bezug auf den gesamten Rahmen vorgenommen werden.

Basierend auf den Grundsätzen und Zielen der Risikobeurteilung, ist es Aufgabe der Organisation die individuell geeignete Vorgehensweise der Risikobeurteilung zu selektieren.

- Identifizierung von Risiken

Der Zweck der Identifizierung von Risiken ist, festzustellen auf welche Art und Weise ein potentieller Schaden entstanden sein könnte. Es sollten auch Risiken erfasst werden, unabhängig davon ob deren Ursprung der Organisation untersteht oder nicht. Um die Risiken vollständig identifizieren zu können, müssen sowohl Werte definiert, Bedrohungen und Schwachstellen ermittelt, bereits bestehende Gegenmaßnahmen bestimmt und die Konsequenzen festgestellt werden. Bei der Ermittlung von Vermögenswerten sollte alles in Betracht gezogen werden, was von Bedeutung für die Organisation ist. Vermögenswerte werden gemäß Anhang B dieser Norm in zwei Teilbereiche untergliedert. Der eine umfasst die primären Vermögenswerte wie Geschäftsprozesse mit deren Aktivitäten und Informationen und der andere Teil die unterstützenden Vermögenswerte wie Hardware, Software, Netzwerke, die gesamte Belegschaft mit ihren Fähigkeiten, der Standort und die Organisationsstruktur. Der Detailierungsgrad der Werteidentifikation sollte so hoch sein, dass ausreichend verwertbare Informationen für die Risikobeurteilung hervortreten. Der Detailierungsgrad bestimmt den gesamten Umfang der Risikobeurteilung. Es sollte der Verantwortliche jedes Vermögenswertes bestimmt werden, da dieser die Vermögenswerte in geeigneter Weise bewerten kann. Um Risiken vollständig identifizieren und analysieren zu können, müssen die Bedrohungen ermittelt werden. Dabei ist zu beachten, dass Bedrohungen sowohl natürlichen oder menschlichen Ursprungs, zufällig oder vorsätzlich entstanden sein und innerhalb oder außerhalb der Organisation auftreten können. Allgemein betrachtet, sollten Bedrohungen immer generisch, entsprechend ihres Typs und ihrer Quelle identifiziert und kategorisiert werden, um keine (unerwarteten) Bedrohungen zu übersehen und die Suche danach zu limitieren. Dabei ist zu beachten, dass eine Bedrohung mehrere Vermögenswerte betreffen kann und somit die Auswirkungen unterschiedlich ausfallen können, abhängig davon welcher Vermögenswert tangiert wurde. Informationsträger der Identifizierung der Vermögenswerte oder der Wahrscheinlichkeitsbeurteilung können die Verantwortlichen der Vermögenswerte, wie beispielsweise die Personalabteilung, Mitarbeiter des Facility Managements, Versicherungsgesellschaften oder sonstige Behörden sein. Daneben sollten Erfahrungen aus früheren Vorfällen oder aus vorangegangenen Risikobeurteilungen sinngemäß in die aktuelle Risikobeurteilung mit aufgenommen werden.

Jedoch ist bei der Benutzung von standardisierten Bedrohungskatalogen oder bei der Verwendung der Ergebnisse alter Risikobeurteilungen zu beachten, dass sich die Bedrohungen kontinuierlich verändern, insbesondere, wenn sich die äußeren Umstände der Organisation ändern. Die nachfolgende Tabelle verschafft einen Überblick über eine detaillierte Klassifizierung von Bedrohungen, die während der Bedrohungsanalyse verwendet werden kann. Die Bedrohungen werden anhand ihres Typs, ihres Ursprungs und ihrer Art und Weise eingeteilt. Bedrohungen können vorsätzlich (D), zufällig (A) oder natürlich, umweltbedingt oder nicht menschlich bedingt (E) sein. Unabhängig von ihrer Wichtigkeit werden sie in der nachfolgenden Tabelle aufgelistet.

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D

Type	Threats	Origin
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D
	Software malfunction	A
	Breach of information system maintainability	A, D
Unauthorised actions	Unauthorised use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E

Abbildung 2: Klassifizierung von Bedrohungen [42]

Besonderes Augenmerk sollte auf die anschließende Tabelle gelegt werden, in der Bedrohungen vorsätzlich durch den Menschen verursacht werden. Die Bedrohungen werden anhand ihres Ursprungs, der Motivation des Täters und der möglichen Konsequenzen eingeteilt.

Origin of threat	Motivation	Possible consequences
Hacker, cracker	Challenge Ego Rebellion Status Money	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g. cyber stalking) • Fraudulent act (e.g. replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge Political Gain Media Coverage	• Bomb/Terrorism • Information warfare • System attack (e.g. distributed denial of service) • System penetration • System tampering

Origin of threat	Motivation	Possible consequences
Industrial espionage (Intelligence, companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Defence advantage • Political advantage • Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g. virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Abbildung 3: Klassifizierung der menschlichen Bedrohungen [42]

Nachdem dieser Teilschritt durchgeführt wurde, sollte eine Liste möglicher Bedrohungen, entsprechend ihres Typs und Quelle kategorisiert, vorliegen. Anschließend werden die bereits vorhandenen Sicherheitsmaßnahmen identifiziert und deren Wirksamkeit überprüft, um Kosten und Ressourcen zu sparen. Falls eine bereits vorhandene Kontrollmaßnahme nicht korrekt ist, können dadurch Schwachstellen entstehen. Gemäß den Anforderungen aus der ISO/IEC 27001, wird der Effektivitätsgrad der Kontrollmaßnahme an dem Reduktionsgrad der Auftrittswahrscheinlichkeit einer Bedrohung, oder an dem Maß, wie das Ausnutzen der Schwachstelle verringert oder die Auswirkungen des Vorfalls reduziert werden kann, gemessen. Daneben können Audit Berichte Auskünfte über die Effektivität der bereits vorhandenen Gegenmaßnahmen erteilen. Bei einer bereits bestehenden uneffektiven Maßnahme muss geprüft werden, ob diese ersetzt oder verbessert oder gar aus Kostengründen erhalten wird und demensprechend begründet werden.

Als nächster Teilprozessschritt in der Risikoidentifizierung werden mögliche Schwachstellen identifiziert. Gemäß der ISO/IEC 27001 können Schwachstellen, die durch Bedrohungen ausgenutzt werden, Schaden an den Vermögenswerten der Organisation oder der Organisation selbst verursachen. Schwachstellen können im gesamten Organisationsprozess vorhanden sein. Sowohl in

den Bereichen der Geschäftsprozesse, der Managementebene, der Personalabteilung, der physischen Umgebung, oder in der Organisationsstruktur, als auch in der Konfiguration eines Informationssystems, im Hard-und Softwarebereich, oder durch die Abhängigkeit von externen Drittparteien können Schwachstellen auftreten. Da das bloße Existieren einer Schwachstelle ohne korrespondierende Bedrohung noch keinen Schaden verursacht, somit nicht als Risiko verstanden wird, muss schließlich dafür auch keine Gegenmaßnahme entwickelt werden. Allerdings sollte diese Schwachstelle unter Beobachtung stehen, da durch Veränderungen eine korrespondierende Bedrohung entstehen und ausgenutzt werden kann und somit ein Risiko darstellt. In diesem Falle ist eine wirksame Gegenmaßnahme zu ergreifen. Es ist zu beachten, dass eine nicht korrekt implementierte, eine falsch funktionierende Sicherheitsmaßnahme oder die nicht ordnungsgemäße Benutzung dieser Gegenmaßnahme selbst eine Schwachstelle sein kann. In einer weiteren Tabelle [42] werden Beispiele für Schwachstellen, die anhand verschiedener Bereiche kategorisiert werden, mit den dazugehörigen möglichen Bedrohungen aufgezeigt. Wie die Übersicht verdeutlicht, können in den Bereichen Hardware, Software, Netzwerk, Personalbereich, Standort und Organisationsstruktur Schwachstellen vorhanden sein und durch passende Bedrohungen ausgenutzt werden. Diese Tabelle kann als Ausgangspunkt für eine wirksame Schwachstellen-und Bedrohungsanalyse verwendet werden. Allerdings ist zu betonen, dass die Aufzählung der Schwachstellen und Bedrohungen nicht abschließend ist und die Tabelle situationsangepasst verwendet werden muss. Nachdem dieser Teilschritt durchgeführt wurde, sollte als Ergebnis sowohl eine Liste mit Schwachstellen mit Bezug auf die Vermögenswerte einer Organisation, die Bedrohungen und die vorhandenen Kontrollmaßnahmen, als auch eine Liste mit Schwachstellen ohne korrespondierenden Bedrohungen, existieren. Der nächste Teilschritt im Prozess der Risikoidentifizierung betrifft die Identifizierung der Konsequenzen, die einen Verlust an Vertraulichkeit, Integrität und Verfügbarkeit der Werte verursachen. Diese Maßnahme identifiziert die Auswirkungen eines Vorfallszenarios, mit Hilfe der Auswirkungskriterien, die in der Definition der Rahmenbedingungen gesetzt wurden. Die Auswirkungen können einen Vermögenswert, einen Teil davon, oder mehrere Vermögenswerte betreffen. Aus diesem Grund sollte den Vermögenswerten sowohl ein finanzieller Wert als auch ein Geschäftswert zu geordnet werden. Auswirkungen können von kurzer oder im Falle einer Zerstörung von permanenter Dauer sein. Die Klassifizierung der Auswirkungen sollten unter folgenden Gesichtspunkten durchgeführt werden.

- Entdeckungs-und Wiederherstellungszeit,
- Verlust der Arbeitszeit,
- Verlust von Chancen,
- Gesundheit und Sicherheit,
- finanzielle Kosten in Bezug auf Fachkenntnisse zur Schadensbehebung
- und Ruf-und Ansehensschädigung.

Als Ergebnis sollte nach Vollendung dieses Teilschrittes eine strukturierte Liste mit Vorfallszenarien, den betroffenen Werten und den damit verursachten Konsequenzen vorhanden sein.

- Risikoanalyse

Nachdem der vorherige Prozessschritt der Risikoidentifikation im Risikomanagementprozess vollendet wurde, wird die Risikoanalyse mit ihren Teilbereichen Bewertung der Auswirkung und der Wahrscheinlichkeit, sowie einer Risikoabschätzung durchgeführt. Dazu wird als erstes eine geeignete Methode zur Durchführung der Risikoanalyse gewählt. Der Detaillierungsgrad einer Risikoanalyse kann sehr unterschiedlich sein, abhängig von der Kritikalität der Vermögenswerte, dem Ausmaß der bekannten Schwachstellen oder der Anzahl früherer Vorfälle. Die Risikoanalyse kann

situationsabhängig mit Hilfe von qualitativen, quantitativen Methoden oder eine Kombination aus beider erfolgen. Oftmals wird anfangs eine qualitative Methode verwendet, um die allgemeine Indikation der Risikostufen herauszufinden und die Hauptrisiken zu ermitteln. Um die Hauptrisiken weiter zu untersuchen wird danach eine quantitative Methode angewendet. Quantitative Methoden sind oftmals kostspieliger und komplexer als qualitative Methoden. Die Gestaltung der Analyse sollte mit den Risikobeurteilungskriterien, die in der Definition der Rahmenbedingungen bestimmt worden sind, übereinstimmen.

Qualitative Risikomethoden verwenden einen Rahmen mit qualifizierenden Attributen (z.B. gering, mittel, hoch), um das Ausmaß potentieller Auswirkungen und deren Auftrittswahrscheinlichkeit zu beschreiben. Abhängig von den gegebenen Umständen kann der Rahmen der qualitativen Methode beliebig angepasst oder erweitert werden. Vorteilhaft an der Verwendung einer qualitativen Methode zur Risikoanalyse ist, die einfache und verständliche Lesbarkeit der Ergebnisse. Wohingegen die Abhängigkeit der subjektiven Rahmenauswahl als Nachteil betrachtet werden kann.

In quantitative Risikoanalysemethoden wird der Rahmen mit nummerischen Werten aus einer großen Anzahl an Quellen versehen. Die Qualität dieser Methode ist abhängig von der Zielgenauigkeit, der Fehlerfreiheit, der Vollständigkeit der nummerischen Werten und der Validität der verwendeten Modelle. Meist werden bei quantitativen Methoden historische Daten aus vorausgegangenen Vorfällen verwendet. Dies bringt den Vorteil mit sich, dass die Schutzziele und die Sorgen der Organisation direkt daraus abgeleitet werden können. Nachteilig ist dabei allerdings das Fehlen von Daten neuer Risiken oder neuer Schwachstellen. Die Art und Weise, wie die Auswirkungen und die Wahrscheinlichkeit dargestellt werden, um das Risikomaß auszudrücken, variiert sehr stark und ist von der Art des Risikos und des Zwecks des Beurteilungsergebnisses abhängig. Die Schwankungen und die Unsicherheit der Auswirkung-und Wahrscheinlichkeitsbetrachtung muss bei der Betrachtung der Analyse beachtet und dementsprechend kommuniziert werden. Ein Nachteil ergibt sich bei der quantitativen Risikoanalysemethode, wenn sachlich prüfbare Daten nicht vorhanden sind. Um eine aussagekräftige Risikoanalyse durchführen zu können, müssen die Auswirkungen beurteilt werden. Als erstes wird den identifizierten Werten der Organisation ein monetärer Wert zugeordnet, indem die Werte gemäß ihrer Kritikalität und ihrer Wichtigkeit klassifiziert werden. Die Wertebestimmung kann durch zwei verschiedene Maßnahmen erfolgen. Zum einen durch die Kostenbestimmung des Ersatzwertes bei Wiederherstellung des Wertes und zum anderen durch die Bestimmung der Kosten, die durch die Auswirkungen auf den Betriebsablauf im Falle des Verlustes oder der Gefährdung der Werte entstehen. Darunter fallen beispielsweise regulatorische oder gesetzliche Konsequenzen, die durch die Enthüllung, Modifikation, Nicht-Verfügbarkeit oder durch die Zerstörung von Informationen oder anderen Vermögenswerten entstehen. In den meisten Fällen ist der Wert, der durch die Auswirkungen auf den Geschäftsablauf entsteht höher, als der einfache Ersatzwert. Die Vermögensbewertung ist ein Schlüsselfaktor in der Beurteilung der Auswirkungen im Vorfallszenariums, da meist mehr als ein Vermögenswert betroffen ist. Unterschiedliche Schwachstellen und Bedrohungen haben unterschiedliche Auswirkungen auf die Werte, wie beispielsweise Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit. Die Konsequenzen können mit monetäre, technische oder menschliche Auswirkungskriterien dargestellt werden. In einigen Fällen kann es erforderlich sein, die Konsequenzen für unterschiedliche Gruppierungen, Zeiträume oder Situationen mit mehr als einem Wert auszudrücken, um eine aussagekräftige Basis zur Entscheidungsfindung hervorzubringen. In der ersten Iteration der Auswirkungsbeurteilung wird meist der einfache Ersatzwert bestimmt, wohingegen in der nächsten Iteration der unmittelbare Schadenswert ermittelt wird, der durch die Auswirkungen eines Vorfallszenarios entstanden ist. Als

Ergebnis dieses Teilschrittes sollte eine Liste mit bewerteten Konsequenzen eines Vorfallszenariums, die mit Werten und Auswirkungskriterien wiedergespiegelt sind, vorhanden sein.

Ein weiterer Bestandteil der Risikoanalyse stellt die Bewertung der Wahrscheinlichkeit eines Vorfalls dar. Nachdem die Störfallszenarien erkannt wurden, ist es notwendig unter Verwendung von qualitativen oder quantitativen Analysemethoden, die Auftrittswahrscheinlichkeit jedes einzelnen Szenariums zu ermitteln. Abhängig von der Auftrittshäufigkeit der Bedrohungen und wie einfach die Schwachstellen auszunützen sind, sollte bei der Wahrscheinlichkeitsbewertung folgende Gesichtspunkte berücksichtigt werden:

- Erfahrungswerte und geeignete Statistiken für die Wahrscheinlichkeit einer Bedrohung
- Vorsätzliche Gefahrenquellen:
    - Motivation des Täters
    - Fähigkeit des Täters
    - Verfügbare Ressourcen des Täters
    - Wahrgenommenen Attraktivität der betroffenen Vermögenswerte
- Zufällige, unbeabsichtigte Gefahrenquellen:
    - Geografischer Standort
    - Extreme Wetterbedingungen
    - Andere Faktoren, die menschliches Verschulden verursachen können
- Einzelne oder gehäufte Schwachstellen
- Effektivität bestehender Gegenmaßnahmen

Es ist zu beachten, dass sich vorsätzliche und unbeabsichtigte Gefahrenquellen kontinuierlich verändern können. Nachdem die Wahrscheinlichkeitsbewertung durchgeführt wurde, sollte eine Aufstellung von Störfallszenarien mit dessen Auftrittswahrscheinlichkeit vorhanden sein.

Schließlich muss das Risikoniveau in einer aussagekräftigen Risikoanalyse bestimmt werden. Dazu wird der Wahrscheinlichkeitswert mit dem Wert der Konsequenzen kombiniert. Zusätzlich können bei der Bestimmung des Risikoniveaus weitere Variablen wie beispielsweise Kosten oder Besorgnisse der Interessengruppen eingesetzt werden. Zur Risikoniveaubestimmung existieren unterschiedliche Methoden.

- verschiedenen Methoden zur Risikobewertung

Im Folgenden erläutert dieser Forschungsbericht unterschiedliche Analysemethoden zur Bewertung des Informationssicherheitsrisikos, stellt die Vor-und Nachteile gegenüber und analysiert unterschiedliche Bewertungsmatrizen. Zur Bewertung des Informationssicherheitsrisikos existiert die „High-level information security risk assessment“ Methode und die „Detailed information security risk assessment“ Methode.

- High-level information security risk assessment

Die „High-Level“ Risikobewertungsmethode wird oftmals zu Beginn eines Risikoassessments verwendet, um einen Überblick über die vorhandenen Risiken zu erhalten. Falls eine gleichzeitige Implementierung aller Sicherheitsmaßnahmen aus Kostengründen nicht möglich ist und somit nur die als kritisch eingestuften Risiken adressiert werden, wird diese Methode zur Risikobewertung herangezogen. Die High-Level“ Risikobewertungsmethode adressiert die globale Perspektive der

Organisation, in der die technischen Gesichtspunkte unabhängig von den Geschäftsprozessen betrachtet werden. Daneben wird eine limitierte Liste von Bedrohung und Schwachstellen, die bereits domänspezifisch gruppiert wurde, analysiert, um den Prozess zu beschleunigen. Der Fokus wird bei dieser Betrachtungsweise auf das gesamte Risikoszenarium gelegt, anstatt auf die einzelnen Elemente. Da in dieser Vorgehensweise die Maßnahmen priorisiert, und organisatorische, nicht-technische bzw. die Management Aspekte der technischen Sicherheitsmaßnahmen fokussiert werden, ist eine verständliche Darstellung der Risikosituation möglich. Vorteilhaft an dieser Methode ist, die direkte Schutzbedarfsfeststellung und die priorisierte Adressierung der Ressourcen zur Durchführung von Sicherheitsmaßnahmen. Aufgrund der Betrachtung der Risiken auf hohem Level, kann es erforderlich sein, eine zweite detaillierte Risikobewertungsiteration durchzuführen, um ein aussagekräftiges Ergebnis zu erhalten. Falls der Mangel an Informationssicherheit verheerende Folgen für die Organisation, für ihre Geschäftsprozesse oder für die Vermögenswerte verursacht, ist eine zweite detaillierte Iteration der Risikobewertung erforderlich, um potentielle Risiken zu identifizieren.

- Detailed information security risk assessment

Die „Detailed“ Risikobewertungsmethode beinhaltet eine detaillierte Identifikation und Bestimmung der Vermögenswerte, deren Bedrohungs- und Schwachstellenbewertung. Die Konsequenzen werden mit Hilfe von quantitativen, qualitativen Analysemethoden oder einer Kombination aus beiden bewertet. Die Auftrittswahrscheinlichkeit ist abhängig von der Attraktivität des betroffenen Wertes, der Ausnutzschwierigkeit einer Schwachstelle, den Fähigkeiten des Täters und der Anfälligkeit der Schwachstelle. Da diese Methode sehr zeitaufwendig ist und ein hohes Maß an Arbeitsaufwand und Fachwissen voraussetzt, wird sie meist bei hochrisikobehafteten Informationssystemen verwendet. Oftmals werden bei dieser Art von Bewertungsmethode subjektive und empirische Maßnahmen angewendet und die Ergebnisse tabellarisch dargestellt. Es ist zu beachten, dass jede Organisation die für sie individuell geeignetste Maßnahme verwenden soll, die vertrauenswürdige und reproduzierbare Ergebnisse liefert. Im Nachfolgenden werden Beispiele für tabellenbezogene Methoden gegeben.

- Matrix mit vordefinierten Werten

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

Abbildung 4: Risikobewertungsmatrix mit vordefinierten Werten [42]

Bei dieser Art von Risikobewertungsmethode wird der Wert jedes Vermögensgegenstandes in Bezug auf die dazugehörigen Ersatz- bzw. Rekonstruktionskosten in die Kategorie 0-4 eingruppiert. Als nächstes wird für jede Art von Bedrohung, sowohl bezüglich der Auftrittswahrscheinlichkeit als auch bezüglich des Schwachstellenniveaus, die Matrix von 0-8 entsprechend befüllt. Resultierend hieraus kann das Bedrohungs- bzw. Schwachstellenlevel jedes Vermögensgegenstandes mit Hilfe dieser Matrix ermittelt werden. Beispielsweise wird ein Vermögensgegenstand mit dem Wert 3 beziffert, die Auftrittswahrscheinlichkeit als „hoch“ eingestuft und die Schwachstellenausnutzung als „gering“ angesehen, wird das Ausmaß des Risikos als 5 dargestellt. Sind alle Risiken bewertet worden, können diese entsprechend ihres Rankings behandelt werden. Um eine entsprechende Einordnung der Vermögensgegenstände, Auftrittswahrscheinlichkeiten und Schwachstellenniveaus durchführen zu können, ist es erforderlich im Vorfeld Informationen von den entsprechenden Stellen zu sammeln. Eine ähnliche Vorgehensweise illustriert die Abbildung 5.

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

Abbildung 5: Risikobewertungsmatrix Variante mit vordefinierten Werten [42]

Eine Risikobeurteilung erfolgt hier durch die Kombination der Wahrscheinlichkeit eines Vorfallszenariums mit den geschätzten Auswirkungen. Ist die Wahrscheinlichkeit eines Störfallszenariums sehr hoch wird somit mit 4 kategorisiert, wohingegen die Auswirkungen des Schadens lediglich mittleren Ausmaßes sind, ist das Gesamtrisiko dennoch sehr hoch und wird mit dem Wert 6 beziffert. Nachdem das resultierende Risiko auf einer Skala von 0-8 kategorisiert wird, wird das Ergebnis in Abhängigkeit der Akzeptanzkriterien bemessen. Auch diese Matrix lässt eine Gesamtrisikoeinschätzung zu.

- Ranking von Bedrohungen mit Hilfe von Risikomaßnahmen

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

Abbildung 6: Risikobewertungsmatrix: Ranking von Bedrohungen [42]

Wie die Abbildung 6 zeigt, werden bei dieser Vorgehensweise im ersten Schritt verschiedene Bedrohungen (Spalte a) aufgelistet. Im zweiten Schritt werden die Auswirkungen auf die Vermögensgegenstände (Spalte b) in einer vordefinierten Skala von 0-5 bewertet. Im nächsten Schritt wird die Auftrittswahrscheinlichkeit (Spalte c) ebenfalls in einer vordefinierten Skala von 0-5 bewertet. Nachdem diese Schritte durchgeführt wurden, werden in der Spalte d die Risikomaßnahmen Produkt aus Spalte b und c berechnet. Schließlich können im letzten Schritt die Bedrohungen (e), abhängig von den Risikomaßnahmen (Spalte d), priorisiert werden. Diese Vorgehensweise erlaubt verschiedene Bedrohungen mit den dazugehörigen Auswirkungen auf die Vermögensgegenstände und Wahrscheinlichkeiten gegenüberzustellen und schließlich zu priorisieren. Neben diesen Methoden zur Bewertung des Informationssicherheitsrisikos existieren weitere Richtlinien und Bewertungsmethoden, die in der Norm ISO/IEC 31010 näher erläutert werden.

- Risikoauswertung

Auf Basis einer aussagekräftigen Risikoanalyse wird im nächsten Prozessschritt der Risikobewertung der Teilprozessschritt der Risikoauswertung durchgeführt. Dabei wird das Risikoniveau mit den Risikoakzeptanz- und den Risikoauswertungskriterien verglichen. Diese Kriterien, die bereits im Anfangsstadium, bei der Definition der Rahmenbedingen gesetzt wurden, sollten in diesem Teilprozessschritt auf Aktualität überprüft bzw. erneut definiert werden. Bei der Risikoauswertung sollte auch in Betracht gezogen werden, dass eine Anhäufung mehrerer geringer Risiken ein hohes Gesamtrisiko darstellen kann. Ebenso sind die für die Organisation bedeutsamen Informationssicherheitseigenschaften zu prüfen. Ist beispielsweise das Kriterium Vertraulichkeit irrelevant für die Organisation, sind auch alle Risiken, die durch dieses Kriterium beeinflusst werden, bedeutungslos. Um eine korrekte Risikoauswertung durchzuführen, ist die Wichtigkeit eines Geschäftsprozesses zu untersuchen. Im Falle einer geringen Wichtigkeit, sollten auch die damit verbundenen Risiken als geringer eingestuft werden. Die Risikoauswertung wird auf Basis der Risikoanalyse für eine zukünftige Entscheidungsfindung herangezogen. Eine adäquate Risikoauswertung stellt die Grundlage für die Priorisierung der Risiken und deren Behandlung dar. Während der Risikoauswertungsphase sollten vertragliche, gesetzliche und regulatorische

Anforderungen zusätzlich als Faktoren berücksichtigt werden. Am Ende dieser Phase sollte eine Liste mit priorisierten Risiken, entsprechend den oben genannten Kriterien, zugeordnet zu den jeweiligen Störfallszenarien, vorhanden sein.

- Risikobehandlung

Nachdem die Risikobeurteilung erfolgreich durchgeführt wurde, kann der nachfolgende Prozessschritt der Risikobehandlung im Informationssicherheitsrisikomanagement vollzogen werden. Wie die nachfolgende Grafik zeigt, existieren vier Maßnahmen, um Risiken zu behandeln.

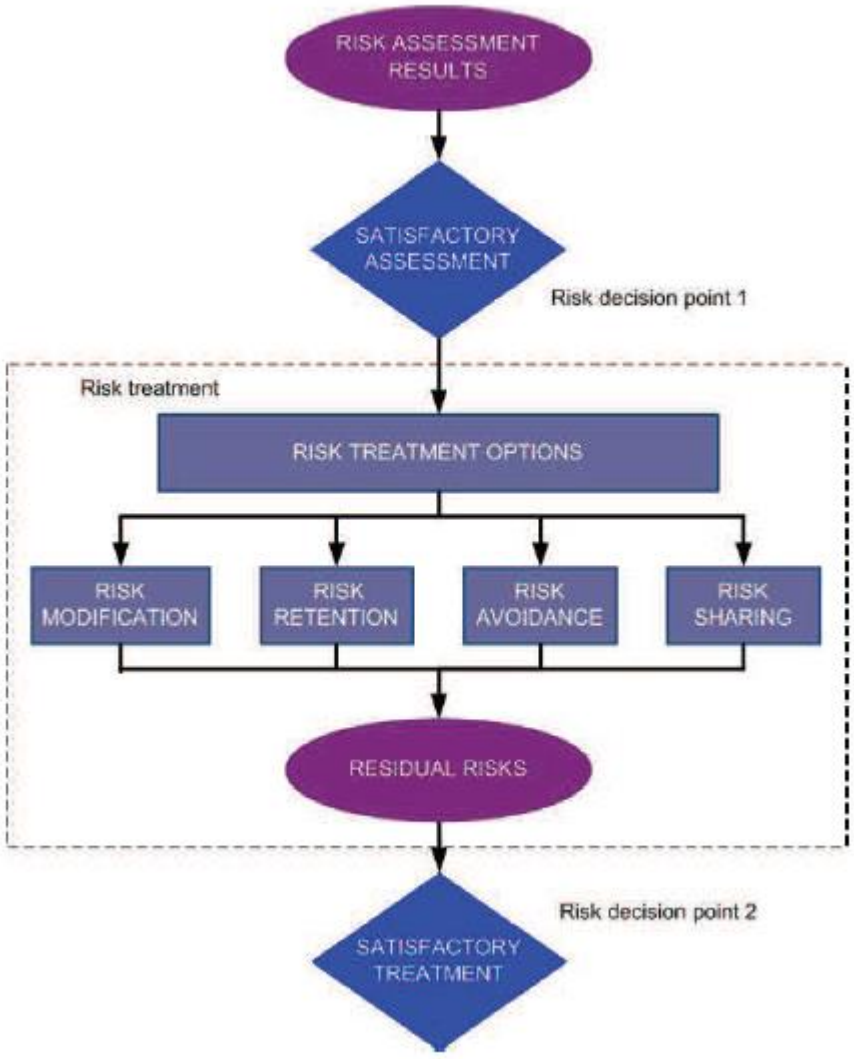

Abbildung 7: Risikomanagementprozess – Risikobehandlung

Die Risikobehandlungsoptionen bestehen aus der Risikoreduktion, der Risikoakzeptanz, der Risikovermeidung und der Risikoübertragung. Die Wahl der Risikobehandlungsoptionen sollte von den Ergebnissen der Risikobeurteilung, den erwarteten Kosten für die Etablierung der entsprechenden

Option und von dem zu erwarteten Erfolg der jeweiligen Möglichkeit abhängig gemacht werden. Diese vier Optionen sollten nicht unabhängig voneinander betrachtet werden. Oftmals ist eine Kombination dieser Optionen das wirksamste Vorgehen in der Risikobehandlung. Beispielsweise kann die Auftrittswahrscheinlichkeit und die Auswirkungen reduziert werden, während das vorhandene Restrisiko auf mehrere Parteien übertragen wird. Um die Risiken wirksam zu behandeln, sollte ein Risikobehandlungsplan definiert werden. Um Kosten zu sparen, sind bereits vorhandene Gegenmaßnahmen auf Effektivität zu untersuchen. Oftmals kann es sinnvoll sein, redundante Sicherheitsmaßnahmen zu erhalten, als einige davon auf Kosten der Sicherheit des Gesamtprozesses zu entfernen. Es liegt in der Verantwortlichkeit der Führungsebene, die Balance zwischen den Implementierungskosten der Sicherheitsmaßnahmen und den durch die Risiken verursachten Schadensauswirkungen zu halten. Nachdem der Risikobehandlungsplan definiert wurde, müssen die verbleibenden Restrisiken ermittelt werden. Die Ermittlung der Restrisiken beinhaltet eine erneute Iteration der Risikobeurteilung unter Beachtung der erwarteten Auswirkungen der definierten Risikobehandlungsmöglichkeiten. Sollte ein verbleibendes Restrisiko nicht den Anforderungen der Risikoakzeptanzkriterien entsprechen, ist eine erneute Iteration der Risikobehandlung vor der Risikoakzeptanzvorgehensweise erforderlich. Der Risikobehandlungsplan beinhaltet die Priorität der bewerteten Risiken und deren Handhabung inklusive festgesetzten Behandlungszeiträumen, zur Einhaltung der Akzeptanzkriterien. In einigen Fällen entsprechen verbleibende Restrisiken nicht den definierten Akzeptanzkriterien, da bei der Definition dieser Kriterien die Zeitumstände nicht berücksichtigt wurden. Beispielsweise wurden Risiken akzeptiert, da der begleitete Nutzen der durch die Risiken entstanden ist sehr attraktiv war oder die Kosten der Risikoreduktion zu hoch waren. Unter diesen Umständen sind die Akzeptanzkriterien nicht adäquat und sollten neu definiert werden. Falls diese Kriterien nicht innerhalb eines angemessenen Zeitraums geändert werden können, müssen Risiken akzeptiert werden, obwohl sie nicht den regulären Akzeptanzkriterien entsprechen. In so einem Fall muss eine begründete Dokumentation vorliegen. Um Risiken zu reduzieren, sollten Sicherheitsmaßnahmen so selektiert werden, dass sie den Anforderungen aus der Risikobeurteilung und der Risikobehandlung entsprechen. Allgemein betrachtet beinhalten Sicherheitsmaßnahmen ein oder mehrere Arten von Schutzvorkehrungen, wie beispielsweise Korrekturmaßnahmen, Löschungen, Präventionsmaßnahmen, Minimierung der Auswirkungen, Wiederherstellung, Überwachung und Awareness. Bei der Auswahl der Schutzmaßnahmen ist es von großer Bedeutung, die Erwerbskosten, die Implementierungskosten, die Administrationskosten, die Instandhaltungskosten und die Kosten der Überwachung im Verhältnis zum Wert des zu schützenden Gutes zu halten. Es ist auch zu berücksichtigen, dass spezielle Fähigkeiten und Fachkenntnisse erforderlich sein können, um neue Sicherheitsmaßnahmen zu entwickeln oder bereits vorhandene anzupassen. Es gibt einige Faktoren, die die Auswahl der Sicherheitsmaßnahmen beeinflussen wie beispielsweise technische, kulturelle, gesetzliche Bedingungen, Zeit-, Finanz-, Umwelt-, Personalvorgaben, oder die Einfachheit der Anwendung. Bei der Auswahl der geeigneten Sicherheitsmaßnahme sollte die Balance zwischen Performance der Maßnahme und Wirksamkeit der Informationssicherheit gehalten werden. Als Ergebnis dieser Risikobehandlungsmethode sollte eine Liste mit möglichen Sicherheitsmaßnahmen mit Kostenaufstellung, Nutzen und Prioritäten vorhanden sein. Erfüllen Risiken die Akzeptanzkriterien, können diese unbehandelt bleiben. In diesem Fall besteht keine Notwenigkeit Sicherheitsmaßnahmen zu erstellen. Die Risikovermeidung als Risikobehandlungsmethode wird verwendet, wenn identifizierte Risiken als zu hoch eingestuft werden oder die Implementierungskosten einer Sicherheitsmaßnahme nicht im Verhältnis zu dem resultierenden Nutzen stehen. In diesem Falle werden sämtliche Aktivitäten, die die Risiken verursachen, zurückgezogen oder deren grundlegende Bedingungen geändert. Bei der letzten Option der Risikobehandlungsmethode werden die Risiken auf Dritte umverteilt. Allerdings ist dabei zu beachten, dass durch diese Methode neue Risiken entstehen können

oder die bereits bestehenden Risiken verändert werden. In diesem Falle ist eine zusätzliche Risikobehandlung erforderlich. Umverteilung kann bedeuten, dass beispielsweise Versicherungen die Schadensauswirkungen tragen oder Dritte für die Überwachung eines Informationssystems und für das Eingreifen im Störfall verantwortlich sind.

- Kommunikation und Beratung des Informationssicherheitsrisikos

Die Kommunikation von Risiken ist eine Maßnahme im Informationssicherheitsrisikomanagementprozess, um ein einheitliches Verständnis für den Umgang mit Risiken zu erzielen, indem Informationen zwischen den Entscheidungsträgern und den betroffenen Interessenparteien ausgetauscht werden. Eine effektive bidirektionale Kommunikation zwischen Entscheidungsträgern und Interessenparteien ist von enormer Wichtigkeit um sicherzustellen, dass alle am Risikomanagementprozess Beteiligten die Basis verstehen, auf der die Entscheidungen getroffen und bestimmte Maßnahmen vollzogen werden. Der Austausch von Informationen im Risikomanagementprozess beinhaltet die Existenz der Risiken, dessen Erscheinungsform, die Art und Weise, die Auftrittswahrscheinlichkeit, den Schweregrad, die Behandlungsmöglichkeiten und die Akzeptanz der Risiken. Daneben sollten Risikokommunikationspläne regelmäßig sowohl für den normalen Betriebsablauf, als auch für Notfälle erstellt werden. Durch Gründung eines Gremiums können Risiken, deren Priorisierung und Behandlung zwischen den Entscheidungsträgern und den betroffenen Interessenparteien debattiert werden. Ziel der Risikokommunikation ist

  - Vertrauen in die Risikomanagementergebnisse zu erbringen,
  - Informationen über Risiken zu sammeln,
  - die Resultate der Risikobeurteilung mitzuteilen und den Risikobehandlungsplan zu präsentieren,
  - Entscheidungsfindungen zu unterstützen,
  - mit anderen Drittparteien zu koordinieren, Verantwortlichkeiten zu übertragen, um die Schadensauswirkungen zu reduzieren,
  - den Entscheidungsträgern und den Drittparteien ein Verantwortungsgefühl über Risiken zu geben
  - und die Awareness zu verbessern.

Besonderes in der Krisenkommunikation ist ausschlaggebend mit der entsprechenden Pressestelle oder Kommunikationseinheit innerhalb der Organisation zu kooperieren, um die Koordination aller Maßnahmen in Bezug zur Risikokommunikation zu gewährleisten.

- Überwachung, Prüfung und Verbesserung der Informationssicherheitsrisiken

Da Risiken und deren Einflussfaktoren (wie der Wert der Vermögensgegenstände, Auswirkungen, Bedrohungen, Schwachstellen, Auftrittswahrscheinlichkeit) sich kontinuierlich verändern, müssen diese regelmäßig überwacht werden, um ein frühzeitiges Eingreifen zu ermöglichen. Um sicherstellen zu können, dass die Rahmenbedingungen, die Ergebnisse aus der Risikobewertung und-behandlung und die Managementpläne den Umständen entsprechen, ist eine kontinuierliche Beobachtung, Überprüfung und eine Verbesserung notwendig. Durch minimale Veränderungen in einem oder mehreren Einflussfaktoren, können gering eingestufte Risiken zu hoch eingestuften Sicherheitsrisiken

mutieren. Auch ein Aggregat von gering eingestuften Risiken kann bei der Veränderung eines Risikos erhebliche Auswirkungen auf die Gesamtrisikobetrachtung mit sich bringen. Aus diesem Grunde müssen Maßnahmen zur Risikoüberwachung regelmäßig wiederholt und die Auswahl der Risikobehandlungsoptionen der gegebenen Situation angepasst werden. Zusätzlich sollten die Prüfkriterien, an denen die Risiken gemessen werden, regelmäßig verifiziert und auf Konsistenz mit den Geschäftszielen, -strategien und -leitlinien überprüft werden. Bei der Beobachtung, der Kontrolle und der Verbesserung der Informationssicherheitsrisiken sollten mindestens folgende Aspekte berücksichtigt werden.

- Gesetzlicher und umweltbezogener Kontext
- wettbewerbsbezogener Kontext
- Vorgehensweise der Risikobewertung
- Werte der Vermögensgegenstände und deren Kategorien
- Auswirkungskriterien, Evaluationskriterien, Risikoakzeptanzkriterien
- die dazu notwendigen Ressourcen

Es sollte sichergestellt werden, dass alle Ressourcen zur Durchführung der Risikobewertung und Risikobehandlung und somit zur Beratung des Managements dauerhaft verfügbar sind. Die Ergebnisse der Risikoüberwachung können Informationsmaterial für weitere Sicherheitsprüfungen darstellen. Abhängig von den identifizierten Veränderungen, der Iteration der Risikobewertung, dem Ziel oder des Gegenstandes des Informationssicherheitsmanagementprozesses kann die Risikomanagementüberprüfung eine Veränderung oder Ergänzung der Vorgehensweise, der Methoden oder der benutzen Tools beinhalten. Ziel dieses Prozessschrittes ist der kontinuierliche Abgleich des Risikomanagements mit den Geschäftszielen der Organisation und den Risikoakzeptanzkriterien. [42]

3.2.2 IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) veröffentlichte Mitte der Neunziger den IT Grundschutz als Standard, der Empfehlungen für Methoden, Prozesse, Verfahrensweisen und Maßnahmen enthält, um den Umgang mit der Informationssicherheit zu beschreiben. Der IT-Grundschutz wird durch vier BSI-Standards und dem Grundschutz-Katalog wiedergespiegelt. Die Grundschutzkataloge beinhalten Bausteine, Gefährdungen und Maßnahmen. Der IT-Grundschutz verfolgt das Ziel, den Aufwand des Informationssicherheitsprozesses zu reduzieren, indem auf bekannte und bereits bewährte Sicherheitsmaßnahmen zurückgegriffen wird. Der BSI-Standard 100-1 [10] beschreibt die Anforderungen an ein ISMS ist damit kompatibel zur ISO/IEC 27001. Daneben werden im BSI-Standard 100-2 [43] die Leitlinien der ISO/IEC 27002 wiedergespiegelt. Daraus ist erkenntlich, dass die Vorgehensweise des IT-Grundschutzes in diesen Bereichen mit der ISO/IEC 27000 Normenfamilie harmoniert. Allerdings wird der Bereich „Datenschutz“ nur von der Grundschutzvorgehensweise abgebildet, da die speziell deutsche Rechtsnorm nicht in der internationalen Norm ISO/IEC 27001 oder in der ISO/IEC 27002 abgebildet werden kann. Eine detaillierte Übersicht der einzelnen Bestandteile der ISO/IEC Standards, die auf die Teile des BSI Standards abgebildet werden, sind in [18] vorhanden. Im Rahmen des BSI Grundschutzes ist eine Zertifizierung möglich. Die vorangegangene autonome Zertifizierung nach dem IT Grundschutz wurde durch die in den BSI-Grundschutz integrierte Zertifizierung nach ISO/IEC 27001 vollständig abgelöst. Die Integration der ISO/IEC 27001 in den IT-Grundschutz ist besonders für international tätige

Institutionen von Bedeutung, da eine internationale Zertifizierung größere Gewichtung hat als eine nationale, insbesondere bei internationaler Zusammenarbeit.

3.2.2.1 BSI Standard 100-1: Managementsysteme für Informationssicherheit

In diesem Standard werden analog zur ISO/IEC 27001 generelle Anforderungen an ein Managementsystem für Informationssicherheit definiert. Somit ist dieser Standard vollständig kompatibel mit der ISO/IEC 27001. Zusätzlich werden Empfehlungen der ISO/IEC 13335 und ISO/IEC 27002 berücksichtigt.

3.2.2.2 BSI Standard 100-2: IT-Grundschutz-Vorgehensweise

Dieser Standard enthält analog zur ISO/IEC 27002 detaillierte Leitlinien zur Umsetzung eines ISMS. In diesem Standard werden unter anderem die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur für Informationssicherheit beschrieben. Wichtige Bestandteile wie die Auswahl der angemessenen Sicherheitsmaßnahmen und die Umsetzung eines Sicherheitskonzeptes werden hier näher erläutert. Die IT-Grundschutzkataloge geben dazu konkrete Umsetzungshinweise auch auf technischer Ebene.

3.2.2.3 BSI-Standard 100-3 (neu 200-3): Risikoanalyse auf der Basis von IT-Grundschutz

Dieser Standard beinhaltet eine Methode zur Risikoanalyse, die mit der IT-Grundschutzvorgehensweise abgestimmt ist. Dieser Standard wird angewendet, wenn der Schutzbedarf als mindestens hoch eingestuft wird. Die Risikoanalyse auf Basis des IT-Grundschutzes umfasst folgende Schritte:

- Vorarbeiten
- Erstellung der Gefährdungsübersicht
- Ermittlung zusätzlicher Gefährdungen
- Gefährdungsbewertung
- Behandlung von Risiken
    - Handlungsalternativen zum Umgang mit Risiken
    - Risiken unter Beobachtung
- Konsolidierung des Sicherheitskonzepts
- Rückführung in den Sicherheitsprozess

Mit Hilfe der IT-Grundschutz-Kataloge wird eine vereinfachte Analyse von Risiken für die Informationssicherheit durchgeführt. Gründe für die vereinfachte Analyse sind

- Hoher oder sehr hoher Schutzbedarf
- Keine Abbildung des Zielobjektes mit existierenden Bausteinen des IT-Grundschutzes möglich
- Fehlende Einsatzszenarien (Umgebung, Anwendung) für die Zielobjekte im IT-Grundschutz

Diese vereinfachte Risikoanalyse wird verwendet, wenn die vorhandenen Maßnahmen in den Grundschutzkatalogen nicht ausreichend sind. Folglich ist diese Vorgehensweise eher mit der Analyse der Restrisiken in der ISO/IEC 27005 zu vergleichen, als mit einer vollständigen Risikomanagementmethode für ein ISMS [13]. Seit Oktober 2016 existiert der neue Standard 200-3 [15] des BSI zur Erstellung einer Risikoanalyse. Allerdings ist dieser Standard zum Erstellungsdatum dieses Forschungsberichts lediglich in der Community Draft-Version verfügbar. Der Standard ist um die Aspekte, Übersicht über elementaren Gefährdungen, Risikoeinstufung, Einführung eines Risikomanagementsystems, Einführung eines Matrix-Ansatzes zur Bewertung von Risiken sowie Einführung des Risikoappetits und des Chancenmanagements erweitert worden. Mit Hilfe des Matrix-Ansatzes kann die Einstufung der Risiken und deren Bewertung veranschaulicht werden.

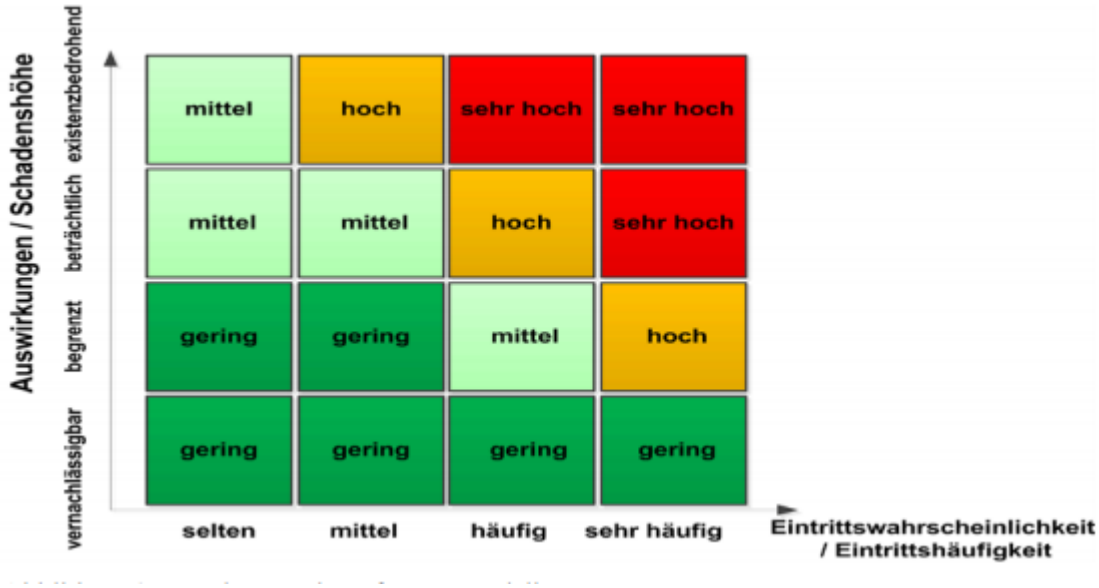

Abbildung 8: Einstufung von Risiken [15]

Zusätzlich wird in dieser Draft-Version davon gesprochen, dass ergänzende Verfahren wie Penetrationstests eine Risikoanalyse sinnvoll ergänzen können. Die Ergebnisse sollten wiederum in das vorhandene Sicherheitskonzept einfließen.[15]

3.2.2.4 BSI-Standard 100-4: Notfallmanagement

Der BSI-Standard 100-4 [44] beschreibt eine Methodik zur Etablierung und Aufrechterhaltung eines behörden- bzw. unternehmensweiten Notfallmanagements. Aufbauend auf der im BSI-Standard 100-2 beschriebenen Vorgehensweise werden darin Methoden erläutert, um ein wirksames Notfallmanagement durchführen zu können.

3.2.2.5 Grundschutzkataloge

Die IT-Grundschutz-Kataloge umfassen Bausteine, Maßnahmen-und Gefährdungskataloge, die konkrete Implementierungshilfen für den Sicherheitsprozess darstellen. Aufgrund der Modularität der

Bausteine kann jede Organisation ihren individuellen Informationsverbund entsprechend den Sicherheitsanforderungen erstellen. Ein zentraler Bestandteil der auf dem IT-Grundschutz basierenden Risikoanalyse sind die vorhandenen Gefährdungen der IT-Grundschutz-Kataloge. Mit Hilfe der Grundschutzkataloge können Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme abgebildet werden, wohingegen seltenere Individuallösungen oder Objekte mit hohem Schutzbedarf extra betrachtet werden müssen. Zusätzlich beinhalten die Grundschutzkataloge eine Darstellung der pauschal angenommenen Gefährdungslage, die mit den Maßnahmen zu Bausteinen kombiniert werden. Die Bausteine bestehen aus einer kurzen Beschreibung, den Gefährdungen und den empfohlenen Maßnahmen. Anhand des im IT-Grundschutz definierten Lebenszyklus eines betrachteten Objekts werden sie dabei in die folgenden Phasen eingeteilt:

- Planung und Konzeption,
- Beschaffung,
- Umsetzung,
- Betrieb,
- Aussonderung
- Notfallvorsorge

Das Sicherheitskonzept nach BSI IT-Grundschutz wird aus diesen Bausteinen zusammensetzt. Die Bausteine sind in nachfolgenden Schichten gegliedert:

- Übergreifende Aspekte
- Infrastruktur
- IT-Systeme
- Netz
- Anwendungen

Mit Hilfe von Kreuzreferenztabellen lassen sich Gefährdungen und Maßnahmen eines Bausteins kombinieren, so dass sichtbar gemacht wird, welche Gefährdung durch welche Maßnahme(n) abgedeckt wird. Wie nachfolgende Tabelle illustriert werden im Baustein B 1.2 Personal, nummerierten Gefährdungen (G) mit nummerierten Maßnahmen (M) kombiniert.

	G 1.1	G 1.2	G 2.2.	G 2.7	…
M 3.10	X			X	…
M 3.11		X	X	X	…
M 3.33				X	…
…	…	…	…	…	…

Abbildung 9: Kreuzreferenztabelle [13]

Die Gefährdungs-Kataloge enthalten ausführliche Beschreibungen und gliedern sich in die fünf Bereiche:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Mit Hilfe dieses Gefährdungskatalogs können Risiken identifiziert werden. Die Maßnahmenkataloge beinhalten praxiserprobte Sicherheitsmaßnahmen, die wie folgt gruppiert werden:

- Infrastruktur
- Organisation
- Personal
- Hard- und Software
- Kommunikation
- Notfallvorsorge

Durch diese Kataloge ist der IT-Grundschutz ein Bausatz, der eine aufwendige Risikoanalyse überflüssig erscheinen lässt. Trotzdem kann ein benutzerdefinierter Baustein, der auf den Grundschutzkatalogen basiert, einer vereinfachten Risikoanalyse nach dem BSI-Standard 100-3 in den oben genannten Fällen unterzogen werden.[45]

3.2.3 ISIS 12

Das InformationsSicherheitsmanagementSystem in 12 Schritten (ISIS 12) wurde seit 2009 vom Bayerischen IT-Sicherheitscluster e.V. entwickelt und andauernd weiterbearbeitet, um einen pragmatischen Ansatz zur Etablierung eines einfachen ISMS zu liefern. Diese Vorgehensweise basiert auf dem IT-Grundschutz des BSI und der ISO/IEC 27001. Allerdings werden die umfangreichen Kataloge des IT-Grundschutzes und die abstrakten Elementen der ISO/IEC 27001 ausgeklammert, so dass ISIS 12 nach dem Prinzip „So einfach wie möglich, aber nicht einfacher“ einen konkreten Handlungsrahmen zur Einführung eines ISMS darstellt. Durch diese Herangehensweise werden nur wenig unternehmenskritische Anwendungen fokussiert und ein reduzierter Maßnahmenkatalog des BSI Grundschutzes angewendet. Daneben beinhaltet das ISIS 12 die groben Mindestanforderungen des IT-Planungsrates [16]. Durch den generischen Aufbau und die Integration der grundlegenden IT-Service-Management-Prozesse (Wartung, Änderung und Störungsbeseitigung) ist diese Vorgehensweise sehr flexibel in 12 sequentiell zu durchlaufenden Schritten anwendbar.

Ursprünglich wurde ISIS 12 für kleine und mittelständische Unternehmen (KMUs) entwickelt. Um auch Anwendung in der öffentlichen Verwaltung zu finden, wurde von dem BSI eine „Standardbehörde“ definiert [17]. Diese Zielgruppen müssen dabei folgende Anforderungen erfüllen:

- nicht mehr als 500 Mitarbeitern
- homogene IT-Basisinfrastruktur
- keine über öffentliche Netze ungeschützt angebundenen Außenstellen
- überwiegend normaler Schutzbedarf

- keinen Hochverfügbarkeitsanforderungen an IT-Systeme
- und keinen kritischen Anwendungen (d.h. keine kritischen Infrastrukturen)

Durch die hohe Skalierbarkeit, den konkreten Handlungsempfehlungen aus dem fokussierten Maßnahmenkatalog, den generischen Aufbau und der einheitlichen Struktur stellt diese Vorgehensweise eine weitere Alternative für die oben genannten Zielgruppen zur Etablierung eines Informationssicherheitskonzeptes dar. Allerdings beinhaltet diese Methode lediglich eine indirekte Risikoanalyse für einen normalen Schutzbedarf. So muss im entsprechenden Fall eine aussagekräftige Risikoanalyse mit Hilfe von anderen Methoden (z.B. ISO/IEC 27005) durchgeführt werden. Mit Hilfe von ISIS 12 können grundlegende Gefährdungen der Informationssicherheit in der öffentlichen Verwaltung eruiert werden, so dass diese Methode als Basis verwendet werden kann, um weitere Schritte, wie eine Zertifizierung nach „ISO 27001 auf Basis von IT-Grundschutz“ bzw. „ISO/IEC 27001 nativ“, durchzuführen.

Auf Grund der Skalierbarkeit dieser Vorgehensweise können die wichtigsten Schritte zur Etablierung eines ISMS mit vergleichsweise geringem Aufwand eingeführt und eine spätere Ergänzung von umfangreicheren Standards vereinfacht werden.

3.2.4 Arbeitshilfe der Bayerische Innovationsstiftung der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)

Auf Grund von kürzlich verabschiedeten Gesetzen wurde von der Innovationsstiftung Bayerische Kommune der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) eine Arbeitshilfe zur Erstellung eines Konzepts zur Informationssicherheit für Kommunen nach Artikel 8 „Informationssicherheit und Datenschutz“ des Gesetzes über die elektronische Verwaltung in Bayern (BayEGovG) erstellt. Diese Arbeitshilfe basiert auf ISIS 12 bzw. dem IT-Grundschutz des BSI. Ziel dieser Arbeitshilfe ist, „den kommunale Einrichtungen eine Hilfe zur Selbsthilfe zugeben, die nicht über ausreichende Möglichkeiten zur Einführung und Umsetzung von Standards zur Informationssicherheit wie BSI IT-Grundschutz oder ISIS12 verfügen, um den Anforderungen des Artikel 8 BayEGovG zu genügen“[46]. Allerdings verspricht diese Arbeitshilfe nicht in Konkurrenz mit den oben genannten Alternativen zu stehen, sondern möchte eher den Mindestanforderungen aus Artikel 8 BayEGovG gerecht werden. Somit soll den kommunalen Einrichtungen, die über keine ausreichenden zeitlichen, personellen oder monetären Ressourcen verfügen, um ein oben genanntes ISMS einzuführen, ein Hilfsmittel zur Entwicklung und Einführung eines eigenen Informationssicherheitskonzepts gegeben werden. Da diese Arbeitshilfe lediglich einen stark reduzierten Fragen- und Maßnahmenkatalog zur Selbstüberprüfung beinhaltet, die Anwendung dieser Arbeitshilfe nicht zertifizierbar ist, und diese Arbeitshilfe kein Ersatz für ein ISMS darstellt, kann sie lediglich als Einstiegspunkt für kleine Kommunen betrachtet werden, die sich noch nicht mit Informationssicherheit beschäftigt haben. Dennoch beschreibt der Verfasser, dass hier ein „Upgrade“ auf ISIS 12 oder IT-Grundschutz möglich sei. In dieser Arbeitshilfe werden folgende Inhalte abgedeckt:

- Informationssicherheit
- Datenschutz
- Gebäudesicherheit
- Zugang zu IT-Systemen
- Berechtigungskonzepte und Protokollierung
- Notfallmanagement (Vorsorge und Notfallplan)

- Richtlinien und Dienstanweisungen
- Schulungen und Sensibilisierung – Mitarbeiter als elementarer Bestandteil der Informationssicherheit
- Externe Dienstleister – Anforderungen an externe Dienstleister, nicht nur im Rahmen einer Auftragsdatenverarbeitung

Die Arbeitshilfe beinhaltet neun Kapitel. Dabei ist jedes Kapitel identisch aufgebaut. Zur erfolgreichen Anwendung dieser Arbeitshilfe müssen die ersten beiden Kapitel chronologisch zu Beginn abgearbeitet werden. Zu Beginn eines Kapitels sind Erläuterungen, Erklärungen und Beispiele zum jeweiligen Thema des Kapitels (Notwendigkeit, Risiken, Möglichkeiten) vorhanden. Daneben existieren ausgewählte Prüfpunkte mit Fragen und Erläuterungen zu dem jeweiligen Thema. Zusätzlich ist neben den Prüffragen bereits eine mögliche Lösung vorhanden. Zudem kann in der Spalte „Ergebnis(se)“ der tatsächliche Zustand beschrieben werden. Mit einem Prüfschema „Erfüllt“, „Nicht erfüllt“, „Nicht anwendbar“ und „In Arbeit“ lässt sich jeder Prüfpunkt bewerten. Abschließend erfolgt eine Gesamtbewertung des Kapitels mit einem Verweis auf beiliegende Mustervorlagen, Dokumente und Weblinks. Nachfolgend ein beispielhafter Ausschnitt der Systematik dieser Arbeitshilfe.

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1. Informationssicherheit	Haben Sie die grundlegenden Anforderungen an Verfahren und Abläufe zur Einführung und kontinuierlicher Aufrechterhaltung von Informationssicherheit sichergestellt? Diese dienen als Basis, um Informationssicherheit als kontinuierlichen Prozess in Ihrer Organisation nicht nur einzuführen, sondern auch aufrechtzuerhalten. Tipp: Nehmen Sie sich diesen Punkt als Erstes vor, bevor Sie mit weiteren Maßnahmen aus diesem Konzept weitermachen. Hinweis: Sofern Sie die Punkte aus Schritt 1 *„Informationssicherheit“* in Ihrer Organisation nicht umsetzen können, sollten Sie der Behördenleitung die Frage stellen, ob eine Fortführung überhaupt noch Sinn ergibt. Denn Ihnen wird im weiteren Verlauf der Umsetzung die notwendige Basis und Unterstützung fehlen, die Sie mit diesem Schritt aufbauen.		

Prüfpunkt	Erläuterungen / Fragen	Ergebnis(se)	Bewertung
1.1. Leitlinie / Dienstanweisung zur Informationssicherheit	Ihre Sicherheitsstrategie sollte in einer Leitlinie zur Informationssicherheit zusammengefasst werden, um die zu verfolgenden Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter zu dokumentieren (und diese einzufordern!). Mit der Sicherheitsleitlinie bekennt sich die Behördenleitung klar zu ihrer Verantwortung für Informationssicherheit. Idealerweise erfolgt die Umsetzung der Leitlinie mittels Inkraftsetzung durch eine Dienstanweisung. Wie jede andere Leitlinie sollte auch die Leitlinie Informationssicherheit regelmäßig, spätestens jährlich, auf notwendige Anpassungen hin geprüft und bei Bedarf aktualisiert werden.		**Dokumente / Anlagen:**
1.1.1. Verantwortung der Behördenleitung	Informationssicherheit hat in Ihrer Einrichtung keine Chance, wenn die Behördenleitung nicht im vollen Umfang hinter den Zielen der Informationssicherheit und den dafür notwendigen Maßnahmen steht. Hat sich die Behördenleitung zu ihrer Gesamtverantwortung für Informationssicherheit bekannt? Wurde die Leitlinie von der Behördenleitung unterschrieben?		☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht anwendbar ☐ Aktuell in Arbeit

Abbildung 10: Prüfkatalog der Arbeitshilfe Bayerische Innovationsstiftung [46]

3.2.5 Weitere Standards mit Bezug zur Informationssicherheit

Zusätzlich existieren neben den bereits vorgestellten Normen und Standards eine große Anzahl an weiteren Standards im Bereich ISMS, die nachfolgend kurz beschrieben werden. Zum einen sind Standards vorhanden, die sich mit dem Management von Sicherheit in den IT-Systemen befassen, zum anderen existieren weitere Standards analog zum IT-Grundschutz, die sich überwiegend an die ISO/IEC 27001 orientieren.

3.2.5.1 COBIT

Control Objectives for Information and related Technology (COBIT) definiert eine Vorgehensweise zur Kontrolle von Risiken, unter Anwendung von Informationstechnologie zur Unterstützung geschäftsrelevanter Betriebsabläufe. Ein zentraler Bestandteil des COBIT, welches von der vom IT Governance Institute (ITGI) der Information Systems Audit and Control Association (ISACA)

weiterentwickelt wird, ist die Beziehung zwischen der Informationssicherheit mit dem Projektmanagement und der IT Governance [47]. Somit werden in diesem Rahmenwerk Prozesse zur Erfüllung der Geschäftsstrategie und der Geschäftsziele im Hinblick auf die IT Governance unter Berücksichtigung der sieben Informationskriterien, Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Compliance und Zuverlässigkeit, definiert. Durch diese Kriterien werden die Grundwerte des IT-Grundschutzes Vertraulichkeit, Integrität und Verfügbarkeit erweitert.

Diese Informationskriterien beinhalten und erweitern die im IT-Grundschutz definierten Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit und vereinen somit die Zielsetzung der beiden Standards.[48] Die Informationssicherheit ist in diesem Rahmenwerk auch als prozessorientierter Ansatz zu versehen, der iterativ durchlaufen wird, um ständige Verbesserungen durchzuführen. Anstelle des PDCA-Prozesses in den ISO Normen bzw. im Grundschutz werden dort die unterschiedlichen Prozessschritte in Domänen abgebildet. Das COBIT-Framework enthält 90% prozentige inhaltliche Überschneidungen mit der ISO/IEC 27001 und der ISO/IEC 20000-1, wohingegen der Detaillierungsgrad der Anforderungen nach ISO/IEC 27001 deutlich höher ist. In Bezug auf den IT Grundschutz ist der Überschneidungsgrad mit diesem Framework auch sehr hoch, insbesondere wenn die Organisation bereits nach der ISO/IEC 27001 basierend auf dem IT Grundschutz konfiguriert ist.[49], [50], [51], [52], [53]

3.2.5.2 ITIL

Die IT Infrastructure Library (ITIL) gilt als Best Practice Referenzmodell für das IT-Servicemanagement (ITSM), indem das IT- Sicherheitsmanagement als eigener Aspekt außerhalb des IT-Servicemanagements betrachtet wird. Ziel dieses weltweit akzeptierten Standards ist die Qualitätsverbesserung der IT-Servicemanagementprozesse und die Optimierung der Kosteneffizienz. Da sich der strategische Planungsprozess mit der Unternehmensstrategie vereinigt, ist dieser Standard mit der zum IT-Servicemanagement-Standard ISO/IEC 20000 [54] kompatibel. Gemäß der Abbildungen in [49] ergeben sich somit auch Überschneidungen mit der DIN/IEC 270001.[51]

3.2.5.3 ISO/IEC 20000-1

In dieser zweigeteilten Norm wird der Aufbau und die Aufrechterhaltung des Service Managements, in der das Security Management verankert ist, beschrieben. Allerdings werden im Abschnitt des Security Managements nur sehr allgemeine und oberflächliche Maßnahmen definiert und auf die ISO/IEC 27002 verwiesen. Da diese Norm als internationaler Standard für die Prüfung und Bewertung des IT-Service Managements gilt, wird sie als Zertifizierungsnorm zu ITIL betrachtet. Diese Norm verweist ebenfalls auf den klassischen PDCA-Kreis von Deming, der die ständige Überprüfung der Maßnahmen betont[48],[54].

3.2.5.4 Regionale Standards

Neben den oben beschriebenen Standards existieren weitere regionale Standards, die sich auf das Management von Informationssicherheit beziehen. Allerdings basieren die folgenden Standards alle auf der ISO/IEC 27001 oder haben Teile davon gänzlich übernommen. Beispielsweise existiert in Österreich das Österreichische Informationssicherheitshandbuch [60], welches auch an die internationalen Normen angeglichen wurde. Daneben gibt es in Großbritannien den Standard BS 7799-3 „Guidelines for information security risk management“, der aus der Ursprungsnormenfamilie des BS 7799[33] entwickelt wurde. Die Normen der ISO/IEC Normenfamilie 27000 basieren auf diesem Ursprungsstandard. Die in Amerika existierende Standards der Veröffentlichungsreihe NIST SP 800 wurden vom US-amerikanische National Institute of Standards and Technology (NIST) entwickelt [55].

4 Vorgehensmodelle

In diesem Abschnitt beschreibt dieser Forschungsbericht die verschiedenen Ansätze zur Erstellung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS. Der Forschungsbericht fokussiert sich dabei auf die vier verschiedenen Hauptmodelle. Es wird das Vorgehensmodell nach der ISO/IEC 2700x Normenfamilie, nach dem IT-Grundschutz des BSI, nach der ISIS 12 und der Arbeitshilfe der Bayerischen Innovationsstiftung analysiert. Die in Kapitel 3.1 und 3.2.5 genannten Normen und Standards werden an dieser Stelle aus bereits genannten Gründen vernachlässigt.

4.1 ISO/IEC 2700x-Normenfamilie

In diesem Unterkapitel analysiert dieser Forschungsbericht den methodischen Aufbau zur Erstellung eines Informationssicherheitskonzeptes nach der DIN ISO 27000er Reihe. Die Methode beinhaltet die Prozessschritte Definition des Kontextes einer Organisation, Festlegung einer Informationssicherheitsrichtlinie, Identifikation von Informationswerten, Unterstützung durch das Management, Identifikation und Festsetzung von Sicherheitsanforderungen, Durchführung eines Informationssicherheitsrisikomanagements, Auswahl und Umsetzung geeigneter Maßnahmen und Entwicklung eigener Leitfäden und die Kontrolle, Instandhaltung und Verbesserung der Wirksamkeit der Sicherheitsmaßnahmen. Diese Methode ist als iterativer Ansatz zu betrachten, der kontinuierlich wiederholt und überprüft werden sollte, um auf Veränderungen zeitnah situationsbezogen reagieren zu können. Für die erfolgreiche Umsetzung eines ISMS sind entscheidende Faktoren, wie beispielsweise die Anpassung der Informationssicherheitspolitik an die Ziele der Organisation, eine wirksame Bewusstseins-, Schulungs-und Fortbildungsprogramm für alle betroffenen Parteien, die Informationssicherheitsrichtlinien einzuhalten, einen effektiven Prozess zur Behandlung von Informationssicherheitsvorfällen und eine effektive Unterstützung der obersten Leitungsebenen zur Informationssicherheitsangelegenheiten, zu berücksichtigen.

- Definition des Kontextes einer Organisation

Als Ausgangspunkt ist der interne und externe Kontext der Organisation zu bestimmen, um ein aussagekräftiges Sicherheitskonzept erstellen zu können. Dabei sind interessierte Parteien zu adressieren und deren Anforderungen zu definieren. Daneben sind interne und externe Themen festzulegen, die für den Zweck der Organisation relevant sind. Bei der Definition des Kontextes sind gesetzliche, regulatorische und vertragliche Bedingungen zu beachten. Zusätzlich muss der Anwendungsbereich des Informationssicherheitsmanagementsystems und dessen Grenzen definiert werden. Dabei sind sämtliche Schnittstellen und Abhängigkeiten sowohl innerhalb als auch außerhalb der Organisation zu interessierten Parteien zu identifizieren. Dieser Prozessschritt sollte in schriftlicher Form dokumentiert werden.

- Unterstützung durch das Management

Nachdem der Kontext der Organisation mit seinem Anwendungsbereich und dessen Grenzen festgelegt wurde, sollte zum einen das Management im Einverständnis darüber sein, zum anderen ist es zur Unterstützung heranzuziehen. Eine Unterstützung des Managements kann erfolgen, indem es die Informationssicherheitspolitik und deren Ziele mit strategischen Organisationsausrichtung vereinbart. Zusätzlich kann eine Unterstützung des Managements erfolgen, indem die Informationssicherheitsmanagementanforderungen in die Geschäftsprozesse der Institution integriert werden oder indem die erforderlichen Ressourcen zur Etablierung, Instandhaltung und Verbesserung eines ISMS zur Verfügung gestellt werden. Entscheidend ist dabei, dass die Wichtigkeit eines ISMS und dessen Anforderungserfüllung durch das Management vermittelt und somit die Ziele des ISMS erreicht werden. Daneben sollten relevante Führungskräfte in den Verantwortungsbereichen des ISMS durch das Management unterstützt werden, um deren Führungsrolle zu verdeutlichen.

- Festlegung einer Informationssicherheitsrichtlinie

Um ein wirksames Informationssicherheitskonzept erstellen zu können, muss durch das Management eine Informationssicherheitsrichtlinie definiert werden, die für den Organisationszweck angemessen ist. Diese Richtlinie umfasst die Informationssicherheitsziele, eine Verpflichtungserklärung zur Erfüllung der Informationssicherheitsanforderung und die Verpflichtung kontinuierlichen Verbesserung des ISMS. Nachdem die Informationssicherheitsrichtlinie in dokumentierter Form erstellt wurde, wird sie als vertrauensbildende Maßnahmen bekannt und interessierten Parteien zugänglich gemacht.

- Identifikation von Informationswerten

Nachdem sämtliche Rahmenbedingungen festgesetzt wurden, ist es erforderlich als nächsten Prozessschritt, die Informationswerte einer Institution zu identifizieren. Die Analyse der Informationswerte bildet eine solide Grundlage, um ein wirksames Informationssicherheitskonzept zu erschaffen. Diese beinhaltet die Klassifizierung von Informationen und anderen Vermögenswerten. Eine Klassifizierung von Informationswerten ist in der Version der DIN ISO/IEC 27002:2008 [56] und in der DIN ISO 27005 [42] beschrieben. Es existieren verschiedene Arten von organisationseigenen Werten, wie beispielsweise Informationen, Software, physische Werte, Dienstleistungen, Personen mit ihren Qualifikationen, Fähigkeiten und Erfahrungen und immaterielle Werte (der gute Ruf, Image der Organisation). Die Vermögenswerte werden anhand ihren Werts, gesetzlicher Anforderungen, ihrer Sensitivität und ihrer Kritikalität eingeteilt.

Daneben ist durch eine zuständige Person ein Inventar über die Informationswerte zu erstellen. Das Inventar sollte Information über die Eigentümerschaft der Informationswerte, der Klassifizierung und alle relevante Informationen zur Rekonstruierung nach einer Katastrophe beinhalten. Abhängig von der Höhe des Geschäftswertes des Informationswertes, der Sicherheitsklassifizierung und der Wichtigkeit, sollte ein Schutzniveau definiert werden, welches die Wertigkeit der Informationswerte wiederspiegelt. Die Erstellung eines Inventars ist ein wichtiges Element zur Erstellung einer

aussagekräftigen Risikoanalyse. Darauf aufbauend müssen im nächsten Prozessschritt die Sicherheitsanforderungen dieser Informationswerte analysiert und bestimmt werden.

- Identifikation und Festsetzung von Sicherheitsanforderungen

Nachdem die Informationswerte analysiert wurden, müssen als weiterfolgender Prozessschritt die Informationssicherheitsanforderungen identifiziert, analysiert und festgesetzt werden. Dieser Schritt ist von großer Bedeutung, um ein wirksames Informationssicherheitskonzept in einer Organisation etablieren zu können. Mögliche Quellen für Anforderungen sind zum einen Organisationsziele, spezifische Richtlinien oder geschäftliche Ansprüche an die Informationsverarbeitung zur Unterstützung des Geschäftsbetriebs der Organisation. Daneben können Anforderungen aus soziokulturellem Umfeld, Verträgen, gesetzlichen Bestimmungen und Verordnungen, politischen Entscheidungen der Organisation und ihren Geschäftspartnern entstehen. Zusätzlich stellt die nachfolgende Risikoeinschätzung eine entscheidende Quelle für Anforderungen der Informationssicherheit dar. Nicht zu vernachlässigen sind die allgemeine Strategie der Organisation mit ihren Zielen.

- Durchführung eines Informationssicherheitsrisikomanagements

Der Mittelpunkt eines Informationssicherheitskonzeptes stellt die Durchführung eines Informationssicherheitsrisikomanagements dar. Um Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten, zu behandeln und zu überwachen, ist gemäß der DIN ISO 27005[42] der nachfolgenden Prozess des Risikomanagements durchzuführen.

- Definition der Rahmenbedingungen (Context establishment)
- Risikobeurteilung (Risk assessment)
    - Identifizierung von Risiken (Risk identification)
    - Abschätzung von Risiken (Risk estimation)
    - Auswertung von Risiken (Risk evaluation)
- Risikobehandlung (Risk treatment)
- Risikoakzeptanz (Risk acceptance)
- Risikokommunikation (Risk communication)
- Risikoüberwachung und Verbesserung (Risk monitoring and review)

Die nachfolgende Graphik verschafft einen Überblick über den Prozess des Informationssicherheitsrisikomanagements. Hierbei soll ein grundlegendes Verständnis für den Prozess des Risikomanagements gelegt werden. Der Forschungsbericht geht in Kapitel 3.2.1.4 detaillierter auf diesen Prozess ein.

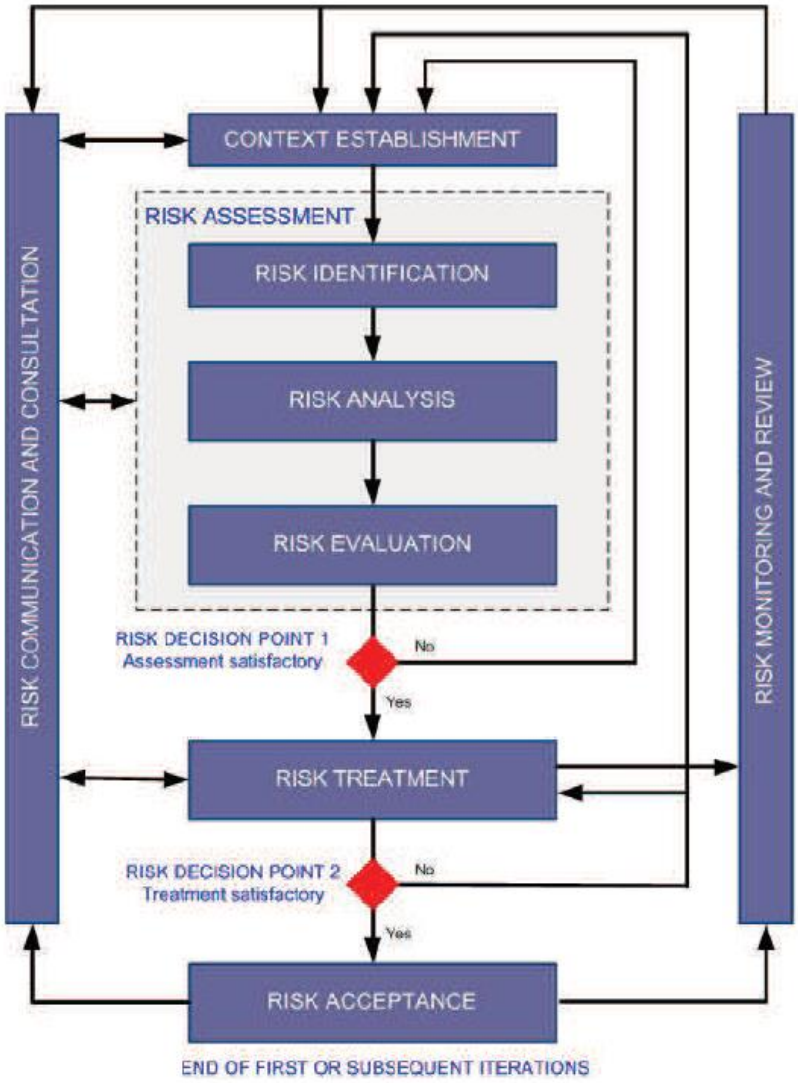

Abbildung 11: Informationssicherheitsrisikomanagementprozess [42]

- Definition der Rahmenbedingungen (Context establishment)

Wie diese Bild illustriert, werden als Einstiegspunkt die Rahmenbedingungen mit ihrem internen und externen Kontext einer Organisation festgesetzt. So werden unter anderem Kriterien zur Bewertung und Akzeptanz von Risiken, der Anwendungsbereich und dessen Grenzen sowie die Etablierung einer Risikomanagementorganisation, definiert.

- Risikobeurteilung (Risk assessment)

Der nachfolgende Prozessschritt Risikobewertung im Informationssicherheitsrisikomanagements enthält die Unterschritte Identifikation von Risiken, Risikoanalyse mit Abschätzen von Risiken und die Auswertung von Risiken.

- Identifizierung von Risiken (Risk identification)
- Risikoanalyse (risk analysis) mit Risikoabschätzung (Risk estimation)
- Auswertung von Risiken (Risk evaluation)

Sobald die Risikobewertung genügend nutzbare Informationen hervorbringt, um eine Entscheidungsgrundlage zur Auswahl von wirksamen Maßnahmen zur Risikobehandlung zu erstellen, ist dieser Prozessschritt erfüllt. Somit kann der Risikoentscheidungspunkt eins (risk decision point 1) mit positiv beantwortet werden und der nachfolgende Prozessschritt durchgeführt werden. Andernfalls wird der bisherige Prozessstand nochmals und so lange iterativ durchlaufen, bis angemessene Informationen vorhanden sind. Es werden die Rahmenbedingungen neu gesetzt und der interne Prozess der Risikobewertung mit seinen Teilelementen erneut durchlaufen, um geeignete Informationen zu erlangen. Bei der Risikobeurteilung müssen unter anderem Risiken im Hinblick auf Vertraulichkeit, Integrität, Verfügbarkeit und Risikoeigentümer und dessen Folgen ermittelt werden, sowie Risiken mit Hilfe von Risikokriterien bewertet werden. Hierbei werden Kriterien für die Risikoakzeptanz und Durchführung der Risikobeurteilung identifiziert, quantifiziert und schließlich priorisiert. Die Analyse der Informationssicherheitsrisiken erfolgt durch die Abschätzung der realistischen Eintrittswahrscheinlichkeiten und deren Folgen nach Eintritt der Risiken. Als Ergebnis der Analyse wird mit Hilfe von Risikobewertungsmethoden, die in ISO/IEC TR 13335-3 (Information technology - Guidelines for the management of IT security -Part 3: Techniques for the managing of IT security) diskutiert werden, das Risikoniveau bestimmt. Im Kapitel 3.2.1 spezifiziert dieser Forschungsbericht unterschiedliche Methoden zur Risikobewertung. Die Bewertung der Risiken erfolgt durch den Vergleich der Ergebnisse der Risikoanalyse mit den festgelegten Kriterien. Dabei werden die ermittelten Risiken für den nächsten Prozessschritt, die Risikobehandlung, priorisiert. Um vergleichbare reproduzierbare Ergebnisse zu erlangen, muss die Risikoeinschätzung systematisch unter gleichen Bedingungen durchgeführt werden. Es ist erforderlich den Prozess der Risikoeinschätzung regelmäßig zu wiederholen, da sich Veränderungen von Organisationszielen und-strategien, Werten und Sicherheitsanforderungen sowohl auf die Ergebnisse der Risikoanalyse und Risikobewertung auswirkt, als auch auf die damit verbundenen Gegenmaßnahmen.

- Risikobehandlung (Risk treatment)

Unter Berücksichtigung der Ergebnisse aus der Risikobeurteilung, werden in diesem Prozessschritt geeignete Optionen zur Behandlung der ermittelten Risiken ausgewählt. Die Effektivität der Risikobehandlung ist abhängig von den Ergebnissen der Risikobeurteilung. Die Risikobehandlung beinhaltet einen zyklischen Prozess mit folgenden Elementen.

- Beurteilung der Risikobehandlung
- Entscheidung über die Akzeptanz des verbleibenden Restrisikos
- Einführung einer erneuten Risikobehandlung im Falle eines unakzeptablen Restrisikos
- Beurteilung der Effektivität dieser Risikobehandlung

Bei der Risikobehandlung sollte eine Konsolidierung mit den Maßnahmenzielen aus der ISO/IEC 27002 vorhanden sein. Dabei ist zu beachten, dass der Aufwand der Maßnahmen im Verhältnis zum Schadensausmaß steht, das heißt die Kosten für Risikobehandlungsmaßnahmen müssen geringer ausfallen, als die für die durch die Risiken verursachten Gefahren. Die Auswahl der wirksamen Maßnahmen zur Erfüllung der Maßnahmenziele muss in einer Anwendbarkeitserklärung dokumentiert sein. Um einen höchstmögliche Wirksamkeit zu erhalten, müssen darin sowohl die Gründe der Auswahl als auch der Nicht-Auswahl der Maßnahmen formuliert sein. Die Maßnahmen und

Maßnahmenziele dienen als Orientierungshilfe und können situationsabhängig und organisationsspezifisch erweitert oder verkürzt werden. Ein nachfolgender Schritt ist die Erstellung eines Risikobehandlungsplan, welcher durch den Risikoeigentümer genehmigt werden muss. Dabei ist die Akzeptanz für jedes einzelne Informationssicherheitsrisiko zu prüfen. Es müssen folgende mögliche Alternativen für den Umgang mit Risiken gewählt werden. Es muss entschieden werden, ob und welche wirksamen Maßnahmen angewendet werden,

- um Risiken zu reduzieren oder
- ob Risiken bewusst und tatsächlich akzeptiert werden, falls sie den Kriterien für die Risikoakzeptanz entsprechen, oder
- ob spezielle Risiken vermieden werden, durch Untersagung Risikoverursachender Aktionen, oder
- ob spezielle Risiken auf dritte Parteien (Versicherer, Lieferanten) übertragen werden können.

Dabei ist zu berücksichtigen, dass die ausgewählten Maßnahmen die Anforderungen erfüllen, die durch die Risikobeurteilung eruiert wurden.

- Risikoakzeptanz (Risk acceptance)

Falls das Level des Restrisikos nicht akzeptabel ist, muss eine erneute Iteration der Risikobeurteilung mit gegebenenfalls veränderten Kontextparametern wie beispielsweise Kriterien für die Risikoakzeptanz oder der Auswirkung durchgeführt werden. Falls notwendig wird das mit einer erneuten Risikobehandlung wie der Entscheidungspunkt zwei (Risk descision point 2) verdeutlicht. Die Maßnahme der Risikoakzeptanz muss sicherstellen, dass das vorhandene Restrisiko explizit von der Führungsebene der Organisation getragen wird, insbesondere in Situationen, in denen die Einführung von Kontrollmaßnahmen ausgelassen oder verschoben wird.

- Risikokommunikation (Risk communication)

Während des gesamten Informationssicherheitsrisikomanagementprozess ist die Kommunikation der Risiken und deren Behandlungsmaßnahmen innerhalb der Organisation von großer Bedeutung. Die Sensibilisierung des betroffenen Personenkreises in Bezug auf die Risiken und die Wirkungsweise der Kontrollmaßnahmen, sind die wirksamsten Methoden, um mit unvorhersehbaren Vorfällen umzugehen.

- Risikoüberwachung und Verbesserung (Risk monitoring and review)

Sowohl die Risiken als auch der Risikomanagementprozess werden kontinuierlich überwacht und fortlaufend verbessert. Die Führungsebene und die Mitarbeiter werden über Risiken und Maßnahmen zur Risikominderung geschult. Dabei werden Informationen erfasst, um die Vorgehensweise für das Risikomanagement zu verbessern. Jede Maßnahme und Entscheidung im gesamten Prozess des Informationssicherheitsrisikomanagements sollte dokumentiert aufbewahrt werden. Der internationale Standard ISO/IEC 27001 spezifiziert, dass alle umgesetzten Gegenmaßnahmen innerhalb des Anwendungsbereiches, des Kontextes und der Grenzen eines ISMS risikobasiert sein

müssen. Diese Anforderung wird durch die Umsetzung eines Informationssicherheitsrisikomanagementprozesses erfüllt. Da viele Vorgehensweisen existieren, wie dieser Prozess umgesetzt werden kann, muss die Organisation diejenige wählen, die sich am besten für die gegebenen Umstände eignet.

Der Prozess des Informationssicherheitsrisikomanagements kann als in sich geschlossener Teilprozess der Erstellung eines Informationssicherheitskonzeptes in die Phasen des Plan-Do-Check-Act („Planen, Durchführen, Prüfen, Handeln“) bzw. „PDCA-Prozess“ Kreises eines ISMS integriert werden. Der prozessorientiere Ansatz dieses Modelles wird auch in weiteren ISO/IEC Standards, wie z.B. dem ISO/IEC 90011 und dem ISO/IEC 20000-13. In der vorherigen Version der ISO 27000 (DIN ISO/IEC 27000:2011) basiert der Gesamtprozess der Erstellung, Instandhaltung, Kontrolle und Verbesserung eines ISMS noch auf dem „Plan-Do-Check-Act-Prozess“ („Planen, Durchführen, Prüfen, Handeln“) bzw. „PDCA-Prozess“ , wohingegen in der aktuellen Version der ISO 27000 (E DIN ISO/IEC 27000:2015) dieser Regelkreis entfallen ist [57][14]. So wird der „PDCA-Regelkreis“ aus Optimierungsgründen lediglich für den in sich geschlossenen Teilprozess des Informationssicherheitsrisikomanagements angewendet. Die nachfolgende Tabelle vergleicht die Maßnahmen des Informationssicherheitsrisikomanagementprozesses mit dem PDCA-Prozess eines ISMS.

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

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

Abbildung 12: Vergleich eines ISMS-Prozesses mit dem Informationssicherheitsrisikoprozess [42]

In der ersten Phase der „Planung“ werden die wie bereits oben näher beschrieben Rahmenbedingungen definiert, die Risikobeurteilung durchgeführt, ein Risikobehandlungsplan erstellt und die Risikoakzeptanz geprüft. Die nächste Phase der „Durchführung“ beschreibt die Implementation des Risikobehandlungsplans, d.h.es werden alle ausgewählten Maßnahmen und Maßnahmenziele anhand des Planes durchgeführt. In der nachfolgenden „Kontroll“-Phase werden die bereits vollzogenen Phasen beobachtet und die Risiken überprüft. Schließlich wird in der letzten Phase der „Handlung“ der gesamte Prozess des Informationssicherheitsmanagements instandgehalten und bei Bedarf Verbesserung vorgenommen, so dass der Kreislauf wieder von vorne beginnen kann.

- Auswahl von Sicherheitsmaßnahmen und Entwicklung eigener Leitfäden

Basierend auf der Wertbestimmung der Vermögenswerte, der Definition der Sicherheitsanforderungen und den Resultaten des Informationssicherheitsrisikomanagements sollten Maßnahmen ausgewählt und umgesetzt werden, um ein wirksames Informationssicherheitskonzept erstellen zu können. Die Maßnahmen können aus der ISO 27002 [40] wie in Kapitel xy näher erläutert, ISO 27005 [42] oder anderen Maßnahmenkatalogen situationsabhängig ausgewählt werden. Die in den ISO-Normen beschriebenen Maßnahmen dienen sowohl als Richtlinie für ein Informationssicherheitsmanagement, als auch als Ausgangspunkt zur Entwicklung neuer, spezifischer auf die jeweilige Situation angepasste Maßnahmen und Leitfäden zur Erstellung eines Informationssicherheitskonzeptes. Die Auswahl der Maßnahmen ist abhängig von gesetzlichen und vertraglichen Bedingungen, dem Organisationskontext, der Informationssicherheitsleitlinie, der Managementunterstützung, der Interagierungsweise einzelnen Maßnahmen unter einander, den getroffenen Entscheidungen, basierend auf den Risikoakzeptanzkriterien und den Risikobehandlungsoptionen und dem allgemeinen Organisationsansatz gegenüber dem Risikomanagement.

- Bewertung der Informationssicherheit

Um ein wirksames und aktuelles Informationssicherheitskonzeptes zu gewährleisten, muss die Informationssicherheit im ISMS kontinuierlich überwacht, gemessen, analysiert und bewertet werden. Eine aussagekräftige Leistungsbewertung umfasst den Gegenstand der Messung, die Informationssicherheitsprozesse mit Maßnahmen, die verwendeten Methoden, die Verantwortlichen der Messung und der Analyse und den Zeitraum der Messung und der Analyse. Zusätzlich sind interne Audits und Managementbewertung erforderlich, die in regelmäßigen Abständen durchgeführt werden, um zu prüfen, ob die Anforderungen der ISO Normen umgesetzt wurden. Abschließend sollte durch die Managementebenen eine Bewertung des ISMS erfolgen, um die Funktionsfähigkeit des ISMS wieder zu spiegeln, falls erforderlich Verbesserungen durchzuführen und auf Veränderungen zeitnah reagieren zu können.

Abschließend ist festzustellen, dass bei dieser Vorgehensweise, sowohl die oben genannten Prozessschritte des Informationssicherheitsrisikomanagements als auch die Schritte des gesamten Prozesses des Informationssicherheitsmanagements kontinuierlich iterativ durchzuführen sind, um Veränderungen von Risiken, Geschäftszielen und Strategien zeitnah zuerkennen und frühzeitig darauf zu reagieren. Allerdings ist bei dieser Methode das hohe Abstraktionslevel zu beachten. Sollten detaillierte Umsetzungsschritte, insbesondere im technischen Bereich, erwünscht sein, sind andere Vorgehensweisen, wie z.B. der IT-Grundschutz des BSI als Ergänzung zu Rate zu ziehen.

4.2 BSI IT-Grundschutz

Die nachfolgende Abbildung verschafft einen Überblick über die Vorgehensweise des IT-Grundschutzes, welche ein systematisches Vorgehen zur Erreichung eines angemessenen Sicherheitsniveaus voraussetzt. [43]

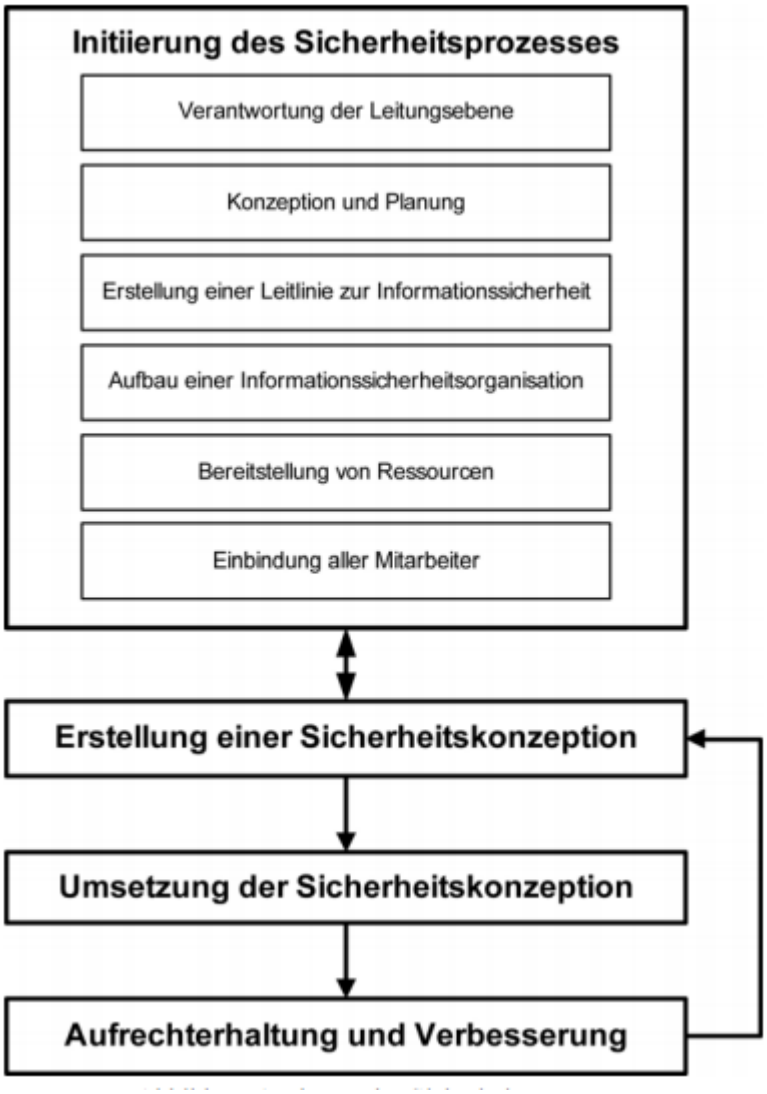

Abbildung 13: Vorgehensweise des IT-Grundschutz [43]

- Initiierung des Sicherheitsprozesses

Zu Beginn dieser Vorgehensweise wird der Sicherheitsprozess von der Leitungsebene initiiert, gesteuert und kontrolliert. Wichtige Bestandteile sind auf der einen Seite strategische Leitaussagen zur Informationssicherheit und auf der anderen Seite das Festlegen von organisatorischen Rahmenbedingungen, wie die Verantwortung der Leitungsebene, die Konzeption und Planung, die Erstellung einer Leitlinie zur Informationssicherheit, den Aufbau einer

Informationssicherheitsorganisation, die Bereitstellung von Ressourcen sowie die Einbindung aller Mitarbeiter.

- Erstellung einer Sicherheitskonzeption

Nachdem die Initiierung des Sicherheitsprozesses erfolgt ist, wird im nachfolgenden Prozessschritt die Sicherheitskonzeption erstellt. Die Sicherheitskonzeption umfasst die folgenden wichtigsten Schritte:

- Definition des Geltungsbereichs
- Strukturanalyse
- Schutzbedarfsfeststellung
- Auswahl und Anpassung von Maßnahmen
- Basis-Sicherheitscheck
- Ergänzende Sicherheitsanalyse

Um eine aussagekräftige Sicherheitskonzeption erstellen zu können, muss als erstes der Geltungsbereich, der im IT-Grundschutz als Informationsverbund bezeichnet wird, klar abgesteckt werden. Danach werden in der Strukturanalyse die Elemente (Informationen, Anwendungen, IT-Systeme, Räume, Gebäude, Kommunikationsnetze) dieses Informationsverbundes beschrieben. Anschließend wird eine Schutzbedarfsfeststellung dieser Elemente durchgeführt. Zur Bestimmung des Schutzbedarfs der einzelnen Werte werden diese, basierend auf den Schutzzielen (Verfügbarkeit, Vertraulichkeit und Integrität), in die Klassen „niedrig bis mittel“, „hoch“ und „sehr hoch“ gruppiert. Allerdings sind die in den Grundschutzkatalog definierten Maßnahmen nur für den niedrigen bis mittleren Schutzbedarf bestimmt, wohingegen bei hohem oder sehr hohem Schutzbedarf weitere Maßnahmen erforderlich sind. Sobald der Schutzbedarf hoch ist, wird der BSI Standard 200-3 (alt 100-3) für die Risikoanalyse verwendet, da der Standard 100-2 nicht mehr ausreichend ist. Es wird eine ergänzende Sicherheitsanalyse, in der entschieden wird, ob weitere Maßnahmen vollzogen werden müssen, durchgeführt. Hier wird angenommen, dass der vorhandene Pool an Sicherheitsmaßnahmen dem genüge. Bei der Verwendung der IT-Grundschutzkataloge können allgemeinen Kategorien von Gefährdungen verwendet werden und somit kann eine aufwendige Risikoanalyse entfallen. Allerdings spiegelt diese Vorgehensweise nur eingeschränkt den Kern eines aussagekräftigen Risikomanagementprozesses wieder. Nachdem die Schutzbedarfsfeststellung der Objekte durchgeführt wurde, werden Maßnahmen ausgewählt und angepasst, indem den Objekten des Informationsverbundes die entsprechenden Bausteine mit Gefährdungen und Maßnahmen zugeordnet werden. Diese Zuordnung wird im IT-Grundschutz als Modellierung bezeichnet. Mit dem anschließenden Basis-Sicherheitscheck wird ein Vergleich des Soll-Zustandes mit dem IST-Zustand durchgeführt und mögliche Defizite in der Umsetzung aufgezeigt.

- Umsetzung der Sicherheitskonzeption

Als nächster Prozessschritt wird die erstellte Sicherheitskonzeption umgesetzt. Als erstes werden die Untersuchungsergebnisse gesichtet, indem die noch nicht umgesetzten IT-Grundschutz-Maßnahmen und ggf. die Maßnahmen aus der Risikoanalyse zusammengestellt werden. Der nächste Schritt umfasst die Konsolidierung der Maßnahmen. Hierbei findet einerseits eine Prüfung statt, ob die ausgewählten Maßnahmen aus den Katalogen durch zusätzliche, aus der Risikoanalyse durchgeführten Maßnahmen ersetzt bzw. ergänzt werden müssen. Andererseits erfolgt bei dieser Umsetzungsplanung eine Analyse, in der geprüft wird, ob eine Konkretisierung oder Anpassung der Maßnahmen hinsichtlich der technischen und organisatorischen Gegebenheiten der Organisation erfolgen muss. Daneben wird unter Berücksichtigung realisierungsbegleitender Maßnahmen eine Kosten-und Aufwandsschätzung

durchgeführt, die Umsetzungsreihenfolge der Maßnahmen festgelegt und der Verantwortungsbereich und mit Aufgaben definiert.

- Aufrechterhaltung und Verbesserung

Die letzte Phase dieser Vorgehensweise umfasst die Aufrechterhaltung und Verbesserung des Informationssicherheitsprozesses hinsichtlich Wirksamkeit und Effizienz. Da es Ziel des Sicherheitsmanagements ist, das angestrebte Sicherheitsniveau zu erreichen und es dauerhaft aufrechtzuerhalten und zu verbessern, muss der Sicherheitsprozess und die Organisationsstrukturen kontinuierlich durch die Leitungsebene geprüft werden. Dabei müssen zwei wesentliche Aspekte berücksichtigt werden. Einerseits sollte die Überprüfung des Informationssicherheitsprozesses auf allen Ebenen erfolgen, indem geeignete Maßnahmen zur Überprüfung dieses Prozesses ausgewählt werden, die Umsetzung der Sicherheitsmaßnahmen geprüft wird, die Eignung der Strategie für die Informationssicherheit kontrolliert und letztendlich die Übernahme der Ergebnisse in diesem Prozess organisiert wird. Der andere Aspekt umfasst die Informationsverteilung in diesem Informationssicherheitsprozess. Sowohl die zielgruppengerechte Aufbereitung der wesentlichen Informationen als auch die zeitnahe Weitergabe dieser Informationen ist von großer Bedeutung. Diese letzte Phase mündet wieder in dem oben genannten Prozessschritt „Erstellung einer Sicherheitskonzeption“[43]. Gemäß des Standards BSI 100-1 unterliegt sowohl die Erstellung eines Sicherheitskonzeptes, als auch der gesamte Informationssicherheitsprozess dem PDCA-Prozess nach Dümig, analog zu der ISO/IEC Normenfamilie 27000 [10].

Allerdings lässt sich diese Annahme nur teilweise bestätigen, da die Anforderungen an einen kontinuierlichen Verbesserungsprozess und die des PDCA-Zyklus nicht gänzlich erfüllt werden. Aufgrund der in sich abgeschlossenen Betrachtungsweise der Grundschutz-Bausteine erfüllt diese Vorgehensweise nicht den Kernbereich eines iterativen Verbesserungsprozesses. Daneben kann eine Verbesserung nur durch das BSI erfolgen. Außerdem werden zuerst die die Maßnahmen der Grundschutzkataloge geplant und umgesetzt und erst dann analysiert [13], [50]. Trotz dieser Feststellung ist zu berücksichtigen, dass die Vorgehensweise nach dem IT-Grundschutz ihre Vorteile mit sich bringt. So kann der Grundschutzkatalog zur strukturierten Vorgehensweise verwendet werden, um Risiken im jeden Teilbereich zu identifizieren und sich in dem Pool der bereits erprobten Standardsicherheitsmaßnahmen zu bedienen. Daneben sollte in Betracht gezogen werden, dass es dem Benutzer der Grundschutzmethodik obliegt, eine beliebige Verfahrensweise zur Etablierung eines Risikomanagementsystems zu verwenden. So kann für das Risikomanagement anstelle des BSI Standards 100-3 bzw. 200-3 beispielsweise der Standard ISO/IEC 27005 als sinnvolle Ergänzung herangezogen werden. Die parallele Verwendung des IT-Grundschutzes, z.B. zur Identifikation von Risiken, und der ISO/IEC 27005 z.B. zur Risikokommunikation und Risikoüberwachung, stellt eine weitere sinnvolle Option dar [13].

4.3 ISIS 12

Die Einführung eines ISMS nach ISIS 12 wird strukturiert in 12 sequentiellen Schritten mit einem Top-Down Ansatz durchlaufen. Diese 12 Prozessschritte werden wiederum in drei Hauptphasen (Initialisierungsphase, Festlegung der Aufbau- und Ablauforganisation, Entwicklung und Umsetzung ISIS12-Konzept) gruppiert.

Abbildung 14: Grobphasen des ISIS 12 Modells [58],[59]

Diese Vorgehensweise basiert auf dem PDCA-Zyklus, in dem die Unternehmensleitung die Hauptverantwortung für die Informationssicherheit trägt, den erforderlichen Sicherheitsprozess initiiert und die erforderlichen Ressourcen zur Verfügung stellt. Diese Aspekte sind Grundvoraussetzung für eine weitere erfolgreiche Vorgehensweise. Durch den sequentiellen Ansatz wird erst nachdem wichtige Vorarbeiten in den ersten beiden Phasen vollzogen wurden, mit den operativen Arbeiten, wie der Entwicklung und Umsetzung der ISIS 12 Konzeption, in der letzten Phase im Schritt sechs begonnen. Die beiden ersten Phasen, die in der ISIS 12 Vorgehensweise sehr ausführlich dargestellt werden, sind auf Grund der zeitabhängigen iterativen Durchführung zur erfolgreichen Einführung eines wirksamen ISMS unerlässlich. Wohingegen bei anderen Vorgehensweisen (IT-Grundschutz, ISO/IEC 27000) diese Schritte nicht so bedeutsam sind. Nachfolgend werden die 12 Schritte kurz erläutert:

Abbildung 15: Die 12 Schritte der ISIS 12 Vorgehensweise

Die Abbildung illustriert die ISIS 12 Vorgehensweise in 12 Schritte zur Einführung eines ISMS.

I. Initialisierungsphase

- 1. Schritt: Erstellung einer Leitlinie: Die Initialisierungsphase beginnt im ersten Prozessschritt mit der Erstellung einer Leitlinie, in der die Informationssicherheitsziele, abgestimmt mit den Geschäftszielen, definiert werden. Darüber hinaus werden das angestrebte Sicherheitsniveau und die daraus abgeleitete Strategie festgelegt. Nachdem die Leitlinie erstellt wurde, wird diese vom Management verabschiedet und allen Mitarbeitern kommuniziert.

- 2. Schritt: Sensibilisierung der Mitarbeiter: Nachdem die Leitlinie den Mitarbeitern kommuniziert wurde, werden die Mitarbeiter in Bezug auf die Informationssicherheit sensibilisiert. Die Sensibilisierungsmaßnahmen beinhalten eine frühzeitige Kooperation, Informationsweitergabe und Mitarbeit aller betroffenen Abteilungen.

II. Festlegung der Aufbau- und Ablauforganisation

- 3. Schritt: Aufbau eines Informationssicherheitsteams: In diesem Prozessschritt wird ein Informationssicherheitsteam erschaffen, indem die Aufgaben, Pflichten und die Zusammensetzung des Teams definiert werden. Der Informationssicherheitsbeauftragte (ISB) ist der zentrale Ansprechpartner des Teams. Darüber hinaus kann das Team u.a. aus Datenschutzbeauftragten, QM-Beauftragten, IT-Mitarbeitern, externer ISIS12-Beratern bestehen.

- 4. Schritt: Erstellung einer IT-Dokumentation: Mit Hilfe einer Struktur für eine aktuelle und ganzheitliche IT-dokumentation wird die Basis für eine erfolgreiche Durchführung der ISIS 12 Vorgehensweise gesetzt. In der erarbeiteten Struktur werden u.a. formale Bedingungen, verpflichtende Dokumenteninformationen, verbindliche Dokumentenvorlagen und Rahmendokumente (Leitlinie, Organigramm, IT-Kompetenzmatrix, IT-Namenskonvention,

Dokumentationsrichtlinie und Verfahrensanweisung) definiert. Dieser Prozessschritt ermöglicht eine nachhaltige Dokumentation und eine Vermeidung von Redundanzen. Basierend auf den Rahmendokumenten wird das IT-Betriebshandbuch und IT-das Notfallhandbuch erstell.

- 5. Schritt: Einführung des IT-Service-Management-Prozess (ITSM): In diesem Schritt werden die grundlegenden IT-Service- Management-Prozesse (Wartung, Änderung und Störungsbeseitigung) definiert, da die ISIS 12 Methodik dies erfordert. Darüber hinaus wird zu jedem ITSM-Prozess ein Prozesssteckbrief, ein IT-Betriebshandbuch erstellt und der dazugehörige Verantwortungsbereich definiert. Zu beachten sind bei der Störungsbeseitigung die maximal tolerierbaren Ausfallzeiten (MTA) der wichtigsten IT-Systeme. (siehe Schritt 7)

III. Operative Arbeiten: Entwicklung und Umsetzung ISIS12-Konzept

- Schritt 6: Identifikation kritischer Anwendungen: Dieser Prozessschritt stellt den Kernpunkt bei der Erstellung eines ISMS dar. Hier sind kritische Anwendungen zu identifizieren und zu bewerten, indem der Schutzbedarf anhand der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit, analog zum BSI Grundschutz, analysiert und klassifiziert wird. Auf Basis der Schutzbedarfsfeststellung werden die MTA (Maximal tolerierbare Ausfallzeit) und SLA (Service Level Agreement) abstrahiert. Daneben wird die Verarbeitung personenbezogener Daten erfasst. Basierend auf diesem Prozessschritt wird das Sicherheitskonzept in den nachfolgenden Schritten erstellt.

- Schritt 7: Analyse der IT-Struktur: Die Analyse der IT-Struktur umfasst die Definition des Informationsverbunds und die Zuordnung der erforderlichen IT-Systeme und der beteiligten Infrastruktur (Gebäude, Client- und Serversysteme, Netzwerk- und TK-Komponenten) zu den identifizierten kritischen Anwendungen. Da bei dem ISIS 12 Ansatz IT-Systeme als Ganzes betrachtet werden, wird der Schutzbedarf, die MTA und das SLA der Applikationen auf die IT-Systeme und infrastrukturelle Objekte vererbt.

- Schritt 8: Modellierung der Sicherheitsmaßnahmen: Um wirksame Sicherheitsmaßnahmen modellieren zu können, werden zu Beginn dieses Schrittes die Ergebnisse der Strukturanalyse (Schritt 7) auf Plausibilität geprüft und im Bedarfsfall entsprechend angepasst. Anschließend wird jedem Objekt (Anwendung, IT-Systeme, Räume, Gebäude etc.) ein entsprechender Baustein zugeordnet. Dieser Baustein enthält analog zum IT-Grundschutz eine Liste mit empfohlenen und umzusetzenden Sicherheitsmaßnahmen aus dem ISIS 12-Kataolog. Mit Hilfe des ISIS12-Tools erfolgt die Verknüpfung der IT-Zielobjekte mit den ISIS 12-Maßnahmen automatisch. Der ISIS 12 Maßnahmenkatalog vereint den extrem hohen Detaillierungsgrad des IT-Grundschutzes mit dem minimalistischen und abstrakten Elementen der ISO/IEC 27001, so dass ein angemessener Maßnahmenpool für die ISIS 12 Zielgruppe geschaffen wurde. Falls dennoch erforderlich können benutzerdefinierte Bausteine beliebig in den vordefinierten Katalog integriert werden. Dieser flexible modulare Ansatz stellt einen eindeutigen Vorteil gegenüber der statischen Vorgehensweise des IT-Grundschutzes dar.

- Schritt 9: IST-SOLL Vergleich: In diesem Prozessschritt erfolgt eine Analyse des aktuellen Umsetzungsgrades der empfohlenen Sicherheitsmaßnahmen (aus Schritt 8) mit einer Bewertung „ja“, „teilweise“, „nein“ oder „nicht notwendig“. Die noch nicht vollständig

umgesetzten Maßnahmen „nein“ sollen identifiziert werden und in den nachfolgenden Schritten umgesetzt werden, wohingegen die bereits vollständig umgesetzten Maßnahmen „ja“ und die vernachlässigbaren „nicht notwendig“ Maßnahmen ein Revisionsdatum erhalten, um eine kontinuierlichen Wirksamkeits-und Angemessenheitsüberprüfung durchführen zu können. Daneben kann in diesem Prozessschritt erstmals der erreichte Informationssicherheitsgrad gemessen werden.

- Schritt 10: Planen der Umsetzung: Ziel dieses Prozessschrittes ist ein konkreter Umsetzungsplan mit Zeiträumen und Reihenfolgen. Dazu erfolgt eine Konsolidierung der noch nicht oder nur teilweise umgesetzten Sicherheitsmaßnahmen mit Priorisierung hinsichtlich dessen Schutzbedarfs und der Breitenwirkung. Anschließend wird eine Kostenplanung (Bewertung der einmaligen und wiederkehrenden Kosten) erstellt und der Geschäftsleitung zur Entscheidungsfindung vorgelegt.

- Schritt 11: Umsetzen: In diesem Schritt werden die genehmigten Sicherheitsmaßnahmen (aus Schritt 10) umgesetzt, gesteuert und die Wirksamkeit der umgesetzten Maßnahmen kontrolliert. Dazu werden für jede Maßnahme der Verantwortliche und der finale Realisierungszeitpunkt definiert.

- Schritt 12: Revision: Der abschließende Schritt beinhaltet eine kontinuierliche Kontrolle der aller bisher durchgeführten elf Schritte mit regelmäßigen Verbesserungsmaßnahmen im Sinne des PDCA-Prinzips. Dabei wird im Rahmen einer Revision die wirksame Umsetzung der noch offenen Sicherheitsmaßnahmen untersucht.

Nach Schritt 11 besteht die Möglichkeit einer optionalen ISIS 12 Zertifizierung. Ziel dieser Zertifizierung ist zum einen extern, den Geschäftspartnern die Qualität des etablierten ISMS intersubjektiv zu belegen und zum anderen intern, die Qualität des ISMS kontinuierlich zu erhalten und zu optimieren. Da das ISIS 12 Vorgehensmodell die Mindestanforderungen des IT-Planungsrates erfüllt, ist es für kleine bis mittelgroße Behörden bzw. Kommunen mit niedrigen bis mittleren Schutzbedarf rechtlich anwendbar. Wohingegen große Behörden, große Verwaltungen und große Städte aber auch Bereiche mit besonderen Sicherheitsansprüchen (wie z.B. Steuerverwaltungen, Polizei, Steuerverwaltungen, Universitätskrankenhäuser) nicht auf das einfache ISIS 12 Modell zurückgreifen können, sondern sich vielmehr auf den IT-Grundschutz bzw. die ISO/IEC 27000er Reihe stützen müssen. In wie weit das ISIS 12 Vorgehensmodell für Hochschulen und Universitäten geeignet ist, wird im Kapitel sechs geprüft und bewertet werden.

4.4 Arbeitshilfe der Bayerische Innovationsstiftung der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)

Die Vorgehensweise der Arbeitshilfe der Bayerische Innovationsstiftung verfolgt nach Angaben des Verfassers den PDCA-Zyklus nach Deming. Wie die nachfolgende Abbildung zeigt, sind dabei folgende Schritte durchzuführen:

Abbildung 16: Vorgehensweise der Arbeitshilfe der Bayerischen Innovationsstiftung [46]

- Erste Bestandsaufnahme
- Übersicht Schwachstellen, Risiken und Lösungsvorschläge erstellen
- Maßnahmenplan erstellen
- Betrieb des Informationssicherheitskonzepts

Allerdings dient diese Arbeitshilfe vielmehr der momentanen Bestandaufnahme, als einem kontinuierlichen Verbesserungsprozess, wie es der PDCA-Zyklus vorschreibt. Diese Arbeitshilfe beinhaltet lediglich einen Prüf-und Maßnahmenkatalog zur aktuellen Bestandsaufnahme. Der Verfasser empfiehlt zwar, dass Einrichtungen geschaffen werden sollen, die eine kontinuierliche Weiterentwicklung und ein Überwachen der geplanten und offenen Maßnahmen durchführen sollen. Allerdings endet hier die Arbeitshilfe und es wird nicht näher darauf eingegangen. Zudem wird in dieser Arbeitshilfe weder eine Risikoanalyse noch ein Risikomanagement durchgeführt, sondern vielmehr versucht, reduzierte Standardschwachstellen zu identifizieren. Wie bereits in den vorherigen Kapiteln beschrieben, ist eine umfassendes Risikomanagement Kern eines erfolgreichen ISMS. Auf Grund des sehr stark reduzierten Prüf-und Maßnahmenkatalogs der Arbeitshilfe, der Nicht- Zertifizierbarkeit und da die Arbeitshilfe kein Ersatz für ein ISMS darstellt, wird dieser Forschungsbericht in den

nachfolgenden Kapiteln, wie der Gegenüberstellung und der Bewertung, nicht weiter auf diese Vorgehensweise eingehen. Zielgruppe dieser Arbeitshilfe sind zudem kleine kommunale Einrichtungen, die über keine ausreichenden zeitlichen, personellen oder monetären Ressourcen verfügen. Damit ist es sehr fraglich, ob der vom BSI definierte Begriff „Standardbehörde“ im Kapitel 2.4 mindestens erfüllt wird. Jedoch ist im wissenschaftlichen Universitäts-und Hochschulbereich diese Arbeitshilfe eventuell als Einführungs-und Überblickslektüre verwendbar, jedoch nicht, um ein ISMS an allen bayerischen Universitäten und Hochschulen einzuführen.

5 Gegenüberstellung

In diesem Kapitel stellt dieser Forschungsbericht die drei priorisierten Vorgehensmodelle, die alle im unterschiedlichen Maße geeignet sind, ein ISMS zu erstellen, erstellen, zu implementieren und aufrechtzuerhalten und zu verbessern, gegenüber. Der wesentliche Unterschied der drei vorgestellten Ansätze im ISMS Umfeld liegt in der Durchführung der Risikoanalyse im Rahmen eines Risikomanagements. Daneben sollten Faktoren wie der Umfang, das Abstraktionslevel, die Zielgruppe oder die internationale Anerkennung nicht außer Acht gelassen werden.

- Risikoanalyse

Ein wirksames Risikomanagement in Form einer aussagekräftigen Risikoanalyse stellt einen zentralen Punkt bei der Erstellung eines ISMS dar. Ziel einer aussagekräftigen Risikoanalyse ist es, alle relevanten Gefährdungen zu identifizieren, die daraus entstehenden Risiken abzuschätzen und mit Hilfe von korrespondierenden Gegenmaßnahmen die Risiken auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent zu machen. Mit Hilfe einer strukturierten Vorgehensweise kann der Umgang mit dem Gesamtrisiko systematisch gesteuert werden und effektiv behandelt werden. Ein wirksames Risikomanagement verfolgt einen iterativen Ansatz einer Risikoanalyse mit einem ständigen Verbesserungsprozess. Bei der Risikoanalyse unterscheiden sich die drei Vorgehensweisen am deutlichsten. Die BSI-Grundschutz-Methodik beinhaltet eine nachgelagerte Risikoanalyse, wohingegen die Vorgehensweise nach der ISO/IEC 2700x eine vollständige, vorangestellte Risikoanalyse beschreibt. Die stark an den Grundschutz orientierte Methode nach ISIS 12 beinhaltet, auf Grund der Designkriterien, lediglich eine immanente Risikoanalyse. Dabei decken die in den ersten beiden Phasen umzusetzenden Sicherheitsmaßnahmen des ISIS 12 Katalogs lediglich die Grundgefährdungen ab. Diese beschriebene Risikoanalyse ist lediglich für eine „Standardbehörde“ mit geringen bis mittleren Schutzbedarf ausgelegt. Für KMU oder Behörden mit hohem Schutzbedarf, wie z.B. Polizei, große Städte oder Universitäten mit kritischen Forschungsbereichen ist die Risikoanalyse nach ISIS 12 nicht ausreichend und muss mit einer anderen Methode zur Risikoanalyse ergänzt oder ersetzt werden. Die nachgelagerte Risikoanalyse des BSI-Grundschutzes bietet sich aus Kompatibilitätsgründen zu ISIS 12 als Ergänzung an. Allerdings ist auch bei der Grundschutz Risikoanalyse Methodik zu beachten, dass der Standard 100-2 auch nur für den geringen bis mittleren Schutzbedarf bestimmt ist. Sobald der Schutzbedarf hoch ist, wird der BSI Standard 200-3 (alt 100-3) verwendet. In diesem Falle wird eine ergänzende Sicherheitsanalyse durchgeführt, in der entschieden wird, ob weitere Maßnahmen durchgeführt werden müssen. Bei dieser nachgelagerten Sicherheitsanalyse wird angenommen, dass der Pool an Sicherheitsmaßnahmen ausreichend ist. Es werden allgemeine Kategorien von Gefährdungen verwendet, so dass eine aufwendige Risikoanalyse dadurch entfallen kann. Allerdings spiegelt dieser Ansatz bei standardabweichenden Gefährdungen nicht den Kern eines wirksamen Risikomanagements. Daneben werden die verwendeten Grundschutz Bausteine als in sich geschlossen betrachtet. Ein iterativer Verbesserungsprozess kann durch den Grundschutzanwender nur schwer erfolgen, da Verbesserungen nur durch das BSI vollzogen werden können. Da jedoch der Grundschutz-Anwender die Wahl hat, welche Methode er zur Risikoanalyse er verwenden möchte, kann eine vollständige Risikoanalysemethode vor allem bei standardabweichenden Gefährdungen nach ISO/IEC 27005 als Ergänzung herangezogen werden.

Aus Synergieeffekten kann für die Identifikation von Risiken bei einer „Standardbehörde“ mit geringen bis mittleren Schutzbedarf ISIS 12 herangezogen werden, um im Vorfeld die Standardgefährdungen mit relativ geringem Aufwand zu eruieren.

Wird im Rahmen dieser Gefährdungsidentifikation festgestellt, dass der Schutzbedarf mindestens hoch ist, die Gefährdungen mit den ISIS 12 Bausteinen nicht abgebildet werden können oder besonderen Einsatzszenarien (z.B. in Umgebungen oder mit Anwendungen) existieren, kann auf die Grundschutzmethodik zur Risikoidentifikation und zur Risikokommunikation ausgewichen werden.

Um eine vollständige, vorangestellte, iterative Risikoanalyse bei standardabweichenden Gefährdungen durchzuführen, kann, basierend auf den durch die vorangegangenen Methoden identifizierten Standardgefährdungen, auf die ISO/IEC 27005 Methode gewechselt werden. Hierbei werden in einem iterativen Prozess zu Beginn die Rahmenbedingungen definiert. Danach wird eine vollständige Risikobeurteilung durchgeführt, in der die Risiken identifiziert, abgeschätzt und ausgewertet werden. In diesem Teilprozessschritt der Risikoidentifikation besteht die Möglichkeit, sich der ISIS 12 oder der Grundschutzmethodik zu bedienen. Durch die Designkriterien des ISIS 12 Ansatzes oder auch durch die vorgefertigten Standardgefährdungen des Grundschutzes ist hier unter den oben genannten Bedingungen eine Prozessbeschleunigung möglich. Nachdem die Beurteilung der Risiken durchgeführt wurde, wird in der ISO/IEC 27005 Methode die Risikobehandlung als nächster Schritt vorgenommen. Weitere Bestandteile in diesem ständigen Verbesserungsprozess sind die Risikoakzeptanz, die Risikokommunikation und schließlich die Risikoüberwachung und Verbesserung. Die nachfolgende Tabelle verdeutlicht die jeweiligen Schwerpunkte der einzelnen Vorgehensmodelle [16],[17].

	ISIS 12	**IT-Grundschutz**	**ISO/IEC 27001**
Verfügbarkeit und Kosten	• ISIS12-Handbuch und ISIS12- Katalog öffentlich zugänglich • gegen eine Schutzgebühr (ca. 150.- € netto) erhältlich • Zertifizierungsschema frei ist verfügbar • alle Dokumente in deutscher Sprache	• Normen, Kataloge öffentlich zugänglich und kostenfrei • vollständiges Zertifizierungsschema frei verfügbar • in deutscher Sprache	• Normen ISO/IEC 27001/27002 über Beuth-Verlag verfügbar • ISO/IEC 27001: ca. 100 € ISO/IEC 27002: 180 € • auch in deutscher Sprache
Umfang	• ISIS12-Handbuch: 96 Seiten • ISIS12- Katalog: 75 Seiten	• Standards 100-1 bis 100-3: mit ca. 160 Seiten; • IT-Grundschutzkataloge: ca. 4.400 Seiten mit ca. 79 Bausteinen, 483 Gefährdungen und ca. 1.200 Maßnahmen	• 27001: etwa 32 Seiten, • 27002: 114 generische Maßnahmen/ Kontrollen in 14 Kontrollgruppen auf ca. 90 Seiten
Bedeutung international	• steigender Bekanntheitsgrad im KMU-Umfeld, sonst eher unbekannt	• hoher Bekanntheitsgrad im deutschsprachigen Raum, insbesondere im öffentlichem Sektor	• international uneingeschränkt anerkannt
Zielgruppe	• KMU und Behörden mit Kriterien für die „Standardbehörde“	• uneingeschränkt	• uneingeschränkt
Detaillierungsgrad technisch	• Konkrete Handlungsempfehlungen, • basiert auf der IT-Grundschutz-Vorgehensweise und –Katalogen • geführte Vorgehensweise	• Technisch sehr detailliert, konkret und umfangreich	• keine technischen Umsetzungsdetails vorgeschrieben; Maßnahmenziele und Maßnahmen gelten nicht mehr (seit Version 2013) verpflichtend;
Toolunterstützung	• ISIS12-Softwaretool und kommerzielles Tool (ibi Systems) stehen zur Verfügung, • Tooleinsatz empfehlenswert, • aber Anwendung und Zertifizierung auch ohne ISIS12-Tool möglich, wenn auch sehr aufwendig	• Mehrere (auch kostenfreie) Tools verfügbar. • eigenes Tool von BSI (GSTOOL) war vorhanden • Tooleinsatz wird dringend empfohlen	• Tools mit sehr differenzierter Qualität und unterschiedlichen Kosten verfügbar, • Anwendung und Zertifizierung auch ohne Tools möglich

Zertifizierungs-aufwand	• Erst-Zertifizierungs-Audit: 2 PT und Überwachungs-Audit: 1 PT	• Zertifizierungsaufwand mindestens 15 PT unabhängig vom Geltungsbereich (Größe des IT-Verbundes) ohne Mängelbehandlung und Rückfragen durch Zertifizierungsstelle, praktische Erfahrungen und Einschätzungen durch BSI selbst: Zertifizierungsaufwand von 14 bis 30 PT	• Zertifizierungsaufwand wird nach ISO 27006 kalkuliert und ist vorrangig abhängig von der Mitarbeiteranzahl des Geltungsbereiches • (Scopes), beginnt bei 5 PT für Erst-Audit (+-30% für konkrete Faktoren wie Komplexität, Standorte, etc.
Zertifizierungs-stellen	• DQS GmbH	• BSI als einzige Zertifizierungsstelle	• Zehn akkreditierte Zertifizierungsstellen frei wählbar
Risikoanalyse	• Nur immanente Risikoanalyse für geringen bis mittleren Schutzbedarf, bei einem höheren Schutzbedarf wird eine andere Methode zur Risikoanalyse empfohlen	• Nur für geringen bis mittleren Schutzbedarf, • Risikoanalyse mit 100-3 bzw. 200-3, • andere Risikoanalysen ebenfalls zulässig	• frei Wahl der Methode, vollständige Risikoanalyse nach ISO/IEC 27005, • vorangestellte Risikoanalyse
Regelkreis	• Regelkreis mit PDCA-Ansatz, • Eher Momentaufnahme ohne Risikomanagement	• Regelkreis mit PDCA-Ansatz, jedoch Verbesserungsmaßnahmen erfolgen nur durch BSI selbst, Bausteine in sich geschlossen • zuerst Maßnahmen, dann Konzept	• Vollständiger Regelkreis mit kontinuierlichen Verbesserungsmaßnahmen, • PDCA-Zyklus ist in der Risikoanalyse integriert

Abbildung 17: Gegenüberstellung der priorisierten Vorgehensmodelle im ISMS-Umfeld

6 Bewertungsmatrix

In diesem Kapitel werden die priorisierten Vorgehensweisen, nach ISIS 12, nach der ISO/IEC 2700x Normenfamilie und nach dem IT-Grundschutz, um ein ISMS an allen bayerischen Hochschulen und Universitäten zu erstellen, mit Hilfe einer Nutzwertanalyse bewertet. Dadurch erschafft dieser Forschungsbericht eine fundierte Grundlage, um eine geeignete Vorgehensweise zur Erstellung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS für alle bayerischen Universitäten- und Hochschulen erstellen zu können. Basierend auf den Anforderungen im Universitäts-und Hochschulbereich, werden die im Kapitel vier beschriebenen Vorgehensweisen mit ihren jeweiligen Stärken und Schwächen analysiert und bewertet. Die drei priorisierten Entscheidungsalternativen sind alle im unterschiedlichen Maße geeignet, ein ISMS zu etablieren. Da die Vorgehensweise nach der Innovationsstiftung Bayerische Kommune dieses Kriterium nicht erfüllt, wird diese Alternative von der nachfolgenden Bewertung ausgeschlossen. Anhand für den Universitäts- und Hochschulbereich relevanter Kriterien werden die verschiedenen Entscheidungsalternativen bewertet.

6.1 Methode

Mit Hilfe einer Nutzwertanalyse werden die verschiedenen Vorgehensweisen anhand von spezifischen Kriterien bewertet. Dabei erhält jede einzelne Alternative einen Nutzwert, mittels dessen eine Priorisierung und somit eine Entscheidung erfolgen kann. Zu Beginn werden die relevanten Entscheidungsalternativen ausgewählt. Anschließend werden für die Entscheidungsfindung relevante Kriterien definiert. Dabei ist zu beachten, dass die Summe der Kriterien zur vollständigen Lösung des Entscheidungsproblems führt. Ebenso sollte jedes Kriterium relevant für die Entscheidungsfindung sein und die Bewertung jedes Kriteriums reproduzierbar. Nachdem alle für die Entscheidungsfindung relevante Kriterien identifiziert wurden, sind diese entsprechend ihrer Bedeutung zu gewichten. Die Summe aller Gewichte der Kriterien entspricht genau 100 %. Anschließend werden den Kriterien Wertnoten, etwa Schulnoten in umgekehrter Reihenfolge von 1 („Kriterium ist sehr schlecht erfüllt“) bis 6 („Kriterium ist sehr gut erfüllt“) zugeteilt. Es ist wichtig, dass die Skala eindeutig und verständlich ist. So bedeutet:

- 1: Kriterium ist nicht bzw. ungenügend erfüllt
- 2: Kriterium ist nur unter Inkaufnahme wesentlicher Mängel erfüllt
- 3: Kriterium ist ausreichend erfüllt
- 4: Kriterium ist in befriedigendem Maße erfüllt
- 5: Kriterium ist gut erfüllt
- 6: Kriterium ist sehr gut erfüllt

Bei jedem Kriterium wird beurteilt, inwieweit dieses für die jeweiligen Entscheidungsalternativen zutrifft bzw. nützlich ist. Anschließend werden für jedes Kriterium, die Wertnoten mit der Kriteriengewichtung multipliziert. Dabei drücken diese einzelnen Produkte (Teilnutzwerte) aus, wie gut eine Entscheidungsvariante das jeweilige Kriterium erfüllt. Abschließend werden für jede Entscheidungsalternative, die zuvor errechneten Teilnutzwerte addiert. Diese Summe wird als Nutzwert bezeichnet. Anhand dieses Nutzwertes lassen sich die Entscheidungsalternativen bewerten.[60],[61],[62].

6.2 Kriterien

6.2.1 Zielgruppe

Das Kriterium Zielgruppe umfasst die Anwendbarkeit der jeweiligen Vorgehensweise im Universitäts- und Hochschulbereich. Das Kriterium spiegelt wieder, in weit sich die jeweilige Alternative für den wissensintensiven Bereich, in dem hochsensible Daten mit hohem oder sehr hohem Schutzbedarf, wie Forschungsergebnisse, Prüfungs-und Zeugnisdaten existieren, eignet. Die Definition einer Standardbehörde im Sinne des BSI kann diese Zielgruppe nicht vollständig umfassen. Selbst bei einer getrennten Betrachtung jeder Hochschule bzw. jeder Universität existieren mehr als 500 Hochschul- bzw. Universitätsangehörige. Weder ist eine homogene IT-Basisinfrastruktur noch sind über öffentliche Netze geschützt angebundene Außenstellen vorhanden. Die Definition eines geringen oder mittleren Schutzbedarfes ist in einem wissensintensiven Bereich, in dem sensiblen Daten das wertvollste und schützend werteste Gut sind, ausgeschlossen. Wie Kapitel 2.4 beschreibt, existieren Hochverfügbarkeitsanforderungen an IT-Systeme und sogar der Begriff KRITIS in diesem wissensintensiven Bereich ließe sich unter bestimmten Voraussetzungen bejahen. Es spielt eine entscheidende Rolle für welche Zielgruppe die jeweilige Lösungsalternative zur Etablierung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS an allen bayerischen Hochschulen und Universitäten am besten geeignet ist.

Da dieses Kriterium die ausschlagebenste Komponente bei der Auswahl der Alternative einnimmt, wird das Kriterium mit 20 % gewichtet.

6.2.2 Ressourceneffizienz

Das Kriterium Ressourceneffizienz ist bei der Einführung, Etablierung, Kontrolle und Verbesserung eines ISMS eine sehr essentielle Komponente und bekommt daher mit 15 % eine entsprechend hohe Gewichtung.

Mit diesem Kriterium wird zum einen der interne Zeit-, Kosten-und Personalaufwand für die Einführung, Implementierung und Aufrechterhaltung eines ISMS bemessen. Zum anderen umfasst dieses Kriterium den externen Aufwand für eine Zertifizierung, der sich bei den verschiedenen Lösungsalternativen deutlich unterscheidet. Beim internen Ressourcenaufwand sind sowohl einmalige strategische Aufgaben (z.B. Bildung des Sicherheitsteams, Erstellung eines Informationssicherheitskonzeptes und einer IT-Sicherheitspolicy), als auch dauerhafte, regelmäßige organisatorische (z.B. Überprüfung von Sicherheitskonzepten, IT-Notfallkonzepts sowie die Sensibilisierung der Mitarbeiter) Tätigkeitsschwerpunkte zu berücksichtigen. Um ein ISMS einführen und aufrechterhalten zu können, sollte sowohl der IT-Sicherheitsbeauftragter (Vertreter) als auch das IT-Sicherheitsteam über ausreichende spezifische Fachkenntnisse verfügen, was wiederum mit hohen Personalkosten verbunden ist. Personalkosten sind ein substantieller Bestandteil der Gesamtkosten. Im öffentlichen Bereich ist der Ressourcenaspekt, wie Personal, Zeit, Kosten, auf Grund der Wirtschaftlichkeitsbetrachtung und der Haushaltsplanung in Bezug auf Drittmittelverwendung ein sehr ausschlaggebender Faktor, so dass dieses Kriterium diesen hohen Stellenwert wiederspiegelt.[63]

6.2.3 Skalierbarkeit

Das Kriterium Skalierbarkeit nimmt einen strategisch bedeutenden Platz in der Bewertung des jeweiligen Lösungsansatzes ein. In einem sich so rasant entwickelnden Umfeld ist es von großer Bedeutung zu prüfen, wie skalierbar die jeweilige Entscheidungsalternative ist. Unter dem Kriterium Skalierbarkeit ist sowohl der quantitative als auch der qualitative Umfang zu verstehen. Durch dieses Kriterium wird einerseits geprüft, wie sich die unterschiedlichen Entscheidungsalternativen im Falle einer quantitativen Veränderung (z.B. Erhöhung der Anzahl der Hochschulen oder Universitäten, Steigerung der Universitäts-und Hochschulangehörigen) und andererseits in der qualitativen Modifikation (z.B. Änderung der Bedrohungen und Schwachstellen, Änderung des Schutzbedarfs) verhalten. Auf Grund der Wichtigkeit des Kriteriums wird die Skalierbarkeit wird mit 13% bewertet.

6.2.4 Risikomanagement

Ein wirksames Risikomanagement ist der zentrale Kern eines erfolgreichen ISMS.[64] Aus diesem Grund wird das Kriterium Risikomanagement als sehr signifikante Komponente in der Bewertungsmatrix mit 19 % gewichtet. Dieses Kriterium bewertet, in wie weit die unterschiedlichen Entscheidungsalternativen die systematischen Vorgehensweisen erfüllen, um alle potentiellen Risiken zu identifizieren, zu bewerten und die hierauf aufbauenden entsprechenden Maßnahmen zur Risikobehandlung, Risikoüberwachung und zur Überprüfung von Risiken durchzuführen. Daneben wird die Früherkennung von Risiken sowie zielgerichtete und anforderungskonforme Steuerung, das Reporting und die Kommunikation von Risiken überprüft, sowohl auf strategischer als auf operativer Ebene. Der Risikomanagementprozess unterliegt mit seinem iterativen Charakter ständigen Verbesserungsmaßnahmen. Wie [65] beschreibt sind beispielsweise „Virus infection for the hosts" und "Phishing" im Universitäts-und Hochschulbereich sehr ernstzunehmende Risiken, die mit einem erfolgreichem Risikomanagement behandelt werden können.

6.2.5 Internationale Bedeutung

Die internationale Bedeutung der vorgestellten Vorgehensweisen ist in einem wissensintensiven Universitäts- und Hochschulbereich von weitreichender Signifikanz. Gerade in Bezug auf den Bologna-Prozess, indem die Förderung von räumlicher und kultureller Mobilität, von internationaler Wettbewerbsfähigkeit sowie von Beschäftigungsfähigkeit durch eine Verzahnung des europäischen Hochschulraumes mit dem europäischen Forschungsraum, insbesondere durch die Eingliederung der Promotionsphase etabliert wurde, ist eine internationale Anerkennung eines ISMS von sehr großer Wichtigkeit. Die Etablierung, die Implementierung und die Instandhaltung eines wirksamen ISMS im Universitäts-und Hochschulbereich sollte international anerkannt sein, insbesondere vor dem Hintergrund einer angestrebten Zertifizierung. Der Bewertungsmaßstab richtet sich danach, wie groß die internationale Anerkennung der jeweiligen Alternative ist. Aus diesem Grund wird dieses Kriterium mit 12 % bewertet.

6.2.6 Toolunterstützung

Eine erfolgreiche Einführung, Umsetzung und Aufrechterhaltung eines ISMS in einem wissensintensiven Bereich benötigt eine adäquate Toolunterstützung. Angefangen von einem Dokumentenverwaltungssystem bis hin zur aufwendigen Prozessplanung mit einem aussagekräftigen Risikomanagementsystem sollte ein ISMS durch leistungsstarke und benutzerfreundliche Werkzeuge unterstützt werden. Dieses Kriterium prüft vordergründig das Vorhandensein entsprechender Tools zu jeder Entscheidungsalternative. Wie Kapitel 2.2 beschreibt, sind die detaillierten Inhalte der Tools nicht Untersuchungsgegenstand dieses Forschungsberichts. Somit wird das Kriterium Toolunterstützung wird 5 % mit beziffert.

6.2.7 Vorgegebene Prozessschritte

Vorgegebene Prozessschritte dienen dazu, den Anwender systematisch und strukturiert durch den gesamten Prozess zu leiten. Mit Hilfe vorgegebener Schritte lässt sich zum einen der Gesamtprozess verkürzen und zum anderen sind oftmals weniger tiefgreifende Detailkenntnisse erforderlich, als wenn der Prozess komplett neu zu etablieren ist. Allerdings sollten vorgegebene Prozessschritte so flexibel gestaltet sein, dass situationsabhängig Erweiterungen bzw. Verkürzungen des Prozesses durchgeführt werden können. Da vorgegebene Prozessschritte als Orientierungshilfe fungieren können und somit den Gesamtumfang des Prozesses zur Einführung und Aufrechterhaltung eines ISMS reduzieren können, wird dieses Kriterium mit 5 % gewichtet.

6.2.8 Mindestanforderungen IT-PLR

Wie dieser Forschungsbericht bereits im Kapitel 3.1.1 beschrieb, ist der IT-Planungsrat (IT-PLR) u.a. für den Aufbau und die Etablierung des Informationssicherheitsmanagements in den öffentlichen Verwaltungen verantwortlich. Anlehnend daran wird überprüft, inwieweit die Mindestanforderungen an ein ISMS, im Universitäts-und Hochschulbereich von den Entscheidungsalternativen erfüllt werden. Diesem Kriterium werden 5 % zugeschrieben.

6.3 Bewertung

In der nachfolgenden Bewertungsmatrix werden sowohl die explizit aufgegliederten Teilnutzwerte jeder vorgestellten Entscheidungsalternative, als auch der Gesamtnutzwert jeder Variante aufgezeigt. Dadurch sind zum einen die Stärken und Schwächen der jeweiligen Vorgehensweise ersichtlich, und zum anderen ist eine Gesamtbeurteilung möglich. Die durchgeführte Nutzwertanalyse zeigt, dass die Entscheidungsalternative ISO/IEC 2700x mit 4.80 den höchsten Nutzwert aufweist. Den zweithöchsten Nutzwert von 3,10 besitzt die Entscheidungsalternative ISIS 12, dicht gefolgt von der dritten Alternative IT-Grundschutz mit 3,08. Um eine aussagekräftige Bewertung mit einem fundierten Ergebnis abgeben zu können, müssen zum einen die Stärken und Schwächen der drei Entscheidungsvarianten explizit betrachtet werden, und zum anderen muss der Hintergrund der Wertnotenvergabe der einzelnen Kriterien je Alternative detailliert analysiert werden. Anhand der Bewertungsmatrix werden folgende Ergebnisse hervorgebracht:

Kriterien	Gewichtung	ISIS 12		IT-Grundschutz		ISO/IEC 2700x	
	G	P	W	P	W	P	W
Zielgruppe	21%	1	0,21	5	1,05	6	1,26
Ressourceneffizienz	15%	6	0,9	2	0,3	1	0,15
Skalierbarkeit	13%	6	0,78	2	0,26	6	0,78
Risikomanagement	19%	1	0,19	2	0,38	6	1,14
Internationale Bedeutung	12%	1	0,12	2	0,24	6	0,72
Toolunterstützung	10%	3	0,3	4	0,4	4	0,4
Vorgegebene Prozessschritte	5%	6	0,3	3	0,15	1	0,05
Mindestanforderungen IT-PLR	5%	6	0,3	6	0,3	6	0,3
Summe	100%		3,10		3,08		4,80

Abbildung 18: Bewertungsmatrix (Quelle: eigene Erstellung)

Die Lösungsalternative ISIS 12 erfüllt das Kriterium Zielgruppe im Universitäts-und Hochschulbereich gar nicht bzw. nur sehr ungenügend. Zwar ist das ISIS 12 Vorgehensmodell für KMU und kleinere öffentliche Verwaltungen in Form einer Standartbehörde optimiert, jedoch nicht für einen wissensintensiven Universitäts-und Hochschulbereich. ISIS 12 kann die geforderte Zielgruppe mit der Definition Standardbehörde nicht vollständig abdecken. Denn in einem wissensintensiven Universitäts-und Hochschulbereich herrschen hochsensible Daten vor, wie beispielsweise Forschungsergebnisse, personenbezogene Hochschul-und Universitätsangehörigen Daten, Firmendaten, Prüfungsergebnisse oder Zeugnisdaten, so dass der Schutzbedarf der Daten nicht mehr als normal eingestuft werden kann. Zudem sind selbst bei einer getrennten Betrachtung jeder Hochschule bzw. jeder Universität mehr als 500 Hochschul-bzw. Universitätsangehörige vorhanden. Daneben existieren im Hochschul- und Universitätsbereich weder eine homogene IT-Basisinfrastruktur noch sind über öffentliche Netze geschützt angebundene Außenstellen vorhanden. Greifen tausende Studenten auf eine Anwendung (z.B. Webserver für Emailverkehr, E-learning, Prüfungsergebnisse) zu, bestehen Hochverfügbarkeitsanforderungen an IT-Systeme. Da sich sogar der Begriff KRITIS in diesem wissensintensiven Bereich unter bestimmten Voraussetzungen (siehe Kapitel 2.4) bejahen ließe, erfüllt die Entscheidungsalternative ISIS 12 das Kriterium der geforderten Zielgruppe Hochschul-und Universitätsbereich gar nicht bzw. nur sehr ungenügend. Wohingegen das Kriterium Ressourcen von dieser Entscheidungsalternative sehr gut erfüllt wird. Auf Grund des reduzierten Maßnahmenkatalogs und der vorgegebenen Prozessschritte lässt sich der interne Zeit,- Kosten,- und Personalaufwand im Vergleich zu den anderen Alternativen verhältnismäßig gering halten. Betrachtet man den internen

Aufwand, ergibt sich aus der Fallstudie für eine Standardbehörde [17] nach der BSI IT-Grundschutz Vorgehensweise, ein Aufwand für Personalressourcen von 160 Personentage (PT) für einmalige, strategische Arbeiten und für regelmäßige, operative Arbeiten von 180 PT mit entsprechenden Zuschlägen für bestimmte Kriterien. Da bei der ISIS 12 Vorgehensweise ein vom BSI abgeleiteter, aber stark reduzierter Maßnahmenkatalog existiert, kann man folglich davon ausgehen, dass der aufzuwendende Ressourcenaufwand ebenfalls entsprechend geringer ausfällt. Daneben lässt sich der Prozess durch die vorgegebenen Prozessschritte in der ISIS 12 Vorgehensweise verkürzen, was wiederum eine zusätzliche Ressourceneinsparung mit sich bringt. Zudem ist der externe Ressourcenaufwand für eine mögliche Zertifizierung, wie in analysiert [16],[17] wurde, mit zwei PT für ein Erst-Zertifizierungs-Audit und einem PT für ein Überwachungs-Audit relativ gering. Im Universitäts- und Hochschulbereich ist der Ressourcenaspekt, wie Personal, Zeit, Kosten, auf Grund der Wirtschaftlichkeitsbetrachtung und der Haushaltsplanung von großer Bedeutung. Die ISIS 12 Vorgehensweise erfüllt dieses Kriterium sehr gut. Das Kriterium Skalierbarkeit wird von der ISIS 12 Vorgehensweise ebenfalls sehr gut erfüllt. Die ISIS 12 Vorgehensweise lässt sich sowohl in quantitativer (z.B. Anzahl der Mitarbeiter), als auch in qualitativer Hinsicht (z.B. Änderung der Bedrohungen und Schwachstellen, Änderung des Schutzbedarfs) modifizieren. Ebenso lassen sich spezielle, benutzerdefinierte Bausteine beliebig in den vordefinierten Katalog integrieren. Dieser flexible modulare Ansatz ist gerade in einem sich rasant entwickeltem Umfeld, im dem wissenskonzentrierte Daten, das wertvollste Gut sind, von weitreichender Bedeutung. Aus diesem Grund erfüllt die ISIS 12 Alternative dieses Kriterium sehr gut. Allerdings wird das Kriterium Risikomanagement von der ISIS 12 Lösungsalternative auf Grund der Designkriterien nur sehr ungenügend erfüllt. Die ISIS 12 Vorgehensweise, die sich stark an den BSI Grundschutz orientiert, beinhaltet lediglich eine immanente Risikoanalyse. Die in den ersten beiden Phasen umzusetzenden Sicherheitsmaßnahmen decken lediglich die Grundgefährdungen für einen geringen bis mittleren Schutzbedarf ab. Da in einem wissensintensiven Bereich der Schutzbedarf der Daten nicht mehr als gering oder mittel eingestuft werden kann, erfüllt die immanente Risikoanalyse der ISIS 12 Vorgehensweise das Kriterium für den Hochschul-und Universitätsbereich nicht bzw. nur sehr ungenügend. Denn Ziel eines erfolgreichen Risikomanagements in Form einer aussagekräftigen Risikoanalyse ist es, alle relevanten Gefährdungen zu identifizieren, die daraus entstehenden Risiken abzuschätzen und mit Hilfe von korrespondierenden Gegenmaßnahmen die Risiken auf ein akzeptables Maß zu reduzieren und die Restrisiken transparent zu machen. Zudem verfolgt ein wirksames Risikomanagement einen iterativen Ansatz mit einem ständigen Verbesserungsprozess, der in der ISIS 12 Vorgehensweise in dieser Form auch nicht gegeben ist. Da jedoch ein wirksames Risikomanagement der Kern eines erfolgreichen ISMS ist, erfüllt ISIS 12 dieses Kriterium nur sehr nur sehr ungenügend. Das Kriterium internationale Bedeutung wird von der Entscheidungsalternative ISIS 12 nur sehr ungenügend erfüllt. Die Vorgehensweise nach ISIS 12 ist besitzt im deutschsprachigen Raum bei mittelständischen Unternehmen und teilweise bei kleineren öffentlichen Verwaltungen steigenden Bekanntheitsgrad. Allerdings findet diese Vorgehensweise auf internationaler Ebene für die Erstellung, Implementierung, Instandhaltung und Verbesserung eines ISMS keine Anerkennung. Da im Hochschul-und Universitätsbereich, gerade vor dem Bologna-Hintergrund, eine internationale Anerkennung von weitreichender Bedeutung ist, wird dieses Kriterium von ISIS 12 nicht bzw. nur sehr ungenügend erfüllt. Für die Entscheidungsalternative ISIS 12 existiert ein eigenes ISIS12-Softwaretool. Daneben steht ein kommerzielles Tool (ibi Systems) zur Verfügung. Der Tooleinsatz wird empfohlen, wenn auch eine Anwendung bzw. Zertifizierung ohne ISIS 12 Tool möglich, aber sehr aufwendig ist. Somit erfüllt ISIS 12 das Kriterium ausreichend. Das nächste Kriterium vorgegebene Prozessschritte wird von dem ISIS 12 Ansatz sehr gut erfüllt. So wird der ISIS 12 Anwender mit Hilfe der 12 sequentiellen vorgegebenen Prozessschritte mit einem Top-Down Ansatz durch die Erstellung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS geführt.

Dabei werden diese 12 Prozessschritte wiederum in drei Hauptphasen (Initialisierungsphase, Festlegung der Aufbau- und Ablauforganisation, Entwicklung und Umsetzung ISIS12-Konzept) gruppiert, die von dem Anwender chronologisch, insbesondere die ersten beiden Phasen, vollzogen werden. Durch diesen geführten Prozessansatz der ISIS 12 Vorgehensweise lässt sich der Gesamtprozess verkürzen, indem die durchzuführenden Prozessschritte bereits etabliert sind und nicht erst neu kreiert werden müssen. Daneben sind durch diese konkreten Handlungsempfehlungen zum Teil weniger tiefgreifende Detailkenntnisse erforderlich, als wenn der Prozess komplett neu erstellt werden muss. Ebenso wird das Kriterium Mindestanforderungen des IT-PLR durch die ISIS 12 Methode sehr gut erfüllt. Da der IT-PLR, u.a. für den Aufbau und die Etablierung des Informationssicherheitsmanagements in den öffentlichen Verwaltungen verantwortlich ist, wird mit Hilfe diesem Kriterium analysiert, inwieweit die Mindestanforderungen an ein ISMS im Universitäts- und Hochschulbereich durch die ISIS 12 Methode eingehalten werden. Die ISIS 12 Methode enthält die im Kapitel 3.1.1 beschriebenen Mindestanforderungen an ein ISMS. Die letztgenannten Anforderungen (Anforderungsgerechte und einheitliche Fortbildung der Informationssicherheitsbeauftragten (ISB), Jahrestagungen der ISB zum gegenseitigen Erfahrungsaustausch) sind keine direkten Anforderungen an ein ISMS, sondern dienen viel mehr als Qualifizierungsmaßnahmen der beruflichen Kompetenzen von Informationssicherheitsbeauftragten. Somit sind diese in dem ISIS 12 Ansatz nur teilweise vorhanden.

Die Entscheidungsalternative IT-Grundschutz des BSI erfüllt das Kriterium Zielgruppe gut. Der IT-Grundschutz ist prinzipiell uneingeschränkt, insbesondere im öffentlichen Sektor, anwendbar. Da der Universitäts-und Hochschulbereich auch Teil der öffentlichen Verwaltung ist, kann der IT-Grundschutz des BSI dort generell angewendet werden. Allerdings geht der IT-Grundschutz bei der Anwendung der Standards 100-1 und 100-2 und 100-4 erstmal von einem geringen bis normalen Schutzbedarf der Daten aus. Wie bereits bei der Bewertung der ISIS 12 Lösungsalternative erläutert, Ist in einem derartig wissenskonzentrierten Umfeld, wie dem Universitäts-und Hochschulbereich, ein geringer oder mittlerer Schutzbedarf der Daten nicht mehr ausreichend. Hochsensible Daten wie Forschungsergebnisse, personenbezogene Angehörige Daten oder Prüfungsergebnisse fordern einen hohen beziehungsweise sehr hohen Schutzbedarf. Ist ein mindestens hoher Schutzbedarf gegeben, behilft sich der IT-Grundschutz mit dem Standard 100-3 bzw. 200-3. Hier wird angenommen, dass der vorhandene Pool an Sicherheitsmaßnahmen ausreichend ist. Existieren standardabweichende Gefährdungen, die entsprechende korrespondierende Sicherheitsmaßnahmen erfordern, ist der IT-Grundschutz hier nicht ausreichend. Der IT-Grundschutz überlässt in diesem Fall die Wahl der erforderlichen Risikoanalyse dem Anwender. Der IT-Grundschutz kann somit als Einstiegsalternative adäquat angewendet werden. Wird im Laufe des Anwendungsprozesses des IT-Grundschutzes festgestellt, dass standardabweichende Gefährdungen existieren, die standardabweichende Sicherheitsmaßnahmen erfordern, kann auf eine andere Alternative ausgewichen werden und auf die bereits durchgeführten Prozessschritte des IT-Grundschutzes aufgebaut werden. Das nächste Kriterium Ressourceneffizienz wird von der Entscheidungsalternative IT-Grundschutz nur unter Inkaufnahme wesentlicher Mängel erfüllt. Der Ressourceneinsatz gliedert sich in externen und in einen internen Ressourceneinsatz. Wie die Fallstudie [17] beschreibt, sind für die Erstellung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS ein interner Ressourcenaufwand von 160 Personentage (PT) für einmalige, strategische Arbeiten und für regelmäßige, operative Arbeiten von 180 PT erforderlich. Diese Angaben beziehen sich auf die Definition einer Standardbehörde. Für die Faktoren, mehr als 500 Mitarbeiter, Grad der Heterogenität der IT-Landschaft und IT-Verfahren, Anzahl der zu betreuenden Außenstellen, Anteil der IT-Anwendungen mit einem Schutzbedarf höher als „normal“, und Hochverfügbarkeitsanforderungen an IT-Anwendungen werden entsprechende Zuschläge aufaddiert. Daneben ergibt sich für den externen

Ressourcenaufwand für eine mögliche Zertifizierung von mindestens 15 PT. Dieser gilt als unabhängig vom Geltungsbereich ohne Mängelbehandlung und Rückfragen durch Zertifizierungsstelle. Erfahrungsgemäß wird dieser Aufwand vom BSI auf 14 bis 30 PT geschätzt. Ausschlaggebend ist bei diesem Bewertungskriterium auch der sehr umfangreiche und aufwendige Baustein-und Maßnahmenkatalog des IT-Grundschutzes, dessen Auswahl und Bearbeitung einen hohen Zeit-, Kosten-und Personaleinsatz in Anspruch nimmt. Da die Prozessschritte, wie Kapitel 4.2 beschreibt, eher vage formuliert sind, ist die Prozesserstellung und Bearbeitung mit zusätzlichem Ressourcenaufwand verbunden. Wird der IT-Grundschutz anhand der Skalierbarkeit bewertet, wird er den Anforderungen an ein ISMS im Hochschul-und Universitätsbereich eher mäßig gerecht. Die Bausteine sind in sich geschlossen und können nur durch das BSI selbst verbessert und aktualisiert werden. Zudem sind die vorgefertigten Bausteine mit Sicherheitsmaßnahmen nur für Standardgefährdungen ausgelegt. Sollten sich, in einem derart rasant entwickelten wissensbasierten Bereich, neue standardabweichende Gefährdungen entwickeln, ist der IT-Grundschutz des BSI hier keine große Hilfe. Somit wird das Kriterium nur unter Inkaufnahme wesentlicher Mängel erfüllt. Ebenso wird das Kriterium Risikomanagement von der Entscheidungsalternative IT-Grundschutz nur unter Inkaufnahme wesentlicher Mängel erfüllt. Zum einen ist der Standard 100-1 und 100-2 nur für den geringen bis mittleren Schutzbedarf ausgerichtet, was bei einem wissensintensiven Hochschul- und Universitätsbereich nicht zielversprechend ist. Auch wenn der IT-Grundschutz bei hohem Schutzbedarf auf den Standard 100-3 beziehungsweise 200-3 verweist, geht der IT-Grundschutz davon aus, dass der vorhandene Pool an Standardsicherheitsmaßnahmen ausreichend ist. In diesem Fall wird eine nachgelagerte Sicherheitsanalyse durchgeführt, in der allgemeine Kategorien von Gefährdungen verwendet werden, so dass eine aufwendige Risikoanalyse entfallen kann. Zum anderen werden die verwendeten Grundschutz Bausteine als in sich geschlossen betrachtet. Ein iterativer Verbesserungsprozess kann durch den Grundschutzanwender nur schwer erfolgen, da Verbesserungen nur durch das BSI vollzogen werden. Jedoch spiegelt diese Vorgehensweise nicht den Kern eines wirksamen Risikomanagements mit einem iterativen Verbesserungsprozess. Sind standardabweichende Maßnahmen auf Grund standardabweichenden Gefährdungen erforderlich, ist der BSI nicht anwendbar. Jedoch überlässt der IT-Grundschutz die Wahl der zu verwendeten Risikoanalyse dem Anwender, so dass der IT-Grundschutz zumindest zur Identifikation aller Standardgefährdungen mit dazugehörigen Gegenmaßnahmen dienen kann. Der IT-Grundschutz besitzt im deutschsprachigen Raum, insbesondere im öffentlichen Sektor, einen relativ hohen Bekanntheitsgrad. Allerdings ist gerade vor dem Bologna Hintergrund eine internationale Anerkennung im Hochschul-und Universitätsbereich von großer Bedeutung. Die Etablierung, die Implementierung und die Aufrechterhaltung eines wirksamen ISMS im Universitäts-und Hochschulbereich sollte international anerkannt sein, insbesondere bei einer angestrebten Zertifizierung. Jedoch kann der IT-Grundschutz diese Anforderung nicht erfüllen. Dadurch wird dieses Kriterium nur unter Inkaufnahme wesentlicher Mängel erfüllt. Der IT-Grundschutz wurde durch das individuell für das BSI entwickelte Tool gstool unterstützt. Jedoch wurde der Vertrieb zum 31. Dezember 2014 und der Support bis Ende 2016 eingestellt [66]. Allerdings existieren ersatzweise andere lizensierte Tools wie z.B. Sidoc ® -Sicherheitsmanagement, INDART® Professional, Verinice Open Source ISMS Tool, HiScout Grundschutz um die Vorgehensweise nach IT-Grundschutz zu unterstützen, so dass dieses Kriterium im befriedigenden Maße erfüllt wird. Die Vorgehensweise nach IT-Grundschutz enthält mit dem im Kapitel 4.2 beschriebenen Prozess eine vage geführte Prozessstruktur. Der Anwender kann die vorgegebenen Prozessschritte wie Initiierung des Sicherheitsprozesses, Erstellung einer Sicherheitskonzeption, Umsetzung der Sicherheitskonzeption und Aufrechterhaltung und Verbesserung als grobe Orientierungshilfe betrachten. Allerdings wird der Anwender im Vergleich zu anderen Entscheidungsalternativen nicht so detailliert durch den Prozess

geführt. Zwar muss der Anwender den Prozess nicht komplett neu erfinden, jedoch exakt vorgegebene Prozessschritte existieren bei dieser Lösungsalternative nicht. Somit wird das Kriterium ausreichend erfüllt. Das letzte Kriterium Mindestanforderung an ein ISMS durch den IT-PLR werden mit der IT-Grundschutzvorgehensweise sehr gut erfüllt. Der IT-Grundschutz beinhaltet alle im Kapitel 3.1.1 geforderten Mindestanforderungen des IT-PLR. Da die letztgenannten Anforderungen (Anforderungsgerechte und einheitliche Fortbildung der Informationssicherheitsbeauftragten (ISB), Jahrestagungen der ISB zum gegenseitigen Erfahrungsaustausch) keine direkten Anforderungen an ein ISMS sind, sondern viel mehr als Qualifizierungsmaßnahmen der beruflichen Kompetenzen von Informationssicherheitsbeauftragten dienen, sind diese Anforderungen auch nur teilweise im IT-Grundschutz vorhanden.

Die ISO/IEC Normenfamilie 2700x erfüllt das Kriterium Zielgruppe im Universitäts-und Hochschulbereich sehr gut, da sie uneingeschränkt anwendbar ist. Diese Lösungsmöglichkeit ist sowohl für geringen als auch für sehr hohen Schutzbedarf geeignet. Da im Universitäts-und Hochschulbereich mit hochsensiblen Daten wie beispielsweise Forschungsergebnissen, Prüfungsleistungen oder personenbezogene Daten hantiert wird, folglich ein mindestens hoher beziehungsweiser sehr hoher Schutzbedarf verlangt wird, entspricht diese Entscheidungsalternative den Anforderungen dieses Kriterium gänzlich. Die Einschränkungen einer Standardbehörde werden bei dieser Alternative außer Acht gelassen. So ist beispielsweise die Forderung nach einer maximalen Anzahl von 500 Angehörigen, einer homogene IT-Basisinfrastruktur, über öffentliche Netze geschützt angebundene Außenstellen und keine Hochverfügbarkeitsanforderungen an IT-Systeme bedeutungslos. Sogar die Definition KRITS kann mit dieser Entscheidungsvariante abgedeckt werden. Somit ist es bedeutungslos, ob der wissensintensiven Universitäts-und Hochschulbereich unter bestimmten Voraussetzungen (siehe Kapitel 2.4) unter den Begriff KRITIS fallen kann. Die Erstellung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS an bayerischen Hochschulen und Universitäten wird mit dieser Entscheidungsalternative in Bezug auf das Kriterium Zielgruppe vollkommen abgedeckt. Allerdings wird das Kriterium Ressourceneinsatz von der ISO/IEC 2700x Entscheidungsalternative nur ungenügend erfüllt. Sowohl durch den sehr abstrakten Charakter ohne vorgeschriebene technische Umsetzungsdetails, als auch durch den eher führungslosen Umsetzungsprozess, ist der Ressourcenaufwand sehr hoch. Es erfordert hochqualifiziertes Personal ein ISMS in einem wissensintensiven Bereich zu erstellen, zu implementieren, aufrechtzuerhalten und zu verbessern. Diese Entscheidungsalternative enthält 114 generische Maßnahmen und Kontrollen, die in 14 Kontrollgruppen unterteilt sind. Jedoch sind diese Maßnahmen und Kontrollen nicht abschließend und dienen für hochqualifizierte Fachkräfte eher als Orientierungshilfe denn als konkrete angeleitete Umsetzungshilfe. Durch den generischen Charakter bietet diese Lösungsalternative eher ein Sammelsurium möglichen Maßnahmen und Kontrollen im Umfeld eines ISMS, als exakt vorgegebene Prozessschritte. Somit muss ein Prozess im Bereich eines ISMS für den Hochschul-und Universitätsbereich erst neu etabliert werden. Dadurch entsteht eine hoher Zeit-, Kosten- und Personalaufwand. Hochqualifizierte Personalressourcen sind mit hohen Kosten verbunden. Darüber hinaus ist der externe Ressourcenaufwand für eine Zertifizierung, der nach ISO 27006 kalkuliert wird und vorrangig von der Mitarbeiteranzahl des Geltungsbereiches abhängig ist, mit 5 PT für das Erst-Audit (+-30% für konkrete Faktoren wie Komplexität, Standorte, usw.) verhältnismäßig sehr hoch. Im Universitäts-und Hochschulbereich ist der Ressourcenaspekt auf Grund der Wirtschaftlichkeitsbetrachtung und der Haushaltsplanung von großer Relevanz. Das Kriterium Skalierbarkeit wird von der ISO/IEC 2700x Normenfamilie sehr gut erfüllt. So lassen sich jederzeit Änderungen sowohl in quantitativer (z.B. Änderung der Anzahl der Hochschulen oder Universitäten, Änderung der Anzahl der Universitäts-und Hochschulangehörigen), als auch in qualitativer (z.B. Änderung der Bedrohungen und Schwachstellen, Änderung des Schutzbedarfs) Hinsicht vornehmen.

Daneben sind die Maßnahmen und Kontrollen nicht abschließend und können beliebig situationsabhängig erweitert beziehungsweise angepasst werden. Gerade in einem sich so schnell entwickelnden wissensintensiven Bereich, ist es von enorm großer Bedeutung, dass eine flexible situationsabhängige Reaktion erfolgen kann. Die Entscheidungsvariante der ISO/IEC 2700x Normenfamilie erfüllt das Kriterium Risikomanagement sehr gut. Die ISO/IEC 27005 enthält ein vollumfängliches Risikomanagement mit einer vorangestellten Risikoanalyse. Das Risikomanagement wird, wie dieser Forschungsbericht im Kapitel 3.2.1 beschreibt, im Sinne des PDCA-Zyklus nach Demig durchgeführt. Dabei sind die einzelnen Schritte wie die Definition der Rahmenbedingungen, die Risikobeurteilung, die Identifizierung von Risiken, das Abschätzung von Risiken, das Auswerten von Risiken, die Risikobehandlung, die Risikoakzeptanz sowie die Risikokommunikation, die Risikoüberwachung und die Verbesserung als iterativer Prozess durchzuführen. Das Risikomanagement nach der Iso/IEC 27005 Entscheidungsvariante ist für einen geringen bis mittleren, aber auch insbesondere für einen hohen bis sehr hohen Schutzbedarf anwendbar. Diese Eigenschaft ist vor dem Hintergrund eines wissensintensiven Bereichs, indem Daten mit hohen beziehungsweise sehr hohen Schutzbedarf existieren, von sehr großer Wichtigkeit. Durch diesen iterativen Ansatz ist es möglich, sehr zeitnah auf Änderung jeglicher Hinsicht wie beispielsweise Änderung des Kontextes, der Bedrohungen, der Risiken, zu reagieren und Verbesserungsmaßnahmen durchzuführen. Zudem lässt sich dieser Risikomanagementansatz individuell, auch auf standardabweichende Gefährdungen, anpassen. Ob dabei eine quantitative oder qualitative Risikoanalysemethode durchgeführt wird, liegt in der Entscheidung des Anwenders. Da im Universitäts-und Hochschulbereich hochsensiblen Daten existieren, die einen hohen bis sehr hohen Schutzbedarf verlangen, ist diese Entscheidungsalternative sehr gut geeignet ein Risikomanagement durchzuführen. In diesem sich sehr rasant entwickelnden wissensintensiven Bereich ist es darüber hinaus von weitreichender Bedeutung, wenn Änderungen, insbesondere standardabweichende, frühzeitig identifiziert werden können und somit zeitnah darauf reagiert werden kann. Die ISO/IEC 2700x Normenfamilie ist ein internationaler Standard, der international uneingeschränkte Anerkennung findet. Da gerade im Universitäts-und Hochschulbereich eine internationale Anerkennung, insbesondere vor dem Bologna Hintergrund, ein folgenreicher Einflussfaktor ist, wird das Kriterium internationale Bedeutung von der ISO/IEC 2700x Normenfamilie sehr gut erfüllt. Zudem sollte angesichts einer etwaigen erstrebten Zertifizierung eine internationale Anerkennung vorliegen. Auf dem Markt existieren einige Tools, wie beispielsweise ChaRMe, verinice oder ISMS Toolbox, die eine ISO/IEC 2700x Normenfamilie unterstützen [67]. Allerdings existieren erhebliche Differenzen in der Qualität und in den Kosten. Vor Beginn einer ISMS Einführung, insbesondere im Universitäts-und Hochschulbereich, sollten die verfügbaren Tools anhand geforderten Anforderungen analysiert werden. Auf Grund der Verfügbarkeit unterschiedlicher Werkzeuge zur ISMS Unterstützung wird dieses Kriterium von der ISO/IEC 2700x Normenfamilie in einem befriedigten Maße erfüllt. Da die ISO/IEC 2700x Normenfamilie die Prozessschritte nicht exakt vorgibt, sondern eher Anforderungen, Maßnahmen und Maßnahmenziele darlegt, wird das Kriterium vorgegebene Prozessschritte ungenügend erfüllt. Im Vergleich zu den anderen Entscheidungsalternativen existiert kein exakt vordefinierter geführter Prozess mit einzelnen konkreten Handlungsempfehlungen. Daher muss ein speziell für den Universitäts-und Hochschulbereich definierter Prozess erst neu erstellt werden. Diese neue Prozessdefinition setzt höheres qualifiziertes Fachwissen voraus, als wenn der gesamte Prozess mit konkreten Handlungsempfehlungen bereits exakt vorgegeben ist. Die im Kapitel 3.1.1 beschriebenen Mindestanforderungen an ein ISMS des IT-PLR werden von der ISO/IEC 2700x Normenfamilie eingehalten. Somit wird das Kriterium von der ISO/IEC 2700x Normenfamilie sehr gut erfüllt. Da die letztgenannten Anforderungen (Anforderungsgerechte und einheitliche Fortbildung der Informationssicherheitsbeauftragten (ISB), Jahrestagungen der ISB zum gegenseitigen

Erfahrungsaustausch) keine direkten Anforderungen an ein ISMS sind, sondern viel mehr als Qualifizierungsmaßnahmen der beruflichen Kompetenzen von Informationssicherheitsbeauftragten dienen, existieren diese Anforderungen auch nur teilweise in der ISO/IEC 2700x Normenfamilie.

Zusammengefasst lässt sich feststellen, dass die Entscheidungsalternative ISIS 12 ihre Stärken im Vergleich zu den Alternativen des IT-Grundschutzes und der Vorgehensweise nach ISO/IEC 2700x in einem wirtschaftlichen Ressourcenaufwand, in der Skalierbarkeit und in den vorgegebenen Prozessschritten aufweist, wohingegen ihre Schwächen in der Zielgruppenorientierung, dem Risikomanagement und in der internationalen Bedeutung liegen. Auf Grund der unterschiedlichen Gewichtung der einzelnen Kriterien besitzt jedoch die ISIS 12 Entscheidungsalternative für die Einführung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS im Universitäts-und Hochschulbereich den Nutzwert von 3,10 %. Anders als die ISIS 12 Entscheidungsalternative, weißt die Vorgehensweise des IT-Grundschutzes keine so deutlichen Stärken und Schwächen auf. Das Kriterium Zielgruppe wird gut erfüllt, wohingegen das Kriterien Ressourceneinsatz, Skalierbarkeit, Risikomanagement und internationale Bedeutung nur mit sehr mäßigem Erfolg erfüllt werden. Als Ergebnis dieser Bewertungsmatrix erhält die IT-Grundschutz-Vorgehensweise zur Einführung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS im Universitäts-und Hochschulbereich den geringsten Nutzwert von 3,08 %. Im Gegensatz dazu, besitzt die ISO/IEC 2700x Normenfamilie, als dritte Entscheidungsvariante zur Einführung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS im Universitäts-und Hochschulbereich den größten Nutzwert von 4,80 %. Die Stärken der ISO/IEC 2700x Normenfamilie liegen eindeutig in der Zielgruppenorientierung, der Skalierbarkeit, dem Risikomanagement und in der internationalen Bedeutung. Trotz des hohen Nutzwertes und den gewichtigen Stärken, weißt diese Entscheidungsalternativen auch Schwächen in dem Ressourceneinsatz und in dem Kriterium vorgegebene Prozessschritte auf. Auch wenn die Entscheidungsalternative ISO/IEC 2700x Normenfamilie den höchsten Nutzwert aufweist, ist es aus Synergieeffekten sehr sinnvoll, die jeweiligen Stärken der drei Modelle auszuwählen und die jeweiligen Schwächen zu vernachlässigen, um ein für den Universitäts-und Hochschulbereich geeignetes Modell zur Einführung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS erstellen zu können.

7 Zusammenfassung und Ausblick

In diesem Forschungsbericht wurde untersucht, welche Methoden und Vorgehensweise im Umfeld der Informationssicherheit geeignet sind, um ein adäquates Model zur Etablierung, Implementierung, Wartung und Verbesserung eines ISMS für den wissensintensiven Universitäts-und Hochschulbereich zu entwickeln.

In einem ersten Schritt wurden allgemeine Anforderungen der öffentlichen Verwaltung, insbesondere des Universitäts-und Hochschulbereich definiert. Dabei wurde festgestellt, dass bei einer bayernweiten Betrachtung aller Universitäten und Fachhochschulen nicht mehr von der Definition einer Standardbehörde (bis zu ca. 500 Mitarbeiter, eine möglichst homogene IT-Basisinfrastruktur, keine über öffentliche Netze ungeschützt angebundene Außenstellen, einen überwiegend normalen Schutzbedarf, keine Hochverfügbarkeitsanforderungen an IT-Systeme und keine kritischen Anwendungen (d.h. keine kritischen Infrastrukturen)) im Sinne des BSI ausgegangen werden kann. Basierend auf dieser Erkenntnis, werden die bereits vorhandenen Konzepte zur Erstellung, Implementierung, Instandhaltung und Verbesserung eines ISMS im Universitäts-und Hochschulbereich untersucht. Dabei wurde eruiert, dass zum einen alte Richtlinien vorhanden sind, die noch nicht zwischen Informationssicherheit und IT-Sicherheit differenzieren und zum anderen, dass der IT-Planungsrat (IT-PLR) Mindestanforderungen an ein ISMS für die öffentliche Verwaltung etablierte. In einem nächsten Schritt wurden die Inhalte der vorhandenen Standards, Normen und Konzepte im Umfeld der Informationssicherheit detailliert untersucht und analysiert. Anhand dessen wurden vier Vorgehensmodelle zur Erstellung, Implementierung, Instandhaltung und Verbesserung eines ISMS entwickelt. Hierbei stellte sich heraus, dass die Methoden der ISO/IEC 2700x Normenfamilie, des IT-Grundschutzes des BSI und der ISIS 12 Vorgehensweise geeignet sind, ein ISMS zu erstellen, zu implementieren, aufrechtzuerhalten und zu verbessern. Wohingegen die Methode der Arbeitshilfe der Bayerischen Innovationstiftung der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) dafür nicht geeignet ist. Als Folge dessen wurden im nächsten Schritt die drei priorisierten Vorgehensweisen gegenübergestellt. Basierend hierauf wurden die priorisierten Vorgehensmodelle im ISMS Umfeld anhand von den im Universitäts-und Hochschulbereich relevanten Kriterien, wie Zielgruppe, Ressourceneffizienz, Skalierbarkeit, Risikomanagement, internationale Bedeutung, Toolunterstützung, vorgegebene Prozessschritte sowie den Mindestanforderungen des IT-Planungsrates mit Hilfe einer Nutzwertanalyse bewertet. Hierbei erzielte dieser Forschungsbericht unter Verwendung der Nutzwertanalyse folgende Ergebnisse: Anhand für den Universitäts-und Hochschulbereich unterschiedlich gewichteten Kriterien erreicht die Vorgehensweise nach der ISO/IEC 2700x Normenfamilie mit 4,80 % den höchsten Nutzwert, den zweithöchsten Nutzwert von 3,10% erzielt die Methode ISIS 12, gefolgt von der Vorgehensweise des IT-Grundschutzes mit einem Nutzwert von 3,08 %. Dabei weißt die Vorgehensweise nach der ISIS 12 Methode ihre Stärken eindeutig in einem wirtschaftlichen Ressourcenaufwand, in der Skalierbarkeit und in den vorgegebenen Prozessschritten auf, wohingegen die Schwächen in den Kriterien Ressourceneinsatz, Skalierbarkeit, Risikomanagement und internationale Bedeutung liegen. Keine so eindeutigen Stärken und Schwächen besitzt die IT-Grundschutzvorgehensweise. Bei dieser Alternative wird das Kriterium Zielgruppe gut erfüllt, wohingegen die Kriterien Ressourceneinsatz, Skalierbarkeit, Risikomanagement und internationale Bedeutung nur mit sehr mäßigem Erfolg erfüllt werden. Im Kontrast dazu, werden die Kriterien Zielgruppenorientierung, Skalierbarkeit, Risikomanagement und internationalen Bedeutung von der dritten Alternative, der ISO/IEC 2700x Normenfamilie, sehr gut erfüllt. Allerdings besitzt auch diese Vorgehensweise trotz des höchsten Nutzwertes, Schwächen in den Kriterien Ressourceneinsatz und vorgegebene Prozessschritte.

Hieraus resultierend wird die Notwendigkeit einer speziell für den wissensintensiven Universitäts-und Hochschulbereich individuellen Lösung verdeutlicht, da von keiner untersuchten Lösungsalternative alle notwendigen Anforderungen vollkommen alleine abgedeckt werden. Um ein für den Universitäts- und Hochschulbereich geeignetes Modell zur Einführung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS erstellen zu können, ist es aus Synergieeffekten sinnvoll, die jeweiligen Stärken der drei Modelle auszuwählen und die jeweiligen Schwächen zu vernachlässigen.

Aus diesem Grund kann es trotz der Nicht-Erfüllung der Standardbehörden-Definition sinnvoll erscheinen, sich in der Anfangsphase (mindestens bis zum Schritt 5) nach den vorgegebenen Schritten der ISIS 12 Vorgehensweise zu orientieren, um die Initialisierungsarbeiten wie Erstellung einer Leitlinie, Sensibilisierung der Mitarbeiter resourcenoptimiert durchzuführen. Daneben kann die Aufbau- und Ablauforganisation, wie beispielsweise Aufbau eines Informationssicherheitsteams, Erstellung der IT-Dokumentation aus Prozessoptimierungsgründen weiterhin mit der ISIS 12 Vorgehensweise vollzogen werden. Zur Identifikation von reduzierten Standardgefährdungen kann die ISIS 12 Alternative als Einstiegshilfe auf Grund ihrer hohen Skalierbarkeit verwendet werden, auch wenn diese Alternative nur für den geringen bis mittleren Schutzbedarf vorgesehen ist. Stellt man während dieses Risikoidentifikationsprozesses fest, dass der Gefährdungs-und Maßnahmenpool nicht ausreichend ist, kann auf den umfangreicheren Bausteinpool des BSI IT-Grundschutzes ausgewichen werden. Allerdings ist dieser, zwar sehr umfangreiche Maßnahmenpool, auch nur für Standardgefährdungen, die grundsätzlich auch einen geringen bis mittleren Schutzbedarf abdecken, ausgerichtet. Bedarf es eines mindestens hohen Schutzbedarfes mit gleichzeitig standardabweichenden Gefährdungen, kann schließlich auf die Alternative der ISO/IEC 2700x Normenfamilie gewechselt werden. Damit kann mit Hilfe der Synergieeffekte auf die bereits durchgeführten Schritte aufgebaut werden. Insbesondere für das Risikomanagement in dem wissensintensiven Universitäts-und Hochschulbereich, sollte die Vorgehensweise der ISO/IEC 2700x Normenfamilie, mit ihrer vorangestellten, vollkommenden Risikoanalyse mit ihrem iterativen Verbesserungsansatz, herangezogen werden. Denn in einem sich derart rasant entwickelnden wissensintensiven Umfeld ist es von großer Bedeutung, sich eines Risikomanagements zu bedienen, welches einen iterativen Ansatz mit einem ständigen Verbesserungsprozess verfolgt, um auf sämtliche Veränderungen (z. B. Änderungen der Gefährdungen, Kontextänderungen) zeitnah reagieren zu können.

Eine stufenweise Zusammenführung der vorgestellten Lösungsalternativen mit ihren jeweiligen Stärken, zur Erstellung, Einführung, Implementierung, Aufrechterhaltung und Verbesserung eines ISMS im Universitäts-und Hochschulbereich, ist Gegenstand für weitere wissenschaftliche Arbeiten.

V. LITERATURVERZEICHNIS

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

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

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

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

[5] S. Hina and D. D. Dominic, “Information security policies: Investigation of compliance in universities,” *2016 3rd Int. Conf. Comput. Inf. Sci.*, pp. 564–569, 2016.

[6] B. Sussy, C. Wilber, L. Milagros, and M. Carlos, “ISO/IEC 27001 implementation in public organizations: A case study,” in *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, 2015, pp. 1–6.

[7] N. F. Doherty, L. Anastasakis, and H. Fulford, “The information security policy unpacked: A critical study of the content of university policies,” *Int. J. Inf. Manage.*, vol. 29, no. 6, pp. 449–457, 2009.

[8] Bundesamt für Sicherheit in der Informationstechnologie, “IT-Grundschutz-Kataloge 15. Ergänzungslieferung.” .

[9] Deutsches Institut für Normen e.V. DIN, “Informationssicherheits-Managementsysteme-Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014).”

[10] B. für Sicherheit in der Informationstechnik, “BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS).”

[11] K.-R. Müller, *IT-Sicherheit mit System*. .

[12] A. Asosheh, P. Hajinazari, and H. Khodkari, “A Practical Implementation of ISMS.”

[13] S. Klipper, *Information Security Risk Management*. .

[14] Deutsches Institut für Normen e.V. DIN, “Informationssicherheits-Managementsysteme - Überblick und Terminologie (E DIN ISO/IEC 27000:2015),” 2016.

[15] Bundesamt für Sicherheit in der Informationstechnologie, “BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschutz - Community Draft.”

[16] Fraunhofer Institut, “Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung.”

[17] Bundesamt für Sicherheit in der Informationstechnologie, “Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams in der öffentlichen Verwaltung.”

[18] Bundesamt für Sicherheit in der Informationstechnologie, “Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz,” *Stand 15. Ergänzungslieferung*. .

[19] Bundesministerium der Justiz und Verbraucherschutz, “GG - Einzelnorm.” [Online]. Available: https://www.gesetze-im-internet.de/gg/art_91b.html. [Accessed: 27-Feb-2017].

[20] Bundesministerium der Justiz und Verbraucherschutz- Vertrag zur Ausführung von Artikel 91c GG, *IT-Staatsvertrag, Art. 91c GG*. .

[21] IT-Planungsrat Kooperationsgruppe „Informationssicherheit des, “Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung- Hauptdokument-,” vol. 8, pp. 1–13, 2013.

[22] Kooperationsgruppe „Informationssicherheit des IT-PLR, “Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung- Umsetzungsplan-,” vol. 6, 2013.

[23] M. Stemmer and G. Goldacker, “IT-STANDARDISIERUNG IN DER ÖFFENTLICHEN VERWALTUNG – EIN DISKUSSIONSPAPIER.”

[24] K. I. Alshitri and A. N. Abanumy, “Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia,” in *2014 International Conference on Information Science & Applications (ICISA)*, 2014, pp. 1–4.

[25] G. D.-I. Schulz, “Informationssicherheit in Kommunen,” *Stellvertreter des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg- Vor.*

[26] “IT-Sicherheitsgesetz – SecuPedia.” [Online]. Available: http://www.secupedia.info/wiki/IT-Sicherheitsgesetz. [Accessed: 23-Jan-2017].

[27] Bundesamt für Sicherheit in der Informationstechnologie, “Kritis - Glossar - K.” [Online]. Available: http://www.kritis.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html?lv2=4968594. [Accessed: 23-Jan-2017].

[28] It-planungsrat, “Kooperationsgruppe „ Informationssicherheit des IT - PLR “ Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung Inhaltsverzeichnis,” vol. 8, pp. 1–13, 2013.

[29] Zentrum für Kommunikation und Informationsverarbeitung e.V. (ZKI) in Lehre und Forschung, “Anforderungen an IT-Sicherheit,” 2005.

[30] Zentrum für Kommunikation und Informationsverarbeitung e.V. (ZKI) in Lehre und Forschung, “Ergänzendes Material zum Papier IT-Sicherheit an Hochschulen, Rechtlicher Rahmen,” *Ergänzendes Mater. zum Pap. IT-Sicherheit an Hochschulen, Rechtl. Rahmen*, vol. 110, no. 35–36, p. A1595, 2013.

[31] Universität Berlin, “IT-Sicherheitsrahmenrichtlinie für die Freie Universität Berlin Gliederung,” pp. 1–67, 2005.

[32] Deutsches Institut für Normung e.V.: NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA), “Deutsches Institut für Normung e.V.: NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA).” [Online]. Available: http://www.din.de/de/mitwirken/normenausschuesse/nia. [Accessed: 01-Jan-2016].

[33] “BS 7799-1:1999 - Information security management. Code of practice for information security management.” [Online]. Available: http://shop.bsigroup.com/ProductDetail?pid=000000000019993902.

[34] Deutsches Institut für Normen e.V. DIN, “Informationssicherheits-Managementsysteme-Überblick und Terminologie (ISO/IEC 27000:2009).”

[35] K. Beckers, S. Faßbender, M. Heisel, and H. Schmidt, “Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation,” in *Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012*, 2012.

[36] M. R. SANS Institute, “INFORMATION SECURITY MANAGEMENT SYSTEM (BS 7799-2:2002) IMPLEMENTATION OVERVIEW,” 2004.

[37] D. Kilian, “SICHERHEITS-UND DATENSCHUTZ-MANAGEMENT,” .

[38] Detlef Kilian, “Einführung in Informationsmanagementsysteme (III): Praktische Umsetzung von Informationssicherheitsstandards,” .

[39] International Organization for Standardization, “ISO 31000 Risk management.” [Online]. Available: https://www.iso.org/iso-31000-risk-management.html. [Accessed: 28-Feb-2017].

[40] Deutsches Institut für Normen e.V. DIN, “Leitfaden für das Informationssicherheits-Management (DIN ISO/IEC 27002:2016-11).”

[41] International Organization for Standardization, “ISO/IEC TR 13335-4:2000 - Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards.” [Online]. Available: https://www.iso.org/standard/29240.html. [Accessed: 28-Feb-2017].

[42] Deutsches Institut für Normen e.V. DIN, “Information security risk management - ISO/IEC 27005:2011(E),” vol. 25021, 2012.

[43] Bundesamt für Sicherheit in der Informationstechnologie, “BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise.”

[44] Bundesamt für Sicherheit in der Informationstechnologie, “BSI-Standard 100-4.”

[45] Bundesamt für Sicherheit in der Informationstechnologie, “Gefährdungskatalog.”

[46] S. Kuhrau, “Erstellung von Informationssicherheitskonzepten für Kommunen, INNOVATIONSSTIFTUNG BAYERISCHE KOMMUNE.”

[47] A. Asosheh, P. Hajinazari, and H. Khodkari, “A practical implementation of ISMS,” in *7th International Conference on e-Commerce in Developing Countries:with focus on e-Security*, 2013, pp. 1–17.

[48] B. für Sicherheit in der Informationstechnik, “Informationssicherheit Ein Vergleich von Standards und Rahmenwerken.”

[49] M. Falk, *Ableitung des Control-Frameworks für IT-Compliance*. .

[50] I. WINDHORST and B. PIRZER, “Managementsysteme für Informationssicherheit,” 2012.

[51] Ralf-T. Grünendahl • Andreas F. Steinbacher and Peter H.L. Will, *Das IT-Gesetz: Compliance in der IT-Sicherheit*. .

[52] W. Goltsche, *COBIT-kompackt und verständlich*. .

[53] The IT Governance Institute, “Cobit 4.1.”

[54] G. Disterer, “Zertifizierung der IT nach ISO 20000.”

[55] National Institute of Standards an Technology, “NIST Computer Security Resource Center.” [Online]. Available: http://csrc.nist.gov/.

[56] Deutsches Institut für Normen e.V. DIN, “Leitfaden für das Informationssicherheits-

Management (DIN ISO/IEC 27002:2008-09)."

[57] Deutsches Institut für Normen e.V. DIN, "Informationsicherheits-Managementsysteme - Überblick und Terminologie (ISO/IEC 27000:2009)."

[58] Bayerischer IT-Sicherheitscluster e.V., "ISIS12 - Katalog," vol. 49, no. 0, pp. 0–75.

[59] Bayerischer IT-Sicherheitscluster e.V., "Informationssicherheit im Mittelstand Impressum-Handbuch," no. September, pp. 0–85, 2016.

[60] J. B. Kühnapfel, "Das Vorgehen bei der Nutzwertanalyse," no. 5.

[61] N. Müller-Prothmann, Tobias, Dörr, *Innovationsmanagement*. 2014.

[62] E. Tiemeyer and H. E. Zsifkovits, *Handbuch IT-Projektmanagement*. 2010.

[63] W. Johannsen, "Status der IT-Governance in der öffentlichen Verwaltung," 10AD.

[64] W. Hommel, S. Metzger, and M. Steinke, "Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization."

[65] I. V Anikin, "Information Security Risks Assessment in Telecommunication Network of the University."

[66] Bundesamt für Sicherheit in der Informationstechnologie, "BSI - IT-Grundschutz Tools - Startseite." [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/gstool_node.html. [Accessed: 15-Feb-2017].

[67] Fraunhofer AISEC, "ManageMentsysteMe für InforMatIonssIcherheIt," 2012.