MASTERARBEIT

KRYPTOGRAPHISCHE ERFORDERNISSE IN DER ÖFFENTLICHEN VERWALTUNG IM KONTEXT DES INFORMATIONSSICHERHEITSMANAGEMENTS

ausgeführt am

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Patrick Wachholz

Personenkennzeichen: 1610320012

Graz, am 15. Dezember 2017 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

Hiermit möchte ich mich bei allen bedanken, die das Verfassen dieser Masterarbeit ermöglicht haben. Dazu gehören mein Vorgesetzter Uwe Lafer und meine Kollegen, die Fachleute, die im Rahmen dieser Arbeit befragt wurden, sowie mein Betreuer Christian Schmid.

Besonderer Dank gebührt meiner Freundin Hannah, die mich während des Studiums und beim Verfassen dieser Arbeit immer wieder motiviert hat. Sie hat immer dafür gesorgt, dass ich das Ziel nicht aus den Augen verliere.

Abschließend möchte ich mich auch bei meinen Freunden und meiner Familie bedanken, die in den vergangenen Monaten noch mehr als sonst auf mich verzichten mussten.

KURZFASSUNG

Die vorliegende Masterarbeit ist im Bereich der Informationssicherheit und dem Informationssicherheitsmanagement angesiedelt. Ziel der Arbeit war es, einen allgemeinen Ansatz für die Entwicklung von Informationssicherheitsrichtlinien zu entwickeln. Aufgrund der Größe des Themenfeldes behandelt diese Arbeit vor allem das Richtliniendesign im Kontext der ISO 27001.

Der erste Teil der Arbeit deckt den theoretischen Hintergrund von Informationssicherheitsmanagement, Kryptographie und den gesetzlichen Vorgaben dazu ab. Das Ergebnis dieses Teils war ein grundsätzliches Verständnis davon, wie Informationssicherheitsmanagement funktioniert und welchen Beitrag Kryptographie dazu leisten kann. Außerdem wurde festgestellt, dass es für die öffentliche Verwaltung keine besonderen Gesetze im Bereich der Informationssicherheit gibt.

Der zweite Teil der Arbeit widmet sich dem Design von Informationssicherheitsrichtlinien. Aufgrund dessen, dass es noch keinen allgemeinen Ansatz für die Entwicklung solcher Richtlinien gab, wurde ein eigenes Vorgehensmodell dafür entwickelt. Basis für die Entwicklung des Modells waren die Erkenntnisse aus der Literaturrecherche hinsichtlich der Erfolgsfaktoren von Informationssicherheit. Im nächsten Schritt wurden fünf Fachleute aus dem Bereich der Informationssicherheit zu dem entwickelten Modell befragt.

Das Ergebnis dieser Befragung war eine verbesserte Version des aufgestellten Modells. Mit Hilfe dieses Modells wurde dann in einem weiteren Schritt eine Richtlinie für die Anwendung von kryptographischen Verfahren entwickelt. Außerdem ist deutlich geworden, dass die verschiedenen Richtlinien für Informationssicherheit so unterschiedlich sind, wie die Unternehmen, in denen sie Anwendung finden und dass die Unternehmenskultur einen großen Einfluss auf den Erfolg dieser Richtlinien hat. Zusätzlich wurde festgestellt, dass es verschiedene Arten von Anforderungen innerhalb der ISO 27002 gibt. Einige können direkt umgesetzt und mit Richtlinien erfüllt werden, und andere wirken sich auf viele Unternehmensbereiche aus. Aufgrund dessen war eine Beantwortung der Forschungsfrage schwierig. Das entwickelte Modell versucht den verschiedenen Ansprüchen verschiedener Organisationen gerecht zu werden, aber die letztendlich entwickelte Richtlinie ist nicht auf andere Organisationen übertragbar.

ABSTRACT

This master's thesis is placed in the fields of information security and information security management. The purpose was to develop a general approach for the design of information security policies. Since the area of information security is vast, this master's thesis particularly covers a general approach, as mentioned above, and the design of a policy for cryptographic controls as defined by the ISO 27001.

The first part of the research covers the theoretical background of information security management systems, cryptography and the potential legal obligations for the regional government. The outcome of this research was a general understanding of how information security management systems and cryptography work and the information that there are no legal obligations, particularly for regional governments.

The second part is dedicated to the design of a policy for cryptographic controls. Since there is no general approach for the development of such a policy or other information security policies, a new procedure model was developed. The first version of the model was based on the findings regarding success factors of information security. In the next step, the model was presented to and discussed with five experts in the field of information security.

The result was an improved version of the model. With this model, the policy for cryptographic controls was designed. Besides that, it became apparent that the policies for information security are as diverse as the organisations implementing them. Moreover, the culture of the organisations has a huge impact on the success of information security policies. Furthermore, there are different kinds of ISO 27001 policies. Some are directly effective and others (like the policy in this master's thesis) have an indirect influence on business processes and services. Thus, it was difficult to clearly answer the research question of this master's thesis. The developed model is trying to cope with the different organisational needs, but the final policy is rather not applicable in other organisations.

INHALTSVERZEICHNIS

1 EINLEITUNG 1

1.1 Motivation 1
1.2 Ziel und Vorgehen 1
1.3 Aufbau der Arbeit 2

2 GRUNDLAGEN 4

2.1 IT-Governance 4
2.2 Informationssicherheitsmanagement 7
2.2.1 Aufbau des Informationssicherheitsmanagements nach ISO 27001 8
2.2.1.1 Kontext der Organisation 10
2.2.1.2 Führung 11
2.2.1.3 Planung 13
2.2.1.4 Unterstützung 18
2.2.1.5 Betrieb 20
2.2.1.6 Evaluierung 21
2.2.1.7 Verbesserung 23
2.2.2 ISO 27002 25
2.2.3 ISO 27005 27
2.2.4 Andere Managementsysteme für Informationssicherheit 27
2.2.5 Nutzen für die Organisation 28
2.3 Kryptographie 29
2.3.1 Grundlagen 29
2.3.2 Kryptographische Verfahren 31
2.3.3 Vertraulichkeit 32
2.3.4 Authentizität 32
2.3.5 Integrität 33
2.3.6 Verbindlichkeit 33
2.3.7 Kryptographie und ISMS 34
2.4 Gesetzliche Vorgaben 34
2.4.1 E-Government-Gesetz 34
2.4.2 Signatur- und Vertrauensdienstegesetz 36
2.4.3 Datenschutzgesetz 37
2.4.4 Datenschutzgrundverordnung 39

2.5 Zusammenfassung 40

3 ENTWICKLUNG EINER RICHTLINIE 45

3.1 Entwicklung des Vorgehensmodells 45
3.1.1 Allgemeine Beobachtungen 45
3.1.2 Ansätze zur Richtlinienerstellung 46
3.1.3 Vorgehensmodell für die Richtlinienerstellung und -pflege 50

3.2 Befragung und Verbesserung 53
3.2.1 Vorbereitung und Durchführung der Interviews 53
3.2.2 Auswertung der Interviews 55
3.2.3 Verbesserung des Modells 60

3.3 Anwendung des Modells 62
3.3.1 Strategische Betrachtung 62
3.3.2 Richtlinienentwicklung 63
3.3.3 Fallbeispiel 65
3.3.4 Prozess- und Standardentwicklung 66

3.4 Zusammenfassung 68

4 ABSCHLUSS DER ARBEIT 70

4.1 Rückblick 70
4.2 Fazit und Diskussion 72
4.3 Ausblick 73

ANHANG A - MODELL ZUR RICHTLINIENENTWICKLUNG I

ABKÜRZUNGSVERZEICHNIS II

ABBILDUNGSVERZEICHNIS III

TABELLENVERZEICHNIS IV

LITERATURVERZEICHNIS V

1 EINLEITUNG

Zu Beginn der Arbeit werden kurz die Motivation für das Verfassen dieser Arbeit, das Ziel und der Weg, wie dieses Ziel erreicht werden soll, sowie der Aufbau der Arbeit vorgestellt.

1.1 Motivation

Informationssicherheit spielt aufgrund der immer weiter steigenden Vernetzung digitaler Systeme und dem hohen Wert von Informationen für die verschiedenen Organisationen eine immer größere Rolle. Die Folgen von Informationsverlust in Form von Kundendaten, Entwicklungsdaten oder Finanzdaten wurden in der jüngsten Vergangenheit des Öfteren in den Medien aufgezeigt und können fatale Folgen sowohl für die Organisationen selbst als auch für die Kunden haben.

Es ist anzunehmen, dass diese Zwischenfälle mit einem effizienten und effektiven Informationssicherheitsmanagement nicht in der vorliegenden Form aufgetreten wären. Einen strukturierten Ansatz für das Schaffen von Informationssicherheit in verschiedenen Belangen bieten diverse Managementsysteme wie die ISO 27001 oder der Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Diese verschiedenen Ansätze haben das Ziel, durch eine ganzheitliche Sicht auf eine Organisation die Informationssicherheit durch verschiedene Vorgaben und Maßnahmen zu erhöhen. Eine dieser Maßnahmen ist unter anderem die Anwendung von kryptographischen Verfahren zur Schaffung von Vertraulichkeit, Integrität und Authentizität von Informationen. Von den Zielen der Kryptographie lassen sich direkt Parallelen zu den Zielen des Informationssicherheitsmanagements (Vertraulichkeit, Integrität und Verfügbarkeit) ziehen.

Die angesprochenen Ansätze und das Informationssicherheitsmanagement an sich sind allerdings so komplex, dass es für Organisationen oft schwer ist, sich dem Thema ohne starke Unterstützung von externen Beratern effektiv anzunehmen. Die Motivation dieser Arbeit liegt darin, dass bei der Entwicklung von Richtlinien im Bereich der Informationssicherheit oft unstrukturiert vorgegangen werden muss, da entweder das entsprechende Wissen fehlt oder das Umfeld einfach zu komplex ist.

1.2 Ziel und Vorgehen

Das Ziel dieser Arbeit ist es, eine Richtlinie für die Verwendung kryptographischer Methoden zu entwickeln, die den Ansprüchen der ISO 27001 gerecht wird.

Mit Hilfe dieser Richtlinie soll die Forschungsfrage „Welchen Beitrag zum Informationssicherheitsmanagement leistet die Einführung einer allgemeinen Vorgabe für die

Anwendung kryptographischer Standards im Umfeld der öffentlichen Verwaltung?“ beantwortet werden. Diese Forschungsfrage wird durch die folgenden Hypothesen konkretisiert:

H_1: Durch die Einführung einer allgemeinen Vorgabe für die Anwendung kryptographischer Standards wird die Effizienz des IT-Sicherheitsmanagements in der Verwaltung gesteigert.

H_0: Die Einführung einer allgemeinen Vorgabe für die Anwendung kryptographischer Standards hat keinen Einfluss auf das IT-Sicherheitsmanagement.

Zu Beginn der Arbeit erfolgt eine Sichtung der vorhandenen Literatur in Hinblick auf Informationssicherheitsmanagementsysteme. Danach werden die Grundzüge der Kryptographie beschrieben und es wird überprüft, ob der Gesetzgeber für die öffentliche Verwaltung spezielle Vorgaben aufstellt.

Aufgrund der gefundenen Informationen soll eine Richtlinie für die Verwendung kryptographischer Verfahren formuliert werden. Zu diesem Zweck wird ein eigenes Vorgehensmodell für die allgemeine Entwicklung von Informationssicherheitsrichtlinien entwickelt.

Dieser erste Entwurf wird dann Fachleuten der Informationssicherheit in einem Interview vorgestellt und anhand der Interviewergebnisse verbessert und finalisiert. Den Kern der Interviews stellen der Nutzen dieses Vorgehens und mögliche Verbesserungen dar. Der Zweck der Interviews ist der Informationsgewinn hinsichtlich des vorgestellten Vorgehensmodells.

Anhand dieser finalen Version wird dann im Rahmen einer Fallstudie die Richtlinie zur Verwendung von kryptographischen Verfahren erstellt.

Eine quantitative Beantwortung der Forschungsfrage ist nicht Ziel dieser Arbeit.

1.3 Aufbau der Arbeit

In diesem Abschnitt wird kurz der Aufbau der Arbeit beschrieben und grafisch dargestellt. Die Arbeit unterteilt sich in die vier Kapitel *Einleitung*, *Grundlagen*, *Entwicklung einer Richtlinie* und *Abschluss der Arbeit*.

Die Einleitung hat Motivation und Ziel dieser Arbeit dargelegt. Außerdem wurde beschrieben, wie dieses Ziel erreicht werden soll. Zum Abschluss des Kapitels wird nun kurz der Aufbau der Arbeit beschrieben.

Das Kapitel *Grundlagen* steckt den theoretischen Rahmen dieser Arbeit ab. Zu Beginn wird der größere Rahmen des Informationssicherheitsmanagements, die IT-Governance, erläutert. Darauf folgt dann eine Beschreibung des Informationssicherheitsmanagements nach ISO 27001 und der damit verknüpften Standards. Aufbauend erfolgt dann eine kurze Beschreibung von Kryptographie und die Begründung, warum Kryptographie für die Informationssicherheit wichtig ist. Zum Abschluss des Kapitels wird überprüft, ob es Gesetze gibt, die großen Einfluss auf die Informationssicherheit und die Verwendung kryptographischer Verfahren haben.

Im darauffolgenden Kapitel *Entwicklung einer Richtlinie* werden zum einen eigene Erkenntnisse und zum anderen Informationen aus der Literatur zusammengefasst, um besondere Einflussfaktoren für die Wirksamkeit von Informationssicherheitsrichtlinien zu erkennen. Anhand dieser Informationen wird dann ein allgemeines Vorgehensmodell zur Entwicklung von Richtlinien für die Informationssicherheit entwickelt und mit Hilfe von Fachleuten verbessert. Mit Hilfe dieses finalen Vorgehensmodells wird dann die eigentliche Richtlinie entworfen.

Der *Abschluss der Arbeit* befasst sich zu Beginn mit einer Zusammenfassung der Arbeit. Anschließend erfolgt das Fazit und die kritische Diskussion der Forschungsergebnisse. Abschließend wird aufgezeigt, welchen Nutzen die Arbeit in der Praxis haben kann und welche weiteren Forschungsmöglichkeiten bestehen.

Die Gliederung der Arbeit ist in der nachfolgenden Abbildung 1 dargestellt.

Abbildung 1: Aufbau der Arbeit

2 GRUNDLAGEN

In diesem Kapitel werden die theoretischen Grundlagen für die Entwicklung einer kryptographischen Richtlinie im Sinne des Information Security Managements erarbeitet. Zu diesem Zweck wird zuerst der Rahmen des Information Security Management Systems – in Form der IT-Governance – beschrieben und dann das Information Security Management System selbst. Als nächstes werden die Grundlagen der Kryptographie und des Identity Managements beschrieben. Zum Abschluss des Kapitels werden die Vorgaben betrachtet, welche bei der Entwicklung der Richtlinie eine Rolle spielen können.

Zu Beginn dieses Kapitels soll aber kurz erläutert werden, wie Informationssicherheit im Kontext dieser Arbeit definiert ist. Dazu liefert der BSI-Grundschutz 200-1 (2017) folgende Definition: „Informationssicherheit hat als Ziel, Informationen jeglicher Art und Herkunft zu schützen. Dabei können Informationen auf Papier, in IT-Systemen oder auch in den Köpfen der Benutzer gespeichert sein“. Informationssicherheit ist demnach nicht nur auf technische Betriebsmittel wie Server oder Clients begrenzt, sondern befasst sich zudem auch mit Problemen wie Datenklau aus dem Unternehmen und Social Engineering. Informationssicherheit ist daher nicht allein durch technische Mittel zu gewährleisten. Die IT-Sicherheit stellt damit einen Teil der Informationssicherheit dar – und zwar den zuvor angesprochenen Schutz der technischen Betriebsmittel.

Die Informationssicherheit sorgt sich dabei nicht nur um bewusste Manipulationen oder Angriffe, sondern plant auch für Fälle höherer Gewalt, technischer Fehler und anderer Missgeschicke. Dies wird bei der später folgenden Beschreibung der ISO 27001 (insbesondere bei der Risikoabschätzung) deutlich.

Die Informationssicherheit hat zum Ziel Integrität, Vertraulichkeit und Verfügbarkeit der Informationen in einer Organisation sicherzustellen. Der BSI-Grundschutz (2017) weist allerdings darauf hin, dass diese Ziele beispielsweise durch Verbindlichkeit oder Zuverlässigkeit ergänzt werden können.

Im folgenden Abschnitt soll kurz der Rahmen vorgestellt werden, in dem Informationssicherheitssysteme üblicherweise angesiedelt werden: die IT-Governance.

2.1 IT-Governance

Um das Thema IT-Governance näher betrachten zu können, muss vorab kurz geklärt werden, wo diese einzuordnen ist. Die IT-Governance ist ein Teil der Corporate Governance, welche für die Ausrichtung des Unternehmens auf externe Faktoren zuständig ist.

Die Corporate Governance sorgt als Steuerungsinstrument dafür, dass das Unternehmen den äußeren und inneren Einflüssen (wie zum Beispiel Ansprüche der Stakeholder, Gesetze oder

das eigene Unternehmensleitbild) gerecht wird (OECD, 2004). Rüter, Schröder, Göldner und Niebuhr (2010) definieren Corporate Governance als Unternehmensverfassung, was aufgrund der Herkunft des Wortes Governance (to govern – bestimmen) naheliegt. Wie auch die Verfassung eines Staates definiert die Unternehmensverfassung den prinzipiellen Aufbau und die Grundsätze des Unternehmens. Zusätzlich dazu werden gewisse Regeln festgelegt. An dieser Stelle lässt sich auch die oben angeführte Definition der OECD wiederfinden – Corporate Governance stellt somit das grundsätzliche Regelwerk dar, nach dem Unternehmen agieren (sollten). Fröhlich und Glasner (2007) fassen die oben angesprochenen Punkte in den Grundprinzipien „accountability", „responsibility", „transparency" und „fairness" zusammen.

Rüter et. al. (2010) ergänzen, dass im Kontext der Corporate Governance „das Zusammenspiel aller Stakeholder oder Stakeholder des Unternehmens, sowohl interner als auch externer, aus Sicht des Unternehmens festzulegen, zu kommunizieren und umzusetzen" ist. Grundsätzlich ist die Corporate Governance für jedes Unternehmen individuell zu definieren, da üblicherweise Unterschiede in den Anspruchsgruppen, Zielen und Werten bestehen. Die Definition der OECD (2004) unterteilt diese Anspruchsgruppen zumindest in Aktionäre und Unternehmensbeteiligte. Rüter et. al. (2010) erweitern diese Unterteilung in Aktionäre (und Vorstand sowie Aufsichtsrat), andere interne Stakeholder und die externen Stakeholder.

Als Hilfsmittel sorgt die IT-Governance nun dafür, dass die Unternehmens-IT bei der Erfüllung dieser Ansprüche unterstützend tätig wird und sich ihrerseits ebenfalls an die Unternehmensvorgaben halten muss. Die IT-Governance ist als Teilbereich der Corporate Governance laut Rüter et. al. (2010) dafür zuständig, dass „mit Hilfe der IT die Geschäftsziele abgedeckt, Ressourcen verantwortungsvoll eingesetzt und Risiken angemessen überwacht werden". Dasselbe sagt auch folgende Definition im Kompakt-Lexikon Wirtschaftsinformatik (2013) aus:

> „IT-Governance – bezeichnet den rechtlichen und faktischen Ordnungsrahmen für die Leitung, Organisation (prozessual wie aufbauorganisatorisch) und Überwachung der IT eines Unternehmens. Mit der IT-Governance soll sichergestellt werden, dass die Unternehmensziele durch den IT-Einsatz unterstützt und vorangetrieben werden."

Durch die IT-Governance wird es der Unternehmens-IT unter anderem ermöglicht, vom notwendigen Kostenverursacher und Unterstützer von bestehenden Prozessen zum Business-Enabler aufzusteigen. Die IT trägt somit nicht nur zum Geschäftserfolg bei, sondern kann auch zu einer Neupositionierung des Unternehmens beitragen. (Fröhlich & Glasner, 2007)

Grundsätzlich befindet sich die IT-Governance im Spannungsfeld der Corporate Governance und der IT. Erst durch die IT-Governance ist es möglich die externen Anforderungen und die internen Fertigkeiten aufeinander abzustimmen und für ein möglichst gutes IT-Business-Alignment zu sorgen. Rüter et. al. (2010) beschreiben die Rolle der IT-Governance im Unternehmen mit den Begriffen „Übersetzer" und „Vermittler". Dieses Gefüge ist auch in der folgenden Abbildung 2 dargestellt.

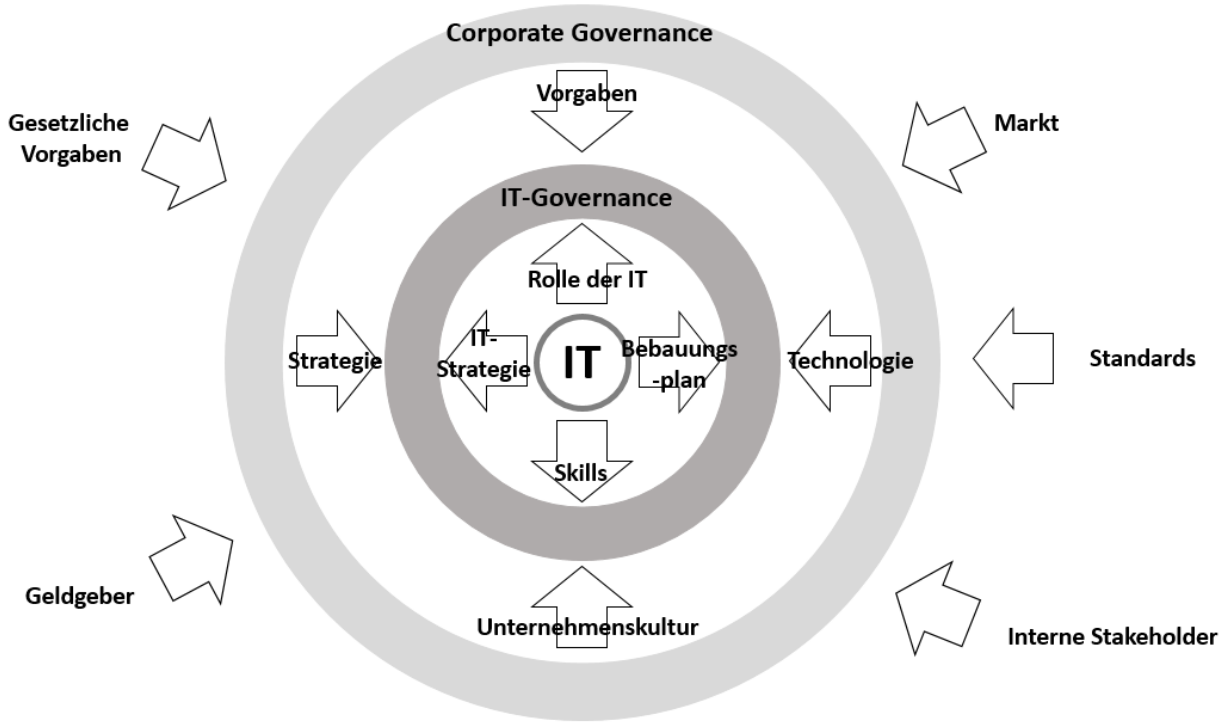

Abbildung 2: Spannungsfeld der IT-Governance (Rüter, Schröder, Göldner, & Niebuhr, 2010)

Um dieses Ziel zu erreichen, hat die IT-Governance laut dem *IT Governance Institute* fünf Entscheidungsdomänen, in denen sie tätig wird. Diese Domänen lauten Strategic Alignment, Value Delivery, Performance Measurement, Risk Management und Resource Management (Williams, 2005). Der Fokus dieser Arbeit befindet sich in der Domäne Risk Management, auf die an dieser Stelle kurz näher eingegangen werden soll.

Die Domäne Risikomanagement befasst sich mit der dokumentierten Einhaltung von gängigen Bestimmungen. Damit wird der immer höheren Integration der IT in die Unternehmensabläufe und dem damit einhergehenden gestiegenen Sicherheitsbedürfnis der Stakeholder Schuldigkeit getan. (Fröhlich & Glasner, 2007)

Auf die Details des Risikomanagements wird bei der Beschreibung der Standards ISO 27001 und ISO 27005 näher eingegangen.

Für die Umsetzung der IT-Governance in einer Organisation findet man in der Literatur verschiedene Standards und Frameworks. Der am häufigsten genannte Standard ist dabei CobiT, welcher eine Sammlung von verschiedenen Prozessen für bestimmte Kontrollziele hinsichtlich der Erreichung von internen und externen Sicherheitsanforderungen enthält. (Rüter, Schröder, Göldner, & Niebuhr, 2010)

Beim Sichten der Literatur wird deutlich, dass ein einziger Standard nicht ausreicht, um alle Domänen der IT-Governance bestmöglich abdecken zu können. So ist die Ausrichtung von CobiT beispielsweise eher strategischer Natur, wohingegen zum Beispiel ITIL oder auch die ISO-27000-Familie eher schon im operativen Bereich anzusiedeln sind. Standards und Bibliotheken, welche in der Literatur im Kontext der IT-Governance erwähnt werden, sind in der nachfolgenden Tabelle dargestellt.

	Rüter, Schröder, Göldner, & Niebuhr, 2010	Fröhlich & Glasner, 2007	Schwertsik, 2012	Van Grembergen & De Haes, 2009
Balanced Score Card				x
CobiT	x	x	x	x
ValIT			x	x
Coso		x		
ITIL v3	x	x	x	
ISO 27001		x		
ISO 17799 bzw. 27002	x	x		
ISO 38500			x	
CISR	x			

Tabelle 1: Standards im Bereich der IT-Governance

Der Wert von Informationssicherheit für Organisationen ist durch die stetige Verzahnung der Unternehmensprozesse mit der IT von hoher Relevanz. Datenverlust oder sogar -diebstahl und der Verlust von Verfügbarkeit stellen inzwischen große Risiken finanzieller und imagetechnischer Natur für Unternehmen dar. Aus diesem Grund spielen Standards, welche sich explizit mit der Informationssicherheit und dem IT-Risikomanagement beschäftigen, eine immer größere Rolle in der Verwaltung von Unternehmen. Einer dieser Standards ist die ISO 27001, welcher in der ISO-27000-Familie angesiedelt ist.

2.2 Informationssicherheitsmanagement

Die ISO 27000 ist die Standard-Familie, welche sich mit der Einrichtung, dem Betrieb und der Verbesserung von Information-Management-Security-Systemen (ISMS) befasst. Jeder Standard stellt dabei einen Baustein für ein funktionierendes ISMS dar.

Die Familie kann dabei in die Kategorien *Anforderungen*, *Leitfäden* und *spezielle Leitfäden für bestimmte Sektoren* eingeteilt werden. Die Anforderungen werden dabei unterteilt in die ISO 27001, welche die Anforderungen an Organisationen definiert, und die ISO 27006, welche Standards für Auditoren wiedergibt. Die Leitfäden bieten Unterstützung für den Betrieb und die Einrichtung eines ISMS. Dabei geht es um das Bereitstellen und Implementieren von Kontrollmaßnahmen für Organisationen (ISO 27002), Risikomanagement (ISO 27005) sowie Implementierungsvorschläge, die Messung des ISMS sowie Empfehlungen für das Auditieren von ISMS. Die letzte Kategorie befasst sich mit dem ISMS für bestimmte Branchen wie die

Energieindustrie, Finanzdienstleister oder Gesundheitsdienstleister. Der Aufbau der ISO-27000-Familie ist in der nachfolgenden Grafik dargestellt, wobei die hervorgehobenen Normen für diese Arbeit eine größere Rolle spielen. (ISO/IEC 27000:2016, 2016)

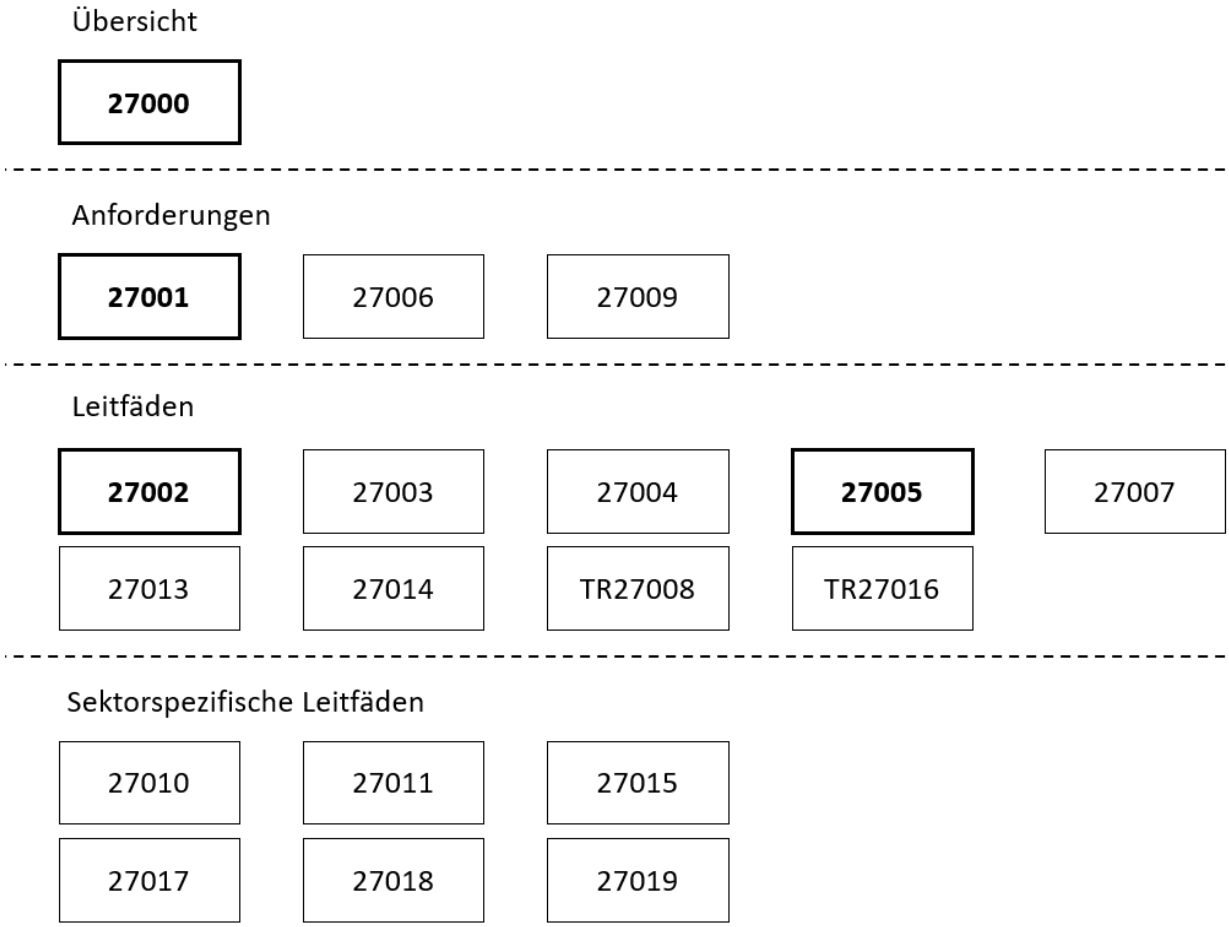

Abbildung 3: Aufbau der ISO-27000-Familie (ISO/IEC 27000:2016, 2016)

Im Rahmen dieser Arbeit werden die Standards ISO 27001, ISO 27002 und ISO 27005 näher behandelt. Dies gebührt dem Umstand, dass die öffentliche Verwaltung keinen branchenspezifischen Standard für die Implementation des ISMS hat und die drei genannten Standards üblicherweise als Mittel der Wahl für die Errichtung eines ISMS herangezogen werden.

Es gibt noch weitere Standards oder Richtlinien für die Einrichtung eines ISMS in einer Organisation, die jedoch im Kern auf die ISO 27001 zurückgreifen, daher werden diese Alternativen im Verlauf der Arbeit nur kurz vorgestellt.

2.2.1 Aufbau des Informationssicherheitsmanagements nach ISO 27001

Wie der Name bereits sagt, verbirgt sich hinter dem Information Security Management System ein Management-System. Mit Hilfe des ISMS wird sichergestellt, dass passende Sicherheitsmaßnahmen für die unternehmenskritischen Daten eines Unternehmens getroffen wurden und die entsprechenden Interessensgruppen über diese Maßnahmen informiert

werden. Das ISMS wird durch die ISO 27001 definiert und ist für alle Unternehmen gleichermaßen anwendbar. (ISO/IEC 27001:2013-10, 2013)

Bis zur Version 2013 sollte ein ISMS nach ISO 27001 anhand eines Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) aufgebaut werden. Das bedeutet, dass sich ein gut gepflegtes ISMS in einem kontinuierlichen Verbesserungsprozess befindet und neue Erkenntnisse – beispielsweise durch aufgetretene Zwischenfälle oder Auditierungen – regelmäßig in das ISMS eingearbeitet werden. Die ISO 27001 (2005) beschreibt die einzelnen Phasen wie folgt:

- Plan: Planung des ISMS und Festlegen der Rahmenbedingungen für das ISMS. Dabei wird das generische Modell, welches in der ISO 27001 vorgestellt wird, an das jeweilige Unternehmen und seine vorherrschenden Regeln und Abläufe angepasst. Außerdem werden in dieser Phase die Ziele und Richtlinien des ISMS definiert.
- Do: In dieser Phase des PDCA-Zyklus werden das ISMS und damit einhergehend die notwendigen Prozesse und Vorgaben in der Organisation implementiert.
- Check: In dieser Phase des Zyklus wird das ISMS auditiert. Diese Auditierung kann entweder intern erfolgen oder durch externe Auditoren vorgenommen werden. Im Rahmen der Auditierung werden die definierten Prozesse gegen die Richtlinien des ISMS geprüft und (sofern möglich) gemessen. Die Ergebnisse dieser Phase werden dem Management zur Begutachtung vorgelegt.
- Act: Ausgehend von den Ergebnissen der vorherigen Phase sowie anderweitig gewonnener Erkenntnisse werden Änderungen – diese können sowohl korrigierend als auch präventiv sein – am ISMS vorgenommen. An diesem Punkt schließt sich der PDCA-Zyklus und es wird wieder bei der ersten Phase begonnen.

Dieser Zyklus ist in der nachfolgenden Abbildung 4 dargestellt.

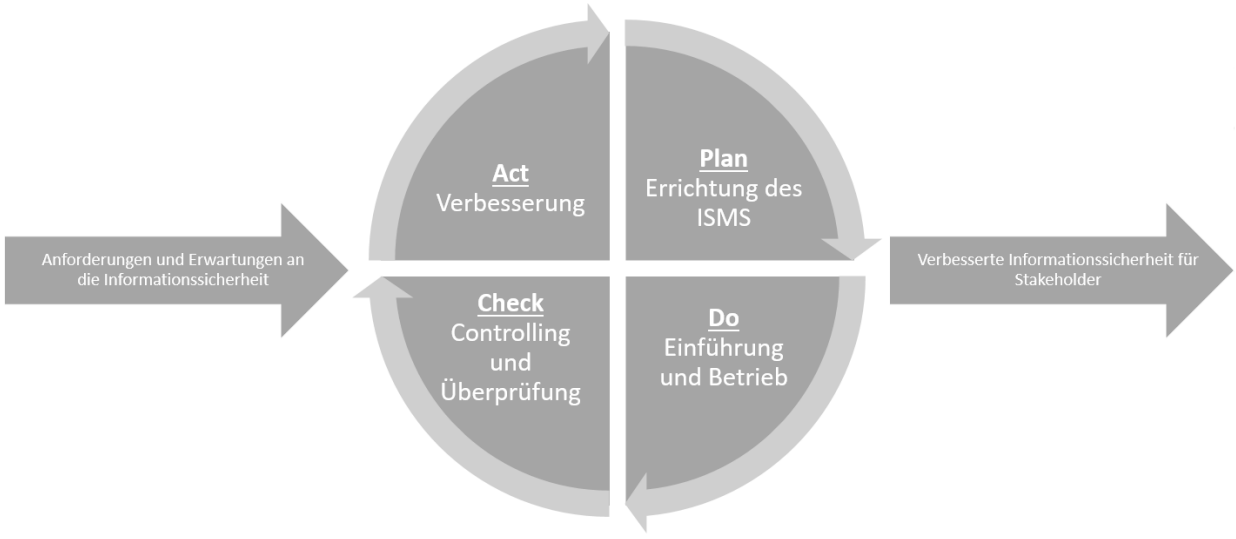

Abbildung 4: PDCA-Zyklus der ISO 27001:2005 (ISO/IEC 27001:2005-10, 2005)

Seit der Version 2013 ist dieser Zyklus allerdings nicht mehr so tiefgreifend in den Vorschriften des Standards verwurzelt, sondern wird nur noch in einem Unterpunkt berücksichtigt. In den

nächsten Unterkapiteln wird allerdings deutlich werden, dass der PDCA-Zyklus noch immer eine wichtige Rolle in einem gut funktionierenden ISMS spielt. Grundsätzlich sind die einzelnen Tätigkeiten auch in der überarbeiteten Version des Standards noch vorhanden, es wird allerdings nicht mehr zwingend die kontinuierliche Verbesserung mit Hilfe des PDCA-Zyklus vorgeschrieben. (ISO/IEC 27001:2013-10, 2013)

Aufgrund dieser Änderung hat sich auch die Struktur der ISO 27001 geändert. So sind die einzelnen Kapitel nicht mehr an eine bestimmte Reihenfolge gebunden, sondern mehr oder weniger unabhängig voneinander. Das heißt selbstverständlich nicht, dass Anwender einzelne Kapitel weglassen können – für eine erfolgreiche Zertifizierung ist es notwendig, dass zumindest die Kapitel vier bis zehn des Standards umgesetzt werden.

Die folgenden Punkte orientieren sich in ihrer Abfolge teilweise an der Struktur der ISO 27001:2013. Konkret werden die Abschnitte vier bis zehn des Standards beschrieben, da diese für eine entsprechende Zertifizierung unabdingbar sind.

2.2.1.1 Kontext der Organisation

Der erste Teil der Anforderungen der ISO 27001:2013 befasst sich mit dem Kontext der Organisation. Während diesem Begriff in der Revision aus dem Jahr 2005 noch deutlich weniger Aufmerksamkeit geschenkt wurde und er eher über die ISO 27005 definiert wurde, scheint der Kontext nun auch für die ISO 27001 von wichtigerer Bedeutung geworden zu sein.

Der Kontext wird im Rahmen der ISO 27001:2013 durch folgende Schritte definiert:

- Das Unternehmen und seinen Kontext verstehen
- Die Bedürfnisse und Erwartungen der Stakeholder verstehen
- Abgrenzung des ISMS
- Einrichtung des ISMS

Die ISO 27001:2013 versteht unter dem Kontext alle internen und externen Faktoren, die wichtig für den Zweck der Organisation sind und die in der Lage sind, den beabsichtigten Nutzen des ISMS zu beeinflussen (hier wird kein Unterschied zwischen positiver oder negativer Beeinflussung gemacht) (ISO/IEC 27001:2013-10, 2013). Der Standard verweist zum Zweck der Feststellung dieser Faktoren auf den ISO Standard 31000:2009, welcher im Gegensatz zur ISO 27005 einen allgemeineren Risikomanagementansatz verfolgt. Beim Vergleich der Standards fällt auf, dass die ISO 31000 (vermutlich) aufgrund der allgemeineren Anwendung auch den Begriff des Kontexts weiter fasst und genauer beleuchtet. Dies erzielt für eine erste Annäherung vermutlich bessere Ergebnisse als die spezialisierte Definition aus der ISO 27005.

Kersten et. al. (2016) bieten für diesen Bereich einige Beispiele an, welche in diesem Zusammenhang betrachtungswürdig sind. Im Bereich der externen Faktoren können dies zum Beispiel das „Umfeld der Tätigkeit“ und „Wettbewerbsaspekte“ sein. Bei den internen Faktoren nennen sie unter anderem die „Aufbau- und Ablauforganisation“, den „Zweck und Umfang der eingesetzten IT“ und „bereits umgesetzte Standards und andere Vorgaben […]“.

Im nächsten Teil der Kontextdefinition liegen die Bedürfnisse und Erwartungen der Stakeholder im Fokus. Die ISO 27001 verlangt, dass alle Stakeholder mit Relevanz für das ISMS bestimmt werden sollen – nach den Erfahrungen des Autors umfasst dies je nach Natur der Organisation durchaus einen Großteil der Stakeholder der Organisation. Relevante Stakeholder könnten zum Beispiel Lieferanten, Kunden und Angestellte sein. Im Falle eines Unternehmens werden zu diesen noch einige weitere hinzukommen. Die Stakeholder sind individuell für jede Organisation zu definieren, da hier von Organisation zu Organisation große Unterschiede vorliegen können. In einer anschließenden Betrachtung sollen die Anforderungen der gefundenen Stakeholder an das ISMS bestimmt werden. An dieser Stelle weist die ISO 27001:2013 explizit darauf hin, dass diese Bedürfnisse rechtliche und regulatorische Bestimmungen sowie vertragliche Vereinbarungen (zum Beispiel mit Lieferanten) sein können. (ISO/IEC 27001:2013-10, 2013)

Nach Einschätzung des Autors liegen hier deutliche Parallelen zu anderen Bereichen, wie zum Beispiel der Unternehmensgründung mit Hilfe des Business Model Canvas oder der Dienstleistungsentwicklung, vor. Es liegt nahe, die dort gefundenen Informationen für einen ersten Ansatz im Bereich des Kontextes des ISMS heranzuziehen, um mehrfache Arbeiten zu vermeiden.

Nachdem die Interessengruppen mit ihren Anforderungen und Erwartungen bestimmt wurden, wird darauf aufbauend der Einsatzbereich des ISMS definiert. Grundsätzlich wird dieser Einsatzbereich mit Hilfe der externen und internen Themen, der Anforderungen der Stakeholder sowie der Schnittstellen und Abhängigkeiten zwischen Tätigkeiten der eigenen Organisation und anderen Organisationen definiert. An dieser Stelle wird deutlich, dass ein ISMS nicht die gesamte Organisation abdecken muss – in den vorhergegangenen Analysen wurde immer der Kontext in Bezug auf ISMS und nicht auf das gesamte Unternehmen hervorgehoben. Auch Kersten et. al. (2016) schreiben, dass ein ISMS „auch auf Teile davon, bestimmte Standorte oder einzelne Geschäftsprozesse beschränkt sein“ kann. Der Einsatzbereich ist Teil der Dokumentensammlung des ISMS. (ISO/IEC 27001:2013-10, 2013)

Zum Abschluss dieses Tätigkeitsbereiches verlangt der Standard, dass das ISMS in Übereinkunft mit dem vorliegenden Standard geplant, eingerichtet, betrieben und regelmäßig verbessert werden soll (ISO/IEC 27001:2013-10, 2013). Im Grunde genommen findet sich hier der PDCA-Zyklus wie er in der Revision 2005 definiert wurde, wieder. Im Gegensatz zur ISO 27001:2005 verlangt die ISO 27001:2013 allerdings nicht mehr explizit den PDCA-Zyklus, sondern nur nachgewiesene Maßnahmen der kontinuierlichen Verbesserung. Kersten et. al. (2016) weisen jedoch darauf hin, dass gerade bei einem bereits bestehenden ISMS mit gelebtem PDCA-Zyklus eine Abkehr von diesem System unratsam ist. Auch wenn der PDCA-Zyklus nicht mehr explizit im Standard erwähnt wird, wird offensichtlich, dass die Wurzeln des Standards genau dort liegen und diese Vorgehensweise den ganzheitlichen Betrieb des ISMS sehr gut unterstützt.

2.2.1.2 Führung

Der nächste Teil des Standards befasst sich mit dem Schlagwort Führung. Im Sinne der ISO 27001:2013 werden darunter die Punkte

- Führung und Einsatz,
- Informationssicherheitsrichtlinie und
- Rollen, Verantwortlichkeiten und Kompetenzen

verstanden. Im Bereich der Informationssicherheitsrichtlinie wird das erste Mal deutlich, dass die einzelnen Kapitel der ISO-Norm mehr sind als nur eine lose und ungebundene Abfolge, da hier auf ein späteres Kapitel der Norm (die Planung) verwiesen wird. (ISO/IEC 27001:2013-10, 2013)

Der Abschnitt Führung und Einsatz widmet sich in erster Linie Kontroll- und Kommunikationsaufgaben. Die ISO 27001:2013 (2013) umreißt dies mit den Worten „Top management shall demonstrate leadership and commitment with respect to the information security management system […]“ und verlangt damit zugleich, dass die Führung einer Organisation voll hinter dem eingeführten oder einzuführenden ISMS steht. Kersten et. al. (2016) heben in diesem Bezug hervor, dass die entsprechenden Aufgaben natürlich „an zuständige Personen oder Stellen delegiert“ werden, da „das Veranlassen aller Aufgaben, das Motivieren und Unterstützen sowie die Kontrolle der Ergebnisse […] Kardinalaufgaben der Führung“ sind.

So soll die Unternehmensführung dafür Sorge tragen, dass die (in der Einführungsphase eines ISMS noch zu definierende) Informationssicherheitsrichtlinie sowie die Informationssicherheitsziele umgesetzt werden und mit der strategischen Ausrichtung der Organisation übereinstimmen. Dies ergibt auch die Eingliederung in die IT-Governance. Zusätzlich dazu muss die Unternehmensführung dafür sorgen, dass die Anforderungen an die Informationssicherheit in alle relevanten Geschäftsprozesse integriert werden. (ISO/IEC 27001:2013-10, 2013)

Eine weitere Führungsaufgabe ist es sicherzustellen, dass die erforderlichen Ressourcen für das ISMS zur Verfügung stehen (seien diese nun personeller oder technischer Natur) (ISO/IEC 27001:2013-10, 2013). Der Autor ortet gerade hier ein mögliches Spannungsfeld, da das Thema Informationssicherheit noch immer ein wenig stiefmütterlich behandelt wird. Meistens sind Unternehmen erst nach einem eingetretenen Ernstfall bereit in dieses Thema zu investieren, obwohl ein entsprechendes Investment im Vorfeld üblicherweise viel Zeit und Geld gespart hätte. Gerade in der Zeit der aufkeimenden Industrie 4.0 oder dem Internet der Dinge steht oftmals im Vordergrund, dass das eingerichtete System funktioniert (und nicht, dass es dabei auch sicher ist) – die damit einhergehenden Risiken sind entweder nicht bewusst oder werden schlimmstenfalls aus Gründen der Kosteneffizienz ignoriert.

Damit kann auch die nächste Managementaufgabe eingeleitet werden. Die Unternehmensführung muss die Wichtigkeit eines funktionierenden(!) ISMS und die damit einhergehende Konformität mit den Anforderungen entsprechend im Unternehmen kommunizieren (ISO/IEC 27001:2013-10, 2013). Ein ISMS ist für eine Organisation wertlos, wenn es nur als Wertesystem in den Köpfen des Managements oder nur als Richtlinie für die IT-Abteilung existiert. IT-Sicherheit betrifft in der heutigen Zeit die gesamte Organisation und jeder Mitarbeiter ist eine mögliche Zielscheibe von Angreifern. An dieser Stelle seien auch veraltete Systeme, Arbeitsweisen oder das typische „das haben wir schon immer so gemacht“

angesprochen: Damit ein System wie das ISMS in einem gewachsenen Unternehmen funktionieren kann, müssen alte Strukturen durchbrochen und angepasst werden. Ergänzend dazu gibt es eine weitere Managementaufgabe, die sicherstellen soll, dass Personen so geleitet und unterstützt werden, dass diese die Wirksamkeit des ISMS erhöhen können (ISO/IEC 27001:2013-10, 2013).

Weitere Aufgaben der Unternehmensführung sind, dafür zu sorgen, dass das ISMS seine erwarteten Ziele erreicht, eine kontinuierliche Verbesserung zu unterstützen und andere Führungspositionen bei den oben angesprochenen Aufgaben zu unterstützen (ISO/IEC 27001:2013-10, 2013).

Der nächste große Block im Bereich der Führung widmet sich der Informationssicherheits-richtlinie. Der Standard verlangt, dass die oberste Führung der Organisation eine Informationssicherheitsrichtlinie einführt und dass diese angemessen in Bezug auf den Geschäftszweck des Unternehmens ist. Diese Richtlinie enthält die Informationssicherheitsziele aus dem Bereich der Planung oder die Rahmenbedingungen für das Festlegen dieser Ziele. Zusätzlich werden in dieser Richtlinie die Verpflichtung zur Erfüllung der Anforderungen der Informationssicherheit und zur ständigen Verbesserung des ISMS festgehalten. (ISO/IEC 27001:2013-10, 2013)

Nachdem bereits darauf aufmerksam gemacht wurde, dass ein ISMS ohne Kommunikation keinen Mehrwert für eine Organisation bringen kann, ist es laut dem Standard eine Führungsaufgabe die definierte Richtlinie innerhalb der Organisation und (sofern sinnvoll) den Stakeholdern zu kommunizieren. In diesen Bereich fällt auch die Dokumentation der Richtlinie. (ISO/IEC 27001:2013-10, 2013)

Unter der Überschrift *Rollen, Verantwortlichkeiten und Kompetenzen* versteht die ISO 27001:2013 die Zuteilung von Verantwortlichkeiten und Kompetenzen im Umfeld des ISMS. Der Standard hebt an dieser Stelle die Verantwortung für die Einhaltung des Standards sowie die Reporting-Funktion an das oberste Management über die Leistung des ISMS hervor. Abgesehen davon können und sollten auch weitere Rollen für die Verwaltung des ISMS definiert werden. Kersten et. al. (2016) weisen an dieser Stelle darauf hin, dass abgesehen vom Sicherheitsmanagement „auch das Asset Management, die Prozessverantwortlichen, Abteilungskoordinatoren, IT-Notfallbeauftragte, […], usw.“ von den definierten Rollen und Verantwortlichkeiten betroffen sind. Üblicherweise haben Organisationen die Möglichkeit, je nach Bedarf Rollen zu definieren und mit den nötigen Verantwortlichkeiten und Kompetenzen auszustatten. Diese Freiheit kann jedoch durch gewisse Kontrollziele des Anhang A eingeschränkt werden. (Kersten, Klett, Reuter, & Schröder, 2016)

2.2.1.3 Planung

Die Planung ist im sechsten Kapitel des Standards beschrieben und hat zum Ziel den Umgang mit Chancen und Risiken zu definieren. Im Gegensatz zur Version von 2005 fällt auf, dass in der aktuellen Version der Risikobegriff um positive Auswirkungen (die Chancen) erweitert wurde. Zusätzlich fällt in diesen Schritt auch die Festlegung von Sicherheitszielen und die

Planung zur Erreichung ebendieser. Dieses Kapitel des Standards setzt sich aus den folgenden Abschnitten zusammen:

- Planung von Maßnahmen zur Behandlung von Chancen und Risiken
- Informationssicherheitsziele und Planung zur Erreichung dieser Ziele

Um ein ISMS planen zu können muss laut Norm der Kontext der Organisation definiert sein. Was diesen Kontext ausmacht wird in Kapitel 4 des Standards behandelt und wurde bereits in Abschnitt 2.2.1 dieser Arbeit beschrieben. In Bezug auf diesen Kontext verlangt der Standard ISO/IEC 27001:2013, dass abhängig davon die Chancen und Risiken identifiziert werden sollen. Die Chancen und Risiken sollen ermittelt werden, um die folgenden Ziele des ISMS erreichen zu können:

- Es soll sichergestellt werden, dass das ISMS den erwarteten Nutzen erbringt.
- Ungewollte Auswirkungen sollen vermieden oder zumindest reduziert werden.
- Kontinuierliche Verbesserung des ISMS

Der Standard schreibt vor, dass die Organisation Maßnahmen definiert, mit denen die erkannten Chancen und Risiken behandelt werden können. Außerdem soll geplant werden, wie diese Maßnahmen umgesetzt und in die ISMS-Prozesse integriert werden können. Ergänzend dazu soll außerdem überlegt werden, wie die Effektivität dieser Maßnahmen gemessen werden kann. Für die Nachweisbarkeit sollten (im Falle einer Zertifizierung: müssen) alle getroffenen Maßnahmen und Prozesse dokumentiert werden. (ISO/IEC 27001:2013-10, 2013)

Ein großer Teil der Planung für das ISMS befasst sich mit dem Risikomanagement beziehungsweise der Risikoabschätzung – dieser Teil stellt vermutlich auch den arbeitsaufwändigsten Teil dieses Arbeitsschrittes dar. Der Standard widmet sich dementsprechend umfangreich der Planung zur Erkennung und Behandlung von Risiken. Das Risikomanagement der ISO-27000-Familie wird durch den Standard 27005 definiert, auf den später noch genauer eingegangen wird. Dieser Standard befasst sich explizit mit dem Risikomanagement von Sicherheitsrisiken im IT-Umfeld und ist in Abbildung 5 dargestellt. Die folgenden Absätze beschreiben den Risikomanagement-Prozess, wie er von der ISO 27001:2013 gefordert wird und stellen zeitgleich einen Bezug zum Prozess der ISO 27005 her.

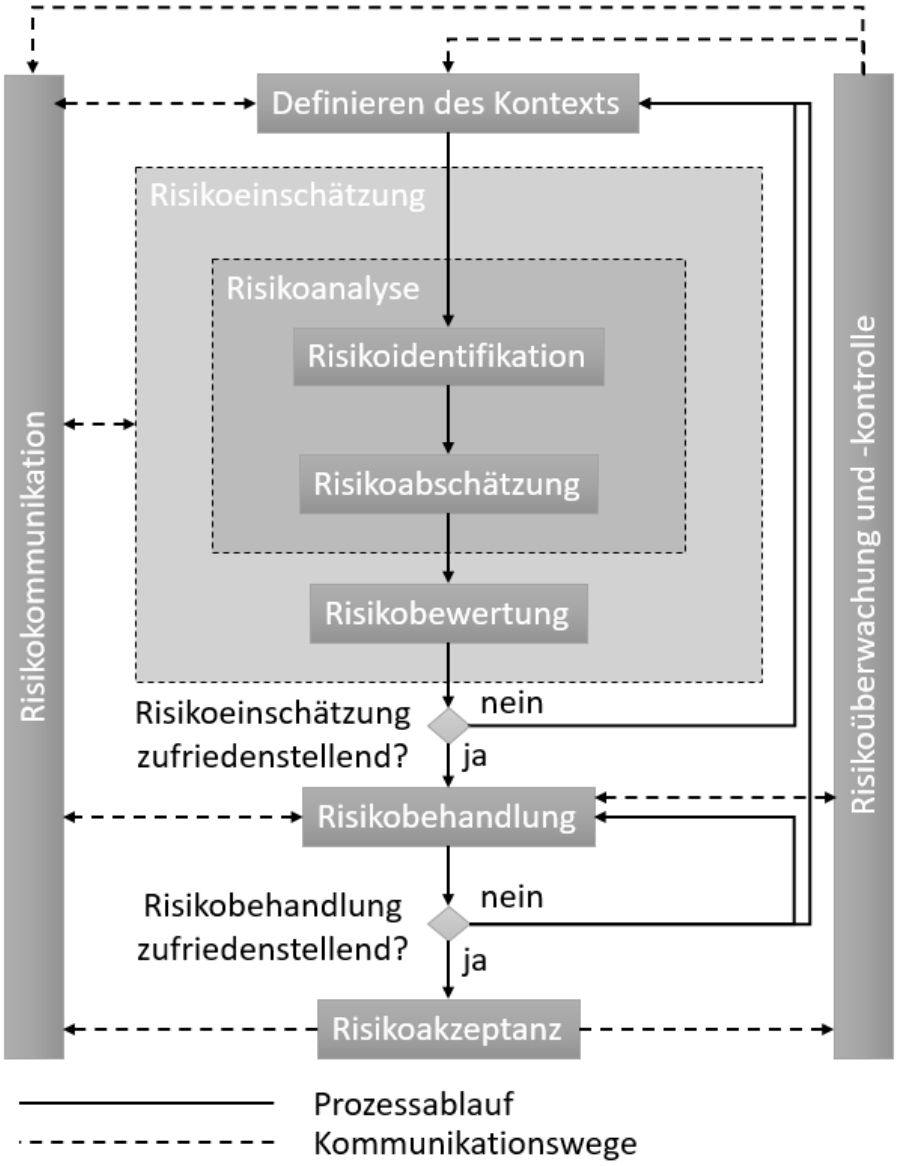

Abbildung 5: Risikomanagementprozess der ISO 27005 (ISO/IEC 27005:2011, 2011)

Für das Risikomanagement im Rahmen der ISO 27001:2013 muss im ersten Schritt ein Prozess für den Umgang mit auftretenden Chancen und Risiken im Bereich der Informationssicherheit definiert werden. Für diesen Prozess müssen nach Anforderung der ISO/IEC 27001:2013 zum einen die Kriterien definiert werden, die spezifizieren unter welchen Umständen Chancen und Risiken akzeptiert werden können, und zum anderen Richtlinien für die Durchführung von Risikobeurteilungen im IT-Umfeld aufgestellt werden. In Abbildung 5 entspricht dies dem Bereich der *Risikoeinschätzung* und stellt den Rahmen für die kommenden Schritte dar. Zusätzlich muss sichergestellt werden, dass dieser Prozess gültige, vergleichbare und stabile Ergebnisse liefert. (ISO/IEC 27001:2013-10, 2013)

Nachdem der Prozess für die Risikobeurteilung definiert wurde, werden anschließend Chancen und Risiken für das Unternehmen identifiziert. Im Risikomanagementprozess (Abbildung 5) entspricht dies dem Block *Risikoanalyse* bestehend aus den Prozessschritten der *Risikoidentifikation* und *-abschätzung*. Während die ISO 27001:2005 noch explizit die

Vermögenswerte beziehungsweise Assets des Unternehmens erwähnt hat, erweitert die Version 2013 den Begriff Risiken in Bezug auf Verlust der Verfügbarkeit, Integrität und/oder Geheimhaltung von Daten im Wirkungsraum des ISMS. Im ersten Prozessschritt wird überprüft, welche Bedrohungen für die Unternehmensdaten bestehen und wer die Verantwortlichen für diese Daten – und dementsprechend auch für die dazugehörigen Risiken – sind. (ISO/IEC 27001:2013-10, 2013)

Nach der erfolgten Risikoidentifizierung für die Daten des Unternehmens wird nun analysiert, welche möglichen Konsequenzen das Eintreten eines identifizierten Risikos hat und wie wahrscheinlich es ist, dass dieses Risiko tatsächlich eintritt. Wichtig ist, dass hier alle möglichen Varianten – auch die unrealistischen beziehungsweise sehr unwahrscheinlichen – in Betracht gezogen werden. Aus diesen zwei Werten (Schadensausmaß x Eintrittswahrscheinlichkeit) ergibt sich die Risikobewertung. Anhand dieses Wertes kann nun entschieden werden, wie mit den Risiken umgegangen wird. Der Block der Risikoeinschätzung im Risikomanagement (Abbildung 5) ist damit durchlaufen. (ISO/IEC 27001:2013-10, 2013)

Anhand der Risikobeurteilung lassen sich die bisher bekannten Risiken nun in verschiedene Kategorien unterteilen. Kersten et. al. (2008) empfehlen hier „zwei bis maximal vier Risikoklassen“, welche sich sinnvoll einsetzen lassen. Die Unterscheidung erfolgt dabei anhand der Auswirkung auf die Informationswerte der Organisation zum Beispiel von *geringe Auswirkungen* bis *unternehmensbedrohend*. Üblicherweise werden Risiken der niedrigsten Kategorie ignoriert (Kersten, Reuter, & Schröder, 2008). Dies muss nach ISO/IEC 27001 beziehungsweise der erarbeiteten Richtlinie zur Akzeptanz von Risiken entsprechend dokumentiert und dem Management kommuniziert werden. Diese Informationsverteilung ist auch im Risikomanagementprozess der ISO 27005 definiert. Alle verbleibenden (schwerwiegenderen) Risiken müssen einzeln behandelt werden.

Die ISO/IEC 27001:2013 schreibt unter Punkt 6.1.3 vor, dass für erkannte Risiken – die aufgrund der Risikoklasse und den definierten Richtlinien noch nicht akzeptiert werden können – angemessene Behandlungsmöglichkeiten gefunden werden müssen. Dies dient dazu, ein Risiko soweit abzumildern, dass es im Rahmen der Risikobeurteilung akzeptiert werden kann. Grundsätzlich gibt es vier (nicht-exklusive) Möglichkeiten der Risikobehandlung:

- Vermeidung von Risiken
- Reduzierung von Risiken
- Transfer von Risiken
- Akzeptanz von Risiken

Bei der Vermeidung von Risiken geht es darum, eine Schwachstelle komplett zu vermeiden oder eine risikobehaftete Tätigkeit zu unterlassen. Dies kann beispielsweise durch den Austausch von Komponenten oder Prozessänderungen erfolgen. Ebenso kann auch die Wahl des Standortes ein Teil der Risikovermeidung sein. Für Unternehmen könnte dies beispielsweise die Wahl des Standortes für das oder die Rechenzentren beeinflussen – das Rechenzentrum wird idealerweise nicht in einem hochwassergefährdeten Gebiet errichtet. (Klipper, 2011)

Die Reduzierung von Risiken wird in der Regel mit proaktiven Maßnahmen erreicht – es werden bereits Pläne für den Schadensfall angefertigt und damit wird zum Beispiel die Ausfallzeit einer zentralen Komponente deutlich minimiert. Diese Möglichkeit ist die aufwändigste der aufgezeigten Alternativen, da hier meistens Änderungen an der Organisation, der Infrastruktur, den Prozessen und anderen Teilen des Unternehmens vorgenommen werden müssen. (Klipper, 2011)

Beim Transfer von Risiken geht es um die Weitergabe der Risiken an Dritte. Im Geschäftsumfeld sind dies üblicherweise Versicherung, Lieferanten und Kunden. Gegen negative Presse im Schadensfall hilft diese Methode der Risikobehandlung allerdings nicht. Problematisch ist, dass zwar die bekannten Risiken behandelt werden, sich allerdings neue Risiken (beispielsweise durch Outsourcing) auftun können, die wiederum behandelt werden müssen. (Klipper, 2011)

Neben diesen gängigen Methoden zur Reduktion von Risiken erlaubt der Standard auch zusätzlich eigene Maßnahmen zur Risikoreduktion zu definieren und anzuwenden. Typisch für die Anforderungen der ISO 27001 kann dies aber nur mit entsprechender Begründung und Dokumentation erfolgen.

Nachdem die grundsätzlichen Möglichkeiten zur Risikobehandlung gesichtet und ausgewählt wurden, müssen nun konkrete Maßnahmen für die Umsetzung der gewählten Optionen definiert werden. Kersten, Klett, Reuter und Schröder (2016) weisen darauf hin, dass es sich dabei um „vertragliche, organisatorische, personelle, technische und sonstige Maßnahmen“ handeln kann. Bei der Auswahl können Maßnahmengruppen auch ausgeschlossen werden, weil beispielsweise die Umsetzung zu aufwändig ist oder die Usability eingeschränkt wird. Im Falle von Ausschlüssen müssen diese dokumentiert werden. (Kersten, Klett, Reuter, & Schröder, 2016)

Der erarbeitete Maßnahmenkatalog muss nun separat für alle betroffenen Daten mit Anhang A der ISO 27001:2013 abgeglichen werden – dies dient dazu, dass keine notwendigen Maßnahmen übersehen werden. Der Anhang A der ISO/IEC 27001 stellt dafür eine umfangreiche Liste und die dazugehörigen Kontrollziele zu Verfügung, aus denen die entsprechenden Maßnahmen für die einzelnen Risiken ausgewählt werden können. Die getroffenen Maßnahmen müssen für alle Risiken zusammen mit der erwarteten Risikoreduktion dokumentiert werden. Falls eine Maßnahme für ein gefundenes Risiko nicht relevant ist, ist dies zu begründen und zu dokumentieren. Diese Maßnahmenbewertung erfolgt mit den schon erwähnten Risikoverantwortlichen. (Kersten, Reuter, & Schröder, 2008)

Im Risikomanagementprozess der ISO 27005:2011 stellt sich nun die Frage, ob ein Risiko ausreichend behandelt wurde und akzeptiert werden kann. Sollte diese Frage nur mit *nein* beantwortet werden können, muss zumindest die Risikobehandlung und gegebenenfalls auch der gesamte Prozess erneut durchlaufen werden, um weitere Möglichkeiten zu finden, die bestehenden Risiken zu minimieren. Für die Akzeptanz von Risiken ist es im Kontext der Planung unerheblich, ob diese Maßnahmen bereits umgesetzt wurden oder nicht. Falls ein Risiko durch die geplanten Maßnahmen ausreichend abgemindert wurde und akzeptiert werden kann, erfolgt eine entsprechende Dokumentation.

Die ISO 27001:2013 verlangt, dass diese Dokumentation der Maßnahmenbewertung in seiner Gesamtheit in das sogenannte *Statement of Applicability* überführt wird. Dieses *Statement of Applicability* kann man sich als eine Liste aller Informationswerte eines Unternehmens zusammen mit den gewählten (unabhängig woher diese stammen) und ausgelassenen Maßnahmen des Anhang A inklusive den entsprechenden Begründungen vorstellen. (ISO/IEC 27001:2013-10, 2013)

Daraus ergibt sich im weiteren Verlauf der Risikobehandlungsplan. Dieser Plan listet alle Risiken zusammen mit den entsprechenden Maßnahmen zur Risikoreduktion auf. Der Plan zur Risikobehandlung muss sowohl von den Risikoeignern als auch vom Management angenommen werden und liefert die Grundlage für die tatsächlichen Tätigkeiten im Rahmen des ISMS. (ISO/IEC 27001:2013-10, 2013)

Wie anfangs bereits erwähnt, befasst sich der zweite große Block der Planungstätigkeit mit den Sicherheitszielen und der dazugehörigen Planung. Der Standard schreibt vor, dass die Organisation für entscheidende Funktionen und Ebenen in der Organisation angemessene Informationssicherheitsziele definieren soll. Diese Ziele müssen in Übereinkunft mit der definierten IT-Sicherheitsrichtlinie stehen und (sofern möglich und sinnvoll) messbar sein. Bei der Definition der Sicherheitsziele sollten sowohl anwendbare Informations-sicherheitsanforderungen als auch die Ergebnisse des Risikomanagementprozesses berücksichtigt werden. Damit diese Ziele auch wirksam werden können, müssen sie den relevanten Rollen kommuniziert werden und in angemessener Art aktualisiert werden. Diese Aktualisierung wird üblicherweise durch die Ergebnisse eines erneuten Durchlaufes des Risikomanagementprozesses angestoßen. (ISO/IEC 27001:2013-10, 2013)

Für die Erreichung der Informationssicherheitsziele schreibt die ISO 27001:2013 vor, dass die Informationssicherheitsziele eine Beschreibung der Maßnahmen, die benötigten Ressourcen, die Verantwortlichen, das Datum der Umsetzung und eine Beschreibung der Bewertung der Zielerreichung beinhalten (ISO/IEC 27001:2013-10, 2013).

Mit der Fertigstellung dieser Schritte ist die Planungstätigkeit für das ISMS abgeschlossen beziehungsweise für weitere Iterationen vorbereitet.

2.2.1.4 Unterstützung

Das Schlagwort Unterstützung bildet das 7. Kapitel des Standards. In diesem Kapitel werden – wie der Name bereits vermuten lässt – die Merkmale behandelt, die den Betrieb des ISMS unterstützen sollen. Das Kapitel der Norm gliedert sich dabei in die folgenden Abschnitte:

- Ressourcen
- Weiterbildungsmaßnahmen
- Bewusstseinsbildung
- Kommunikation
- Dokumentation

Unter dem Punkt *Ressourcen* verbirgt sich eigentlich ein Punkt, der bereits im fünften Kapitel der Norm (Führung) angesprochen wurde. Die Organisation (und damit das Management) hat die Aufgabe, die notwendigen Ressourcen für Planung, Umsetzung, Betrieb und Verbesserung des ISMS zu ermitteln und zur Verfügung zu stellen. Unter Ressourcen fallen in diesem Fall beispielsweise technische Mittel und Personal, allerdings können auch Beratungsleistungen von externen Dienstleistern hierunter fallen. An dieser Stelle wird wieder die enge Verbundenheit des Standards mit dem PDCA-Zyklus offensichtlich. Auch Kersten et. al. (2016) weisen darauf hin, dass die Ressourcen für den kompletten „Lebenszyklus“ des ISMS abzuschätzen und bereitzustellen sind. Außerdem heben sie hervor, dass auch der Risikobehandlungsplan Ressourcen bindet, die nicht außer Acht gelassen werden dürfen.

Der Bereich *Kompetenz* behandelt den Wissensaufbau in der Organisation. Der Standard schreibt vor, dass für alle Rollen des ISMS die notwendigen Kompetenzen ermittelt werden sollen. Auf dieser Basis hat die Organisation sicherzustellen, dass die Personen, die diese Rollen einnehmen, tatsächlich den geforderten Wissensstand aufweisen. Falls es hier eine Abweichung vom geforderten Wissen geben sollte, muss die Organisation (wenn möglich) für entsprechende Weiterbildungsmaßnahmen sorgen. Die Dokumentation dieser Weiterbildungsmaßnahmen stellt einen Teil der Dokumentensammlung des ISMS dar. (ISO/IEC 27001:2013-10, 2013)

Der nächste Abschnitt dieses Kapitels im Standard widmet sich der *Bewusstseinsbildung*. Dieser Abschnitt besagt, dass allen Mitarbeitern der Organisation die Informationssicherheitsrichtlinie zur Kenntnis gebracht werden muss. Darüberhinausgehend soll aber auch der Beitrag der einzelnen Personen zum Gesamtziel des funktionierenden ISMS und die Vorteile einer verbesserten Informationssicherheit hervorgehoben werden. Ergänzend zu den Vorteilen soll auch darauf hingewiesen werden, welche Folgen ein Verstoß gegen die Anforderungen des ISMS nach sich zieht (ISO/IEC 27001:2013-10, 2013). Zu diesen Folgen können laut Kersten et. al. (2016) unter anderem zusätzliche Weiterbildungsmaßnahmen, dienstrechtliche Konsequenzen und Vertragsstrafen zählen.

Nach der Bewusstseinsbildung folgt im Kapitel *Unterstützung* der Abschnitt *Kommunikation*. Der Standard gibt an dieser Stelle keine wirklichen Auflagen, sondern verlangt nur, dass die Organisation den Bedarf an interner und externer Kommunikation ermitteln soll. Dieser Bedarf schließt ein, was wann wem kommuniziert wird und vom wem diese Kommunikation ausgeht. Des Weiteren verlangt die Norm eine Darstellung dieses Prozesses (ISO/IEC 27001:2013-10, 2013). In einem ersten Ansatz könnte man hierunter die Einführung einer Kommunikationskultur, wie es zum Beispiel in Projekten der Fall ist, verstehen. Kersten et. al. (2016) erläutern in ihrem Buch über die ISO 27001:2013 was mit diesem Abschnitt der Norm versucht wird zu erreichen: Es sollen hierdurch gewisse Kommunikationswege entweder unterstützt beziehungsweise erzwungen werden (beispielsweise Reporting an das Management oder die Kommunikation mit Vertragspartnern) oder sogar verboten werden (zum Beispiel die Herausgabe von Informationen an unbeteiligte Dritte).

Der letzte Teil des Kapitels *Unterstützung* befasst sich mit der Dokumentation des ISMS. Grundsätzlich soll das ISMS sämtliche Dokumente enthalten, die vom Standard gefordert

werden und ergänzend dazu die Informationen, welche dem Betrieb des ISMS dienlich sind (ISO/IEC 27001:2013-10, 2013). Beim letzten Punkt hat die Organisation Wahlfreiheit (auch wenn ein Auditor vermutlich kritisch hinterfragen wird, warum keine zusätzliche Dokumentation vorhanden ist). Ansonsten stellen die folgenden Dokumente das absolute Mindestmaß an nötiger Dokumentation dar:

- Der Anwendungsbereich des ISMS
- Die Informationssicherheitsrichtlinie
- Der Risikoabschätzungsprozess
- Der Risikobehandlungsprozess
- Die Informationssicherheitsziele
- Die Kompetenznachweise
- Die Prozessdokumentation
- Die Ergebnisse der Risikoabschätzung
- Die Ergebnisse der Risikobehandlung
- Nachweise für Monitoring und Messung
- Nachweise über vorgenommene Audits
- Nachweise über die Ergebnisse der Management Reviews
- Nachweise über Abweichungen und korrektive Maßnahmen (sowie deren Ergebnisse)

Im Standard wird hervorgehoben, dass die Menge an Dokumentation von Unternehmen zu Unternehmen unterschiedlich sein kann, da dies von der Größe und Art des Unternehmens, der Komplexität der Unternehmensabläufe und dem Wissensstand der Personen abhängen kann. Aufgrund der Anzahl an zwingend erforderlichen Dokumenten verlangt der Standard im gleichen Abschnitt auch die Einführung eines Informations-Lifecycles. Beim Erstellen und Aktualisieren von Dokumenten hat die Organisation sicherzustellen, dass Dokumente nach gewissen Standards angelegt werden. So sollen die Informationen identifizierbar sein, ein gewisses Format (sowohl inhaltlich als auch medienbezogen) aufweisen und vor Veröffentlichung genehmigt werden. (ISO/IEC 27001:2013-10, 2013)

Neben der Erstellung und Aktualisierung müssen Informationen auch kontrolliert werden. Auch diesem Bereich widmet sich der Standard und schreibt vor, dass die Organisation sicherstellen muss, dass die (für den Betrieb des ISMS) erforderlichen Dokumente im Bedarfsfall verfüg- und verwendbar sind. Zusätzlich ist sicherzustellen, dass die Informationen gegen unerlaubte Veränderung geschützt sind. Abgesehen davon sollte, sofern anwendbar, kontrolliert werden wie Informationen verteilt beziehungsweise bezogen und verwendet werden und welche Personen dazu berechtigt sind. Außerdem soll sichergestellt werden, dass die Informationen entsprechend gelagert werden, Änderungen nachvollzogen werden können und veraltete oder überarbeitete Dokumente zurückgezogen werden können. Dies schließt natürlich auch Informationen aus externen Quellen mit ein. (ISO/IEC 27001:2013-10, 2013)

2.2.1.5 Betrieb

Während in der Version von 2005 in diesem Bereich überwiegend der Risikobehandlungsplan behandelt wurde, wird in der aktuellen Version des Standards überwiegend tatsächlich der

Betrieb des ISMS beschrieben. Der Standard unterscheidet hier drei verschiedene Tätigkeiten beziehungsweise Tätigkeitsfelder:

- Planung, Betrieb und Kontrolle der Prozesse
- Informationssicherheitsrisikobewertung
- Informationssicherheitsrisikobehandlung

Tatsächlich widmet sich dieses Kapitel viel mehr der eigentlichen Durchführung als das gleiche Kapitel in der Version aus dem Jahr 2005, es wurde eine deutlichere Abgrenzung zwischen Planungs- und Durchführungstätigkeiten vorgenommen (ISO/IEC 27001:2013-10, 2013). Auch Kersten et. al. (2016) heben hervor, dass es in diesem Abschnitt der Norm um die Durchführung der Maßnahmen aus Kapitel 4 der Norm (2.2.1 in dieser Arbeit) und um das tatsächliche Durchlaufen des Risikomanagementprozesses aus Kapitel 6 des Standards (2.2.3 in dieser Arbeit) geht.

Unter dem ersten angesprochenen Punkt versteht der Standard die Planung, Einführung und Kontrolle der Geschäftsprozesse, um den Anforderungen an die Informationssicherheit gerecht zu werden. Üblicherweise bedeutet dieser Schritt eher nicht die Einführung neuer Prozesse, sondern die Adaption bestehender Geschäftsprozesse. Außerdem sollen die Maßnahmen zur Risikobehandlung und zur Erreichung der Informationssicherheitsziele umgesetzt werden. Wie bereits bei der Dokumentation angesprochen, sind diese Anpassungen und vorgenommenen Maßnahmen entsprechend zu dokumentieren. (ISO/IEC 27001:2013-10, 2013)

Die Norm sieht vor, dass geplante Änderungen an den Geschäftsprozessen hinsichtlich unerwarteter Folgen überprüft werden sollen und gegebenenfalls Gegenmaßnahmen ergriffen werden müssen, um negative Effekte zu vermeiden. (ISO/IEC 27001:2013-10, 2013)

Prinzipiell müssen alle ausgelagerten Prozesse mit der gleichen Sorgfalt geprüft werden, wie die internen Prozesse. Kersten et. al. (2016) heben hervor, dass dies ein Punkt ist, der in der Praxis üblicherweise auf den entsprechenden Dienstleister ausgelagert wird. Das einfache Weitergeben von Verantwortung soll dadurch vermieden werden.

In den folgenden zwei Abschnitten der Norm wird verlangt, dass die Risikobewertung und Risikobehandlung entsprechend der im Planungskapitel festgelegten Kriterien umgesetzt werden. Die Risikobewertung soll regelmäßig oder nach größeren Änderungen durchgeführt werden. Die Ergebnisse beider Tätigkeiten sind dabei zu dokumentieren. (Kersten, Klett, Reuter, & Schröder, 2016)

2.2.1.6 Evaluierung

In diesem Kapitel der Norm geht es um die Überwachung und Bewertung der Leistung beziehungsweise der Effektivität des ISMS. Dabei wird dieser Schritt in drei Abschnitte gegliedert:

- Überwachung, Messung, Analyse und Bewertung
- Interne Überprüfungen

- Management Review

Der erste Abschnitt befasst sich mit der konkreten Bewertung des ISMS. Zu diesem Zweck schreibt der Standard vor, dass zum einen erfasst werden muss, welche Informationen, Prozesse und Anforderungen gemessen werden sollen und zum anderen, welche Methoden für diese Messung zum Einsatz kommen sollen (ISO/IEC 27001:2013-10, 2013). Dabei steht im Vordergrund, dass diese Methoden wiederholt ähnliche Ergebnisse erzeugen und damit vergleichbar sind. Kersten et. al. (2016) weisen ebenfalls darauf hin, dass die eingesetzten „Methoden zu aussagekräftigen und vergleichbaren Daten führen“ sowie reproduzierbare Ergebnisse erzeugen müssen.

In diesem Abschnitt wird außerdem festgelegt, wann die erforderlichen Daten erhoben werden und wer für die Erhebung dieser Daten zuständig ist (ISO/IEC 27001:2013-10, 2013). Dabei ist darauf zu achten, dass ein Monitoring auf regelmäßiger Basis (zum Beispiel durch automatisierte Logfile-Analysen) vorgenommen wird. Kersten et. al. (2016) heben dazu hervor, dass gerade das Monitoring in kurzen Intervallen vorgenommen werden sollte und „Management-Aspekte“ durchaus in größeren Abständen überprüft werden können. Wichtig ist, dass es regelmäßig passiert.

Neben der Zuständigkeit für die Datenerhebung ist auch erforderlich, dass definiert wird, wann diese Daten evaluiert werden und wer für diese Evaluierung zuständig ist (ISO/IEC 27001:2013-10, 2013). Um unangenehme Fragen im Rahmen eines Audits zu vermeiden, ist es sinnvoll, die Erhebung und die Evaluierung der Daten von verschiedenen Personen vornehmen zu lassen. Analog dazu sollten Prozesse oder Applikationen ebenso nicht von den Prozess- oder Applikationsverantwortlichen bewertet werden. Dies unterstreichen auch Kersten et. al. (2016) bei der Beschreibung dieses Abschnittes des Standards.

Grundsätzlich sind die erfassten Daten und die Ergebnisse der Evaluierung im Rahmen der ISMS-Tätigkeit zu dokumentieren, damit im Rahmen einer Zertifizierung belegt werden kann, dass dieser Abschnitt behandelt wurde.

Der nächste Abschnitt des Standards legt die Bedingungen für interne Auditierungen fest. Dabei gilt es zu überprüfen, ob das ISMS zum einen den eigenen Anforderungen und zum anderen den Anforderungen der ISO 27001 entspricht sowie wie erwartet arbeitet (ISO/IEC 27001:2013-10, 2013). Im Standard wird es nicht explizit erwähnt, aber Kersten et. al. (2016) ergänzen, dass für die internen Audits die gleichen Regeln wie für die regelmäßigen Messungen gelten sollen. Das heißt, dass die Audits reproduzierbare und objektive Ergebnisse liefern sollen.

Für die Audits hat die jeweilige Organisation dafür zu sorgen, dass entsprechende Audits geplant und durchgeführt werden. Teil dieser Planung ist, dass definiert wird, wie oft diese durchgeführt werden, welche Vorgehensweise dafür angewendet wird, wer dafür verantwortlich ist und wie die Reporting-Struktur aussieht. Der Standard weist darauf hin, dass die Wichtigkeit der zu überprüfenden Prozesse und vorhergegangenen Ergebnisse mit in diese Planung einfließen sollen. Zusätzlich sind die Kriterien für Audits und der Geltungsbereich für jedes Audit festzulegen. Bei der Wahl der Auditoren ist darauf zu achten, dass diese objektiv und unabhängig agieren können. Dies entspricht auch der bereits angesprochenen Trennung von

Datenerfassung und -analyse im vorhergehenden Abschnitt des Standards. Da die internen Audits eines der wichtigsten Werkzeuge für die Leistungsbewertung des ISMS darstellen, ist es wichtig, dass die Ergebnisse dem Management kommuniziert und entsprechend dokumentiert werden. (ISO/IEC 27001:2013-10, 2013)

Im letzten Teil dieses Abschnittes in der Norm wird der Management Review behandelt. Der Sinn des Management Reviews liegt darin, dass die Unternehmensführung in regelmäßigen Abständen über die Tätigkeiten des ISMS informiert wird. Ziel dieses Reportings ist es, festzustellen, ob das ISMS noch den Anforderungen des Unternehmens entspricht.

Der Standard definiert, dass der Management Review (wenn vorhanden) den Bearbeitungsstand von geforderten Tätigkeit aus vorhergegangen Management Reviews enthält. Zusätzlich ist gefordert, dass ISMS-relevante Änderungen bei internen oder externen Umwelten im Managementbericht enthalten sind. Außerdem müssen Trends hinsichtlich Regelabweichungen, Monitoring und Audits sowie Rückmeldungen der Stakeholder enthalten sein. Darüberhinausgehend ist das Management über die Ergebnisse der Risikoabschätzung und der Risikobehandlung zu informieren. Abschließend sollen mögliche Ansätze für kontinuierliche Verbesserungsmaßnahmen enthalten sein. Die Ergebnisse (Änderungen und Entscheidungen) dieses Management Reviews sind zu dokumentieren. (ISO/IEC 27001:2013-10, 2013)

2.2.1.7 Verbesserung

Das letzte (für eine Zertifizierung verpflichtende) Kapitel des Standards widmet sich der (kontinuierlichen) Verbesserung. Nachdem der Standard nicht mehr explizit auf einem PDCA-Zyklus aufsetzt, hat dieses Thema nun ein eigenes Kapitel in der Norm erhalten. Inhalt dieses Kapitels sind Abweichungen (und daraus resultierende Korrekturen) und die kontinuierliche Verbesserung.

Der erste Teil dieses Kapitels beschreibt, was das Unternehmen bei Abweichungen von den Anforderungen des ISMS zu tun hat. Und zwar hat die Organisation im ersten Schritt dafür zu sorgen, dass die Abweichung kontrolliert und dann behoben wird. Im Zuge der notwendigen Nacharbeiten ist mit den entstandenen Folgen umzugehen. Nachdem die Abweichung selbst korrigiert wurde, ist die Organisation dazu aufgefordert, Ursachenforschung zu betreiben, damit die Abweichung nicht mehr auftritt (auch nicht an anderer Stelle). Zu diesem Zweck muss die Abweichung analysiert werden, die Ursache für die Abweichung gefunden werden und anschließend überprüft werden, ob die gefundenen Ursachen (und damit langfristig auch die Abweichung) auch noch an anderen Stellen vorhanden sind. Darauf aufbauend verlangt der Standard, dass notwendige Maßnahmen umgesetzt werden und der Erfolg dieser Maßnahmen überprüft wird. Gegebenenfalls können auch Änderungen am ISMS die Folge sein. (ISO/IEC 27001:2013-10, 2013)

Kersten et. al. (2016) ergänzen dazu, dass die korrektiven Maßnahmen angemessen sein müssen. Das heißt, dass kleine Abweichungen keine Maßnahmen mit exorbitanten Kosten

nach sich ziehen sollten. Eine Abschätzung der (unter anderem finanziellen) Folgen ist zwingend notwendig.

Weitergedacht kann es auch durchaus vorkommen, dass eine korrigierende Maßnahme an einer Stelle eine negative Folge an anderer Stelle (zum Beispiel in einem anderen Prozess) nach sich zieht. In diesem Fall muss abgewogen werden, welcher Nachteil der kleinere ist oder ob es vielleicht eine andere Möglichkeit der Korrektur gibt, welche keine oder weniger gravierende Folgen hat.

Die Eingriffe sind gemäß den Anforderungen der ISO 27001 zu dokumentieren. Die Dokumentation setzt sich dabei aus der Art der Abweichung, den Maßnahmen und dem Ergebnis dieser Maßnahmen zusammen (ISO/IEC 27001:2013-10, 2013).

Der letzte Abschnitt der Norm stellt explizit die kontinuierliche Verbesserung in den Vordergrund und verlangt, dass die Organisation fortlaufend die Eignung, Angemessenheit und Effizienz des ISMS verbessern muss (ISO/IEC 27001:2013-10, 2013). Im ersten Augenblick wirkt das erneute erwähnen dieser Verbesserung ein wenig redundant, da sie auch in den entsprechenden Kapiteln der Norm verlangt wird. Allerdings wird dadurch hervorgehoben, wie wichtig das ständige Verbessern des ISMS in der Praxis ist. Ein ISMS, welches nicht ständig an neue Gegebenheiten (seien dies nun neue Bedrohungen oder geänderte Anforderungen der Stakeholder) angepasst wird, ist für das Unternehmen nur noch Ballast und hat keinen Nutzen mehr. Im schlimmsten Fall vermittelt das (veraltete) ISMS nur eine Sicherheit, die nicht mehr vorhanden ist.

Damit sind die Grundanforderungen der ISO 27001 beschrieben und der folgende Unterabschnitt beschreibt, wie sich diese Anforderungen in die Praxis übertragen lassen könnten. Die folgende Abbildung 6 stellt die ISO 27001:2013 dar.

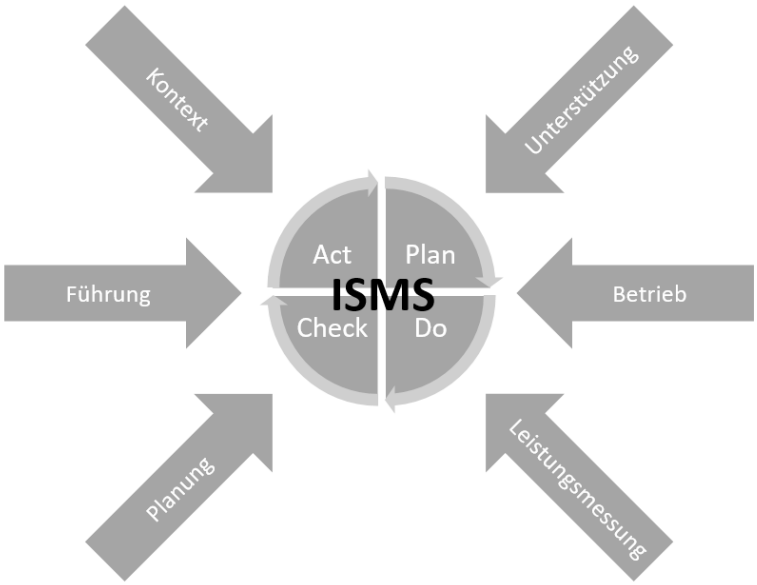

Abbildung 6: Aufbau der ISO 27001:2013

2.2.2 ISO 27002

Ein wichtiger Bestandteil der ISO 27001 wurde bisher nur am Rande erwähnt: der Anhang A. Der Anhang A stellt eine Referenzliste für mögliche Sicherheitsanforderungen und Maßnahmen im Kontext der ISO 27001 dar. Dieser Anhang ist direkt an den Standard ISO 27002 geknüpft und hat den gleichen Aufbau. Allgemein gehalten deckt der Anhang A verschiedenste Ziele hinsichtlich des ISMS ab – angefangen beim Erstellen und Aktualisieren der Policies, über Kontrollziele für mobile Endgeräte und Teleworking, bis hin zur Sicherheit in Entwicklungsprozessen. (ISO/IEC 27001:2013-10, 2013)

Grundsätzlich sind alle dieser Anforderungen zu behandeln, dies kann aber auch über Hierarchien innerhalb des Assetmanagements einer Organisation vereinfacht werden – es wird davon ausgegangen, dass eine nachgeordnete Ressource die Anforderungen an die höherrangige Ressource ebenfalls erfüllt (Kersten, Klett, Reuter, & Schröder, 2016). Die ISO sieht die ISO 27002 eher als möglichen Anfangspunkt für die Entwicklung von eigenen Richtlinien (ISO/IEC 27002:2013, 2013).

Die gesammelten Sicherheitsanforderungen stellen, zusammen mit den Maßnahmen der Risikobehandlung, den Inhalt des Statement of Applicability dar. Hier werden entsprechende Anforderungen mit konkreten Maßnahmen, wie diese Anforderungen erreicht werden sollen, dokumentiert. Kersten et. al. (2016) heben in Bezug auf den Anhang A hervor, dass nicht alle Anforderungen ausgewählt werden müssen, die Auslassungen aber dokumentiert und entsprechend durch gleichwertige Anforderungen ersetzt werden müssen.

Die einzelnen Kapitel der ISO 27002 sind so aufgebaut, dass zuerst das Ziel, welches durch die jeweilige Anforderung erreicht werden soll, angeführt wird und darauf aufbauend eine oder mehrere Maßnahmen sowie Umsetzungsempfehlungen angeführt werden.

Die ISO 27002 ist in 14 Themenbereiche untergliedert, die verschiedene Aspekte der Informationssicherheit aufgreifen und Organisationen bei der Umsetzung der Anforderungen aus der ISO 27001 unterstützen sollen. Diese Themenbereiche sind in der nachfolgenden Tabelle aufgelistet.

Informations-sicherheits-richtlinien	Organisation der Informations-sicherheit	Personelle Sicherheit	Asset-Management	Zugriffskontrolle
Kryptographie	Physische Sicherheit	Sicherheit im Betrieb	Sicherheit in der Kommunikation	Beschaffung, Entwicklung und Instandhaltung von Systemen
Lieferanten-beziehungen	Informations-sicherheits-vorfälle	Informations-sicherheit im Business Continuity Management		

Tabelle 2: Inhalt der ISO 27002 (ISO/IEC 27002:2013, 2013)

Bei der Betrachtung der einzelnen Kapitel fällt auf, dass gewisse Themenbereiche wie die Zugriffskontrolle oder die Kryptographie eigentlich in vielen weiteren internen Standards oder Prozessen wiederzufinden sind und andere Themenbereiche wie die personelle Sicherheit durchaus auch ohne wechselseitige Beziehungen verwendet werden können. Dies muss besonders im Entwicklungsprozess und bei der Dokumentation der jeweiligen Richtlinien bedacht werden.

Da eine komplette Beschreibung des Standards in dieser Arbeit zu umfassend wäre, wird nur auf das Kapitel 10 der ISO 27002 näher eingegangen. Dieses Kapitel befasst sich mit der angemessenen und effektiven Nutzung von Kryptographie um Vertraulichkeit, Authentizität sowie Integrität von Informationen zu gewährleisten. Die zwei im Standard vorgeschlagenen Maßnahmen befassen sich zum einen mit dem Verfassen einer Richtlinie zum Einsatz von kryptographischen Methoden und zum anderen mit dem Verfassen einer Richtlinie zum Schlüsselmanagement. Diese beiden Maßnahmen bzw. Richtlinien werden im Folgenden kurz beschrieben. (ISO/IEC 27002:2013, 2013)

Grundsätzlich soll die Richtlinie A.10 den Einsatz von kryptographischen Maßnahmen regeln. Dies betrifft vor allem die Punkte *Was ist zu schützen?* und *Wie ist es schützen?,* um die bereits angesprochenen Sicherheitsziele gewährleisten zu können. Dementsprechend ist für das Entwickeln dieser Richtlinie wieder das Risikomanagement ausschlaggebend, da es im Sinne der ISO 27005 beide Fragestellungen abdecken kann. Die ISO 27002 schlägt außerdem vor, dass entsprechende Rollen für die Verwaltung der kryptographischen Maßnahmen geschaffen werden und weist darauf hin, dass die kryptographischen Maßnahmen (genau genommen die Verschlüsselung) mit Bedacht einzusetzen sind. Diese Verschlüsselung kann Auswirkungen auf die Effektivität von anderen Security-Bausteinen (wie zum Beispiel Webfilter, Mailfilter und Antivirusprogramme) haben. Die genauen Anforderungen werden in einem späteren Teil der Arbeit, wenn es um die Formulierung genau dieser Richtlinie geht, beschrieben.

Bei der Richtlinie für Schlüsselmanagement geht es im Kern darum, einen kompletten Lebenszyklus für die kryptographischen Schlüssel einer Organisation zu implementieren. Angefangen beim Generieren und Ausstellen der Schlüssel, über das Verteilen der Schlüssel bis zum Außerkraftsetzen bei Ablauf oder Diebstahl/Verlust müssen für alle Schritte des Lebenszyklus entsprechende Prozesse eingeführt werden. Kersten et. al. (2016) heben hervor, dass auch die Verfügbarkeit der ausgestellten Schlüssel ein wichtiger Punkt ist, um diese im Verlustfall erneut einsetzen zu können.

Abschließend fällt auf, dass die Anforderungen zu kryptographischen Maßnahmen im Vergleich mit den anderen Anforderungen relativ kurzgehalten sind und das Thema eher gestreift wird. Auch Kersten et. al. (2016) weisen darauf hin, dass es sinnvoll ist, sich intensiv mit diesem Thema auseinander zu setzen. Den gestiegenen Stellenwert der kryptographischen Maßnahmen kann man im Versionsvergleich der ISO 27002 von 2013 und 2005 erkennen: im alten Standard wurde das Thema Kryptographie nicht behandelt.

2.2.3 ISO 27005

Die ISO 27005 ist wie auch die ISO 27002 als Leitlinie oder Handlungsempfehlung zu verstehen und bietet, wie bereits erwähnt, einen auf das ISMS zugeschnittenen Risikomanagementprozess. Der grundsätzliche Prozess wurde bereits im entsprechenden Kapitel zum ISMS beschrieben und wird daher an dieser Stelle nicht erneut erläutert.

Wie bereits deutlich geworden ist, sind die zwei Standards ISO 27005 und ISO 27001 sehr eng miteinander verzahnt. Ohne eine fundierte Risikoanalyse werden die getroffenen Maßnahmen im Rahmen des ISMS entweder nicht wirksam sein, komplett über das Ziel hinausschießen (und damit zu viele Ressourcen binden) oder im schlimmsten Fall beides sein. Aus diesem Grund liegt es nahe, eine hohe Integration von Sicherheits- und Risikomanagement anzustreben.

Klipper (2011) stellt die Frage, warum die ISO 27005 nicht komplett in die ISO 27001 integriert ist und beantwortet diese Frage auch selbst: Wie bereits erwähnt, ist die ISO 27001 der einzige Standard in der ISO 27000-Famile, über den sich eine Organisation zertifizieren lassen kann. Wenn nun allerdings der komplette Risikomanagementprozess ebenfalls zertifiziert wird, haben Unternehmen keinen großen Spielraum mehr bei der Anpassung dieses Risikomanagementprozesses – dieser Anpassungsspielraum wird jedoch für ein effektiv gelebtes Risikomanagement benötigt. Daher liegt es nahe diese zwei Standards zu trennen.

2.2.4 Andere Managementsysteme für Informationssicherheit

Abgesehen von der ISO-27000-Familie gibt es auch noch weitere Standards oder Umsetzungsempfehlungen für ISMS in Organisationen. Im deutschsprachigen Raum sind dies vor allem der IT-Grundschutz vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) und das österreichische Informationssicherheitshandbuch. In der Literatur wird auch häufig CobiT im Zusammenhang mit Informationssicherheit erwähnt – allerdings stellt die Informationssicherheit nur einen Teilaspekt von CobiT dar, weswegen nicht weiter auf diesen Standard eingegangen wird. Der IT-Grundschutz des BSI und das österreichische Sicherheitshandbuch werden an dieser Stelle kurz näher beschrieben und mit der ISO-27000-Familie verglichen.

Das österreichische Informationssicherheitshandbuch, herausgegeben vom österreichischen Bundeskanzleramt und dem Zentrum für sichere Informationsformationstechnologie – Austria (A-SIT), orientiert sich sehr stark an der ISO 27001 und stellt eher einen erweiterten Umsetzungsleitfaden als einen eigenen Standard dar. Im Gegensatz zur ISO 27002 bietet das österreichische Informationssicherheitshandbuch aber deutlich detailliertere (und an das österreichische Recht angepasste) Empfehlungen und Umsetzungshinweise. Eine Zertifizierung des ISMS nach dem österreichischen Informationssicherheitshandbuch ist nicht möglich.

Gerade im Bereich der Kryptographie bietet das österreichische Informationssicherheitshandbuch deutlich mehr Informationen als das entsprechende Kapitel in der ISO 27002. So werden auch konkrete Empfehlungen hinsichtlich der eingesetzten

Schlüssellängen von kryptographischen Verfahren, der Auswahl von Kryptomodulen und dem Schlüsselmanagement abgegeben.

Der IT-Grundschutz des BSI verfolgt einen etwas anderen Ansatz als das österreichische Informationssicherheitshandbuch und orientiert sich nicht so stark an der ISO-27000-Familie. Außerdem ist es möglich ein ISMS nach IT-Grundschutz zertifizieren zu lassen. Auch der IT-Grundschutz bietet deutlich mehr Informationen zur Umsetzung und ist weniger generisch als die ISO 27002.

Im Bereich der Kryptographie bietet das BSI einen Baustein im IT-Grundschutz-Kompendium an. Dieser Baustein stellt im Prinzip ähnliche Anforderungen wie das entsprechende Kapitel in der ISO 27002 und vertieft diese. Zusätzlich dazu werden auch noch Empfehlungen hinsichtlich der Verantwortlichkeiten für die Umsetzung der einzelnen Schritte in der Organisation abgegeben.

2.2.5 Nutzen für die Organisation

Trotz des nicht unerheblichen Aufwands der Einrichtung und des Betriebs eines ISMS, hat ein ISMS einen Nutzen für die Organisation. Zum einen wird das Thema der Informationssicherheit für die Geschäftsführung greifbarer gemacht und mit echten Risiken untermauert. Zum anderen fördert der zyklische Ansatz, der den meisten ISMS zugrunde liegt, eine stetige Verbesserung der Risikobeurteilung und damit auch der Sicherheitsvorkehrungen.

Die ISO 27002 führt an, dass Unternehmenswerte und Informationen bewusst (beispielsweise Industriespionage) und unbewusst (beispielsweise Hardwarefehler) herbeigeführten Risiken ausgesetzt sind. Ein ISMS, wie es im Standard ISO 27001 definiert wird, trägt zu einer ganzheitlichen und koordinierten Risikobehandlung bei. (ISO/IEC 27002:2013, 2013)

Das BSI schreibt im BSI-Standard 200-1 (Managementsysteme für Informationssicherheit), dass es für Organisationen schwierig ist, eine ausreichende Informationssicherheit aufzubauen und zu halten. Dies liegt unter anderem an der stetig steigenden Komplexität von IT-Umgebungen, aber auch an der im Grunde immer vorhandenen Ressourcenknappheit (sei dies nun Geld oder Personal). Auch das BSI führt den ganzheitlichen Ansatz zur Erhöhung der Informationssicherheit als großen Nutzen für Unternehmen an. Aber auch, um mit den immer kürzeren Entwicklungszyklen in der IT-Branche schritthalten zu können, ist es unabdingbar ein systematisches und koordiniertes Vorgehen für die Informationssicherheit zu wählen. (Bundesamt für Sicherheit in der Informationstechnik, 2017)

Carlson (2008) hebt zusätzlich zu den genannten Punkten auch hervor, dass ein ISMS zum einen als Alleinstellungsmerkmal dienen kann und zum anderen auch bei der Erschließung neuer Märkte hilft. So kann bei einer Auftragsvergabe der Anbieter mit einem nachweisbaren Informationssicherheitsmanagement durchaus den Vorzug vor anderen Anbietern bekommen und für manche Ausschreibungen kann eine Zertifizierung nach ISO 27001 auch zwingend vorgeschrieben sein.

Es wird deutlich, dass sich der Aufwand eines ISMS gerade auf langfristige Sicht lohnt. Bei immer kürzeren Entwicklungszyklen ist es unabdingbar, auch hinsichtlich potenzieller Risiken für Informationen und Unternehmenswerte, auf aktuellem Stand zu bleiben. Außerdem stellt eine Zertifizierung nach ISO 27001 oder vergleichbaren Standards zumindest einen Mehrwert gegenüber der Konkurrenz dar oder ist sogar zwingend notwendig, um bestimmte Aufträge annehmen zu können.

2.3 Kryptographie

In diesem Abschnitt wird erläutert warum die Kryptographie wichtig für ein wirksames ISMS ist, welche Grundziele die Kryptographie zu erreichen versucht, und welche Mechanismen es dafür gibt.

Wie bereits angedeutet, hat das ISMS zum Ziel, Verfügbarkeit, Vertraulichkeit und Integrität von Unternehmensinformationen mit Hilfe von definierten Sicherheitsanforderungen zu gewährleisten. Kersten et. al. (2016) fügen diesen Zielen auch noch weitere Ziele, wie zum Beispiel Authentizität, Nichtabstreitbarkeit und Compliance, hinzu. In der Praxis werden kryptographische Verfahren insbesondere dazu eingesetzt, Vertraulichkeit, Integrität, Nichtabstreitbarkeit und Authentizität zu gewährleisten – es wird deutlich, dass hier eine große Überschneidung vorhanden ist und sich viele Ziele hinsichtlich der Informationssicherheit in einer Organisation mithilfe von kryptographischen Verfahren erreichen lassen. Daraus ergibt sich auch die Wichtigkeit einer Richtlinie für kryptographische Verfahren, wie sie in dieser Arbeit erarbeitet wird.

2.3.1 Grundlagen

Die Kryptographie ist die Wissenschaft der Verschlüsselung von Informationen durch geheime Schlüssel und wird schon seit ca. 500 vor Christus in ihrer einfachsten Form angewendet. Die ersten angewendeten Verfahren waren seinerzeit Syktale und die Caesar-Chiffre. Die Caesar-Chiffre sorgt dabei durch eine Verschiebung der Zeichen im Alphabet um einen bestimmten Wert für eine Verschlüsselung der Nachricht (aus dem A wird ein D, aus dem B ein E und so weiter). Die Skytale besteht aus einem Stab mit einem bestimmten Durchmesser, um den beispielsweise Pergament gewickelt und beschrieben wird. Wird das Pergament abgewickelt, ergibt sich eine andere Zeichenfolge als die Ursprüngliche. Zur Entschlüsselung wurde ein weiterer Stab mit dem gleichen Durchmesser benötigt. (Spitz, Pramateftakis, & Swoboda, 2011)

Die oben angesprochenen Verfahren nennt man Substitution (das Ersetzen von Zeichen) und Transposition (das Vertauschen von Zeichen). Beide Verfahren haben einen relativ kleinen Schlüsselraum (das sind die maximal möglichen Schlüssel) verwendet – im Falle der Caesar-Chiffre war dieser Schlüsselraum 26 Zeichen groß. Es wird schnell deutlich, dass durch einfaches Ausprobieren eine Nachricht entschlüsselt werden kann (wenn man weiß, welches Verfahren angewendet wurde).

Abgesehen vom einfachen Ausprobieren von möglichen Schlüsseln (der Brute-Force-Methode) gibt es auch noch die Möglichkeit der Kryptoanalyse. Die Kryptoanalyse befasst sich mit dem Analysieren von Verschlüsselungen und dem Suchen nach möglichen Schwachstellen. Im Falle der Caesar-Chiffre war es möglich, anhand der Häufigkeitsverteilung der einzelnen Buchstaben, Rückschlüsse auf den verwendeten Schlüssel (die Verschiebung) zu ziehen. In der deutschen Sprache ist zum Beispiel der Buchstabe *E* der häufigste Buchstabe. Wenn in einem verschlüsselten Text nun *X* der häufigste Buchstabe ist, kann ein Angreifer davon ausgehen, dass das Alphabet um 19 Stellen verschoben wurde. (Spitz, Pramateftakis, & Swoboda, 2011)

Eine der großen Herausforderungen der Kryptographie war es, nun den verwendeten Schlüsselraum zu vergrößern. Eine Weiterentwicklung der Caesar-Chiffre stellt dabei die Vigenére-Chiffre dar, welche statt einem Alphabet nun mehrere Alphabete mit unterschiedlicher Verschiebung benutzt hat. Bis zu aktuellen kryptographischen Verfahren sind noch weitere Verfahren, wie zum Beispiel die Vernam-Chiffre oder die Enigma, entwickelt worden. Die Vernam-Chiffre ist grundsätzlich nicht unknackbar, hat allerdings große Nachteile in Bezug auf die Schlüsselgenerierung und den Schlüsselaustausch (der Schlüssel muss so lang sein, wie die zu verschlüsselnde Botschaft). Auf diese Entwicklungen wird an dieser Stelle nicht weiter eingegangen.

Eines der Grundprinzipien der Kryptographie ist das Kerckhoffs'sche Prinzip. Dieses Prinzip sagt aus, dass die Sicherheit eines kryptographischen Verfahrens nicht durch das Verfahren an sich, sondern allein durch den Schlüssel erzeugt werden muss. Aus diesem Grund sind beispielsweise Ausschreibungen des National Institute of Standards and Technology (NIST) kein Problem, sondern im Gegenteil erwünscht, da neue Verfahren von möglichst vielen Fachleuten untersucht werden können. (Spitz, Pramateftakis, & Swoboda, 2011)

Eine weitere große Herausforderung der Kryptographie war beziehungsweise ist der Schlüsselaustausch. Gerade in modernen Kommunikationsnetzen muss davon ausgegangen werden, dass übermittelte Nachrichten von Dritten mitgelesen werden können. Stellt dies bei kurzen Kommunikationswegen und wenigen Kommunikationspartnern nur ein kleines Problem dar (da der Schlüssel zum Beispiel durch ein direktes Treffen ausgetauscht werden kann), so ist dies bei vielen Kommunikationspartnern oder langen Wegstrecken eine große Hürde. Wie kann nun ein Schlüssel sicher übermittelt werden? Die Lösung für dieses Problem ist die sogenannte asymmetrische Verschlüsselung.

Die Sicherheit der asymmetrischen Verschlüsselung liegt darin, dass zwei Schlüssel (einer für die Ver- und einer für die Entschlüsselung) beziehungsweise ein Schlüsselpaar zum Einsatz kommen. Der Sender einer Nachricht ist dabei im Besitz des öffentlichen Schlüssels des Empfängers und verschlüsselt die Nachricht für den Empfänger mit dem öffentlichen Schlüssel. Diese Nachricht ist nun ausschließlich mit dem privaten Schlüssel des Empfängers lesbar und durch den öffentlichen Schlüssel sind keine Rückschlüsse auf den privaten Schlüssel möglich. Wie der Name schon sagt, hat nur der Empfänger seinen privaten Schlüssel. Bekannte asymmetrische Verfahren sind zum Beispiel der Rivest-Shamir-Adelman- (RSA) und der Diffie-Hellman-Algorithmus (DH). (Beutelspacher, Schwenk, & Wolfenstetter, 2015)

Nachfolgend werden kurz die wichtigsten kryptographischen Verfahren und ihre Funktionsweisen vorgestellt.

2.3.2 Kryptographische Verfahren

Zu Beginn dieses Unterabschnitts wird erneut kurz auf die symmetrische Verschlüsselung eingegangen. Die bereits erwähnten Chiffren, wie die Caesar-Chiffre oder die Vernam-Chiffre, sind symmetrische Verfahren. Dies bedeutet, dass Sender und Empfänger im Besitz des gleichen Schlüssels sind und Nachrichten mit diesem Schlüssel ver- und entschlüsselt werden können. (Schwenk, 2014)

Die symmetrischen Verschlüsselungsverfahren lassen sich grundsätzlich in Block- und Stromchiffren unterteilen. Bei Blockchiffren werden zu verschlüsselnde Daten in Blöcke mit einer bestimmten Größe aufgeteilt, die dann durch die Verschlüsselungsfunktion geleitet werden. Auf die Unterschiede zwischen den verschiedenen Modi der Blockchiffren wird an dieser Stelle nicht näher eingegangen. Bekannte Vertreter der Blockchiffren sind beispielsweise 3DES (Triple Data Encryption Standard) und AES (Advanced Encryption Standard). (Schwenk, 2014)

Im Falle der Stromchiffren wird der Datenstrom bit-, byte- oder zeichenweise mit einem Bit, Byte oder Zeichen des Schlüssels verknüpft. Die Vernam-Chiffre ist ein sehr gutes Beispiel für eine Stromchiffre, da dieses Verfahren (sofern der Schlüssel nur ein einziges Mal verwendet wird) die sogenannte perfekte Sicherheit erzeugt. Andere Stromchiffren, wie zum Beispiel RC4, nutzen einen Initialvektor für die Schlüsselerzeugung. (Spitz, Pramateftakis, & Swoboda, 2011)

Die grundsätzlichen Vorteile (Schlüsselmanagement und Schlüsselübertragung) der asymmetrischen Verschlüsselung wurden bereits im vorangegangenen Unterabschnitt kurz erläutert. An dieser Stelle soll zusätzlich noch die Signatur erwähnt werden, welche ebenfalls durch asymmetrische Verschlüsselung erzeugt wird. In diesem Fall wird eine Nachricht (oder der Hashwert einer Nachricht) mit dem privaten Schlüssel des Absenders signiert und die Echtheit der Signatur kann von allen Personen mit dem öffentlichen Schlüssel des Absenders überprüft werden. (Schwenk, 2014)

Eine Besonderheit stellen Protokolle dar, welche asymmetrische und symmetrische Verfahren kombinieren. Als Beispiel soll hierfür TLS (Transport Layer Security) angeführt werden. Die Kombination der Verfahren ergibt sich aus den jeweiligen Schwachstellen der einzelnen Verfahren: die symmetrische Verschlüsselung ist zwar schnell, allerdings ist das Schlüsselmanagement und der Schlüsselaustausch problematisch – die asymmetrische Verschlüsselung bietet auf der anderen Seite Möglichkeiten, Schlüssel über einen öffentlichen Kommunikationsweg zu erzeugen und ist dafür zu langsam, um große Datenmengen effizient zu verschlüsseln.

Eine weitere wichtige Rolle in der Kryptographie spielen die Hash- oder Einwegfunktionen. Mit ihnen wird ein Wert errechnet, welcher nur durch die ursprünglichen Daten erzeugt werden kann. Die Fachliteratur spricht hier vom Fingerabdruck von Nachrichten. Hashfunktionen werden auch Einwegfunktionen genannt, weil aus der errechneten Prüfsumme nicht auf das

Ursprungsdokument geschlossen werden kann. (Beutelspacher, Schwenk, & Wolfenstetter, 2015)

In den nachfolgenden Unterabschnitten wird auf die Ziele der Kryptographie eingegangen, mit welchen der genannten Verfahren diese erreicht werden können und welche Implikationen dies auf ein ISMS haben kann.

2.3.3 Vertraulichkeit

Das ISMS will sicherstellen, dass bestimmte Informationen nur einem bestimmten Personenkreis zugänglich sind. Dies kann nun heißen, dass diese Informationen das Unternehmen nicht verlassen dürfen oder dass nur bestimmte Rollen oder Positionen Zugriff auf gewisse Informationen haben sollen. Dies kann nun beispielsweise durch organisatorische Vorgaben erzielt werden – es ist allerdings davon auszugehen, dass sich nicht jeder an diese Vorgaben halten wird (man denke hier zum Beispiel an Industriespionage). An dieser Stelle können nun – ergänzend zu den organisatorischen Vorgaben – kryptographische Verfahren eingesetzt werden.

Für die Gewährleistung der Vertraulichkeit können sowohl symmetrische als auch asymmetrische Verfahren eingesetzt werden. Im Falle der symmetrischen Verfahren besitzen Sender und Empfänger den gleichen Schlüssel – die Information wird also mit ein und demselben Schlüssel ver- und entschlüsselt. (Spitz, Pramateftakis, & Swoboda, 2011)

Für eine kryptographische Richtlinie kann dies nun zur Folge haben, dass bestimmte Daten zum Beispiel nur verschlüsselt übertragen oder sogar nur verschlüsselt gespeichert werden dürfen. Zusätzlich sollten in einer solchen Richtlinie Mindeststandards angeführt werden und/oder nachweislich geknackte Verfahren ausgeschlossen werden.

2.3.4 Authentizität

Ziel der Authentizität ist es sicherzustellen, dass der Absender einer Nachricht auch tatsächlich die Person ist, für die er sich ausgibt. Im täglichen Leben passiert dies zum Beispiel mit der eigenen Unterschrift oder mit dem Vorzeigen eines Lichtbildausweises. Ein bekanntes Beispiel für das Herstellen von Authentizität ist das Wachssiegel aus dem Mittelalter.

In der digitalen Welt kann diese Authentizität zum Beispiel durch ein Kennwort, ein Zertifikat/eine Signatur oder ein gemeinsames Geheimnis (zum Beispiel den Schlüssel eines symmetrischen Verschlüsselungsverfahrens) hergestellt werden. Beutelspacher, Schwenk und Wolfenstetter (2015) unterscheiden hier zwischen der Teilnehmer- und der Nachrichtenauthentifikation. Ein Teilnehmer kann sich durch ein persönliches Merkmal oder ein gemeinsames Geheimnis authentifizieren. Eine Nachricht kann mit Hilfe kryptographischer Verfahren signiert werden. (Beutelspacher, Schwenk, & Wolfenstetter, 2015)

Zum Herstellen von Authentizität eignen sich grundsätzlich symmetrische Verfahren oder digitale Signaturen.

Für die Informationssicherheit kann dies nun zur Folge haben, dass bestimmte Nachrichten oder Dokumente signiert werden müssen. Im Rahmen der Zugriffssteuerung müssen sich auch Benutzer authentifizieren können, um Zugriff auf bestimmte Informationen erlangen zu können. Auch der Bereich der Benutzeranmeldung (sei dies nun über Portale oder direkt im Netzwerk) kann bei der Ausgestaltung einer kryptographischen Richtlinie eine Rolle spielen.

2.3.5 Integrität

Integrität sorgt in der digitalen Welt dafür, dass Daten unverändert vom Absender zum Empfänger gelangen. Spitz, Pramateftakis und Swoboda (2011) heben hervor, dass Integrität Grundvoraussetzung für die Authentizität einer Nachricht ist. Wenn nicht sichergestellt werden kann, dass eine Nachricht nicht verändert wurde, kann auch nicht sichergestellt werden, dass die Nachricht tatsächlich vom angeblichen Kommunikationspartner stammt.

Integrität von Informationen wird in erster Linie durch Hashfunktionen sichergestellt. Durch diesen speziellen Fingerabdruck einer Datei kann sichergestellt werden, dass sich Daten (zum Beispiel auf dem Transport über eine unsichere Leitung) nicht verändert haben. Auch können einige Signaturverfahren die Integrität eines Dokuments sicherstellen (im Kern funktioniert dies allerdings wieder über eine Hashfunktion).

Als einzelner Bestandteil kann die Integrität ebenfalls eine Rolle innerhalb einer kryptographischen Richtlinie innerhalb des ISMS spielen. So verlangt die ISO 27001 schon für die Dokumente des ISMS, dass diese vor Änderungen geschützt werden müssen. Ebenso muss für gewisse Informationen sichergestellt werden, dass diese nicht ohne Weiteres von Dritten geändert werden können. Allerdings kann angenommen werden, dass die Integrität oftmals in einem Schritt oder durch die gleichen Verfahren wie die Authentizität abgehandelt wird.

2.3.6 Verbindlichkeit

Die Verbindlichkeit stellt eine Sonderform der Authentizität dar. Sie gewährleistet nicht nur die Authentizität der eigenen Person gegenüber einer weiteren Person, sondern auch gegenüber Dritten. Durch die Verbindlichkeit wird sichergestellt, dass zum Beispiel das Verfassen und Absenden einer Nachricht nicht abgestritten werden kann.

Verbindlichkeit kann in der digitalen Welt nur mit Hilfe der digitalen Signatur erzeugt werden. Wie bereits erwähnt, werden in diesem Verfahren Informationen (oder die Hashes dieser Informationen) mit dem privaten Schlüssel des Absenders verschlüsselt beziehungsweise signiert. Verbindlichkeit erfordert Authentizität und Integrität. (Spitz, Pramateftakis, & Swoboda, 2011)

Auch die Verbindlichkeit kann bei der Definition einer kryptographischen Richtlinie im ISMS-Kontext eine Rolle spielen. So könnte es zum Beispiel sein, dass bestimmte Nachrichten signiert werden müssen, um Verbindlichkeit herzustellen. Als Beispiel sei hier ein Bescheid angeführt, der durch die Amtssignatur signiert wurde.

2.3.7 Kryptographie und ISMS

Anhand der Beschreibungen zu den kryptographischen Verfahren wird deutlich, dass alle Ziele und Verfahren mehr oder weniger starke Auswirkungen auf eine Richtlinie zur Nutzung kryptographischer Verfahren haben können. Grundsätzlich ist dies allerdings von der Art der Organisation, ihres Geschäftsfeldes und anderen Faktoren abhängig.

Wie bereits angesprochen, ist es eines der Ziele eines ISMS, Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Werten einer Organisation sicherzustellen. Angesichts der beschriebenen Verfahren ist klar, dass kryptographische Verfahren keinen Nutzen hinsichtlich der Verfügbarkeit von Informationen bringen. In Bezug auf Integrität und Vertraulichkeit stellen kryptographische Verfahren wahrscheinlich eine sehr gute Ergänzung zu organisatorischen Maßnahmen dar, weswegen es auch Sinn macht, die Nutzung dieser Verfahren in einer Richtlinie zu regeln.

Im folgenden Abschnitt wird analysiert, welche Vorgaben der Gesetzgeber in Bezug auf die Anwendung kryptographischer Verfahren macht beziehungsweise welche Vorgaben den Einsatz kryptographischer Verfahren erzwingen.

2.4 Gesetzliche Vorgaben

Dieser Abschnitt behandelt Gesetze und Verordnungen, welche die Informationssicherheit für Unternehmen und Behörden in Österreich regeln. Zu diesem Zweck werden die entsprechenden Gesetze und Verordnungen kurz beschrieben, relevante Passagen diskutiert und abschließend analysiert, welche Auswirkungen diese Passagen auf das ISMS und die kryptographischen Maßnahmen haben können.

Das österreichische Informationssicherheitshandbuch verweist in dem Abschnitt, welcher die Kryptographie behandelt, vor allem auf das Signaturgesetz beziehungsweise die Signaturverordnung (A-SIT, 2016). Aber auch andere Gesetze, wie zum Beispiel das Datenschutzgesetz 2000 und ab Mai 2018 auch die Datenschutzgrundverordnung, regeln, wie Dienstleister mit Daten von Auftraggebern umzugehen haben. Auch im E-Government-Gesetz finden sich Passagen zu Identität und Authentizität von Nutzern.

In den folgenden Unterabschnitten werden die angesprochenen Gesetze und Verordnungen kurz vorgestellt und die Anknüpfungspunkte zur Informationssicherheit hervorgehoben. Es wird ausdrücklich darauf hingewiesen, dass an dieser Stelle keine juristische Bewertung vorgenommen wird.

2.4.1 E-Government-Gesetz

Das Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (kurz E-Government-Gesetz, E-GovG) (2017) schafft die gesetzlichen Grundlagen für „die Förderung rechtserheblicher elektronischer Kommunikation“.

Konkret heißt dies, dass Behörden nicht mehr ausschließlich über persönliche Vorstellung oder den Postweg kontaktiert werden müssen, sondern auch über das Internet und Onlineformulare kontaktiert werden können. Im Gegenzug ist es den Behörden möglich, ihre Erledigungen ebenfalls (sofern vom Bürger gewünscht) digital zuzustellen. Das E-Government-Gesetz wurde 2016 novelliert, um den Anforderungen der *Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG* (eIDAS-VO) gerecht zu werden. (Digitales Österreich, 2016)

Im Detail regelt das E-Government-Gesetz die Nutzung des elektronischen Identitätsnachweises (bekannt als Bürgerkarte) sowie die damit einhergehenden Probleme der Identifikation und Authentizität, die Ableitung von bereichsspezifischen Personenkennzeichen (bPK) und die Nutzung der Amtssignatur. (Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-GovG), 2004)

In Paragraph 3 des Gesetzes wird auf das Datenschutzgesetz 2000 (DSG 2000) verwiesen, auf das später noch näher eingegangen wird. Dieser Paragraph sagt aus, dass anderen Behörden der Zugriff auf Daten, an denen ein schutzwürdiges Geheimhaltungsinteresse besteht, nur gestattet werden kann, wenn Identität und Authentizität der ansuchenden Behörde elektronisch nachvollziehbar nachgewiesen wurden. Zusätzlich dürfen Betroffene nur eindeutig identifiziert werden, wenn dies zur Wahrnehmung der Aufgabe des jeweiligen Organs notwendig ist. (Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-GovG), 2004)

In der Praxis geschieht dieser Identitätsnachweis über den sogenannten Portalverbund, über den Applikationen für andere Behörden freigegeben werden können. Technisch funktioniert dies mittels eines Single-Sign-On-Verfahrens, wodurch sich Benutzer nur an ihrem „eigenen“ Portal anmelden müssen und aufgrund ihrer jeweiligen Rolle und Sicherheitsstufe ihre verfügbaren Anwendungen angezeigt bekommen. Die eingesetzten Algorithmen zur Authentifikation und Kommunikation werden verwaltungsübergreifend in einem Treffen von Spezialisten bestimmt und entsprechen einem hohen Standard.

Typische Beispiele für den aktuellen Stand der Technik in Sachen E-Government in Österreich sind beispielsweise FinanzOnline oder die elektronische Gesundheitsakte. Beide Applikationen bieten die Möglichkeit, sich mittels Bürgerkarte oder Handysignatur zu authentifizieren und die entsprechenden Informationen online auf sichere Art und Weise abzurufen.

Für das eigene ISMS einer Behörde ergeben sich aus dem E-Government-Gesetz nur indirekte Auswirkungen. Die eingesetzten Protokolle werden, wie bereits angesprochen, verwaltungsübergreifend festgelegt und sind in der Regel nicht durch einzelne Behörden zu bestimmen. Es ist allerdings wichtig, dass auch dieser Baustein innerhalb des ISMS betrachtet und einer Risikoanalyse unterzogen wird, um gegebenenfalls Änderungswünsche innerhalb des Portalverbundes äußern zu können.

2.4.2 Signatur- und Vertrauensdienstegesetz

Das Signatur- und Vertrauensdienstegesetz (SVG oder Bundegesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen) führt die bereits beim E-Government-Gesetz angesprochene eIDAS-VO durch (Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (SVG), 2016). Wie der Name schon sagt, regelt dieses Gesetz zum einen die Rechtswirksamkeit von elektronischen Siegeln und Signaturen und zum anderen die Rechte und Pflichten der sogenannten Vertrauensdiensteanbieter.

Das SVG definiert die Rechtswirksamkeit der elektronischen Signatur und sagt aus, dass die in §886 ABGB geforderte Schriftlichkeit durch elektronische Signaturen erfüllt wird. Es muss allerdings dennoch auf zusätzliche Formerfordernisse, wie zum Beispiel die notarielle Beglaubigung, geachtet werden. Bei Willenserklärungen des Familien- und Erbrechts, die an die Schriftform (oder strengere Formerfordernisse) gebunden sind, ist die elektronische Signatur nur dann gültig, wenn das signierte Dokument die Aufklärung eines Notars oder Rechtsanwalts über die möglichen Rechtsfolgen enthält. Testamente können grundsätzlich nicht digital signiert werden. (Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (SVG), 2016)

Außerdem ist im SVG enthalten, unter welchen Umständen ein Vertrauensdiensteanbieter ein qualifiziertes Zertifikat temporär zurückrufen muss beziehungsweise wann Signatoren und Siegelersteller den Vertrauensdiensteanbieter zum Widerruf des Zertifikats aufzufordern haben.

Das SVG regelt außerdem, welche Voraussetzungen für die Ausstellung eines qualifizierten Zertifikats (persönliche Anwesenheit oder gleichwertige Methoden, die nicht die persönliche Anwesenheit erfordern) gelten, wie ein Vertrauensdiensteanbieter seine Tätigkeit einstellen kann und unter welchen Bedingungen ein Vertrauensdiensteanbieter Behörden Zugriff auf die Dokumentation zu seiner Zertifikatsdatenbank gewähren muss. Zusätzlich sind auch noch Aufbewahrungspflichten (30 Jahre nach Ablauf des Zertifikats) und Haftungsfragen geregelt (Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (SVG), 2016).

Bekannte österreichische Vertrauensdiensteanbieter (oder Zertifizierungsstellen) sind die A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, das Bundesamt für Eich- und Vermessungswesen, die A1 Telekom Austria AG, die e-commerce monitoring GmbH und die PrimeSign GmbH.

Nach Einschätzung des Autors erwachsen aus diesem Gesetz ebenfalls keine unmittelbaren Pflichten hinsichtlich des Informationssicherheitsmanagements (sofern die betroffene Organisation kein Vertrauensdiensteanbieter ist). Einzig muss sichergestellt werden, dass (gerade im Falle einer Behörde) die entsprechenden Informationen über die vertrauenswürdigen Zertifizierungsstellen aktuell gehalten werden, um die Funktion der elektronischen Signaturen gewährleisten zu können.

2.4.3 Datenschutzgesetz

Das nächste Gesetz, das in diesem Zuge behandelt wird, ist das Datenschutzgesetz 2000 (DSG 2000). Das DSG 2000 definiert das Grundrecht auf Datenschutz und regelt unter anderem die grundsätzliche Verwendung von Daten, die Anforderungen an die Datensicherheit, Rechte von Betroffenen, die Publizität der Datenverarbeitungen, den Rechtsschutz und die Kontrollorgane für den Datenschutz. Zudem werden besondere Arten und Zwecke der Verwendung von Daten (zum Beispiel die Videoüberwachung) sowie Strafbestimmungen definiert.

Kilches (1999) und Souhrada-Kirchmayer (2000) und heben hervor, dass das DSG 2000 die EG-Datenschutz-Richtlinie (Richtlinie 95/46/EG) umsetzt und in Erweiterung zur EG-Richtlinie auch juristische Personen umfasst, da Grundrechte jeder Person zustehen.

Für die Verwendung von Daten sieht das DSG 2000 vor, dass Daten unter bestimmten Voraussetzungen verwendet werden dürfen. Dies heißt, dass Daten nur für definierte und rechtskonforme Zwecke gesammelt werden und die gesammelten Daten nicht über die notwendigen Daten (welche für den Betrieb einer Anwendung notwendig sind) hinausgehen dürfen. (Kilches, 1999)

Zusätzlich spielen bei der Datenverarbeitung auch die sogenannten schutzwürdigen Geheimhaltungsinteressen von sensiblen und nicht-sensiblen Daten eine große Rolle. Für die Verarbeitung von nicht-sensiblen Daten ist eine Zustimmung des Betroffenen (die jederzeit widerrufen werden kann) oder eine ausdrückliche Befugnis oder Pflicht notwendig. Außerdem können nicht-sensible Daten verwendet werden, wenn das Leben eines Dritten davon abhängt. Für die Datenverarbeitung von sensiblen Daten (beispielsweise die ethnische Herkunft, Gesundheitsdaten oder das Sexualleben) sieht das Gesetz eine taxative Aufzählung von Ausnahmen vor, von denen die wichtigste vermutliche die Veröffentlichung der Daten durch den Betroffenen selbst ist. In diesem Abschnitt werden auch noch die Pflichten des Dienstleisters sowie die Übermittlung und Überlassung der gesammelten Daten in das Ausland geregelt. (Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000), 1999)

Der nächste Abschnitt des Gesetzes befasst sich mit der Datensicherheit und sieht vor, dass Datenverarbeiter die Datensicherheit gewährleisten müssen. Das Gesetz hebt dabei hervor, dass je nach Datenart und Zweck der Verarbeitung unterschiedliche Maßnahmen notwendig sind. Ziel dieser Maßnahmen ist es, dass die Daten vor unberechtigtem Zugriff geschützt und ausreichend gegen Zerstörung oder Verlust gesichert sind. Als Handlungsrahmen sind zum einen die technischen Möglichkeiten und zum anderen die Wirtschaftlichkeit definiert. Grundsätzlich müssen je ein Berechtigungs-, Zugriffs- und Zutrittskonzept für die Daten erstellt werden und die Mitarbeiter über die Bestimmungen des DSG 2000 beziehungsweise organisatorische Vorschriften aufklärt werden. Dieser Abschnitt hat große Auswirkungen auf den Betrieb eines Informationsmanagementsystems, auf die am Ende dieses Unterabschnitts noch näher eingegangen wird. Des Weiteren sieht das Gesetz vor, dass Daten, welche aus der beruflichen Tätigkeit bekannt geworden sind, der Geheimhaltung unterliegen. (Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000), 1999)

Pollirer (2016) weist darauf hin, dass die Mindestmaßnahmen, wie sie das Gesetz in §14 Absatz 2 vorschreibt, nicht ausreichend sind, um die in Absatz 1 definierte Zielsetzung erfüllen zu können. Aus diesem Grund empfiehlt er die Einführung eines Informationssicherheitsmanagements inklusive einer Sicherheitsleitlinie und einer Risikoanalyse (wie sie sich durch §14 Absatz 1 ergibt). Hier sind deutliche Parallelen zur ISO 27001 beziehungsweise den entsprechenden Ablegern, wie dem IT-Grundschutz des BSI oder dem österreichischen Informationssicherheitshandbuch, zu erkennen.

Im vierten Abschnitt des Gesetzes werden das Datenverarbeitungsregister sowie die damit einhergehenden Pflichten definiert. Grundsätzlich müssen Datenanwendungen vor dem Betrieb dem Datenverarbeitungsregister gemeldet werden. Diese Meldung muss den Namen des Auftraggebers, sofern erforderlich, die rechtliche Befugnis und den Zweck der Anwendung enthalten. Zusätzlich sind die Betroffenen und die zu sammelnden Datenarten, Empfänger von Datenübermittlungen und welche Datenarten übermittelt werden sowie getroffene Maßnahmen für die Sicherheit der Daten anzuführen. Es gibt allerdings auch Ausnahmen von der Meldepflicht. Wenn eine Anwendung zum Beispiel nur öffentliche oder indirekt personenbezogene (beispielsweise verschlüsselte) Daten enthält, ist diese von der Meldepflicht ausgenommen. Das Datenverarbeitungsregister wird von der Datenschutzbehörde gepflegt und ist für alle Bürger und Bürgerinnen einsehbar. Neben der Meldepflicht bestehen auch noch weitere Pflichten, zum Beispiel die Pflicht nicht-meldepflichtige Anwendungen auf Anfrage der Datenschutzbehörde offenzulegen. (Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000), 1999)

Das DSG 2000 räumt Betroffenen auch bestimmte Rechte gegenüber den Auftraggebern einer Datenanwendung ein. So haben alle Betroffenen ein Auskunftsrecht, mit dem sie Auskunft über die verarbeiteten Daten verlangen können. Auskünfte müssen im Zeitraum von acht Wochen nach Aufforderung erteilt werden. Abgesehen von dem Recht auf Auskunft haben Betroffene auch das Recht ihre Daten entweder richtigstellen oder löschen zu lassen. Zuletzt haben Betroffene auch das Recht der Verarbeitung ihrer Daten zu widersprechen (sofern diese nicht gesetzlich vorgesehen ist). Die erwähnten Rechte können bei der Verwendung von indirekt personenbezogenen Daten nicht geltend gemacht werden. (Souhrada-Kirchmayer, 2000)

Im DSG 2000 wird auch die Einrichtung der Datenschutzbehörde und des Datenschutzrats begründet. Die Datenschutzbehörde ist für das Datenschutzregister sowie die Einhaltung des Datenschutzgesetzes zuständig und vertritt dabei die Rechte der Betroffenen. Zusätzlich ist die Datenschutzbehörde auch zur Begutachtung von Gesetzesentwürfen hinsichtlich des Datenschutzes heranzuziehen. Der Datenschutzrat ist eine Einrichtung des Bundeskanzleramtes und hat Beratungsfunktionen gegenüber Bundes- und Landesregierungen bei Fragen grundsätzlicher Bedeutung für den Datenschutz und kann Stellungnahmen zu Gesetzesentwürfen abgeben, wenn diese von datenschutzrechtlicher Bedeutung sind. (Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000), 1999)

Vor allem der dritte Abschnitt des DSG 2000 hat mehrere Auswirkungen auf das ISMS einer Organisation. In §14 Absatz 2 Z8 wird eine Dokumentation der getroffenen Maßnahmen zur Datensicherheit für Kontrolle und Beweissicherung verlangt. Natürlich könnte eine Organisation

dieser Dokumentationspflicht auch ohne ISMS nachkommen, aber vermutlich ist das strukturierte Vorgehen der ISO 27001 ressourcensparender als eine freie Dokumentation der geforderten Maßnahmen.

Zusätzlich ist das DSG 2000 auch ein zusätzlicher Input für den Kontext des ISMS und den Risikomanagementprozess – schließlich ist eine, mit einem Verstoß gegen das DSG einhergehende, Strafe gerade für kleine Unternehmen ein relevantes Risiko. Im Rahmen der Datenschutzgrundverordnung, auf die im nächsten Unterabschnitt eingegangen wird, wird dieses Risiko auch für größere Unternehmen und Konzerne größer werden.

Des Weiteren ist im Gesetz gefordert, dass Unternehmen Maßnahmen am Stand der Technik (unter Berücksichtigung der Kosten) durchführen. Dies erfordert eine immer wiederkehrende Kontrolle der bisher vorgenommenen Maßnahmen, welche sich durch die Kontrollzyklen innerhalb eines ISMS sehr gut durchführen lässt.

Es wird deutlich, dass sich durch die Anforderungen des DSG 2000 auch größere Anforderungen an das ISMS einer Organisation ergeben, die auf jeden Fall bei der Planung und dem Betrieb eines ISMS berücksichtigt werden sollten.

2.4.4 Datenschutzgrundverordnung

Die Datenschutz-Grundverordnung (DSGVO) ist mit Mitte Mai 2016 in Kraft getreten und gilt ab dem 25. Mai 2018. Grundsätzlich dient sie zur Harmonisierung der einzelnen Gesetze zum Schutz personenbezogener Daten in den Mitgliedsstaaten der europäischen Union.

Die DSGVO ist in 99 Artikel unterteilt, wobei ungefähr die Hälfte dieser Artikel die Rechte der Betroffenen, die Pflichten der Verantwortlichen sowie die Übermittlung der personenbezogenen Daten in Drittländer regelt. Die zweite Hälfte regelt überwiegend formelle Themen. Inhaltlich ist die DSGVO stark an die bereits erwähnte Datenschutzrichtlinie 94/46/EG angelehnt, hat aber durch den Verordnungs-Charakter weniger Auslegungsspielraum als die vorhergehende Richtlinie. Änderungen bestehen unter anderem darin, dass Betroffene nun die Übertragung ihrer persönlichen Daten von einem Datenverarbeiter zu einem anderen veranlassen können – die Verordnung nennt dies das Recht auf Datenübertragbarkeit. Zusätzlich haben Datenverarbeiter datenschutzfreundliche Voreinstellungen zu treffen (ähnlich einem Opt-In) und eine Datenschutz-Folgeabschätzung vorzunehmen. Diese Datenschutz-Folgeabschätzung ist erforderlich, wenn die persönlichen Daten von Personen durch die Datenverarbeitung vermutlich einem hohen Risiko ausgesetzt sind. Abgesehen davon sieht die DSGVO deutlich drastischere Strafen im Falle eines Verstoßes vor. (Roßnagel, 2017)

Die DSGVO räumt den Mitgliedsstaaten mit der Hilfe von Öffnungsklauseln Gestaltungsspielräume bei der Auslegung der Verordnung ein. In Österreich haben diese Öffnungsklauseln eine Anpassung des bisher bestehenden Datenschutzgesetzes zur Folge. Dadurch ergibt sich nur eine minimale Umsetzung der DSGVO. (Anderl & Tlapak, 2017)

Durch die erforderlichen Anpassungen zieht das Gültig-werden der Datenschutzgrundverordnung eine Novelle des oben beschriebenen Datenschutzgesetzes nach

sich – ein Entwurf dieser Novelle liegt in Form des Datenschutz-Anpassungsgesetzes vor. Im Folgenden sind Konkretisierungen der Datenschutzgrundverordnung aufgezählt. Verstöße gegen das Datenschutzgesetz können nun deutlich schwerer geahndet werden als es im alten Gesetz der Fall war (alt: bis zu 25.000 Euro; neu: bis zu 20 Millionen Euro oder 4 % des jährlichen Konzernumsatzes). Ob juristische Personen durch das neue DSG weiterhin geschützt werden ist derzeit noch unklar – hier besteht zum aktuellen Zeitpunkt noch eine laufende Diskussion mit verschiedenen Auslegungen des Gesetzestextes. Auch öffentlich zugängliche Daten unterliegen (anders als bisher) nun dem Datenschutz (Ausnahme: Verwendung zu wissenschaftlichen oder statistischen Zwecken ohne personenbezogene Ziele). Zusätzlich wird das Recht auf Löschung konkretisiert. So müssen Daten, die aus technischen Gründen nicht sofort gelöscht werden können, gesperrt werden. (Knyrim & Tretzmüller, 2017)

Grundsätzlich lässt sich sagen, dass die Datenschutz-Grundverordnung das Thema Informationssicherheit noch wichtiger macht, als es bisher schon war. Dies ergibt sich nicht zuletzt aus den deutlich drastischeren Strafen. Dieser Punkt wird auch von Knyrim und Tretzmüller (2017) in *Datenschutz konkret* unterstrichen. Zusätzlich erfordert zum Beispiel das neue Recht auf Datenübertragbarkeit die Schaffung von Schnittstellen, die ihrerseits auch entsprechend sicher sein müssen.

Für das Informationssicherheitsmanagement einer Organisation hat dies zur Folge, dass vermutlich spätestens jetzt die entsprechende Unterstützung der Unternehmensführung zur Umsetzung eines Informationssicherheitsmanagementsystems vorhanden ist. Damit einher gehen allerdings auch gestiegene Anforderungen sowie ein größeres Kontrollbedürfnis seitens der Unternehmensführung.

Konkrete Anforderungen hinsichtlich kryptographischer Maßnahmen ergeben sich auch aus der DSGVO nicht unmittelbar. Allerdings können die Ziele der DSGVO, wie auch beim Datenschutzgesetz, nicht ohne entsprechende kryptographische Verfahren erreicht werden.

2.5 Zusammenfassung

Zum Abschluss dieses Kapitels wird kurz dieser Teil der Arbeit zusammengefasst. Dazu werden zuerst die Informationen über Informationsmanagementsysteme wiederholt. Anschließend wird auf den Abschnitt Kryptographie eingegangen und zum Abschluss werden die Auswirkungen von Gesetzen auf das Informationssicherheitsmanagement dargelegt.

Im Abschnitt *Information Security Management System* wurde zu Beginn erläutert, in welchem Rahmen ein Informationsmanagementsystem angesiedelt ist. Dabei ist deutlich geworden, dass Informationssicherheitsmanagement ein Teil der Corporate Governance oder, um genauer zu sein, der IT-Governance ist.

Anschließend wurde auf die ISO-27000-Familie und im Detail auf die ISO 27001 eingegangen. Entgegen früherer Versionen ist die ISO 27001:2013 nicht mehr explizit nach einem Plan-Do-Check-Act-Zyklus aufgebaut, sondern die Abfolge der verschiedenen Phasen ist mehr oder weniger frei wählbar. Wichtige Bestandteile der ISO 27001 (sowohl für eine Zertifizierung als

auch für ein effizient funktionierendes Informationsmanagement) sind die Kapitel *Kontext der Organisation, Führung, Planung, Unterstützung, Betrieb, Evaluierung* und *Verbesserung*.

Im Normkapitel *Kontext der Organisation* werden der Rahmen des ISMS sowie die entsprechenden Stakeholder analysiert. Zusätzlich wird hervorgehoben, dass nicht unbedingt eine gesamte Organisation Gegenstand des ISMS sein muss, sondern sich das ISMS auch auf einzelne Prozesse, Abteilungen, Dienststellen und Ähnliches beziehen kann. Essentiell für dieses Kapitel ist, dass hier die Einrichtung eines ISMS gefordert wird.

Das Normkapitel *Führung* der ISO 27001 sorgt dafür, dass für das Informationssicherheitsmanagement der notwendige Rückhalt von der Unternehmensführung vorhanden ist. Kurz zusammengefasst ist es Aufgabe der Unternehmensführung passende Rahmenbedingungen in Form von Ressourcen und Rollen für Betrieb, Einrichtung und Verbesserung des ISMS zu schaffen. Besonders erwähnenswert ist, dass die Veröffentlichung der Informationssicherheitsrichtlinie ebenfalls eine Führungsaufgabe ist.

Als nächstes wurde das, für das Informationssicherheitsmanagement unbedingt erforderliche, Risikomanagement beschrieben. Im Rahmen der ISO 27001 wird ein Risikomanagementprozess nach ISO 27005 empfohlen (aber nicht explizit verlangt). Dieses Kapitel beschäftigt sich in erster Linie mit der Planung des Risikomanagements. Das heißt, dass Prozesse und Regeln definiert werden, wie Risiken zu analysieren, zu bewerten und zu behandeln sind. Die tatsächliche Durchführung dieser Tätigkeiten passiert im Schritt *Betrieb*.

Ein wichtiger Punkt der ISO 27001 ist auch das Thema *Unterstützung*. Hier wurde hervorgehoben, dass entsprechende Ressourcen für den Betrieb eines ISMS bereitgestellt werden müssen – vor allem die Organisationsführung steht dabei in der Verantwortung. Abgesehen davon stellen auch die Punkte Weiterbildung, Bewusstseinsbildung, Kommunikation und Dokumentation wichtige Themen dar. Hervorgehoben wurden besonders die Bewusstseinsbildung, da ein ISMS ohne entsprechende Awareness bei den Mitarbeitern wertlos ist, und die Dokumentation, da gerade im Rahmen der Zertifizierung Nachweise über die Tätigkeiten innerhalb des ISMS erbracht werden müssen.

Anschließend wurde der Betrieb des ISMS näher beschrieben. Wie vorher angesprochen, wird an dieser Stelle die Risikoplanung in die Tat umgesetzt – es werden also tatsächlich Risiken gesucht, bewertet und behandelt. Zusätzlich wurde beschrieben, dass in dieser Phase des ISMS auch die Geschäftsprozesse überprüft und an die Erfordernisse des Informationssicherheitsmanagements angepasst werden.

Abschließend wurden die verbleibenden Normkapitel *Evaluierung* und *Verbesserung* der ISO 27001 beschrieben. In Kontext der Evaluierung wurden vor allem die internen Audits und der Managementreview hervorgehoben – auch hier spielt die kontinuierliche Verbesserung eine große Rolle. Die Erkenntnisse von Audits und Reviews müssen in den zukünftigen Betrieb des ISMS einfließen. Das Kapitel *Verbesserung* befasst sich nicht, wie zu erwarten wäre, mit der kontinuierlichen Verbesserung, sondern mit der Behandlung von auftretenden Abweichungen. Wichtig ist, dass bei der Korrektur von Abweichungen eine Folgenabschätzung vorgenommen wird, um zu verhindern, dass die Korrekturen schlimmere Probleme an anderen Stellen zur Folge haben.

Im Anschluss an die Bestandteile der ISO 27001 wurden zwei weitere, aber nicht weniger wichtige, Bestandteile der ISO-27000-Familie beschrieben. Zuerst wurde auf die ISO 27002 (beziehungsweise den Anhang A der ISO 27001) eingegangen, welche einen Leitfaden zur Umsetzung der ISO 27001 darstellt. Die ISO 27002 enthält diverse Sicherheitsanforderungen zusammen mit Maßnahmen und dazugehörigen Zielen. Auffällig waren hier die neuen Anforderungen an kryptographische Maßnahmen, welche in alten Versionen noch nicht vorhanden waren. Anschließend wurde kurz die ISO 27005 beschrieben. Dieser Standard definiert ein Risikomanagement für Informationssicherheit. Es wurde hervorgehoben, dass die Standards ISO 27001 und ISO 27005 zwar eng verzahnt sind, die ISO 27005 aber nicht explizit verlangt wird. Dies dient dem Zweck, Unternehmen eine gewisse Wahlfreiheit bei der Wahl des Risikomanagementansatzes zu gewähren.

In der Folge wurde kurz auf zwei weitere Standards für Informationssicherheitsmanagement im deutschsprachigen Raum und deren Berücksichtigung der kryptographischen Maßnahmen eingegangen. Zum einen gibt es das österreichische Informationssicherheitshandbuch, welches im Grunde ein erweiterter Umsetzungsleitfaden ist, und zum anderen den IT-Grundschutz des deutschen BSI, welcher ursprünglich aus der ISO 27001 entstanden, inzwischen aber sehr eigenständig ist.

Zum Abschluss dieses Abschnitts wurde der Nutzen eines Informationssicherheitsmanagement-systems für eine Organisation herausgearbeitet. Ein großer Nutzen liegt im Ansatz der kontinuierlichen Verbesserung – dadurch ist es möglich, zyklisch auf die sich immer wieder ändernden Sicherheitsanforderungen (beispielsweise aufgrund neuer Gesetze oder Technologien) reagieren zu können. Zusätzlich wurde erwähnt, dass ein zertifiziertes Informationssicherheitsmanagement, gerade in der Dienstleistungsbranche, durchaus ein Alleinstellungsmerkmal oder sogar für die Teilnahme an Ausschreibungen erforderlich sein kann. Nicht zuletzt soll erwähnt werden, dass eine strukturierte Vorgehensweise auch bei der Bewältigung der (oftmals komplexen) Sicherheitsanforderungen unterstützt.

Im darauffolgenden Abschnitt wurden die Grundlagen und Ziele der Kryptographie erarbeitet. Angefangen mit den Ursprüngen der Kryptographie (zum Beispiel der Caesar-Chiffre), über die Vignére-Chiffre, bis zur Funktionsweise der modernen Kryptographie, wurde die grundsätzliche Funktionsweise der typischen kryptographischen Verfahren beschrieben.

Im Anschluss daran wurde erörtert, welche Ziele der Kryptographie verfolgt und mit welchen Verfahren welches Ziel am ehesten erreicht werden kann. So eignen sich für die Sicherstellung der Vertraulichkeit am besten symmetrische Verfahren, wie zum Beispiel AES. Für die Gewährleistung von Authentizität werden in der Regel ebenfalls symmetrische Verfahren oder Signaturen herangezogen. Symmetrische Verfahren bieten sich in diesem Fall allerdings nur an, wenn sich maximal zwei Kommunikationsteilnehmer einen Schlüssel teilen – ansonsten kann nicht mehr sichergestellt werden, welcher Teilnehmer mit dem Schlüssel nun verschlüsselt hat. Ein weiteres Ziel von Kryptographie ist es, die Integrität von Informationen oder Daten zu schützen. Zu diesem Zweck werden Hash- beziehungsweise Einwegfunktionen verwendet. Diese Funktionen bilden quasi den Fingerabdruck eines Dokuments indem mittels logischer Operationen der Dokumenteninhalt auf eine begrenzte Zeichenlänge komprimiert wird.

Oberstes Ziel ist es, dass jedes Dokument einen einmaligen Hashwert erhält. Zum Abschluss wurde das Ziel der Verbindlichkeit beschrieben. Dabei geht es darum, bestimmte Handlungen (wie zum Beispiel das Senden einer Datei) gegenüber Dritten beweisbar zu machen. Zu diesem Zweck wurde die asymmetrische Verschlüsselung umgekehrt und der Signator signiert den Hash seines Dokuments mit seinem privaten Schlüssel. Andere Personen können die Echtheit des Dokuments nun durch das Entschlüsseln der Hashs mit dem öffentlichen Schlüssel des Signators verifizieren.

Zum Abschluss dieses Abschnitts wurde hervorgehoben, welchen Nutzen kryptographische Verfahren für die Informationssicherheit haben und warum eine Richtlinie für kryptographische Verfahren innerhalb eines ISMS wichtig ist: Vertraulichkeit kann zwar noch durch organisatorische Mittel und Berechtigungskonzepte gewährleistet werden, im Falle der Integrität und Verbindlichkeit wird dies allerdings schon schwierig. In diesem Fall helfen nur kryptographische Verfahren. Es wurde deutlich gemacht, dass ein Großteil der Ziele der Informationssicherheit auch mit den Zielen der Kryptographie übereinstimmt.

Im letzten Abschnitt dieses Kapitels wurden einige, für die Informationssicherheit wichtige Gesetze auf Hinweise nach kryptographischen Anforderungen analysiert. Grundsätzlich lässt sich sagen, dass keines der betrachteten Gesetze (E-Government-Gesetz, Signatur- und Vertrauensdienstegesetz, Datenschutzgesetz und Datenschutz-Grundverordnung) explizite Anforderungen an kryptographische Maßnahmen stellt.

Das E-Government-Gesetz hat zum Ziel, die elektronische Kommunikation mit den Behörden zu vereinfachen und schafft den Rechtsrahmen für rechtswirksamen digitalen Schriftverkehr. Im konkreten Fall geht es vor allem um die typischen Erledigungen im Verwaltungsverfahrensrecht, wie die Bescheidzustellung oder den Einspruch. Zusätzlich definiert das E-Government-Gesetz auch die Nutzung des elektronischen Identitätsnachweises beziehungsweise der Bürgerkarte. In Sachen Informationssicherheit verweist das EGovG in erster Linie auf das Datenschutzgesetz.

Im Anschluss wurde das Signatur- und Vertrauensdienstegesetz betrachtet. In diesem Gesetz wird zum einen die Rechtsgültigkeit einer (qualifizierten) Signatur begründet und zum anderen werden die Pflichten der Vertrauensdiensteanbieter festgeschrieben. Die Vertrauensdiensteanbieter können eine qualifizierte Signatur ausstellen, wie sie das Gesetz fordert. Sofern das betroffene Unternehmen kein Vertrauensdiensteanbieter ist, verweist auch dieses Gesetz in der Informationssicherheit vor allem auf das Datenschutzgesetz.

Das DSG 2000 begründet in Österreich das Grundrecht auf Datenschutz von natürlichen und juristischen Personen und regelt unter anderem die grundsätzliche Verwendung von Daten, die Anforderungen an die Datensicherheit, Rechte von Betroffenen, die Publizität der Datenverarbeitungen, den Rechtsschutz und die Kontrollorgane für den Datenschutz. Das Datenschutzgesetz stellt große Anforderungen an das Informationssicherheitsmanagement und es wurde deutlich, dass die Anforderungen des Datenschutzgesetzes ohne ein funktionierendes Informationssicherheitsmanagement nur sehr schwer zu erfüllen sind.

Die Datenschutz-Grundverordnung sorgt nun ab Mai 2018 für eine Homogenisierung der einzelnen staatsspezifischen Datenschutzgesetze innerhalb der Europäischen Union. Die

Datenschutz-Grundverordnung ersetzt die Datenschutz-Richtlinie von 1995 und ist für die einzelnen Mitgliedsstaaten verbindlich und direkt wirksam. Die Mitgliedsstaaten haben allerdings die Möglichkeit aufgrund der Öffnungsklauseln gewisse Anpassungen in ihren eigenen Gesetzen vorzunehmen. In Österreich wird dies wahrscheinlich durch eine Novellierung des Datenschutzgesetzes geschehen. Grundsätzlich erhöht die Datenschutz-Grundverordnung den Stellenwert der Informationssicherheit für Unternehmen, da nun bei einem Verstoß gegen den Datenschutz mit deutlich höhere Strafen (bis zu 20 Millionen Euro oder 4 % des Konzernumsatzes) zu rechnen ist.

Es lässt sich sagen, dass vor allem das Datenschutzgesetz und die kommende Datenschutz-Grundverordnung großen Einfluss auf die Planung und den Betrieb eines ISMS haben beziehungsweise die Themen Datenschutz und Informationssicherheit für die Organisationsleitung in den Fokus holen.

Sowohl die Anforderungen des aktuellen Datenschutzgesetzes als auch die Anforderungen, die durch die Novellierung des Datenschutzgesetzes aufgrund der Datenschutz-Grundverordnung entstehen, lassen sich ohne ein durchdachtes Informationssicherheitsmanagement nur schwer erfüllen. Hier sind Unternehmen, die bereits ein System für sich implementiert haben, sicher besser aufgestellt als Unternehmen, die sich dem Thema erst jetzt oder kurz vor dem Wirksamwerden der DSGVO widmen.

Grundsätzlich lässt sich sagen, dass für die öffentliche Verwaltung keine besonderen Anforderungen seitens des Gesetzgebers bestehen. Es bleibt allerdings zu bedenken, dass im Bereich der Verwaltung sehr oft mit sensiblen, personenbezogenen Daten gearbeitet wird und diese dementsprechend geschützt werden müssen.

Das folgende Kapitel behandelt die Erstellung einer Richtlinie, welche den angesprochen Anforderungen gerecht werden kann.

3 ENTWICKLUNG EINER RICHTLINIE

Dieses Kapitel der Arbeit behandelt die Entwicklung einer speziellen Richtlinie für den Einsatz kryptographischer Verfahren. Zu diesem Zweck wird zuerst ein Vorgehensmodell für die Richtlinienerstellung entwickelt. Im zweiten Abschnitt werden Fachleute zu dem Vorgehensmodell befragt um Verbesserungspotenziale erkennen zu können. Der dritte Abschnitt beschreibt die exemplarische Anwendung des Modells im Rahmen einer Fallstudie.

3.1 Entwicklung des Vorgehensmodells

Sowohl ISO 27001 als auch die ISO 27002 bieten zwar Sicherheitsanforderungen und dazugehörige Ziele, allerdings wird keine Hilfestellung hinsichtlich der Formulierung beziehungsweise Ausgestaltung dieser Richtlinien gegeben. Peltier (2002) und Purser (2004) beschreiben in ihren Werken jeweils einen möglichen Ansatz zum Erstellen einer Richtlinie für das Informationssicherheitsmanagement. Beide Ansätze werden in diesem Abschnitt kurz vorgestellt.

3.1.1 Allgemeine Beobachtungen

Bevor die zwei erwähnten Ansätze beschrieben werden, wird an dieser Stelle noch kurz auf die grundsätzlichen Kriterien für ein effektives und effizientes Informationssicherheitsmanagement eingegangen. Wie bereits geschildert, stellen die Punkte Führung und Unterstützung wichtige Eckpfeiler des ISMS dar. Ohne Rückhalt von der Unternehmensführung kann ein Informationssicherheitsmanagementsystem nicht funktionieren, da in der Regel die nötigen Ressourcen und die erforderliche Durchsetzungskraft fehlen.

Aber es gibt auch weniger offensichtliche Punkte, die nach Erfahrung des Autors in der Praxis immer wieder ignoriert oder zumindest nicht ernst genommen werden. Einer dieser wichtigen Punkte ist die Kommunikation. Ohne Kommunikation über die Funktion, den Zweck (dies schließt auch die Kommunikation möglicher Bedrohungen mit ein) und den Mehrwert des ISMS an die Personen, die von den Richtlinien oder Leitfäden betroffen sind (also nach ihnen arbeiten müssen), wird ein ISMS nicht den Schutz bieten können, der theoretisch möglich wäre.

Der andere Punkt ist ein (gutes) Dokumentenmanagement. Ohne eine funktionelle Struktur des Dokumentenverzeichnisses und eine entsprechende Versionierung werden spätestens beim erneuten Audit erste Probleme bezüglich Auffindbarkeit, Version und/oder Gültigkeit auftreten. Zusätzlich sollten die entsprechenden Richtlinien auch dem Personal oder Dienstleister zur Verfügung gestellt werden, damit diese im Zweifels- oder Bedarfsfall erneut konsultiert werden können. Hier ergibt sich dann auch der erste Stolperstein, bei dem kryptographische

Maßnahmen sinnvoll angewendet werden können: Wie kann die Authentizität der Richtlinie nachgewiesen werden? Es liegt also nahe hinsichtlich Verschlüsselung und Signatur von Informationen die offensichtlichen Punkte abzuarbeiten – eine modifizierte Richt- oder sogar Leitlinie kann mittelfristig ebenso schwere Folgen nach sich ziehen wie korrumpierte oder gestohlene Unternehmensdaten.

Die beiden genannten Punkte sollten bei Planung und Betrieb eines ISMS, aber auch beim Verfassen von Richtlinien, im Hinterkopf behalten werden, um die Wirksamkeit des ISMS beziehungsweise der Richtlinien sicherzustellen.

An dieser Stelle muss auch kurz auf das sogenannte Tailoring eines Managementsystems eingegangen werden. Beim Tailoring eines ISMS geht es darum, die Einzelaspekte eines Managementsystems so zu interpretieren und abzustimmen, dass diese möglichst effektiv und effizient in der Organisation wirken können und idealerweise Synergien schaffen. Aufgrund der weitreichenden Konsequenzen der Einführung eines ISMS ist es selbstverständlich, dass dieses Tailoring nur mit Unterstützung des obersten Managements eines Unternehmens erfolgreich sein kann. Wenn ein Managementsystem wie das ISMS nicht an das Unternehmen beziehungsweise die Organisation angepasst wird, kann damit gerechnet werden, dass ein hohes Maß an zusätzlichen Prozessen, aber kein zusätzlicher Nutzen für die Organisation geschaffen wird. (Kersten, Reuter, & Schröder, 2008)

Ähnliches deutet auch Klipper in seinem Buch *Information Security Risk Management* (2011) an. Dort schreibt er, dass man sich das eigene ISMS selbst erarbeiten muss und dass es kein fertiges ISO/IEC-27000 gibt. Bereits im Schritt der Planung ist es wichtig, eigenständig Risiken zu identifizieren und den Kontext des ISMS zu definieren.

Auch Carlson (2008) schreibt, dass ein erfolgreiches ISMS die organisatorischen Faktoren miteinbeziehen muss, da diese den ISMS-Framework beeinflussen werden. Ebenso haben Kultur und regulatorische Anforderungen Einfluss auf die Ausgestaltung des ISMS.

Es hat den Anschein, dass ein Managementsystem nach ISO/IEC 27001 nur mit entsprechenden Anpassungen wirksam betrieben werden kann. Konkret wirkt sich dieses Anpassen oder Tailoring auf die Definition des Kontextes aus. In diesem Schritt werden der Anwendungsbereich und die Grenzen, die Rollen und Verantwortlichkeiten sowie die Basiskriterien des ISMS definiert. Dieser hohe Anpassungsbedarf spiegelt sich auch in der Planungsphase der ISO/IEC 27001 wieder: Es wird explizit darauf hingewiesen, dass Ziele, Grenzen und Regeln abhängig von der Art des Unternehmens, der Organisationsform, des Standortes und den jeweiligen Vermögenswerten definiert werden müssen. (ISO/IEC 27001:2013-10, 2013)

3.1.2 Ansätze zur Richtlinienerstellung

In diesem Unterabschnitt werden zwei Ansichten zur Richtlinienerstellung für das Informationssicherheitsmanagement beschrieben.

Peltier (2002) führt für den Begriff Richtlinie beziehungsweise Policy zu Beginn drei Definitionen ein. Es gibt die „General Program Policy“, welche auch als Strategiestatement gesehen werden kann und in der ISO 27001 die Informationssicherheitsleitlinie ist. Zudem gibt es auch die „System/Application-Specific Policy“, welche zum Schutz eines bestimmten Systems dient. Die dritte Definition ist die „Topic-Specific Policy“ – mit dieser Richtlinie werden gesamte Themenbereiche behandelt und in diesen Bereich fällt auch die Richtlinie, die in dieser Arbeit erstellt wird. Grundsätzlich lässt sich dieses Gefüge ähnlich eines Baums darstellen. An der Spitze befindet sich die Informationssicherheitsleitlinie, die durch themenspezifische Richtlinien und systembezogene Richtlinien unterstützt wird – dieses Verhältnis ist in Abbildung 7 dargestellt.

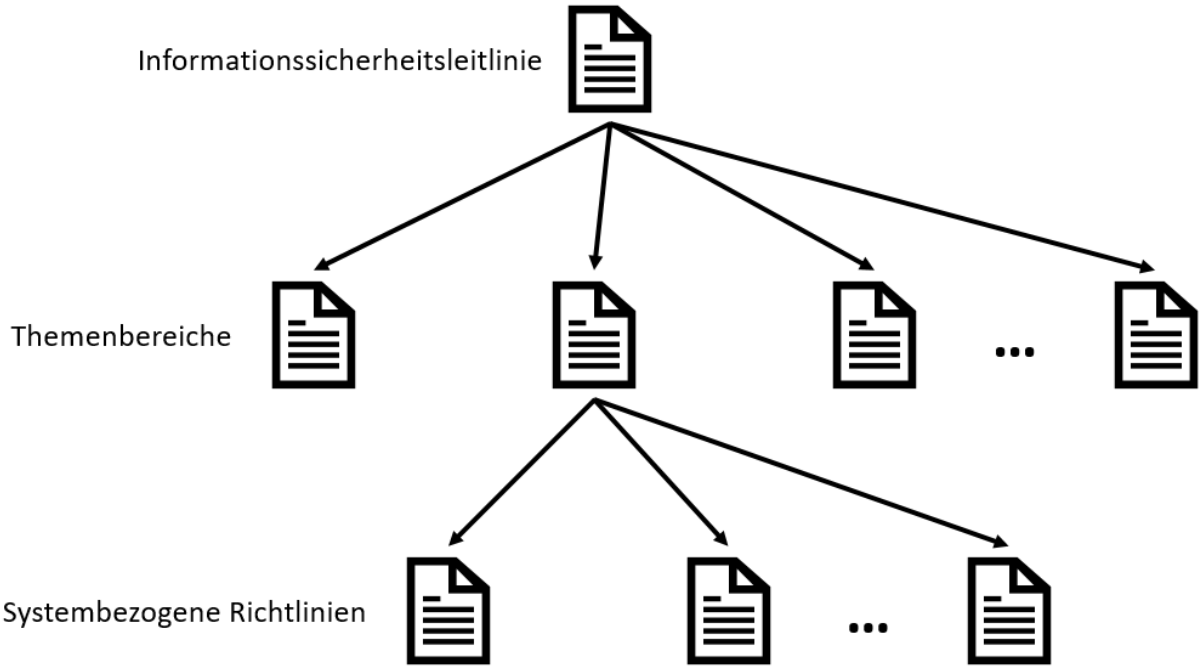

Abbildung 7: Richtlinienstruktur

Damit eine Richtlinie die Anforderungen des Unternehmens erfüllen kann, sind laut Peltier einige Schlüsselfaktoren wichtig, die an dieser Stelle kurz vorgestellt werden sollen. Eine Richtlinie sollte unter anderem leicht verständlich und an die Zielgruppe angepasst sein. Des Weiteren sollten Richtlinien nicht einfach von anderen Organisationen übernommen werden, sondern immer auf die speziellen Anforderungen einer Organisation abgestimmt werden – dies schließt auch die Sichtung bestehender Richtlinien und die Verzahnung mit diesen ein. Einen der wichtigeren Punkte stellt der Faktor Umsetzbarkeit dar: Die beste Security-Richtlinie ist wertlos, wenn durch sie die Tätigkeit der Organisation behindert oder sogar zum Stillstand gebracht wird und schlussendlich die Organisationsziele nicht mehr erreicht werden können. Es ist essentiell, dass vor der Inkraftsetzung einer Richtlinie eine Folgenabschätzung durchgeführt wird. Ein weiterer Punkt ist die Proaktivität – eine Richtlinie sollte keine Verbotsliste darstellen, sondern Handlungsempfehlungen enthalten. Zusammengefasst heißt das, dass eine Richtlinie

im Rahmen des Informationssicherheitsmanagements zum einen an die Anforderungen von Unternehmen und Zielgruppe angepasst sein sollte und zum anderen den Betrieb nicht (zu sehr) einschränken sollte. (Peltier, 2002)

Für den Methodeneinsatz bei der Richtlinienerstellung impliziert dies, dass zumindest zwei Methoden empfehlenswert sind: die Umweltanalyse und die Folgenabschätzung. Die Umweltanalyse sorgt für einen Blick auf bestehende Richtlinien und die angepeilte Zielgruppe, wohingegen die Folgenabschätzung einen Blick in die Zukunft ermöglicht. Dieser Blick klärt zum einen, ob die proklamierten Ziele der Richtlinie überhaupt erreicht werden können und zum anderen, ob die Richtlinie die Unternehmenstätigkeit nicht auf eine nachteilige Art und Weise beeinflusst.

Eine themenspezifische Richtlinie sollte zumindest erklären, was durch diese Richtlinie erreicht werden soll und warum die Richtlinie relevant ist (und das kann nicht nur durch die anstehende Zertifizierung gegeben sein). Zusätzlich soll geklärt werden, welche Rollen oder Positionen durch diese Richtlinie berührt werden. Abschließend soll auch in der Richtlinie enthalten sein, wie Compliance sichergestellt werden kann und was bei einer Abweichung von der Richtlinie passieren soll. Gegebenenfalls sollten der Richtlinie auch zusätzliche Informationen, wie zum Beispiel Kontakte für Rückfragen, hinzugefügt werden. (Peltier, 2002)

Ergänzend zu den Bestandteilen der verschiedenen Richtlinienarten hat Peltier auch einen zehnstufigen Ansatz für das Informationssicherheitsmanagement definiert, welcher an dieser Stelle kurz angesprochen wird. Die ersten zwei Schritte befassen sich mit der Analyse von bereits Bestehendem. So sollen zuerst bestehende Richtlinien überprüft und abgewogen werden, ob überhaupt eine neue Richtlinie von Nöten ist. Der zweite Schritt sorgt für einen Blick auf die Organisation. Hier wird dafür gesorgt, dass die Richtlinie im Einklang mit den Geschäftszielen liegt. Die folgenden drei Schritte befassen sich eher mit dem Aufbau und der Sprache der Richtlinie als mit dem tatsächlichen Inhalt. Hierbei geht es auf der einen Seite um den Aufbau des Dokumentes – dieser sollte bereits bestehenden Richtlinien entsprechen, um Ablenkung durch andere Formatierung und Ähnliches zu verhindern. Die Punkte 4 und 5 sagen aus, dass auch Entwürfe auf Rechtschreibung und Grammatikfehler überprüft werden sollten sowie dass die Sprache eher einfach gehalten werden sollte. Ersteres vermittelt dem Publikum einfach eine gewisse Sorgfalt und sorgt dafür, dass die Richtlinie auch ernst genommen wird. Der zweite Punkt erhöht die Lesbarkeit der Richtlinie. Der sechste Punkt des Ansatzes ist vermutlich einer der wichtigsten: Es muss immer ein Kompromiss zwischen Sicherheit und den damit einhergehenden Einschränkungen gefunden werden. Die letzten vier Punkte behandeln besonders die Kommunikation der Richtlinie. Beim Verfassen der Richtlinie sollte nicht vergessen werden, dass die Adressaten der Richtlinie keine IT- oder Sicherheitsfachleute sind. Bevor eine Richtlinie zur Genehmigung an die Unternehmensführung übermittelt wird, muss die Unternehmensführung bereits über den Zweck, Mehrwert und mögliche Einschränkungen der Richtlinie informiert sein. Zusätzlich sollte die Richtlinie so lang wie nötig, aber so kurz wie möglich sein. Dies sorgt dafür, dass man sich bei der Erstellung nicht in unnötige Details verliert. Als letzten Punkt führt Peltier an, dass das Personal ebenfalls über die Richtlinie informiert werden muss und gegebenenfalls bewusstseinsbildende Maßnahmen getroffen werden müssen. (Peltier, 2002)

Diese zehn Phasen geben im Grunde die bereits angesprochenen Schlüsselfaktoren einer Richtlinie wieder. Die Richtlinie muss auf das bestehende Informationssicherheitsframework und die Organisation abgestimmt sein. Im Bereich der Organisation umfasst das nicht nur die grundsätzlichen Strukturen, sondern auch Punkte wie Unternehmenskultur und Unternehmenssprache – dadurch wird eine Akzeptanz der Richtlinie unterstützt. Ein weiterer wichtiger Punkt ist die Kommunikation. Die Richtlinie muss in ihrer sprachlichen Ausgestaltung zielgruppengerecht sein. Zusätzlich sollte kommuniziert werden, was mit der Richtlinie erreicht werden soll und welche möglichen Einschränkungen es geben könnte – dies ist auch wichtig für den Risikomanagementprozess.

Auch Steve Purser hat sich umfassend dem Informationssicherheitsmanagement, einem möglichen Vorgehen und wichtigen Eckpfeilern gewidmet. Grundsätzlich sieht er Richtlinien als Richtungsgeber für das Informationssicherheitsmanagement – dabei bezieht er sich vor allem auf die Informationssicherheitsleitlinie. Er hebt an dieser Stelle hervor, dass Richtlinien keine Detailanweisungen für bestimmte Problemstellungen enthalten, sondern eher einen Handlungsrahmen vorgeben. Davon abgeleitet folgen dann bereits Prozesse und Standards, wobei die Standards tatsächlich auf bekannten Best-Practices beruhen sollten. Durch diese Prozesse und Standards wird das tatsächliche Tagesgeschäft bestimmt. (Purser, 2004)

Im Vergleich zu Peltier wird hier keine weitere Schicht an themenspezifischen Richtlinien eingezogen, welches das Mapping von Prozessen und Standards zur Informationssicherheits-leitlinie in der Praxis etwas kompliziert gestalten wird. Bei der genauen Ausgestaltung der Richtlinien stellt sich auch bei Purser eine Hierarchie von verschiedenen Richtlinien ein, die allerdings nicht so ausgeprägt ist wie bei Peltier.

Richtlinien für das Informationssicherheitsmanagement müssen eindeutig formuliert und verständlich sein sowie keine Informationen enthalten, von den bekannt ist, dass sie in Zukunft ungültig werden könnten (Purser, 2004). Hier (und auch in späteren Punkten) sind deutliche Parallelen zu den Ansichten Peltiers erkennbar.

Eine Richtlinie sollte laut Purser auf die Kultur einer Organisation angepasst sein und auch rechtliche und regulatorische Anforderungen enthalten. Zudem sollte beschrieben werden, welche Bedrohungen durch die jeweilige Richtlinie behandelt werden. Zusätzlich können je nach Fokus der Richtlinie auch weitere Informationen oder Anforderungen enthalten sein. Wichtig für die Erstellung einer Richtlinie sind vor allem die betroffenen Personen. (Purser, 2004)

Grundsätzlich scheinen Peltier und Purser ähnliche Auffassungen der relevanten Faktoren für ein funktionierendes Informationssicherheitsmanagement und den entsprechenden Richtlinien zu haben. Beide heben besonders hervor, dass es wichtig ist, die Richtlinien an die unternehmensspezifischen Gegebenheiten und die entsprechende Zielgruppe anzupassen. Purser betont ein wenig stärker, wie wichtig es ist, bei der Ausgestaltung der Richtlinie die betroffenen Personen miteinzubeziehen.

3.1.3 Vorgehensmodell für die Richtlinienerstellung und -pflege

Anhand der gefundenen Informationen lässt sich ein grobes Vorgehensmodell für die Richtlinienerstellung im Rahmen des Informationssicherheitsmanagements erstellen. Dieses Modell wird in diesem Unterabschnitt kurz vorgestellt.

Das Modell untergliedert sich in die drei Phasen *Strategische Betrachtung*, *Richtlinienentwicklung* und *Prozess- und Standardentwicklung*. In der Phase der strategischen Betrachtung geht es entweder um die initiale Erstellung des Informationssicherheitsleitbilds oder um die zyklische Verbesserung dieses Leitbilds. Die Richtlinienentwicklung behandelt die verschiedenen Themen des Informationssicherheitsmanagements in Anlehnung an den Anhang A der ISO 27001. In der Prozess- und Standardentwicklung werden die einzelnen Prozesse und Standards für die Themenrichtlinien genau definiert. Hier wird bereits deutlich, dass sich der Ansatz stark an der, von Peltier und Purser erkannten, Hierarchie der einzelnen Richtlinien und Standards orientiert.

Für die einzelnen Phasen kommen grundsätzlich ähnliche Methoden zum Einsatz, wobei der Unterschied in der jeweiligen Sichtweise liegt. Im Bereich der Prozess- und Standardentwicklung werden in der Regel andere Faktoren bei der Ist-Analyse relevant sein als bei der strategischen Betrachtung. Abhängig von der ISO 27001 und den Erfolgskriterien des Informationssicherheitsmanagements, wie sie in diesem Kapitel erarbeitet wurden, können gewisse Methoden vorgeschlagen werden.

Für die Informationssicherheitsleitlinie, welche im Rahmen der strategischen Betrachtung verfasst wird, ist es erforderlich den Geltungsbereich sowie die Anforderungen der relevanten Stakeholder zu erfassen und zu dokumentieren. Zudem sollte geklärt werden, was das Ziel der Leitlinie darstellt und wie dieses erreicht werden soll. Schlussendlich sollte auch enthalten sein, warum die Leitlinie, beziehungsweise das Informationssicherheitsmanagement als solches, relevant für das Unternehmen sind. Um diese Faktoren erfassen zu können, bieten sich zum Beispiel Umwelt- und Ist-Analysen an. Zusätzlich kann an dieser Stelle auch eine Bedrohungsanalyse vorgenommen werden, um die Relevanz des Themas zu unterstreichen. Die oben angesprochene Folgenabschätzung ist auf dieser Ebene noch nicht allzu relevant, da die Informationssicherheitsleitlinie als solche meistens noch keine Auswirkungen nach sich zieht.

Für die Themenrichtlinien sind ebenfalls Ist- und Umweltanalysen relevant. Mit Hilfe der Ist-Analyse wird geklärt, ob (und falls ja: welche) Abläufe für einen bestimmten Bereich vorhanden sind. Durch die Stakeholderanalyse wird geklärt, welche Unternehmensbereiche und Personengruppen von dieser Richtlinie betroffen sein könnten. Die betroffenen Benutzergruppen sollten bereits bei der Konzeption der Richtlinie informiert oder sogar konsultiert werden. Nicht zu vernachlässigen sind an dieser Stelle unter anderem auch Meinungen aus der Literatur und Best-Practices. Ebenfalls wird hier die Bedrohungsanalyse aufgegriffen. Im Gegensatz zur ersten Phase sollen in diesem Schritt allerdings bereits konkrete Bedrohungen, welche zum Beispiel im Risikomanagementprozess erkannt wurden, betrachtet werden. Aufgrund der unmittelbaren Auswirkung auf Abläufe und interne Standards wird in

dieser Phase eine genaue Folgenabschätzung empfohlen, um negative Auswirkungen der Richtlinie zu vermeiden. Die Folgenabschätzung erfolgt nach einem ersten Entwurf der Themenrichtlinie. Erst wenn die Folgenabschätzung positiv (das heißt, dass die entstehenden Einschränkungen tragbar sind) ausfällt, wird die Richtlinie freigegeben.

In der folgenden Phase, der Prozess- und Standardentwicklung, werden anhand der Use-Cases in den Themenrichtlinien Prozesse und interne Standards definiert oder überarbeitet. Es kann allerdings auf diesen Schritt verzichtet werden, wenn zum Beispiel keine eigenen Prozesse notwendig sind oder die Beschreibung in der Themenrichtlinie zu einem Use-Case ausreichend ist – in der Praxis wird dies aber selten der Fall sein. Auch hier kommen wieder die Ist- und Stakeholderanalysen zum Einsatz. Die Stakeholderanalyse erfolgt mit dem Fokus auf die betroffenen Benutzergruppen und eine frühestmögliche Einbindung dieser Gruppen in den Sicherheitsprozess. Außerdem ist das Sichten von externem Wissen vorgesehen, um andere, relevante Standards zu überprüfen und gegebenenfalls für die eigenen Zwecke zu adaptieren. Im Rahmen der Ist-Analyse sollen besonders bereits gelebte Prozesse erfasst und gegebenenfalls verbessert werden. Zusätzlich soll hier auch aktiv nach bestehenden Sicherheitslücken oder anderen Bedrohungen gesucht werden.

Anhand der Erkenntnisse in den einzelnen Phasen kann es notwendig sein, in übergeordnete Phasen zurückzuspringen und Anpassungen an den jeweiligen Richtlinien vorzunehmen. Dies ist kein Problem und es wird empfohlen nach dem erstmaligen Durchlauf wieder mit der Pflege der Richtlinien zu beginnen. Hierdurch wird auch die kontinuierliche Verbesserung, wie sie von der ISO 27001 gefordert ist, unterstützt. Die Phasen des Vorgehensmodells sind in der folgenden Abbildung (Abbildung 8) dargestellt.

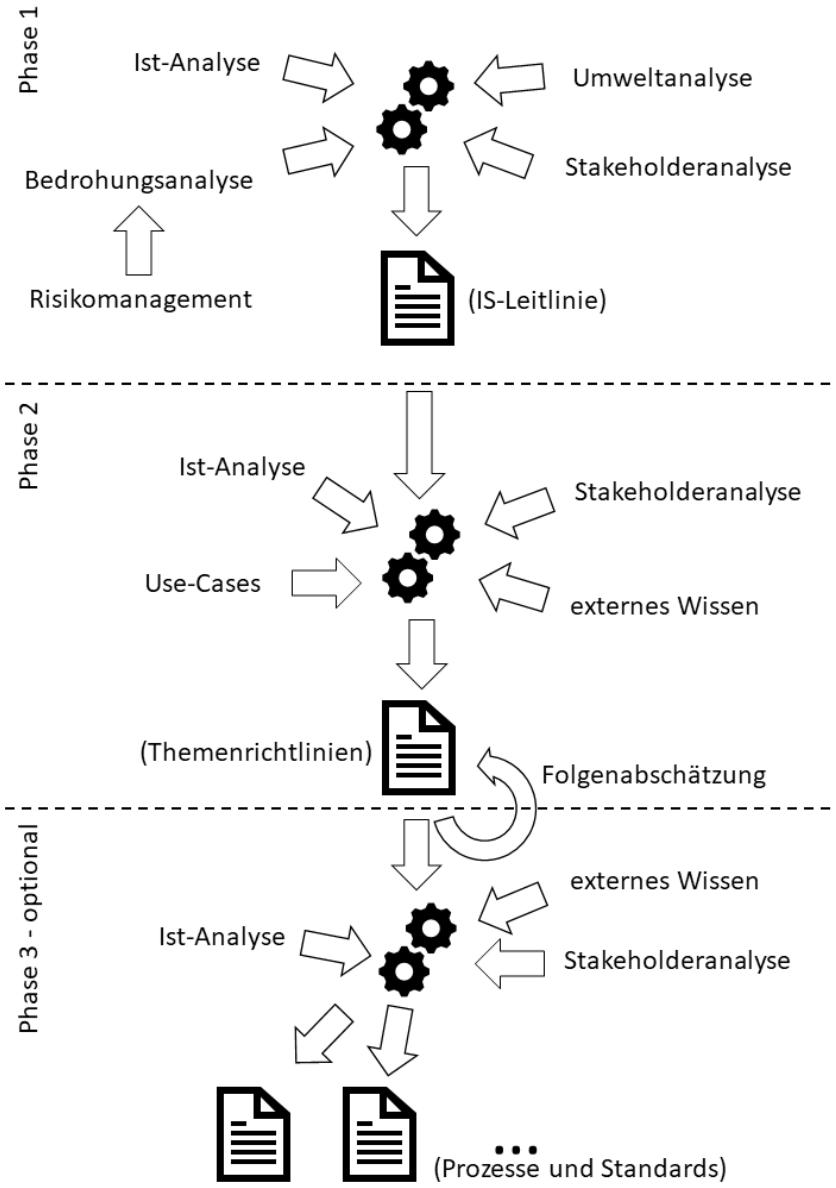

Abbildung 8: Erstes Vorgehensmodell für die Erstellung von ISMS-Richtlinien

Aufgrund des Aufbaus lässt sich, bei bestehendem Bedarf, auch direkt die Dokumentenstruktur für das Informationssicherheitsmanagement übernehmen. Zuoberst steht die Informationssicherheitsleitlinie mit den entsprechenden Ordnern für die Themenrichtlinien. Diese Ordner enthalten die Themenrichtlinie selber, sowie die definierten Standards und Prozesse. Auf diese Art und Weise lassen sich die Dokumente schnell auffinden und anhand der, in den Richtlinien definierten Zielgruppen, kommunizieren.

Es bleibt anzumerken, dass das Vorgehensmodell vorsieht, dass das Informationssicherheitsmanagement mit der Zeit wächst und initial kein perfektes Ergebnis erzielt werden kann. Dies ergibt sich vor allem aus der Komplexität von einigen Applikationen und Unternehmensstrukturen. Es sollte bei der Konzeption schrittweise vorgegangen werden und eingangs überlegt werden, welche Anforderungen auf jeden Fall erfüllt werden müssen und welche Anforderungen auch in weiteren Iterationen umgesetzt werden können. Ebenso verhält

es sich mit den gegebenenfalls anwendbaren Metriken. Im ersten Entwurf sollte hier auf einfache Metriken zurückgegriffen werden, die im Laufe der Zeit verfeinert werden können.

Was eine Richtlinie im Rahmen des Informationssicherheitsmanagements mindestens enthalten sollte, wurde bereits im vorhergehenden Abschnitt beschrieben und von diesen Inhalten soll auch im Rahmen dieses Modells nicht abgewichen werden. Allerdings wird empfohlen den entsprechenden Richtlinien zusätzliche Punkte hinzuzufügen. Dazu gehören zum einen die Auswirkungen, die im Rahmen der Folgenabschätzung entdeckt und in Kauf genommen werden. Positive Auswirkungen können ebenfalls erwähnt werden, werden aber wahrscheinlich eher in der Zielformulierung der Richtlinie untergebracht sein. Zum anderen erscheint es sinnvoll, die Richtlinien um einen Ausblick zu erweitern. Dieser Ausblick bietet die Möglichkeit Entwicklungspotenziale aufzuzeigen und sorgt dafür, dass die Richtlinien stets mit einem Blick in die Zukunft entwickelt werden. Gegebenenfalls könnte dieser Ausblick auch ein Begleitdokument der entsprechenden Richtlinie werden.

Im Sinne der ISO 27001 sieht dieses Vorgehensmodell vor, dass die einzelnen Phasen in regelmäßigen Abständen erneut durchlaufen werden. Dies sorgt auf der einen Seite dafür, dass die geforderten Revisionen durchgeführt werden und dass aktiv überprüft wird, ob die Richtlinie noch dem aktuellen Stand der Dinge entspricht. Auf der anderen Seite wird dadurch auch der kontinuierliche Verbesserungsprozess abgebildet und dafür gesorgt, dass die Richtlinien nicht nur in der bestehenden Form weitergeführt, sondern auch tatsächlich verbessert werden.

Im folgenden Abschnitt werden Fachleute aus dem Bereich der Informationssicherheit zu diesem Vorgehensmodell befragt. Anhand dieser Befragung soll überprüft werden, ob Verbesserungspotenziale bestehen und in welcher Art diese Verbesserungen vorgenommen werden können.

3.2 Befragung und Verbesserung

Dieser Abschnitt beschreibt Vorbereitung, Durchführung und Auswertung der angesprochenen Interviews mit Fachleuten aus dem Bereich der Informationssicherheit. Aufgrund der Ergebnisse der Interviews werden Verbesserungen an dem aufgestellten Modell vorgenommen.

3.2.1 Vorbereitung und Durchführung der Interviews

Das Ziel der Interviews ist es, das Wissen der befragten Fachleute für eine Verbesserung des Vorgehensmodells zu nutzen und gegebenenfalls auch schon Informationen über die Anforderungen an eine kryptographische Richtlinie zu erhalten. Um dieses Ziel erreichen zu können, werden die gestellten Fragen in erster Linie auf Prozess- und Domänenwissen im Bereich der Informationssicherheit abzielen.

Die Interviews werden in Form von leitfadengestützten Interviews geführt. Zu diesem Zweck werden zur Vorbereitung auf die jeweiligen Interviews bestimmte Themenbereiche beziehungsweise Pflichtfragen ausgewählt, um die es im Gespräch in erster Linie gehen soll. Diese Themenbereiche werden in den nachfolgenden Absätzen beschrieben.

Zur Beantwortung der Forschungsfrage dieser Arbeit wird ein Themenblock die Frage nach den Auswirkungen eines Vorgehens wie im beschriebenen Vorgehensmodell behandeln. Hierbei soll vor allem erfragt werden, ob ein strukturiertes Vorgehen die Richtlinienerstellung positiv beeinflusst oder ob die Richtlinienerstellung dadurch eher eingeschränkt werden kann (da zum Beispiel in zu engen Bahnen gedacht wird). Insbesondere liegt das Augenmerk auch auf der Verwaltbarkeit des gesamten Informationssicherheitsmanagementsystems.

Im zweiten Teil des Gesprächs soll es um den generellen Aufbau des Modells gehen. Ziel dieses Blocks ist es, zu überprüfen, ob die Fachleute den Aufbau des Modells in seiner jetzigen Form für gut erachten oder ob beispielsweise noch eine weitere Phase fehlt. Außerdem soll erfragt werden, ob der Detailierungsgrad der jeweiligen Phasen angebracht ist.

Der nächste Gesprächsblock behandelt die eingesetzten Methoden. Hierbei geht es darum herauszufinden, ob die ausgewählten Methoden/Arbeitsschritte in dieser Form angemessen sind oder ob es bessere Methoden für die Zielerreichung gibt.

Abschließend wird es einen weiteren Block geben, der explizit die möglichen Informationen für eine kryptographische Richtlinie erfragen soll. Hierbei geht es zum einen darum, ob sich bestimmte Methoden besonders anbieten und zum anderen sollen auch Faktoren erfragt werden, die bei der Richtlinienerstellung einen besonders großen Einfluss spielen. Dieser Block ist für das eigentliche Modell nicht mehr direkt relevant, hat aber Einfluss auf die Richtlinie, die im Rahmen dieser Arbeit erstellt werden soll.

Zum Abschluss des Gesprächs ist es zusätzlich geplant, die Fachleute aufzufordern, Anmerkungen oder Kritik anzubringen, die im bisherigen Gesprächsverlauf vielleicht noch nicht zur Sprache gekommen sind.

Aus diesen Themenblöcken werden gleich Kategorien für die spätere Auswertung abgeleitet. Diese Kategorien lauten *Nutzen*, *Aufbau und Verbesserung*, *Kryptographie* und *Sonstiges*.

Auf einen Pretest wird aufgrund der losen Strukturierung der Interviews verzichtet. Es ist vorgesehen, dass sich die Interviews zwar an einem groben roten Faden orientieren, allerdings werden Interviews erwartungsgemäß je nach Gesprächspunkt einen anderen Schwerpunkt haben. Ein Pretest hätte hier nur bedingte positive Auswirkungen auf die Gesprächsführung.

Nachdem die groben Eckpunkte des Interviews feststehen, geht es nun um die Auswahl der Fachleute für diese Interviews. Bogner, Littig und Menz (2014) schreiben, dass sich das Sampling der Fachleute „in erster Linie an der (den) Forschungsfrage(n)“ orientiert. Im Kontext dieser Arbeit heißt das, dass sich die Gruppe der Fachleute in erster Linie aus Personen zusammensetzt, die fundiertes Wissen in Bezug auf Informationssicherheit und/oder Kryptographie vorweisen können. Um mehrere Perspektiven auf das Vorgehensmodell gewinnen zu können, werden sowohl Praktiker als auch Theoretiker im Bereich der Informationssicherheit und Kryptographie als mögliche Interviewpartner in Betracht gezogen.

Die Interviews werden je nach Örtlichkeit der Interviewpartner entweder vor Ort beim jeweiligen Interviewpartner oder aber telefonisch durchgeführt. Zu Beginn des Gesprächs werden zuerst das Vorgehensmodell und eine beispielhafte Richtlinie, die mit diesem Modell erstellt wurde, vorgestellt. Nachdem die Fachleute mit den Grundlagen der Richtlinie vertraut gemacht wurden,

erfolgt die Abarbeitung des Interviewleitfadens inklusive der Aufzeichnung des Gesprächs. Die Fachleute werden bereits bei der Terminvereinbarung nach dem Einverständnis zur Aufzeichnung gefragt. Falls keine Zustimmung erfolgt, wird das Gespräch stichwortartig mitgeschrieben, um die wichtigsten Aussagen wiedergeben zu können.

3.2.2 Auswertung der Interviews

In diesem Unterabschnitt erfolgt die Auswertung der einzelnen Interviews. Zu diesem Zweck werden die Hauptpunkte der jeweiligen Interviews kurz vorgestellt und anschließend wird überprüft, wo Gemeinsamkeiten zu finden sind. Diese Gemeinsamkeiten werden dann analysiert und, sofern möglich, in das Modell übernommen beziehungsweise dort abgebildet.

Die Auswertung der Interviews orientiert sich in gewissen Teilen an dem von Gläser und Laudel (2009) beschriebenen Verfahren. Dieses Vorgehen unterteilt sich in die Schritte Vorbereitung, Extraktion, Aufbereitung und Auswertung. Die vorbereitenden Schritte wurden bereits durch die Erstellung des Leitfadens und der anschließenden groben Kategorisierung durchgeführt. Bevor die einzelnen Interviews tatsächlich ausgewertet werden können, werden die wesentlichen Aussagen der Gesprächspartner nachfolgend kurz zusammengefasst. Diese Aussagen werden dann den entsprechenden Kategorien zugeordnet.

Die erste befragte Person (Person A) ist IT-Sicherheitsexperte bei einem gemeinnützigen Verein, der sich auf technische Evaluierungen, Technologiebeobachtungen und Unterstützung von öffentlichen Stellen im Bereich der IT-Sicherheit spezialisiert hat.

Grundsätzlich ist das Modell nach Ansicht von Person A gut aufgebaut und unterstützt die Bedürfnisse der Organisation. Für eine Umsetzung in den Echtbetrieb könnte das Modell allerdings noch zu generisch sein. (Person A, persönliche Kommunikation, 17. November 2017)

Innerhalb des Modells wurden nach Meinung von Person A keine wichtigen Phasen oder Methoden vergessen. Als Verbesserungsmöglichkeiten wurden eine Evaluierungsphase und die Nutzung von internem Wissen hervorgehoben. Im Bereich der Folgenabschätzung wurde ergänzt, dass nicht nur ein Gedankenexperiment, sondern auch eine Pilotphase vorgenommen werden sollte. (Person A, persönliche Kommunikation, 17. November 2017)

Für die Erstellung einer Richtlinie für die Verwendung von kryptographischen Verfahren wurde besonders auf die Angemessenheit der verwendeten Verfahren hingewiesen. Im Kontext des Fallbeispiels im Bereich der öffentlichen Verwaltung wurde auf eine Veröffentlichung des A-SIT für die Nutzung von kryptographischen Verfahren im öffentlichen Sektor hingewiesen. (Person A, persönliche Kommunikation, 17. November 2017)

Hervorgehoben wurde, dass der Faktor Mensch (in der Rolle als Stakeholder) für den Erfolg von Richtlinien beziehungsweise Informationssicherheit als wichtig erachtet wird. Außerdem sollten der Lebenszyklus sowie die generelle Sicherheit der verwendeten Algorithmen nicht aus den Augen verloren werden. (Person A, persönliche Kommunikation, 17. November 2017)

Das zweite Interview wurde mit einem ISMS-Auditor (Person B) mit mehrjähriger Erfahrung sowie Lehrtätigkeit geführt.

Person B sagte, dass das Modell eine gute Arbeitsbasis für die Richtlinienerstellung und den Betrieb eines ISMS darstellt. Grundsätzlich sollte aber bei der Formulierung von ISMS-Leitlinien nicht die Unternehmensvision und -mission aus den Augen verloren werden, da der Anspruch für Informationssicherheit in der Regel nicht aus der Informationssicherheit selber, sondern aus den Unternehmenszielen erwächst. Ebenso spielt auch die Unternehmenskultur eine große Rolle für das ISMS und sollte zumindest über eine der vorhandenen Methoden überprüft werden. (Person B, persönliche Kommunikation, 23. November 2017)

Für den Bereich der Methodenanwendung und möglichen Inputs wurde unter anderem angemerkt, dass die Ergebnisse des Risikomanagementprozesses eher in Phase 2 als in Phase 1 genutzt werden sollten. Auch die Abhängigkeiten und Agenden der einzelnen Stakeholder untereinander sollten betrachtet und idealerweise grafisch dargestellt werden. Weitere Inputs für die zweite Phase stellen der BSI-Grundschutz und/oder die ISO 27002 dar. Unterstrichen wurde auch die Wichtigkeit der einzelnen Zielgruppen, auch was die Sprache der zu verfassenden Dokumente angeht. Die Folgenabschätzung sollte laut Person B mit Vorsicht genossen werden, da es auch durchaus vorkommen kann, dass Anforderungen komplett weggekürzt werden. Für die Phase 3 wurde hervorgehoben, dass die Verknüpfung von Anforderungen der Informationssicherheit und operativen Tätigkeiten wichtig für die Umsetzung der definierten Richtlinien wichtig sind. Außerdem muss bei den operativen Tätigkeiten darauf geachtet werden, dass in Punkto Informations- oder IT-Sicherheit ein entsprechendes Bewusstsein beim Personal geschaffen wird. Auch sollten hier ebenfalls die Ergebnisse des Risikomanagementprozesses miteinfließen. (Person B, persönliche Kommunikation, 23. November 2017)

Für den Aufbau des Modells wurde herausgehoben, dass es unterhalb der Informationssicherheitsleitlinie einen weiteren Pfad in Form der ISMS-Dokumentation gibt. Dieser Pfad umfasst und beschreibt die Arbeitsweise des Informationssicherheitsmanagements sowie die notwendigen Dokumente, wie Vorlagen oder Ähnliches. Grundsätzlich sollten Feedback-Schleifen zu den vorhergehenden Schleifen vorhanden sein und intern vorhandenes Wissen auf allen Ebenen genutzt werden. Außerdem würde es Person B begrüßen, wenn die generischen Methodennamen durch mögliche Quellen und Ziele ergänzt werden. Zudem sollte der Sinn der Pfeile im Modell beschrieben werden. (Person B, persönliche Kommunikation, 23. November 2017)

In Bezug auf die Anforderungen für kryptographische Verfahren wurde darauf hingewiesen, dass eine eigene Richtlinie für kryptographische Verfahren nur wenig Sinn macht, da es sich bei dieser Richtlinie um so etwas wie eine Basisanforderung handelt. Diese Anforderungen schlagen sich in vielen Anwendungsfällen nieder und sollten dort entsprechend dokumentiert werden. An dieser Stelle wurde auch die Wichtigkeit der Use-Case-Analyse hervorgehoben. (Person B, persönliche Kommunikation, 23. November 2017)

Der dritte Interviewpartner ist ein Experte für Informationssicherheit und Datenschutz, in einem mittelständischen Forschungsunternehmen tätig und wird im folgenden Person C genannt.

Person C unterstreicht vor allem für die initiale Einführung eines Informationssicherheitsmanagementsystems einen gewissen Nutzen des Modells, da die zuständigen

Personen hier die Möglichkeit haben, sich an einem gegebenen Rahmen zu orientieren. Dies ist bei Standards wie der ISO 27001 oder dem BSI-Grundschutz nur schwer möglich. (Person C, persönliche Kommunikation, 23. November 2017)

Beim grundsätzlichen Aufbau hat Person C die bereits angesprochenen Feedback-Schleifen zurück in die oberen Phasen vermisst. Zum Verfassen der Richtlinien sollten auch die Stimmungsmacher innerhalb eines Unternehmens hinzugezogen oder zumindest identifiziert werden. Das heißt konkret, dass bereits in Phase 2 auch schon das Personal, welches von Prozessen oder Standards betroffen ist, beachtet werden sollte. Im Bereich der Phase 1 sollte auch schon externes Wissen beziehungsweise ein Berater hinzugezogen werden, um Betriebsblindheit zu vermeiden. (Person C, persönliche Kommunikation, 23. November 2017)

Die Richtlinie zur Verwendung von kryptographischen Verfahren wird so gehandhabt, dass die spezifischen Anforderungen im Bereich der jeweiligen Business Services, wie zum Beispiel E-Mail oder Webservices, verfasst werden. Dieser Ansatz wurde gewählt, um die Anzahl der Richtlinien pro Mitarbeiter zu reduzieren. (Person C, persönliche Kommunikation, 23. November 2017)

Grundsätzlich ist Person C auch der Meinung, dass die Möglichkeit einer Zukunftsperspektive beziehungsweise einer Zieldefinition erfasst werden sollte. Der Nutzen liegt zum einen darin, dass bei der Umsetzung der Maßnahmen nicht am eigentlichen Ziel vorbei gearbeitet werden kann und zum anderen darin, dass die Maßnahmen gegenüber der Organisationsführung auch begründet werden können. (Person C, persönliche Kommunikation, 23. November 2017)

Das vierte Gespräch wurde mit einer Spezialistin für IT- und Informationssicherheit in der öffentlichen Verwaltung geführt. In den folgenden Absätzen wird diese Spezialistin Person D genannt.

Person D ist der Meinung, dass das Modell sehr hilfreich ist und auch durch die Darstellung und den Aufbau dafür gesorgt wird, dass im Entwicklungsprozess der jeweiligen Richtlinien bestimmte Einflussfaktoren nicht vergessen werden. Zusätzlich wurde die Folgenabschätzung als besonders relevant hervorgehoben, da diese über Erfolg oder Scheitern der Informationssicherheit entscheiden kann. (Person D, persönliche Kommunikation, 27. November 2017)

Von zusätzlichen Phasen innerhalb des Modells hat Person D abgeraten, da dies das Vorgehen nur noch mehr verkomplizieren würde. Dies wurde vor allem im Hinblick auf die Managementprozesse im Bereich der Informationssicherheit und des Risikomanagements hervorgehoben. Grundsätzlich fehlen Person D Punkte wie die Bewusstseinsbildung und Schulung. (Person D, persönliche Kommunikation, 27. November 2017)

Für die Richtlinie für kryptographische Verfahren wurde von Person D besonders die Analyse der verschiedenen Use-Cases als wichtig empfunden, um eine möglichst große Abdeckung der tatsächlichen Anwendungsfälle erreichen zu können. Dies wird von Person D besonders bei Querschnittsthemen wie der Kryptographie als wichtig empfunden. Auch hervorgehoben wurden Möglichkeiten der Automatisierung, um dennoch einen gewissen Komfort bei der Nutzung von kryptographischen Verfahren gewährleisten zu können. Ähnlich wie Person A sieht

auch Person D einen hohen Bedarf an stetiger Kontrolle der eingesetzten Algorithmen. (Person D, persönliche Kommunikation, 27. November 2017)

Beim fünften Gespräch wurde der IT-Leiter eines Steuerberatungsunternehmens (in der weiteren Arbeit Person E genannt) befragt, der sich gerade im Kontext der Kundendaten des Unternehmens und der bevorstehenden Datenschutzgrundverordnung ebenfalls intensiv mit Informationssicherheit auseinandergesetzt hat.

Auch Person E sieht grundsätzlich positive Auswirkungen auf das Informationssicherheits-management bei Anwendung des vorgestellten Modells. Das Modell ist gut strukturiert und erfüllt den gewünschten Zweck. Im Modell fehlen allerdings noch die Feedbackschleifen zurück in die vorhergehenden Phasen. (Person E, persönliche Kommunikation, 29. November 2017)

Verbesserungsmöglichkeiten hat Person E vor allem in Phase 2 gesehen. Es sollte angegeben werden, welche Punkte mit den einzelnen Methoden genau erreicht werden sollen. Bei der Folgenabschätzung sollte auch unbedingt darauf geachtet werden, dass die Geschäftstätigkeit des Unternehmens nicht eingeschränkt wird. Damit die Folgenabschätzung im Modell funktionieren kann, müssen in der zweiten Phase im Rahmen der Ist-Analyse unbedingt die bereits vorhandenen Prozesse betrachtet werden. Zusätzlich wurde hervorgehoben, dass der Risikomanagementprozess nicht nur in der ersten Phase einen Input darstellt, sondern auf allen Ebenen des Modells wichtig ist. Auch für Person E ist die Nutzung des intern vorhandenen Wissens besonders wichtig, um die entstehenden oder geänderten Prozesse so effektiv und effizient wie möglich gestalten zu können. (Person E, persönliche Kommunikation, 29. November 2017)

Als kritisch für den Erfolg von ISMS-Richtlinien sieht Person E vor allem das Personal und die Zieldefinitionen. Daher wird auch Training beziehungsweise Awareness als zusätzliche Methode für das Modell vorgeschlagen. (Person E, persönliche Kommunikation, 29. November 2017)

Die nachfolgende Tabelle (Tabelle 3) zeigt die Zuordnung des Gesagten zu den vorab definierten Kategorien. Dadurch sollen Überschneidungen sichtbar gemacht werden, die dann gegebenenfalls zur Verbesserung des Modells herangezogen werden können.

	Nutzen	Aufbau und Verbesserung	Kryptographie	Sonstiges
A	• Unterstützung	• Evaluierung • Pilotierung der Richtlinie • Internes Wissen nutzen	• Angemessenheit • A-SIT-Empfehlung • Lebenszyklus der Algorithmen	• Faktor Mensch
B	• Gute Arbeitsbasis	• Risikomanagement • ISMS-Prozesse • Feedbackschleifen • Konkretisierung der Methoden	• Eine zentrale Richtlinie nicht zweckmäßig	• Schulung • Awareness • Kultur • Mission/Vision
C	• Unterstützung bei Einführung	• Feedbackschleifen • Externes Wissen in Phase 1	• Richtlinie wird aufgeteilt	• Zieldefinition • Kultur
D	• hilfreich	• Keine weiteren Phasen oder Methoden	• Analyse der Use-Cases wichtig • Abwägung von Komfort und Einschränkungen • Lebenszyklus der Algorithmen	• Schulung • Awareness
E	• Positive Auswirkung auf ISMS	• Feedbackschleifen • Konkretisierung der Methoden • Prozessanalyse in Phase 2 • Risikomanagement		• Zieldefinition • Schulung • Awareness

Tabelle 3: Auswertung der Interviews

Anhand der Auswertung wird deutlich, dass mehrere Änderungen am Modell vorgenommen werden sollten.

Alle befragten Fachleute sagten, dass das Modell einen grundsätzlichen Nutzen in verschiedenen Formen (Strukturierung, Unterstützung bei der Einführung und beim Betrieb des

ISMS) bietet. Allerdings sollten am Modell auf verschiedenen Ebenen Änderungen vorgenommen werden, um eine noch bessere Unterstützung bieten zu können.

Zum einen sollte das Modell in den umliegenden Kontext von Informationssicherheitsmanagement und Risikomanagement eingegliedert werden. Zum anderen wird deutlich, wie wichtig der Faktor Mensch in der Informationssicherheit ist – dies sollte auch im Modell stärker als bisher berücksichtigt werden. Außerdem sollten die Feedbackschleifen, wie sie bereits beschrieben wurden, auch in der Grafik dargestellt werden.

Die Informationen für die Gestaltung von kryptographischen Richtlinien werden an späterer Stelle in das Beispiel miteinfließen.

3.2.3 Verbesserung des Modells

Wie bereits angesprochen, wird das Modell aufgrund der Interviews in verschiedenen Bereichen angepasst. Die umfassendsten Änderungen betreffen die eingesetzten Methoden. Diese werden in der finalen Version des Modells näher beschrieben, um eine bessere Unterstützung beim Richtlinienentwurf bieten zu können und nicht noch weitere Fragen aufzuwerfen.

Das Modell wird im ersten Schritt mit den anderen genannten Einflussfaktoren ISMS und Risikomanagementprozess in Bezug gesetzt. Gerade das Risikomanagement hat Einfluss auf alle Phasen des aufgestellten Modells und sollte dementsprechend hervorgehoben werden. Auf der anderen Seite wird das ISMS abgebildet, welches ebenfalls Einflüsse auf die verschiedenen Richtlinien hat. Zusätzlich werden die Feedbackschleifen im Modell eingezeichnet.

In Phase 1 wird die Ist-Analyse um die erforderlichen Betrachtungsgegenstände erweitert. So sollen auf dieser Ebene explizit die Vision und Mission des Unternehmens abgefragt werden. Anhand von Vision und Mission kann das Ziel der Informationssicherheitsleitlinie herausgearbeitet werden. Einen weiteren Teil der Ist-Analyse stellt weiterhin die Sichtung von bereits vorhandenen Prozessen und Dokumenten in Bezug auf die Informationssicherheit dar. Dies erfolgt aus zwei Gründen: Zum einen soll dadurch ein Gefühl für die Unternehmenskultur entwickelt werden und zum anderen soll überprüft werden, ob man schon vorhandenes Wissen nutzen kann. Umwelt- und Stakeholderanalyse werden auf dieser Ebene zusammengefasst, da die beiden Methoden ohnehin sehr ähnlich sind. Als weiterer Input wird auch auf dieser Ebene externes Wissen abgefragt.

In der zweiten Phase wird weiterhin die Ist-Analyse durchgeführt. Dabei liegt der Fokus auf bereits vorhandenen Prozesse und der Erkennung von bereits vorhandenem internen Wissen. Ein weiteres Ergebnis dieser Analyse können nun die jeweiligen Anwendungsfälle sein, die durch die Informationssicherheitsanforderungen betroffen sind. Anhand dieser Anwendungsfälle ist es auch möglich, weitere Anspruchsgruppen identifizieren zu können. Hier ist nun deutlich eine Abhängigkeit der Methoden untereinander zu erkennen. Der Input *externes Wissen* wird um die ISO 27002, den Grundschutz des BSI sowie externe Berater ergänzt – hier können allerdings, je nach Bedarf, noch weitere Quellen hinzugezogen werden. Anhand der Themenrichtlinie kann bereits ein erster Schulungsbedarf festgestellt und entsprechendes Bewusstsein bei den Mitarbeitern geschaffen werden.

Innerhalb der dritten Phase gibt es keine gravierenden Änderungen an den verwendeten Methoden. Die Ist-Analyse auf dieser Ebene widmet sich besonders der vorhandenen Dokumentation und den gelebten Prozessen – ein Teil davon kann auch aus Phase 2 weiterverwendet werden. Anhand dieser Prozesse können die relevanten Stakeholder identifiziert und in den Entwicklungs- oder Änderungsprozess der Standards und Prozesse miteinbezogen werden. Diese Phase lässt sich nur durch einen starken Austausch mit den entsprechenden Verantwortlichen realisieren, da der Person, die für die Informationssicherheit zuständig ist, meistens das entsprechende Wissen fehlt. Der Begriff *externes Wissen* wird auch auf dieser Ebene konkretisiert. Gemeint sind an dieser Stelle Standards und Best Practices (wie zum Beispiel die OWASP Guidelines im Bereich der Webentwicklung), um Anhaltspunkte für funktionierende Prozesse zu erhalten.

Das Modell ist in der nachfolgenden Abbildung (Abbildung 9) und zusätzlich im Anhang A dieser Arbeit dargestellt.

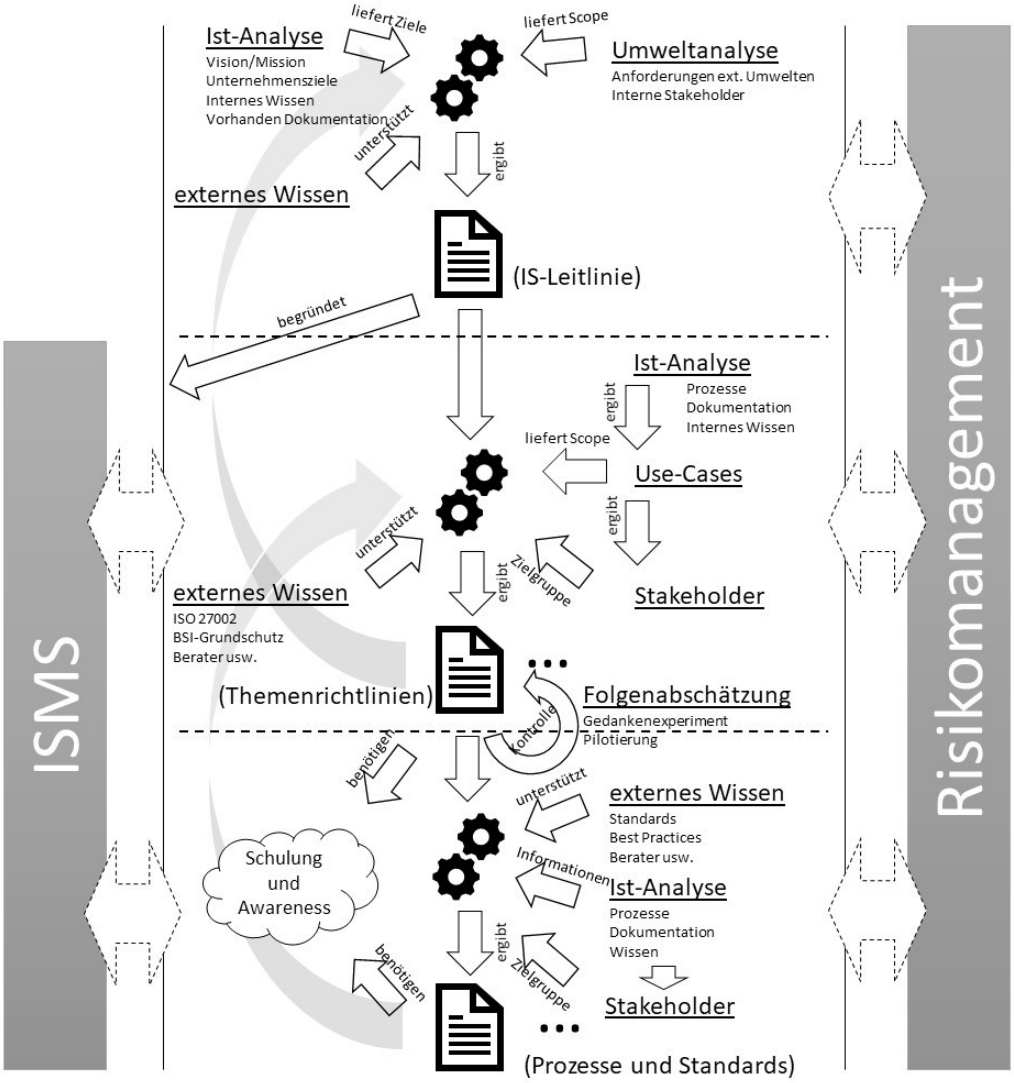

Abbildung 9: Finales Modell

3.3 Anwendung des Modells

In diesem Abschnitt wird die Anwendung des Vorgehensmodells beschrieben. Zu diesem Zweck werden die einzelnen Phasen im Rahmen der Erstellung einer kryptographischen Richtlinie durchlaufen und die Anwendung der einzelnen Methoden sowie deren Ergebnisse beschrieben. Der Fokus liegt dabei besonders auf der Richtlinienentwicklung – also auf der Erstellung einer Themenrichtlinie. Zum Abschluss des Kapitels werden die Grundzüge der Richtlinie kurz erläutert.

3.3.1 Strategische Betrachtung

Ausgehend vom aufgestellten Vorgehensmodell ist es die Aufgabe der ersten Phase, für die initiale Erstellung der Informationssicherheitsleitlinie zu sorgen oder eben diese Leitlinie zu überarbeiten und damit den kontinuierlichen Verbesserungsprozess einzuleiten. Im Rahmen dieser Arbeit wird davon ausgegangen, dass der Verbesserungsprozess bereits durchlaufen wurde. Der Grund dafür liegt darin, dass zum einen der komplette Durchlauf des Vorgehensmodells den Rahmen dieser Arbeit sprengen würde und zum anderen die Informationssicherheitsrichtlinie im Fallbeispiel schon vorhanden ist und eine gegebene Größe darstellt – eine Änderung im Rahmen des Fallbeispiels ist ausgeschlossen.

Dennoch sollen kurz die Rahmenbedingungen des Fallbeispiels anhand der einzelnen Methoden geschildert werden. Dies dient auch dazu, der nächsten Phase einen Kontext zu geben und nicht ohne nachvollziehbare Rahmenbedingungen in die Richtlinienentwicklung zu starten.

Im ersten Schritt sollen die Anspruchsgruppen, welche auf Ebene der Informationssicherheitsleitlinie existieren, analysiert werden. Ansprüche an das Informationssicherheitsmanagement der Landesverwaltung haben natürlich die Bürger, da die Landesverwaltung teilweise sogar sensible personenbezogene Daten verarbeitet. Aber es gibt noch weitere Anspruchsgruppen wie zum Beispiel die einzelnen Abteilungen der Landesverwaltung, andere Landesverwaltungen beziehungsweise Portalverbundteilnehmer und den Bund als Datenlieferant für gewisse Anwendungen. Nicht zuletzt hat auch die Landesregierung, in der Rolle des Auftraggebers, Ansprüche an das Informationssicherheitsmanagement. Die Vertragsbediensteten und Beamten haben gleich in mehrfacher Hinsicht Ansprüche an das Informationssicherheitsmanagement – sie sind darauf angewiesen, dass ihre persönlichen Daten adäquat geschützt sind und sind zeitgleich als Zielgruppe von der Informationssicherheitsrichtlinie betroffen.

Im nächsten Schritt, der Ist-Analyse, soll betrachtet werden, was bereits im Rahmen des Informationssicherheitsmanagements für Maßnahmen getroffen wurden. Zusätzlich sollen Vision und/oder Mission des zu betrachtenden Bereichs analysiert werden. Als Scope des zertifizierten ISMS ist die IT-Abteilung der steirischen Landesverwaltung definiert worden, der Wirkungsbereich erstreckt sich dennoch auf die gesamte Landesverwaltung. Die Mission dieser Abteilung sagt aus, dass sowohl Aufbau- als auch Ablauforganisation verbessert werden sollen, um den Nutzen der Kunden und Kundinnen zu steigern. Zusätzlich soll die Rolle als interner

Dienstleister für die anderen Abteilungen wahrgenommen werden. Diese Faktoren haben Einfluss auf die Ziele des betrachteten ISMS. Die IT-Abteilung der steirischen Landesverwaltung hat bereits ein funktionierendes und zertifiziertes ISMS mit entsprechenden Richtlinien und Prozessen. Wie bereits erwähnt, erstreckt sich der Wirkungsbereich des ISMS nur auf die IT-Abteilung, allerdings existieren dennoch Richtlinien, die sich auf alle Teile der Organisation erstrecken.

Im Bereich des Risikomanagements wird CRISAM angewendet, um besonders anfällige Bestandteile der Infrastruktur zu erkennen und somit den Stillstand von Business-Services zu vermeiden. Hier werden vor allem Risiken erfasst, die die Verfügbarkeit von Services betreffen. Abstraktere Risiken, wie zum Beispiel das aktive Ausschleusen von Daten oder andere Varianten des Datendiebstahls, werden hier ungenügend erfasst. Es sollte aber angestrebt werden, auch abseits der Toolunterstützung ein Gefühl für die aktuelle Risikosituation zu bekommen, gerade was nicht-technische Risiken angeht. Neben einer strukturierten und softwaregestützten Vorgehensweise mittels Tools wie zum Beispiel CRISAM sollten auch weiterhin eher unstrukturierte Methoden (wie das Brainstorming) genutzt werden, um eher versteckte Bedrohungen zu finden. Im Rahmen der strategischen Betrachtung sollen eher generelle Bedrohungen gefunden werden, um ein Gefühl für die aktuelle Bedrohungslage zu bekommen. Mit dem Fortschreiten im Vorgehensmodell werden diese Risiken gegebenenfalls wieder aufgegriffen und granularer analysiert. Zusätzlich werden ziemlich sicher weitere Risiken gefunden, die auf einem hohen Abstraktionslevel noch keine große Rolle spielen.

Anhand der gesammelten Informationen würde an dieser Stelle die Informationssicherheits-leitlinie entweder angepasst oder als noch zutreffend deklariert werden. Die Informationssicherheitsleitlinie stellt einen Input für die Richtlinienentwicklung dar.

3.3.2 Richtlinienentwicklung

Auf Basis der Informationssicherheitsleitlinie und den verschiedenen Kapiteln der ISO 27001 soll nun eine Richtlinie entwickelt oder überarbeitet werden. Im Fallbeispiel geht es konkret um eine neue Richtlinie, die Kapitel A.10 der ISO 27001 abdeckt und damit die Nutzung von kryptographischen Methoden sowie das dazugehörige Schlüsselmanagement regelt.

Der Grundstein für diese Phase wird durch die Ist-Analyse gelegt. Hier werden vorhandene Prozesse und Dokumentationen gesichtet sowie bereits vorhandenes Wissen abgefragt. Durch diese Vorgehensweise kann direkt auf betroffene Anwendungsfälle geschlossen werden.

In der Fallstudie gibt es Prozesse zur Ausstellung von Zertifikaten, zur Einrichtung von Webservices und diverse andere Tätigkeiten, bei denen kryptographische Verfahren erforderlich sind. Daraus ergeben sich verschiedene Anwendungsfälle. So wird bereits eine interne Public Key Infrastructure (PKI) verwendet, um Zertifikate für unterschiedliche Zwecke (beispielsweise Benutzerauthentifizierung oder Webserver-Zertifikate) auszustellen. Zusätzlich werden die meisten Webseiten und Webservices nur noch über Verbindungen angeboten, die mit Transport Layer Security (TLS) geschützt sind. Offensichtlich besteht hier bereits ein Schutzbedarf, der auch ohne eine spezielle Richtlinie erfüllt wird. Weitere Use-Cases sind zum

Beispiel die Authentifizierung von Benutzern, Virtual-Private-Network-Verbindungen sowie die Übertragung von Daten. Es muss an dieser Stelle darauf hingewiesen werden, dass bei dieser Betrachtung durchaus auch Anwendungsfälle übersehen werden können. Diese müssen dann in einer späteren Iteration in die Richtlinie integriert werden. Genau so kann es sein, dass Anwendungsfälle wegfallen oder ersetzt werden.

Anhand dieser Use-Cases können im nächsten Schritt gewisse Stakeholder identifiziert werden. So gibt es einen Verantwortlichen für die Verwaltung der PKI und verschiedene Teams, die regelmäßig Zertifikate für Webserver anfordern und nutzen. Weitere Stakeholder stellen die Mitglieder des Teams dar, welches für den Betrieb des Sterz-Portals[1] verantwortlich ist. Neben den bereits genannten sind auch die einzelnen Anwendungsverantwortlichen Stakeholder. Diese Gruppen und Personen sollten bereits bei der Entwicklung der Richtlinie miteinbezogen werden, da diese Erkenntnisse liefern können, die der sicherheitsverantwortlichen Person noch nicht bewusst sind.

Die vorhandenen Use-Cases müssen durch die neu zu entwickelnde Richtlinie abgedeckt werden. Einen weiteren Einflussfaktor stellen die bestehende ISO 27001-Zertifizierung und damit auch die Anforderungen der ISO 27002 dar. In Bezug auf die kryptographischen Methoden verlangt die ISO 27002 auch ein Schlüsselmanagement. Kersten et. al. (2016) schreiben, dass es zweckdienlich ist, beide Anforderungen – also die Verwendung von kryptographischen Verfahren und das Schlüsselmanagement – in einer Richtlinie zu behandeln.

An dieser Stelle wird die Richtlinie das erste Mal ausformuliert oder, falls sie bereits vorhanden ist, überarbeitet. Im Fallbeispiel wurde eine neue Richtlinie formuliert, die im folgenden Unterabschnitt im Detail vorgestellt wird. Hilfreich kann hier auch die Nutzung von externem Wissen sein, wie die Handlungsempfehlung in der ISO 27002. Durch die Charakteristik der kryptographischen Richtlinie, wie sie bereits im Grundlagenkapitel zur ISO 27002 erläutert wurde, werden innerhalb der Richtlinie keine genauen Prozesse oder technischen Details festgelegt, sondern nur ein grober Handlungsrahmen entworfen. Die technischen Details werden dann anhand der Richtlinie in der Dokumentation der jeweiligen Dienste niedergeschrieben. Die Richtlinie verweist auf diese Dokumente. Im Bereich des externen Wissens muss auch deutlich gemacht werden, dass für die öffentliche Verwaltung von Seiten des Gesetzgebers keine erhöhten Anforderungen gestellt werden. Es muss allerdings bedacht werden, dass im Regelfall personenbezogene Daten verarbeitet werden und diese gemäß DSG 2000 geschützt werden müssen.

Aufbauend auf dem ersten Entwurf der Richtlinie wird eine Folgenabschätzung vorgenommen. Im betrachteten Fallbeispiel spielt zum Beispiel die PKI eine zentrale Rolle und es muss bedacht werden, was bei einem Ausfall dieser Einrichtung für Folgen auftreten. Im konkreten Fall ist ein Ausfall von unter sieben Tagen verkraftbar. Bei einem Ausfall, der darüber hinaus geht, werden für interne Services erste Fehler angezeigt. Ein Handlungsspielraum von sieben Tagen spielt in der Praxis keine große Rolle und kann daher in Kauf genommen werden. Im

[1] Das Sterz-Portal stellt eine Plattform zur Rechte- und Rollenvergabe dar und bietet überdies auch Zugang zum Portalverbund.

Fallbeispiel spielt die Folgenabschätzung noch keine große Rolle, da im ersten Durchlauf erst der Ist-Stand erhoben wird und noch keine gravierenden Änderungen an bestehenden Diensten und Prozessen vorgenommen werden.

Der abschließende Teil dieser Phase befasst sich mit einem Blick in die Zukunft. Eine Weiterentwicklungsmöglichkeit stellt zum Beispiel die Verschlüsselung des Mailverkehrs dar. Zusätzlich könnte das Schlüsselmanagement für bestimmte Bereiche teilautomatisiert werden. Diese Sammlung an Möglichkeiten stellt im ersten Ansatz tatsächlich nur eine lose Sammlung dar, die eventuell bereits Vor- und Nachteile enthalten – entsprechende Machbarkeitsstudien werden allerdings separat vorgenommen. In diesem Schritt geht es einzig darum, Entwicklungspotenziale aufzuzeigen und in Zukunft nutzbar zu machen.

3.3.3 Fallbeispiel

Dieser Abschnitt beinhaltet den letzten Entwurf der Richtlinie. Beschrieben werden dabei die notwendigen und zusätzlich hinzugefügten Bestandteile einer Themenrichtlinie. Das tatsächliche Dokument enthält eine entsprechende Gliederung sowie ein Änderungsverzeichnis. Aus Gründen der Lesbarkeit sind diese Teile in diesem Abschnitt nicht vorhanden.

Die Richtlinie beginnt mit dem Formulieren des Ziels und der Relevanz der Richtlinie. Ziel der Richtlinie ist es, die Vertraulichkeit, Integrität und Authentizität von Informationen der Steiermärkischen Landesverwaltung sowie die Authentizität von Benutzern zu gewährleisten.

Im nächsten Schritt wird, wie auch in der Informationssicherheitsleitlinie, der Geltungsbereich definiert. Der Geltungsbereich ist der gleiche wie bei der übergeordneten Informationssicherheitsleitlinie und deckt damit die gesamte Landesverwaltung ab. Daten müssen dort verschlüsselt werden, wo davon ausgegangen werden kann, dass sie entweder über öffentliche Verkehrswege übertragen werden (Mail, FTP oder sonstige Datentransfers) oder aber durch physischen Zugriff ausgelesen werden können (Wechseldatenträger, Festplatten und Ähnliches). Grundsätzlich richtet sich der Einsatz von Verschlüsselung nach der Schutzklasse der betroffenen Informationen – das bedeutet, dass öffentliche Daten nicht verschlüsselt werden müssen.

Der nächste Abschnitt der Richtlinie befasst sich mit den definierten Anwendungsfällen. Diese Anwendungsfälle sind nachfolgend kurz beschrieben. Für alle Anwendungsfälle gilt, dass keine schwachen oder bekanntermaßen unsicheren Verschlüsselungsalgorithmen genutzt werden dürfen. Eine genauere Spezifikation der genutzten Algorithmen ist in den jeweiligen Standards zu den Anwendungsfällen hinterlegt.

Sowohl interne als auch externe Webseiten sowie Webservices müssen mittels TLS gesichert werden. Für interne Dienste steht zu diesem Zweck die interne PKI zur Verfügung, für externe Dienste muss ein Zertifikat bei der entsprechenden Zertifizierungsstelle angefordert werden.

Ein weiterer Anwendungsfall ist das Erlangen einer höheren Sicherheitsstufe für den Zugriff auf Applikationen innerhalb des Portalverbundes. Zu diesem Zweck bekommen Benutzer entweder ein Zertifikat auf ihrem Dienstausweis oder auf dem entsprechenden Computer installiert. Diese

Zertifikate werden von der internen PKI ausgestellt und vom aufgerufenen Portal überprüft. Somit wird eine Mehrfaktorauthentifizierung gewährleistet.

Der externe Zugriff auf das Landesdatennetz (VPN, Citrix, Webmail oder XenMobile) darf ausschließlich über gesicherte Verbindungen erfolgen. Es obliegt den jeweiligen Produktverantwortlichen für die entsprechenden Maßnahmen zu sorgen.

Der Austausch von sensiblen Daten mit externen Kommunikationspartnern darf ausschließlich über entsprechend gesicherte Wege erfolgen. Gegebenenfalls sind diese Daten auch durch den zentralen Zustelladapter zu signieren. Zusätzlich sind auch externe Datenträger vor der Weitergabe an externe Parteien zu verschlüsseln.

Die Festspeicher von mobilen Geräten (Notebooks, Tablets, Mobiltelefone) sind mittels BitLocker oder adäquater Maßnahmen zu verschlüsseln. Seitens der IT-Abteilung ist sicherzustellen, dass entsprechende Maßnahmen zur Schlüsselverwaltung (beispielsweise über das Active Directory) getroffen werden, um den Zugriff auf die Daten im Notfall gewährleisten zu können.

Das Schlüsselmanagement erfolgt grundsätzlich über die interne PKI und die damit verbundenen Prozesse. Sollte ein System den Einsatz von Zertifikaten nicht unterstützen, ist es auch möglich, andere Maßnahmen zur Schlüsselverwaltung zu nutzen. Diese Abweichungen müssen in der entsprechenden Dokumentation vermerkt werden.

Im Fall von Abweichungen von dieser Richtlinie müssen diese dokumentiert und schnellstmöglich korrigiert werden. Falls eine Korrektur der Abweichung nicht möglich ist, muss dieser Sonderfall dem Security Board zur Kenntnis gebracht und vom selbigen genehmigt werden.

Durch die Richtlinie kann mit Einschränkungen bei der Kommunikation mit alten und/oder nicht gewarteten Computern gerechnet werden. Aufgrund der mit einer Abschwächung der kryptographischen Verfahren verbundenen Sicherheitseinbußen werden diese Einschränkungen in Kauf genommen.

Mögliche weitere Anwendungsfelder für Verschlüsselung stellen sowohl die Verschlüsselung von Dateifreigaben als auch die Verschlüsselung von Datenbanken dar. In beiden Fällen ist allerdings noch eine entsprechende Evaluierung hinsichtlich der Umsetzbarkeit erforderlich. Eine Weiterentwicklungsmöglichkeit stellt die Teilautomatisierung des Schlüsselmanagements dar. Dies ist allerdings erst mit Windows Server 2016 effizient möglich.

Damit ist die Richtlinie im jetzigen Entwurf vollständig. Das Modell sieht vor, dass nun abhängig von den jeweiligen Use-Cases die Detailentwürfe mit Standards und Prozessen vorgesehen werden. Im nächsten Abschnitt werden exemplarisch Standards und Prozesse für das Schlüsselmanagement beziehungsweise den Betrieb der internen PKI aufgezeigt.

3.3.4 Prozess- und Standardentwicklung

In diesem Abschnitt wird der Detailentwurf für zwei Dienste innerhalb der Abteilung umrissen. Die betrachteten Fälle sind zum einen das grundsätzliche Schlüsselmanagement und zum

anderen der Betrieb von Webservern. Im Gegensatz zu den anderen Phasen ist das Ergebnis dieser Phase nicht nur ein einzelnes Dokument, sondern eher eine Sammlung von Detailabläufen und Beschreibungen. Wie die anderen Phasen auch, beginnt diese Phase mit der Ist-Analyse der bestehenden Gegebenheiten, anschließend werden gängige Standards analysiert und Prozesse erfasst und/oder definiert. Auf den Detailentwurf wird an dieser Stelle nur in einer gekürzten Version eingegangen.

Bei einem kompletten Durchlauf des Vorgehensmodells würden nun die verschiedenen Use-Cases durchgegangen werden. Bei einfachen Szenarien müssten dafür keine extra Dokumente angelegt werden. Die entsprechenden Vorschriften können direkt in der Themenrichtlinie erfasst werden.

Im Rahmen des Fallbeispiels existiert bereits ein Schlüsselmanagement in Form einer internen PKI. Dieses System basiert auf einer Windows-Server-Umgebung und ist mehrstufig aufgebaut. Es existieren bereits Prozesse, die allerdings nur oberflächlich dokumentiert sind. Wie bereits geschildert, sind mehrere Use-Cases mit der internen PKI verknüpft (Server- und Benutzerzertifikate).

Nach der Ist-Analyse werden interne Standards für den Betrieb der PKI definiert. Diese Standards umfassen im Fallbeispiel unter anderem die Laufzeiten für Zertifikate, den Umgang mit mehreren Hostnamen, die Laufzeit der Zertifikatsperrlisten und die eingesetzten Algorithmen. So wurden beispielsweise die verfügbaren Templates angepasst, damit die Zertifikathashwerte nur noch auf SHA-256 basieren.

Des Weiteren existieren, wie bereits angedeutet, mehrere Prozesse für die Beantragung und die Ausfolgung von digitalen Zertifikaten. An dieser Stelle wird kurz der Prozess für das Ausstellen von Webserver-Zertifikaten beschrieben. Wenn ein neues Webservice in Betrieb genommen wird oder ein bestehendes Zertifikat abläuft, wird vom produktverantwortlichen Referat ein Ticket mit den gewünschten Attributen oder dem Certificate Signing Request eröffnet. Anhand dieser Daten wird eine Anfrage an die interne PKI gestellt. Diese Anfrage wird von der Person, die für die PKI verantwortlich ist, überprüft und – vorbehaltlich der Richtigkeit der Daten – genehmigt. Nach der Genehmigung wird das Zertifikat mit einem Passwort versehen und ausgefolgt. Zertifikat und Passwort werden getrennt voneinander übermittelt.

Der zweite Anwendungsfall ist die Verwendung von Zertifikaten zur Absicherung der Client-Server-Kommunikation im Webserver-Umfeld. Das A-SIT hat zu diesem Zweck bereits umfassende Empfehlungen[2] herausgegeben. In der Dokumentation zum Webserverbetrieb lassen sich diese Anforderungen als Merkmal für den Betrieb von Webservern abbilden.

Damit wurde das Vorgehensmodell einmal komplett durchlaufen und eine Themenrichtlinie im Detail beschrieben. Der nächste Abschnitt fast das Kapitel zusammen.

[2] https://demo.a-sit.at/sicherheitsempfehlungen-fuer-behoerden/

3.4 Zusammenfassung

In diesem Kapitel wurden zuerst Meinungen aus der Literatur zur Richtlinienerstellung im Rahmen des Informationssicherheitsmanagements analysiert. Darauf aufbauend wurde ein erstes Vorgehensmodell erstellt, welches dann mit Hilfe von Interviews mit Fachleuten aus dem Bereich der Informationssicherheit verbessert wurde. Anhand des verbesserten Vorgehensmodells wurde ein Fallbeispiel vorgestellt und mit Hilfe des Vorgehensmodells eine Themenrichtlinie entwickelt.

Bei der Literaturanalyse ist deutlich geworden, dass neben den Inhalten, die von der ISO 27001 gefordert werden, auch weitere Faktoren bei der Erstellung von Richtlinien im Informationssicherheitsmanagement eine wichtige Rolle spielen. Zu diesen Faktoren gehört beispielsweise die Anpassung der Richtlinie an das Unternehmen und die betroffene Zielgruppe sowie ihre Umsetzbarkeit. Außerdem sollte eine Richtlinie verständlich formuliert sein, da diese in der Regel nicht vom Verfasser, sondern von anderen Beteiligten umgesetzt werden muss. Aus diesem Umstand ergibt sich auch, dass Kommunikation ein wichtiger Faktor ist.

Zusätzlich ist aufgefallen, dass eine hierarchische Beziehung zwischen den einzelnen Richtlinienarten vorhanden ist. Dies ergibt sich zwar bereits aus den Anforderungen der ISO 27001, allerdings wurde die Unterteilung der Richtlinien granularer gewählt, als es die ISO 27001 verlangt. Dadurch ergibt sich eine Unterteilung der Richtlinien in Informationssicherheitsleitlinie, Themenrichtlinien und Systemrichtlinien. Auf gleicher Ebene mit den Systemrichtlinien stehen zusätzlich noch interne Standards und Prozesse.

Richtlinien sind über alle drei Ebenen ähnlich aufgebaut. Auf jeder Ebene muss das Ziel einer Richtlinie erklärt und die Relevanz des Themas dargelegt werden. Zusätzlich ist auch der Gültigkeitsbereich enthalten – von diesem leiten sich auch die entsprechenden Stakeholder einer Richtlinie ab. Außerdem müssen innerhalb der Richtlinie Verantwortlichkeiten definiert werden.

Anhand der Informationen aus der Literatur wurde nun ein Vorgehensmodell für die Entwicklung von Informationssicherheitsrichtlinien entwickelt. Das Modell ist in drei Phasen unterteilt, wobei jede Phase den Detaillierungsgrad ein wenig erhöht. In der ersten Phase wird besonders die Informationssicherheitsleitlinie betrachtet, von der sich auch die Themenrichtlinien ableiten lassen. Diese Themenrichtlinien werden in der zweiten Phase des Vorgehensmodells spezifiziert. Anhand der Anwendungsfälle der Themenrichtlinien werden im Bedarfsfall in einer dritten Phase noch systemspezifische Richtlinien, Standards und Prozesse entworfen.

Durch das systematische Vorgehen wird gewährleistet, dass die verschiedenen Richtlinien aufeinander und auf das Unternehmen zugeschnitten sind. In jeder Phase wird überprüft, welche Richtlinien und sonstige Gegebenheiten bereits vorhanden sind – diese Informationen fließen in die Erstellung oder Überarbeitung der Richtlinie mit ein. Ebenso essentiell ist die Risikobetrachtung. Im Rahmen des Vorgehensmodells wurden den Richtlinien auch noch weitere Aspekte hinzugefügt. So sollten in den Richtlinien sowohl eine Folgenabschätzung als auch Weiterentwicklungsmöglichkeiten für weitere Iterationen angeführt werden.

Dieses Vorgehensmodell hat die Basis für die folgenden Interviews geliefert. Ziel dieser Interviews war es, vor allem den Nutzen eines strukturierten Vorgehens zu ermitteln und Verbesserungspotenziale am Modell identifizieren zu können. Daher wurden die Interviews so aufgebaut, dass bereits vor dem Interview das Modell grundsätzlich erklärt wurde und dann nach dem Nutzen, nach Verbesserungsmöglichkeiten und dem konkreten Anwendungsfall (der Richtlinie für kryptographische Verfahren) gefragt wurde.

Die Interviews haben verschiedene Erkenntnisse gebracht. Auf der einen Seite konnte das Modell durch den Beitrag der Fachleute verbessert werden. Die genauen Verbesserungen sind in Abschnitt 3.2.3 dieser Arbeit dargelegt. Auf der anderen Seite wurden Erfolgskriterien für die Informationssicherheit identifiziert.

Es macht den Anschein, dass Informationssicherheit nur geschaffen werden kann, wenn allen Ebenen in der Organisation klar ist, welcher Zweck dadurch verfolgt wird und warum gewisse Einschränkungen notwendig sind. Ohne entsprechendes Bewusstsein auf der Führungs- **und** Sachbearbeiterebene wird langfristig kein erfolgreiches ISMS etabliert werden können. Dieser Punkt lässt sich auch im Vorgehensmodell durch die intensive Betrachtung und Einbeziehung der Anspruchsgruppen wiederfinden.

Zum Abschluss des Kapitels wurde das entwickelte Vorgehensmodell anhand eines Fallbeispiels bei der Steiermärkischen Landesverwaltung angewendet. Dabei wurde der Fokus vor allem auf die Erstellung einer Themenrichtlinie für die Verwendung von kryptographischen Verfahren gelegt.

Damit ist dieses Kapitel abgeschlossen. Im nachfolgenden Kapitel wird die Arbeit kurz zusammengefasst und die Ergebnisse werden diskutiert. Abschließend erfolgt ein Ausblick auf weitere Forschungs- und Weiterentwicklungsmöglichkeiten.

4 ABSCHLUSS DER ARBEIT

Dieses Kapitel befasst sich mit dem Abschluss der Arbeit. Dazu erfolgt zuerst ein Rückblick auf die Ergebnisse dieser Arbeit. Anschließend werden diese Ergebnisse zur Beantwortung der Forschungsfrage herangezogen und diskutiert. Zum Abschluss erfolgt ein Ausblick auf weitere Forschungs- und Entwicklungsmöglichkeiten.

4.1 Rückblick

Zu Beginn dieses Kapitels werden kurz die wesentlichen Erkenntnisse und Ergebnisse dieser Arbeit zusammengefasst.

Im Kapitel Grundlagen wurde zuerst betrachtet, welche Rolle die Informationssicherheit im Bereich der IT-Governance spielt. Es ist deutlich geworden, dass für die erfolgreiche Abstimmung der IT auf die Organisationsziele auch die Informationssicherheit eine wesentliche Rolle spielt. So ist ein strukturiertes Vorgehen, wie es durch die ISO 27001 oder vergleichbare Managementsysteme vorgegeben wird, für den Schutz der Informationswerte einer Organisation unabdingbar.

Im nächsten Schritt wurde der grundsätzliche Aufbau eines Informationssicherheitsmanagementsystems anhand der ISO 27001 erläutert. Die wesentlichen Ziele eines ISMS sind die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen innerhalb einer Organisation. Grundsätzlich unterliegt ein ISMS einem kontinuierlichen Verbesserungsprozess, der es ermöglicht, zeitnah auf geänderte Rahmenbedingungen zu reagieren. Einflussgrößen auf das Managementsystem sind der Kontext des Unternehmens, die Führung, die Planung, die Unterstützung, der Betrieb und das Controlling (des ISMS). Bereits hier ist aufgefallen, dass Kommunikation und Unterstützung der Geschäftsführung tragende Elemente dieses Managementsystems sind, obwohl diese per se nichts mit der Informationssicherheit zu tun haben. Ebenfalls ist aufgefallen, dass die Anforderungen und Ziele eines ISMS so unterschiedlich wie die verschiedenen Unternehmen selbst sind, da die ISO 27001 eine hohe Anpassung an das jeweilige Unternehmen verlangt.

Neben dem Managementsystem an sich existieren auch noch die Vorgaben aus dem Anhang der ISO 27001 beziehungsweise der ISO 27002. Diese Vorgaben stellen die eigentlichen Wirkungsziele des ISMS dar und geben die wesentlichen Betrachtungsgegenstände vor. Einige dieser Domänen sind die Zugriffskontrolle, die Kryptographie oder die Sicherheit im Personalmanagement. Auffällig ist, dass einige dieser Bereiche mit anderen Bereichen wechselseitige Beziehungen eingehen und andere Bereiche auch komplett isoliert betrachtet werden können. Dieser Fakt wird Auswirkungen auf die Beantwortung der Forschungsfrage haben, aber dazu mehr im folgenden Abschnitt.

Im nächsten Teil der Arbeit wurden der Grundschutz des BSI und das österreichische Informationssicherheitshandbuch als weitere Managementsysteme beziehungsweise Vertiefung der ISO 27001 vorgestellt. Das österreichische Informationssicherheitshandbuch stellt hier eher einen Implementierungsleitfaden als einen eigenständigen Standard dar. Der Grundschutz des BSI wurde ursprünglich ebenfalls auf Basis der ISO 27001 entwickelt, ist nun aber ein eigenständiger Standard, der auch zertifiziert werden kann. Den Unternehmen im deutschsprachigen Raum ist hier mehr oder weniger die freie Wahl gelassen, allerdings muss beachtet werden, dass Kunden einen bestimmten Standard vorschreiben können.

Abschließend wurde der Nutzen eines ISMS für ein Unternehmen vorgestellt. Am schwersten wiegt das Argument, dass moderne Informationssystem immer komplexer werden und es eines strukturierten Vorgehens bedarf, um in diesem Umfeld eine hohe Informationssicherheit gewährleisten zu können. Zusätzlich kann ein ISMS die Bedingung für die Erschließung bestimmter Märkte darstellen und/oder von Kunden gefordert werden.

Im nächsten Abschnitt wurden die Grundlagen der Kryptographie dargelegt und argumentiert, warum kryptographische Verfahren für das gewährleisten von Informationssicherheit essentiell sind. Die wesentlichen Ziele der Kryptographie sind Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit. Darauf, wie diese Ziele erreicht werden, wird an dieser Stelle nicht näher eingegangen. Anhand der Ziele der Kryptographie wird bereits eine große Überschneidung mit den Zielen eines ISMS deutlich. Natürlich können diese Ziele im Rahmen eines ISMS auch durch organisatorische Maßnahmen erreicht werden. Diese organisatorischen Maßnahmen können allerdings ohne Weiteres umgangen werden oder erschweren bestimmte Abläufe im Unternehmen. Der angemessene Einsatz von kryptographischen Verfahren kann an dieser Stelle eine Prozessverbesserung nach sich ziehen.

Der letzte Abschnitt des Grundlagenkapitels stellte eine Analyse der gesetzlichen Vorgaben und deren Auswirkungen auf die öffentliche Verwaltung dar. In diesem Abschnitt wurden besonders das E-Government-Gesetz, das Signatur- und Vertrauensdienstegesetz, das Datenschutzgesetz und die Datenschutzgrundverordnung betrachtet. Dabei ist deutlich geworden, dass für die öffentliche Verwaltung prinzipiell keine höheren Anforderungen bestehen als für private Organisationen. Es muss allerdings bedacht werden, dass im Bereich der öffentlichen Verwaltung sehr oft Daten mit erhöhtem Schutzbedarf (personenbezogene und sensible Daten) verarbeitet werden und dementsprechende Maßnahmen getroffen werden müssen. Ebenso hat sich gezeigt, dass den Anforderungen und Dokumentationspflichten im Datenschutzgesetz nur durch ein strukturiertes Vorgehen nachgekommen werden kann.

Das nächste Kapitel hat die Entwicklung einer Informationssicherheitsrichtlinie behandelt. Aufgrund dessen, dass es noch kein allgemeingültiges Vorgehensmodell für die Richtlinienentwicklung gegeben hat, wurde dazu im ersten Schritt ein Vorgehensmodell entwickelt. In die Entwicklung sind in einem ersten Ansatz sowohl Erfahrungen des Autors als auch Erkenntnisse aus der Literatur eingeflossen. Die größten Erkenntnisse aus diesem Arbeitsschritt sind zum einen das mehrstufige Vorgehen, um von einer strategischen Ebene bis zu den einzelnen Geschäftsprozessen vordringen zu können, sowie der große Einfluss des Faktors Mensch auf die Informationssicherheit.

Anhand dieser Erkenntnisse wurde ein erstes Vorgehensmodell entwickelt, um den Anforderungen an die Informationssicherheitsrichtlinien gerecht zu werden. Das Vorgehensmodell unterteilt sich in die drei Phasen *strategische Betrachtung*, *Richtlinien-entwicklung* und *Prozess- und Standardentwicklung*.

Dieses Modell wurde im nächsten Schritt fünf Fachleuten aus dem Bereich der Informationssicherheit vorgelegt und die befragten Personen wurden zum Nutzen dieses Modells, Verbesserungsmöglichkeiten und dem Anwendungsfall der kryptographischen Richtlinie befragt. Das Ergebnis dieser Befragung war, dass das strukturierte Vorgehen, wie es durch das Modell erreicht wird, einen großen Nutzen für die Informationssicherheit einer Organisation hat. Anhand der Interviews wurde das Vorgehensmodell optimiert. So wurde besonders der menschliche Aspekt noch weiter in den Vordergrund gerückt sowie Anpassungen und Konkretisierungen bei der Methodenauswahl vorgenommen.

Das optimierte Vorgehensmodell wurde zum Abschluss des Kapitels im Rahmen einer Fallstudie zur Anwendung gebracht. In der Fallstudie wurde eine Richtlinie für die Verwendung kryptographischer Verfahren beim Amt der Steiermärkischen Landesregierung entwickelt. Das Ergebnis dieses Arbeitsschrittes war die Erkenntnis, dass bei der Entwicklung des Vorgehensmodells für dieses besondere Szenario keine besonderen Faktoren übersehen wurden. Als Nebenprodukt wurde auch eine, der ISO 27001 entsprechende, Richtlinie für die Anwendung kryptographischer Verfahren entwickelt.

Anhand dieser Erkenntnisse wird im nächsten Abschnitt die Forschungsfrage dieser Arbeit beantwortet.

4.2 Fazit und Diskussion

In diesem Abschnitt wird die Forschungsfrage „Welchen Beitrag zum Informationssicherheits-management leistet die Einführung einer allgemeinen Vorgabe für die Anwendung kryptographischer Standards im Umfeld der öffentlichen Verwaltung?“ beantwortet.

Zur Beantwortung der Frage wird zuerst überprüft, welche der beiden Hypothesen dieser Arbeit zutrifft. Die beiden Hypothesen lauten:

H_1: Durch die Einführung einer allgemeinen Vorgabe für die Anwendung kryptographischer Standards wird die Effizienz des IT-Sicherheitsmanagements in der Verwaltung gesteigert.

H_0: Die Einführung einer allgemeinen Vorgabe für die Anwendung kryptographischer Standards hat keinen Einfluss auf das IT-Sicherheitsmanagement.

Anhand der Informationen aus der Literatur und den Meinungen der Fachleute kann davon ausgegangen werden, dass H_1 verworfen werden und H_0 angenommen werden muss. Für eine definitive Entscheidung ist die befragte Testgruppe allerdings zu klein.

Durch die Vielzahl an unterschiedlichen Anforderungen, die für die unterschiedlichen Organisationen bestehen, macht eine generische oder allgemeine Richtlinie nur wenig Sinn und erreicht nicht den Anpassungsgrad an die Organisation, der für eine Erfüllung der jeweiligen

Informationssicherheitsziele erforderlich wäre. Auch wenn Organisationen betrachtet werden, die ähnlicher Art sind (wie zum Beispiel verschiedene Landesverwaltungen), kann nicht davon ausgegangen werden, dass diese Organisationen automatisch ähnliche Anforderungen an die kryptographischen Maßnahmen haben.

Damit lässt sich auch die Forschungsfrage dieser Arbeit beantworten. Es wird durch eine generische Vorgabe kein Beitrag zum Informationssicherheitsmanagement geleistet.

Vielmehr wurde durch die Fachleute das strukturierte Vorgehen anhand des entwickelten Vorgehensmodells als positiv hervorgehoben. Organisationen haben in jedem Reifegrad des Managementsystems die Möglichkeit strukturiert zu überprüfen, ob die eigenen Richtlinien noch den Anforderungen der Organisation genügen. Zudem bietet sich das Modell auch an, wenn noch gar kein ISMS in einer Organisation vorhanden ist.

Das entwickelte Modell versucht besonders den Faktor Mensch mit in die Richtlinienentwicklung auf den verschiedenen Ebenen zu berücksichtigen. So ist von der obersten Ebene der Informationssicherheitsrichtlinie bis zu den einzelnen Prozessen eine starke Einbeziehung der betroffenen Personen vorgesehen. Dadurch sollen zum einen Widerstände minimiert und zum anderen die Nutzung von bereits vorhandenen Informationen maximiert werden. Das Vorgehensmodell ist erneut im Anhang A dargestellt.

Die Erkenntnisse aus der Literaturrecherche und den Interviews zeigen wie Wichtig der Mensch für den Erfolg von Informationssicherheitsrichtlinien ist. Es ist notwendig, dass internes Wissen (zum Beispiel in Bezug auf die Prozesse des Unternehmens) bei der Erstellung von Richtlinien genutzt wird und dass den Mitarbeitern bewusst ist, warum bestimmte Vorgaben getroffen wurden. Es sollte darauf geachtet werden, dass für eine hohe Akzeptanz innerhalb der Belegschaft gesorgt wird, da sonst mit hoher Wahrscheinlichkeit die Richtlinien nicht beachtet oder umgangen werden.

Die entwickelte Richtlinie erfüllt bereits in der ersten Iteration ihren Zweck. Es ist allerdings davon auszugehen, dass in weiteren Revisionen Änderungen an den Anwendungsfällen vorgenommen werden müssen. Die betrachtete Richtlinie zur Verwendung von kryptographischen Verfahren stellt zudem noch einen Sonderfall dar: die einzelnen Verfahren zeigen sich in unterschiedlichsten Business-Cases, was die Abhandlung der einzelnen Vorgaben verkomplizieren kann. Eine Dokumentation aller Geschäftsvorgänge, bei den kryptographische Verfahren eingesetzt werden, in einem Dokument wird nicht zweckdienlich sein. Zwar befinden sich die Informationen gesammelt an einem Ort und sind daher leicht auffindbar, allerdings müsste die Richtlinie dann im weiteren Verlauf (aufgrund von Schwächen in den verwendeten Algorithmen oder geänderten Anforderungen) in regelmäßigen Abständen aktualisiert und genehmigt werden.

4.3 Ausblick

Zum Abschluss dieser Arbeit wird noch ein Ausblick über weitere und/oder vertiefende Forschungsmöglichkeiten auf Basis der Ergebnisse dieser Arbeit gegeben.

Ausgehend von dieser Arbeit sollte in einem ersten Ansatz überprüft werden, ob das Vorgehensmodell auch einem breiteren Anforderungsrahmen standhält und für weitere Branchen nutzbar ist.

Ein wichtiges Ziel weiterer Forschungen könnte auch die Rolle der Benutzerakzeptanz im Bereich der Informationssicherheit spielen und wie man diese bestmöglich erreichen kann. Es finden sich zwar viele Indizien in der Literatur und auch die Fachleute sind sich einig, dass die Akzeptanz der Belegschaft wichtig für den Erfolg von Informationssicherheit ist, allerdings finden sich keine Informationen über den konkreten Einfluss der Benutzerakzeptanz.

ANHANG A - Modell zur Richtlinienentwicklung

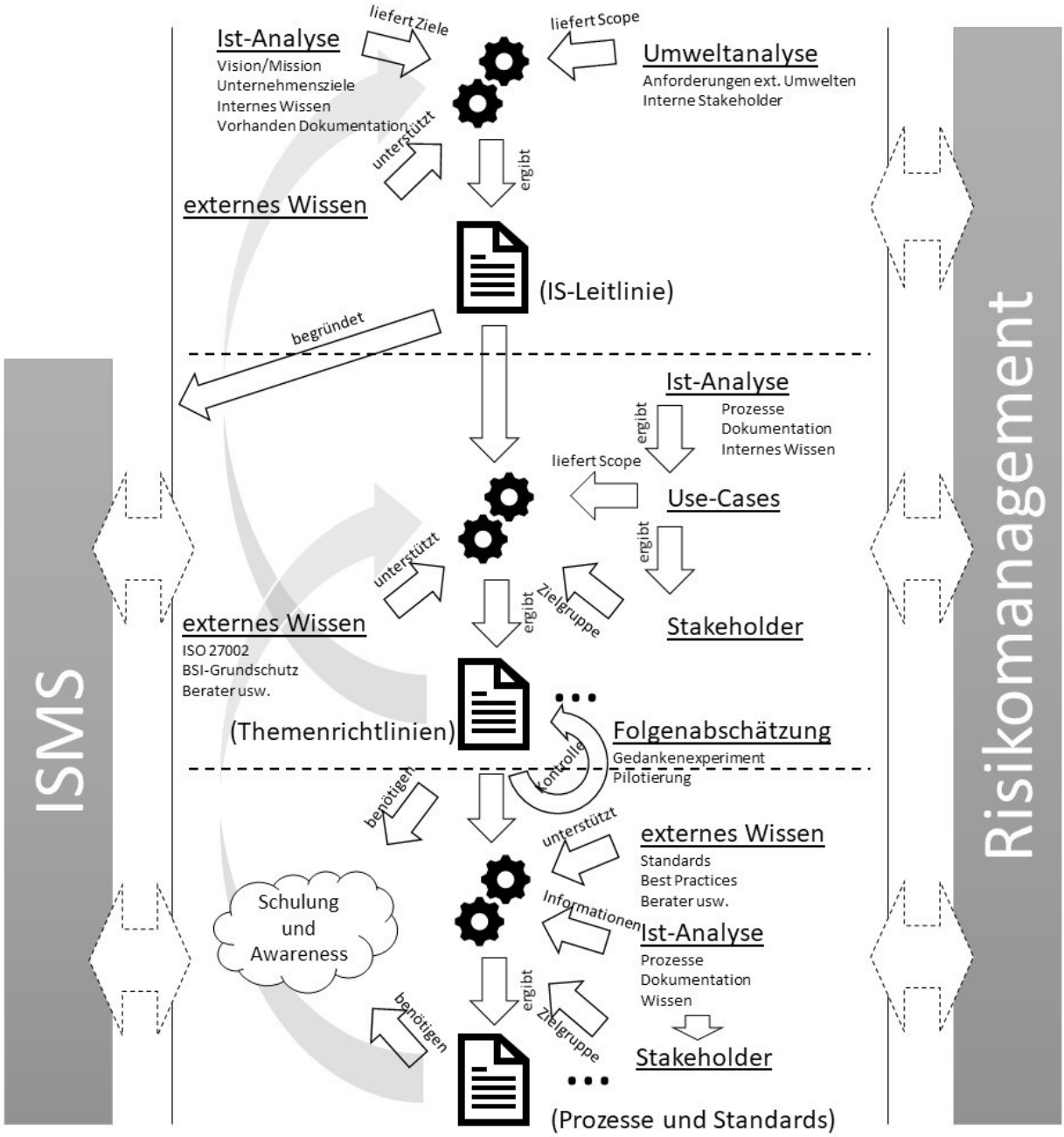

Abbildung 10: Vorgehensmodell für die Richtlinienerstellung

ABKÜRZUNGSVERZEICHNIS

3DES ..... *Triple Data Encryption Standard*
AES ..... *Advanced Encryption Standard*
BSI ..... *Bundesamt für Sicherheit in der Informationstechnik*
DH ..... *Diffie Hellman*
DSG 2000 ..... *Datenschutzgesetz 2000*
DSGVO ..... Datenschutz-Grundverordnung
eIDAS-VO *Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG*
ISMS ..... *Information Security Management System*
NIST ..... *National Institute of Standards and Technology*
PDCA-Zyklus ..... *Plan-Do-Check-Act-Zyklus*
RSA ..... *Rivest-Shamir-Adelman*
SVG ..... *Signatur- und Vertrauensdienstegesetz*
TLS ..... *Transport Layer Security*

ABBILDUNGSVERZEICHNIS

Abbildung 1: Aufbau der Arbeit 3
Abbildung 2: Spannungsfeld der IT-Governance (Rüter, Schröder, Göldner, & Niebuhr, 2010) 6
Abbildung 3: Aufbau der ISO-27000-Familie (ISO/IEC 27000:2016, 2016) 8
Abbildung 4: PDCA-Zyklus der ISO 27001:2005 (ISO/IEC 27001:2005-10, 2005) 9
Abbildung 5: Risikomanagementprozess der ISO 27005 (ISO/IEC 27005:2011, 2011) 15
Abbildung 6: Aufbau der ISO 27001:2013 24
Abbildung 7: Richtlinienstruktur 47
Abbildung 8: Erstes Vorgehensmodell für die Erstellung von ISMS-Richtlinien 52
Abbildung 9: Finales Modell 61
Abbildung 10: Vorgehensmodell für die Richtlinienerstellung i

TABELLENVERZEICHNIS

Tabelle 1: Standards im Bereich der IT-Governance 7
Tabelle 2: Inhalt der ISO 27002 (ISO/IEC 27002:2013, 2013) 25
Tabelle 3: Auswertung der Interviews 59

LITERATURVERZEICHNIS

Anderl, A., & Tlapak, N. (5. September 2017). Vorbereitung auf die DSGVO europaweit in den Kinderschuhen. *Datenschutz Konkret*, S. 82.

A-SIT. (2016). *Österreichisches Informationssicherheitshandbuch.*

Beutelspacher, A., Schwenk, J., & Wolfenstetter, K.-D. (2015). *Moderne Verfahren der Kryptographie.* Wiesbaden: Springer Fachmedien.

Bogner, A., Littig, B., & Menz, W. (2014). *Interviews mit Experten.* Wiesbaden: Springer Fachmedien.

Bundesamt für Sicherheit in der Informationstechnik. (2017). *BSI-Standard 200-1.* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000). (1999). *BGBl. I Nr. 165/1999 idF BGBl. I Nr. 120/2017*.

Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (SVG). (2016). *BGBl. I Nr. 50/2016*.

Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-GovG). (2004). *BGBl. I Nr. 10/2004 idF BGBl. I Nr. 121/2017*.

Carlson, T. (2008). Understanding Information Security Management Systems. In H. Tipton, & M. Krause, *Information Security Management Handbook* (S. 15-25). Boca Raton: Auerbach Publications.

Digitales Österreich. (2016). Abgerufen am 31. Oktober 2017 von Was ist E-Government: https://www.digitales.oesterreich.gv.at/was-ist-e-government-

Fröhlich, M., & Glasner, K. (2007). *IT Governance.* Wiesbaden: Gabler Verlag.

Gläser, J., & Laudel, G. (2009). *Experteninterviews und qualitative Inhaltsanalyse.* Wiesbaden: Springer Science+Business Media.

ISO/IEC 27000:2016. (2016). *Information technology - Security techniques - Information security management systems - Overview and vocabulary*.

ISO/IEC 27001:2005-10. (2005). *Information technology - Security techniques - Information security management systems - Requirements*.

ISO/IEC 27001:2013-10. (2013). *Information technology - Security techniques - Information security management systems - Requirements*.

ISO/IEC 27002:2013. (2013). *Information technology - Security techniques - Code of practice for information security controls*.

ISO/IEC 27005:2011. (2011). *Information technology - Security techniques - Information security risk management*.

Kersten, H., Klett, G., Reuter, J., & Schröder, K.-W. (2016). *IT-Sicherheitsmanagement nach der neuen ISO 27001.* Wiesbaden: Springer Fachmedien.

Kersten, H., Reuter, J., & Schröder, K.-W. (2008). *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz.* Wiesbaden: Friedr.Vieweg & Sohn Verlag.

Kilches, R. (01. Juli 1999). Datenschutzgesetz 2000 - Selbstbestimmter Datenschutz. *Medien und Recht*, S. 261.

Klipper, S. (2011). *Information Security Risk Management.* Wiesbaden: Vieweg+Teubner Verlag.

Knyrim, R., & Tretzmüller, T. (14. Juni 2017). DSG neu - Durchführungsgesetz zur DSGVO im Entwurf veröffentlicht. *Datenschutz konkret*, S. 52.

Kompakt-Lexikon Wirtschaftsinformatik. (2013). Wiesbaden: Springer Fachmediena.

OECD. (2004). *OECD-Grundsätze der Corporate Governance.* OECD.

Peltier, T. R. (2002). *Information Security Policies, Procedures, and Standards.* Boca Raton: CRC Press LLC.

Pollirer, H.-J. (1. April 2016). Checkliste - Datensicherheitsmaßnahmen gem § 14 DSG 2000 (Teil I). *Datenschutz Konkret*, S. 40.

Purser, S. (2004). *A Practical Guide to Managing Information Security.* Norwood: Artech House, Inc.

Roßnagel, A. (2017). *Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung.* Wiesbaden: Springer Vieweg.

Rüter, A., Schröder, J., Göldner, A., & Niebuhr, J. (2010). *IT-Governance in der Praxis.* Berlin: Springer-Verlag.

Schwenk, J. (2014). *Sicherheit und Kryptographie im Internet.* Wiesbaden: Springer Fachmedien.

Souhrada-Kirchmayer, E. (1. November 2000). DAS DATENSCHUTZGESETZ 2000. *Soziale Sicherheit*, S. 938.

Spitz, S., Pramateftakis, M., & Swoboda, J. (2011). *Kryptographie und IT-Sicherheit.* Wiesbaden: Vieweg + Teubner Verlag.

Williams, P. A. (2005). *Optimising Value Creation From IT Investments.* Rolling Meadows: IT Governance Institute.