Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

Umsetzungs-Studie ISMS

Evaluation und Einführung einer Software-Lösung zum Aufbau eines ISMS mit Betrachtung der Umsetzung von Maßnahmen ausgewählter Komponenten am Beispiel der Firma dotSource GmbH

Abschlussarbeit zur Erlangung des Grades eines

Master of Engineering (M.Eng.)

der Hochschule Wismar

eingereicht von:	Richard Spillner
	geboren am DD.MM.YYYY in ORT
	Studiengang Master IT-Sicherheit und Forensik
Matrikelnummer:	
Erstgutachterin:	Prof. Dr. Ing. Antje Raab-Düsterhöft
Zweitgutachter:	Prof. Dr. Ing. habil. Andreas Ahrens

Für die Veröffentlichung ohne Sperrvermerk gekürzte Version.

Jena, der 20. November 2022

Aufgabenstellung

Das Ziel der Master-Thesis ist die Erarbeitung und kritische Betrachtung eines idealen ISMS nach persönlicher Vorstellung und die Bewertung dessen anhand einer praktischen Realisierung.
Dabei wird das ideale ISMS im ersten Teil mit mindestens einer standardisierten Variante verglichen und kontrastiert. Anschließend wird eine geeignete Software für das ISMS evaluiert. Die verschiedenen Lösungsansätze werden beleuchtet und miteinander verglichen, um eine geeignete Lösung zu bestimmen. Mittels der ausgewählten Softwarelösung wird das ISMS für das Unternehmen aufgebaut und weitestgehend umgesetzt. Abschließend werden die Umsetzungen von Maßnahmen für ausgewählte Systeme genauer beleuchtet und deren Realisierung dargestellt werden.
Der Mehrwert der Master-Thesis liegt in der Kritik etablierter Standards zum Aufbau und Betreiben eines ISMS und den ausgearbeiteten Verbesserungsvorschlägen.

Danksagung

Ich möchte an dieser Stelle die Gelegenheit nutzen, um mich bei allen zu Bedanken, die mich im generellen oder auch im spezifischen unterstützt haben.
Mein Dank gilt der Firma. Nachdem ich mit dem Wunsch des Fernstudiums zum Master auf diese zugegangen bin, wurde ohne weitere Hindernisse ein Plan ausgearbeitet, wie sie mich bei diesem Wunsch unterstützen kann. Ich möchte mich auch bei meinem Teamleiter und meinen Kolleg:innen, insbesondere der internen IT, bedanken, dass sie mich in den schweren Zeiten motiviert, an mich geglaubt, mir den Rücken freigehalten haben und stets ein offenes Ohr hatten.
Weiterhin gilt mein Dank der Hochschule, die es in der schweren Zeit der Corona-Pandemie geschafft hat, mir ein angenehmes und nachhaltiges Masterstudium zu bieten. Insbesondere möchte ich Frau Schissler und Frau Nedel für ihre schier grenzenlose Geduld und Energie danken. Gleichsam bedanke ich mich bei meiner Gutachterin und meinem Gutachter für die Zeit und Betreuung meiner Masterarbeit. Insbesondere Frau Raab-Düsterhöft möchte ich für ihre beeindruckend konstruktive Form der Kritik danken. Zusätzlich möchte ich meinen Kommiliton:innen, insbesondere den Mitgliedern der Arbeitsgruppe BER05, für die bereichernden und nachhallenden Gespräche danke.
Zuletzt möchte ich mich bei meinen Freunden und meiner Familie bedanken, die in der letzten Zeit auf mich verzichten mussten und dies verständnisvoll und wohlwollend angenommen haben. Über dies möchte ich mich besonders bei meiner Freundin Lydia bedanken. Sie hat mich stets motiviert, bot mir die Möglichkeit meine Gedanken auf gerade Linie zu bringen und gab mir den Raum, um meine Energie auf die Masterarbeit zu fokussieren.

Vorwort

Die vorliegende Master-Thesis enthielt in der eingereichten Form sicherheitskritische Informationen und musste daher für die Veröffentlichung ohne Sperrvermerk gekürzt werden. Die gekürzten Inhalte werden in der Arbeit mit „[..]“ angezeigt.

Kurzfassung

Deutscher Titel:

Umsetzungsstudie ISMS
Evaluation und Einführung einer Software-Lösung zum Aufbau eines ISMS mit Betrachtung der Umsetzung von Maßnahmen ausgewählter Komponenten am Beispiel der Firma dotSource GmbH

Die Informationssicherheit gewinnt in Unternehmen immer mehr Raum und wird in der Regel durch die Einführung und das Betreiben eines ISMS gesichert und nachgewiesen. Zusätzlich achten Firmen vermehrt darauf, dass auch die Zuliefernden den eigenen Anforderungen an Informationssicherheit nachkommen und diese auch nachweisen. Das ISMS wird dabei auf Basis von Standards, wie der ISO / IEC 27001, und Richtlinien, wie der VdS 10000 aufgebaut. Dabei stellt sich die Frage, ob diese Ausarbeitungen Verbesserungsmöglichkeiten bieten.
Das Ziel der Master-Thesis ist es daher ein konzeptionell überarbeitetes ISMS zu erstellen und kritisch zu betrachten, wobei die etablierten Normen als Ausgangsbasis detailliert betrachtet, genutzt und mit Verbesserungsvorschlägen angereichert werden. Anschließend wird das überarbeitete ISMS in einer Praxisumsetzung geprüft. Für die Umsetzung werden verschieden Softwarelösungen betrachtet, wobei drei Lösungsansätze ausgearbeitet werden. Der ausgewählte Ansatz wird für die Praxisrealisierung genutzt. Abschließend wird das überarbeitete ISMS und der ausgewählte Lösungsansatz einer kritischen Nachbetrachtung unterzogen.
Im Ergebnis liefert die Arbeit eine Kritik an den etablierten Normen, das überarbeitete ISMS, eine Praxisumsetzung des ISMS mittels Atlassian Jira und Confluence und einen ersten reflektierten Umsetzungsbericht.

Abstract

Title in English:

ISMS implementation study
Evaluation and introduction of a software solution for the establishment of an ISMS with consideration of the implementation of measures of selected components using the example of dotSource GmbH

Information security is becoming more and more important in companies and is usually ensured and proven by the introduction and operation of an ISMS. In addition, companies are increasingly ensuring that their suppliers also meet their own information security requirements and provide evidence accordingly. The ISMS is based on standards such as ISO / IEC 27001 and guidelines such as VdS 10000. The question arises whether these elaborations offer possibilities for improvement.
The goal of this master thesis is therefore to create and critically examine a conceptual revised ISMS, whereby the established standards are considered in detail as a starting point, used and enriched with suggestions for improvement. Subsequently, the revised ISMS is tested in a practical implementation. For the implementation three different approaches are considered. The selected approach is used for the practical implementation. Finally, the revised ISMS and the selected solution approach are critically reviewed.
As a result, the paper provides a critique of the established standards, the revised ISMS, a practice implementation of the ISMS using Atlassian Jira and Confluence, and an initial reflective implementation report.

Inhaltsverzeichnis

1 Einleitung

„Nur was sich ändert, bleibt bestehen.“[1]

In kleinen bis mittelständischen Unternehmen wird oft die Meinung vertreten, dass diese durch Angriffe auf ihre IT-Infrastruktur nicht gefährdet seien. Viel mehr ginge es den Angreifenden darum große Unternehmen ins Visier zu nehmen und dort für Schaden zu sorgen. Die Realität zeigt jedoch ein anderes Bild. Cyberangriffe auf Kleine und mittelständische Unternehmen (KMU) nehmen immer mehr zu, eben weil hier die Sicherheitsvorkehrungen geringer sind[2]. Dies stellt wiederum für größere Unternehmen ein beachtliches Risiko dar. Sichern diese sich intern weitestgehend ab, stellt ein KMU als Zulieferer ein mögliches Einfallstor für Angreifende dar. Daher bestehen immer mehr Großunternehmen auf den Nachweis von praktizierter IT-Sicherheit im Partnerfirmen. Geht ein Unternehmen dieser Forderung bspw. durch die Umsetzung eines Informationssicherheitsmanagementsystem (ISMS) nach, führt diese Änderung im betroffenen Unternehmen nicht nur zu Wettbewerbsvorteilen, sondern sorgt gleichzeitig für eine Verbesserung der IT-Sicherheit im eigenen Betrieb.

1.1 Motivation

In vielen Bereichen der Wirtschaft und der Industrie ist das ISMS[3] ein essentieller Bestandteil der Infrastruktur. Es ermöglicht die qualifizierte Bewertung der Informationssicherheit im betrachteten System. Bei einigen Unternehmen, so zum Beispiel im Automobil-Sektor, ist die Teilnahme an Ausschreibungen, bzw. der Vertragsabschluss für Projekte ohne Nachweis der Betreibung eines ISMS nur noch schwer zu realisieren. In diesem Bereich hat sich beispielsweise „TISAX“[4] durchgesetzt. In diesem Portal können Unternehmen in unterschiedlichen Leveln eine Selbstauskunft zur Informationssicherheit im Unternehmen geben und diese extern bewerten lassen. Das Ergebnis dieser sogenannten „Scopes“ kann mit

[1] Quelle: von einer Hauswand in Jena
[2] Vgl. Kus22.
[3] BSI17a.
[4] ENXoJ, URL: https://www.enx.com/en-US/TISAX/.

anderen Teilnehmenden geteilt werden und dient damit potentiellen Vertragspartner:innen zur Einschätzung der Informationssicherheit des jeweils anderen. Doch um diese Auskunft geben zu können, steht jedes Unternehmen zunächst vor der Herausforderung ein ISMS aufzubauen und dieses auch nachhaltig zu betreiben. Gleichsam stehen in diesem Zusammenhang auch die Umsetzung der Maßnahmen für die einzelnen Systeme im Raum.
Doch was ist unter dem abstrakten Begriff „ISMS“ und unter der realen Umsetzung zu verstehen? Dazu gibt es verschiedene Standards, wie zum Beispiel die BSI 200-1[5] oder die ISO 27001[6], die eine Hilfestellung bieten bzw. standardisierte Beschreibungen vorlegen. Jedoch können diese Ausführungen nicht in jedem Unternehmen gleich umgesetzt werden, da zum einen die Unternehmen unterschiedlich sind und zum anderen, weil jedes Unternehmen eine eigene Vorstellung von einem ISMS hat. Oft kommt es daher zu einer angepassten Umsetzung eines ISMS.

1.2 Ausgangssituation und Problemstellung

Wie einleitend beschrieben, ergibt sich die Ausgangssituation, dass unterschiedliche Realisierungen von ISMS im Umlauf sind, obwohl doch eine standardisierte Form gegeben ist. Somit stellt sich die Frage, ob die Standards an der Praxis vorbei arbeiten und eine Verbesserung dieser im Raum steht. Genau dieser Frage wird in der vorliegenden Arbeit nachgegangen. Als Fallbeispiel für die Untersuchung wird die Digital-Agentur dotSource GmbH[7] genutzt.
Wie bereits im ersten Kapitel beschrieben, ist ein Bewusstsein für Informationssicherheit in der Wirtschaft und in der Industrie angekommen. Dem entsprechend fordern vermehrt potentielle Vertragspartner:innen eine Auskunft zur Informationssicherheit im Unternehmen, um so auch das eigene Risiko beim Abschluss des Vertrages einschätzen zu können. Dabei haben sich die Zertifizierungen, wie zum Beispiel die Zertifizierung nach ISO 27001[8], durchgesetzt. Da diese aber oft zeit- und kostenintensiv sind und die Anforderungen bestimmter Bereiche nicht abdecken, haben sich abseits dessen Portale etabliert, bei denen eine gezielte Selbstauskunft hinterlegt werden kann. Diese kann dann von Vertragspartner:innen eingesehen oder bei Lieferantenaudits und zur Risiko-Analyse und -Bewertung genutzt werden. Die digital Agentur dotSource GmbH strebt an, Kund:innen im Sektor Automobil-Industrie zu bedienen. Dabei wird von den Betreibenden eine

[5] BSI17a.
[6] ISOoJa.
[7] URL: https://www.dotsource.de/
[8] TÜVoJ.

Auskunft Level 2 im TISAX-Portal gefordert. Um diese vorweisen zu können, muss das Unternehmen ein ISMS einführen und betreiben. Abseits dessen ist die Firma dotSource GmbH mittlerweile auf eine Größe angewachsen, bei der das Betreiben eines ISMS für die qualifizierte Einschätzung und Verbesserung der Informationssicherheit im Unternehmen notwendig geworden ist. Darüber hinaus können somit auch weitere potentielle Kunden aus anderen Bereichen angesprochen oder es kann an deren Ausschreibungen teilgenommen werden.

1.3 Zielstellung

Das Ziel dieser Master-Thesis ist die Erarbeitung und kritische Betrachtung eines konzeptionell überarbeiteten Informationssicherheitsmanagementsystem (ISMS) nach persönlicher Vorstellung und die Bewertung dessen anhand einer praktischen Realisierung.
Das überarbeitete ISMS baut auf den zwei Standards ISO / IEC 27001 und BSI Standard 200-1 und der Richtlinie VDS 10000 auf und wird durch Verbesserungsvorschläge ergänzt. Anschließend wird eine geeignete Software für das ISMS evaluiert. Die verschiedenen Lösungsansätze werden beleuchtet und miteinander verglichen, um einen geeigneten Weg zu bestimmen. Mittels der ausgewählten Software wird das überarbeitete ISMS für das Unternehmen aufgebaut und weitestgehend umgesetzt. Abschließend werden die Umsetzungen von Maßnahmen für ausgewählte Systeme genauer beleuchtet und deren Realisierung dargestellt.
Der Mehrwert der Master-Thesis liegt in der Kritik etablierter Standards zum Aufbau und Betreiben eines ISMS und den ausgearbeiteten Verbesserungsvorschlägen.

1.4 Vorgehensweise

Die vorliegende Arbeit ist in fünf Kapitel eingeteilt, deren Überschriften durch Einleitung, theoretische Aufarbeitung, Konzeption, Umsetzung und Fazit beschrieben werden können.
Im 1. Teil „Einleitung“ wurde nach einer Einführung die Motivation und die Zielstellung in der Arbeit dargelegt und anschließend wird hier die Vorgehensweise beschrieben.
Das 2. Kapitel „Grundlagen und theoretische Aufarbeitung ISMS“ legt den Grundstein für das Verständnis der Thematik. Es werden die grundlegenden Begrifflichkeiten erläutert, verbreitete Standards und Richtlinien dargelegt und es findet eine Einarbeitung in das Thema statt.

Unter dem Titel „Vorstellung des konzeptionell überarbeiteten ISMS“ wird im Kapitel 3 das überarbeitete ISMS vorgestellt, eingeführt und beschrieben. Dabei erfolgt zunächst eine Ausführung der Gemeinsamkeiten der Standards und Richtlinien aus Kapitel 2. Anschließend wird das konzeptionell überarbeitete ISMS beschrieben, indem der Aufbau und die Phasen des ISMS dargelegt werden. Darauffolgend werden die Anforderung der Firma dotSource GmbH und die bereits vorhandene Vorarbeit aufgeführt. Das Kapitel schließt mit der Evaluation einer geeigneten Softwarelösung für das vorgestellte ISMS ab, wobei verschiedene existierende Softwarelösungen verglichen und getestet werden.
Das 4. Kapitel „Einführung des überarbeiteten ISMS mittels Atlassian Jira und Confluence“ nimmt sich der Realisierung des ISMS an. Das ausgewählte System wird in die Produktivumgebung überführt und für den Aufbau des vorgestellten ISMS genutzt. Anschließend wird die Umsetzung der Maßnahmen für ausgewählte Komponenten in den Fokus gestellt und beschrieben. Am Ende des Kapitels wird die Umsetzung reflektiert. Dabei wird konstruktive Kritik am konzipierten ISMS und am ausgewählten Lösungsansatz vorgenommen.
Das letzte Kapitel (5) „Auswertung und Ausblick“ fasst die Arbeit zusammen und zieht ein Fazit. Das Kapitel endet mit dem Ausblick.

2 Grundlagen und theoretische Aufarbeitung ISMS

Im folgenden Kapitel werden die Grundlagen für das Verständnis der Arbeit gelegt und es findet eine theoretische Aufarbeitung des Begriffes ISMS statt. Im ersten Teil werden die Grundbegriffe erklärte und im zweiten Teil des Kapitels werden die gängigen Standards detailliert betrachtet.

2.1 Grundbegriffe

In diesem Teil sollen für das Verständnis der Thematik grundlegende Begriffe kurz erklärt werden, sodass eine einheitliche Basis für die Arbeit gelegt wird.

2.1.1 Informationssicherheit

Informationssicherheit (IS)[1] hat nach Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel „[..], Informationen jeglicher Art und Herkunft zu schützen“[2]. Dabei umfasst die Begrifflichkeit sowohl die verarbeitenden Systeme, als auch die informationstragenden Elemente. Davon abzugrenzen ist die IT-Sicherheit, die sich nur mit den informationsverarbeitenden Systeme beschäftigt. Laut BSI wird der klassische IT-Sicherheitsbegriff in der Moderne durch den Begriff Cyber-Sicherheit ersetzt:„Das Aktionsfeld der klassischen IT-Sicherheit wird unter dem Begriff „Cyber-Sicherheit“ auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein“[3].

2.1.2 Informationssicherheitsmanagementsystem

Das BSI beschreibt das ISMS als die „Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur

[1] Der Begriff „Informationssicherheit“ wird im weiteren Verlauf mit „IS“ abgekürzt.
[2] BSI17a, S. 8.
[3] Ebd., S. 8.

Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen“[4].Luber und Schmitz ergänzen die Definition des BSI um den Aspekt der Optimierung, bzw. kontinuierlichen Verbesserung und führen den Top-Down-Ansatz des Konzeptes an:„Innerhalb des ISMS sind Regeln, Verfahren, Maßnahmen und Tools definiert, mit denen sich die Informationssicherheit steuern, kontrollieren, sicherstellen und optimieren lässt. Durch die IT verursachte Risiken [für die Informationen der Organisation oder des Unternehmens] sollen identifizierbar und beherrschbar werden. Da das Information Security Management System[5] in den Verantwortungsbereich der Unternehmensführung fällt, nutzt es einen Top-Down-Ansatz zur Durchsetzung der IT-Sicherheit.“[6]. Im Grunde ist das ISMS ein Werkzeug, dass es ermöglicht die Sicherheit von Informationen und Werten innerhalb eines betrachteten Systems zu bewerten und durch die Umsetzung von Maßnahmen kontinuierlich zu verbessern. Dabei werden zunächst die relevanten Informationen und Werte definiert, wie auch der Anwendungsbereich und die Grenzen festgelegt[7]. Die identifizierten Assets sind bestimmten Risiken ausgesetzt, die weiter beleuchtet werden müssen. Dabei geht es darum, eine Übersicht zu erarbeiten, welche Folgen von Risiken vertretbar sind und welche durch Maßnahmen vermindert werden müssen. Die Einordnung der Risiken erfolgt in der Regel durch gesetzliche Anforderungen, Richtlinien[8] oder auch durch die Geschäftsführung. „Es muss klar erkennbar sein, welche Auswirkungen durch die einzelnen Risiken entstehen können. Die Folgen, die durch den Verlust von Vertraulichkeit, Integrität und Verfügbarkeit eintreten, sind dabei zu berücksichtigen. Ebenfalls Teil der Risikobewertung sind die Eintrittswahrscheinlichkeiten der Risiken.“[9] Nachdem diese Risikobewertung stattgefunden hat und die Übersichten erstellt wurden, können nun zielgerichtet Maßnahmen angewendet werden, die die Informationssicherheit des Systems verbessern und damit eine Risikoreduzierung bewirken. Der beschriebene Prozess wird regelmäßig wiederholt, sodass die Maßnahmen kontinuierlich überprüft und verbessert werden können und auch neue Risiken berücksichtigt werden.[10]

[4] BSIoJb.
[5] englische Bezeichnung des ISMS
[6] LS17b.
[7] Vgl. ebd.
[8] Vgl. ebd.
[9] Ebd.
[10] Vgl. ebd.

2.2 Standards

Das Thema ISMS ist in einigen Bereichen bereits zum Hauptbestandteil des Betriebsalltags geworden. Um eine Vergleichbarkeit der IT-Sicherheit zu gewährleisten, wurden daher Standards etabliert, in denen die Anforderungen und der Aufbau eines ISMS festgelegt sind. Diese Standards zeichnen sich durch eine hohe Akzeptanz, bzw. Verbreitung aus und deren erfolgreiche Umsetzung kann durch eine Zertifizierung belegt werden. Zudem ermöglichen sie die Vergleichbarkeit der Qualität der IT-Sicherheit eines Unternehmens mit anderen Unternehmen. Drei dieser Standards werden im Folgenden näher beleuchtet.

2.2.1 Allgemeine Gegenüberstellung

Bevor nachfolgend die einzelnen Standards und die Norm dargelegt werden, erfolgt zuvor ein genereller Vergleich. Die Informationen aus der Tabelle „Vergleich der Standards / Richtlinien“ aus dem Anhang A.3 werden durch weitere allgemeine Merkmale ergänzt und sollen einen ersten Eindruck vermitteln.
Die älteste und wohl bekannteste Formulierung stellt die **ISO / IEC 27001** dar. Sie wird international genutzt und existiert bereits seit 2013. Die Norm wird alle fünf Jahre einem Review unterzogen und im Jahr 2022 aktualisiert publiziert. Die Norm für sich genommen ist für Fachpersonal ausgelegt und bietet eine hohe Einstiegshürde. Dadurch ist auch der Aufwand zur Umsetzung im Vergleich zu den anderen beiden Dokumenten hoch. Dennoch gibt es unterstützende Dokumente, die bei der Umsetzung hilfreich sind. Die Norm und die ergänzenden Dokumente müssen kostenpflichtig erworben werden.
Der **BSI Standard 200-2** existiert seit 2017 und wird europaweit, insbesondere in Deutschland, genutzt. Er ist durch seine ausführlichen Erläuterungen einstiegsfreundlich gehalten und bietet durch die drei Absicherungsmodelle einen flexiblen ausbaufähigen Lösungsweg an, dessen Resultat teilweise zertifizierbar ist. Der Standard wird ergänzt durch weitere ausführliche Standards und Begleitdokumente. Alle Veröffentlichungen werden vom BSI kostenfrei zur Verfügung gestellt.
Die jüngste Publikation ist die **VdS 10000**. 2018 veröffentlicht, steht sie den Anwender:innen kostenpflichtig zur Verfügung. Die Umsetzung der Norm ist im Vergleich zu den anderen beiden Publikationen aufwandsarm. Dennoch werden für diese Einsparung bestimmte Kernelemente, wie das differenzierte Betrachten des Schutzbedarfs von IT-Systemen, mangelhaft bedient, was zu einer Reduzierung der IT-Sicherheit beitragen könnte. Abseits dessen hat die VdS branchenspezifische Publikationen veröffentlicht, die bei der Umsetzung der VdS 10000

in den jeweiligen Bereichen unterstützt. Dies ist insbesondere dann von Vorteil, wenn kleine Betriebe IT-Sicherheit etablieren wollen aber zu wenig Ressourcen für die Beschäftigung von Fachpersonal haben. Die Umsetzung eines ISMS nach VdS 10000 ist durch ein VdS-spezifisches Zertifikat belegbar.

2.2.2 ISO 27001

Die ISO 27001 ist die wohl bekannteste Norm im Bezug auf ISMS. Die ursprüngliche von International Organization for Standardization (ISO) verabschiedete Variante vom Oktober 2013 kann unter [ISO13] bezogen werden. Es wurden seitdem zwei Korrekturen vorgenommen, die unter [DIN14] und [DIN15] erworben werden können. Für die vorliegende Arbeit wurde die aktuelle Variante in der deutschen Übersetzung verwendet, die die DIN unter [DIN17a] im Beuth Verlag zum Kauf anbietet. Die Norm besteht aus der ursprünglichen Variante inklusive der Korrekturen von 2014 und 2015. Darüber hinaus sei angemerkt, dass bereits eine Neufassung der Norm in der Entwicklung ist, die unter dem Namen „ISO/IEC FDIS 27001“ publiziert und auf [ISOoJb] angeboten werden wird.

Ergänzende Dokumente

Da die ISO/IEC 27001 generisch die Anforderungen an ein ISMS beschreibt, wurden weiterführende Normen publiziert, die die Umsetzung erleichtern, vertiefende Informationen bieten oder auch ganze Methodiken abbilden. Die Tabelle 2.1 zeigt diese Normen im Überblick. Nachfolgend wird jedoch ausschließlich die ISO 27001 näher beleuchtet.

Norm	**Titel / Schwerpunkt**
ISO/IEC 27000	Überblick und Terminologie
ISO/IEC 27001	Anforderungen
ISO/IEC 27002	Informationssicherheitsmaßnahmen
ISO/IEC 27003	Anleitung
ISO/IEC 27004	Überwachung, Messung, Analyse und Evaluation
ISO/IEC 27005	Informationssicherheits-Risikomanagement

Tabelle 2.1: ISO/IEC 2700X Normen

Inhalt und Aufbau der Norm

Die ISO 27001 legt auf aktuell 35 Seiten die Anforderungen für den Aufbau, der Einführung, der Instandhaltung und der kontinuierlichen Verbesserung eines

ISMS fest. Dabei ist die Norm so ausgelegt, dass sie „auf alle Organisationen, ungeachtet ihrer Art und Größe“[11] angewendet werden kann. Die Norm ist in zehn Kapitel aufgeteilt.

Kapitel 0 bis 3 Nachdem die Einleitung formuliert, der Anwendungsbereich des Standards definiert und die Handhabung der normativen Verweise beschrieben wurden, verweist die Norm bei der Definition von Begriffen auf die „ISO/IEC 27000“[12]. In dieser sind das Vokabular und die Terminologien, die im Zusammenhang mit ISMS stehen festgelegt.

Kapitel 4 Kontext der Organisation Das vierte Kapitel widmet sich der Definition des Kontextes der Organisation. Dabei geht es darum, ein Verständnis für die relevanten Informationen einer Organisation zu erarbeiten. Ergänzt wird das Bild durch gesetzliche und rechtliche Anforderungen, sowie interne wie auch externe Schnittstellen zwischen Tätigkeiten. Diese Informationen werden genutzt, um den Anwendungsbereich des ISMS zu definieren[13].

Kapitel 5 Führung Das fünfte Kapitel definiert die Aufgaben und Verantwortung der Leitung der Organisation. Dabei werden zunächst die Verpflichtungen aufgelistet, wie bspw. die Sicherstellung, dass „die Anforderungen des Informationssicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden“[14] oder, dass „die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen“[15]. Die Norm gibt weiterhin vor, dass die Geschäftsführung die Informationssicherheit als politisches Ziel mit aufnimmt und somit sicherstellt, dass bspw. die kontinuierliche Verbesserung des ISMS verpflichtend angestrebt und umgesetzt wird. Diese geformte Informationssicherheitspolitik muss dann dokumentiert und zugänglich gemacht werden. Abschließend werden in diesem Kapitel die Rollen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation festgelegt, sodass die Rollen definiert, zugewiesen und veröffentlicht werden[16].

Kapitel 6 Planung Das sechste Kapitel thematisiert zunächst Risiken und Chancen. Im Allgemeinen wird hierbei gefordert, dass die Themen und Anforderungen von weiter oben berücksichtigt und das ISMS funktional umgesetzt und

[11] DIN17a.
[12] Einsehbar unter DIN20.
[13] Vgl. DIN17a, S. 7.
[14] Ebd., S. 7.
[15] Ebd., S. 7.
[16] Vgl. ebd., S. 8.

kontinuierlich verbessert wird. Darüber hinaus soll eine Organisation Maßnahmen zum Umgang mit Risiken und Chancen planen, im Betriebsalltag integrieren und deren Wirksamkeit bewerten. Um die Notwendigkeit von Maßnahmen zum Verhindern oder zum Mindern eines Risikos zu rechtfertigen, muss eben dieses Risiko beurteilt werden. So fordert die Norm die Etablierung des Risikobeurteilungsprozesses. Demnach müssen Risikokriterien festgelegt werden, die zu einer Akzeptanz oder einer tieferen Beurteilung des Risikos führen. Zudem müssen Risiken identifiziert, analysiert und bewertet werden. Der Beurteilung schließt sich die Risikobehandlung an. Hier fordert die Norm die Auswahl geeigneter Optionen entsprechend der Beurteilung, die Umsetzung der daraus resultierenden Maßnahmen und die ausführliche Dokumentation der Behandlung, wie auch das Einholen der Genehmigung des Plans von Risikoeigentümer:innen. Das Kapitel schließt mit der Betrachtung von Sicherheitszielen ab.

Kapitel 7 Unterstützung Im siebte Kapitel wird festgelegt, dass die Leitung der Organisation „die erforderlichen Ressourcen für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die fortlaufende Verbesserung des Informationssicherheitsmanagementsystems bestimmen und bereitstellen“[17] muss. Ferner obliegt der Leitung die Verantwortung geeignete Kompetenzen für die Aufgaben zu bestimmen, zu fördern und zu dokumentierten. Die ausgewählten Personen müssen sich ihrer Tätigkeit und der Konsequenzen bei nicht Erfüllung der Anforderungen an das ISMS bewusst sein. Die Norm fordert weiterhin, dass ein Kommunikationsprozess bestimmt wird, der die Kommunikationsteilnehmer:innen, den Zeitpunkt und den Inhalt festlegt. Der letzte Teil des Kapitels widmet sich der dokumentierten Information, wobei Anforderungen an den Inhalt, die Erstellung und die Aktualisierung aufgeführt werden.

Kapitel 8 Betrieb Das achte Kapitel beschreibt den Betrieb des ISMS. Hierbei geht es darum, dass getroffene Maßnahmen wirksam umgesetzt und dokumentiert werden. Weiterhin wird auch die Risiko-Beurteilung und Behandlung angeführt, wobei es sich um die Umsetzung der im sechsten Kapitel geplanten Schritte handelt.

Kapitel 9 Bewertung der Leistung Das vorletzte Kapitel hält die Anforderungen an die Überprüfung der ausgeführten Leistungen fest. Es wird generell festgelegt, dass die Organisation die IS-Leistungen und die Wirksamkeit des ISMS bewerten muss. Dabei soll dokumentiert werden, wer was wie überwacht und von

[17] DIN17a, S. 11.

wem die Ergebnisse der Überwachung wann analysiert und ausgewertet werden. Gleichsam erfordert die Norm auch ein internes Audit, dass regelmäßig, objektiv und unparteilich überprüft, ob die Norm eingehalten und die Anforderungen des ISMS erfüllt werden. Auch die Leitung der Organisation muss in regelmäßigen Abständen eine Bewertung des ISMS vornehmen. Dabei sollen vor allem zuvor getroffene Einschätzungen und Entscheidungen, bspw. bezüglich der relevanten Themen (siehe Kapitel 4 weiter oben) oder der Risikokriterien (siehe Kapitel 6 weiter oben), überprüft und ggf. aktualisiert werden. Auch diese Betrachtungen gilt es in geeigneter Form zu dokumentieren[18].

Kapitel 10 Verbesserung Das letzte Kapitel umfasst die kontinuierliche Verbesserung. Im ersten Schritt sollen dabei Nichtkonformitäten identifiziert und korrigiert werden. Diese können sich bspw. aus der Bewertung der Leistung durch das Management oder durch ein internes Audit nach Kapitel 9 ergeben haben. Die Situation wie auch die eingeleiteten Korrekturmaßnahmen gilt es zu dokumentieren. Abschließend wird gefordert, dass eine generelle fortlaufende Verbesserung des ISMS erfolgen muss.

Anhang Die Norm schließt mit dem Anhang A ab, in dem Ziele und Maßnahmen aufgeführt sind. Diese wurden direkt aus [DIN22] abgeleitet und zeigen welche Maßnahmen für welches Ziel umgesetzt werden müssen. Dabei sind die Maßnahmen allgemein formuliert, sodass der Organisation die technische Umsetzung überlassen bleibt.

Fazit

Die ISO 27001 stellt ausschließlich die Anforderungen an das ISMS vor. Die Umsetzung dessen bleibt den Anwender:innen überlassen. Damit ist die Norm für sich genommen eher für fachkundiges und erfahrenes Personal gedacht. Allerdings hat die ISO die Norm „ISO/IEC 27002“[19] formuliert, in der die geforderten Maßnahmen genauer formuliert werden. Ergänzend wurde die „ISO/IEC 27003“[20] als Anleitung für die Umsetzung des ISMS und die „ISO/IEC 27005“[21] als Anleitung für das Risikomanagement verabschiedet. Alle vier Normen bieten eine solide Grundlage um ein ISMS umzusetzen und dies auch international anerkannt zertifizieren zu lassen. Abgesehen vom hohen Aufwand der Umsetzung ist aber auch der Erwerb der Normen kostenpflichtig.

[18] Vgl. DIN17a, S. 14.
[19] Gelistet unter DIN22.
[20] Gelistet unter DIN17b.
[21] Gelistet unter DIN18.

2.2.3 IT-Grundschutz, bzw. BSI-Standard 200-X

Der IT-Grundschutz, bzw. der BSI-Standard 200-x ist ein Standard, der vom BSI veröffentlicht wurde und im europäischen Raum, insbesondere in Deutschland, etabliert ist. Im Oktober 2017 wurde die BSI-100-x Reihe durch die modernisierte 200-x Reihe teilweise ersetzt und aktualisiert[22]. Die Norm leitet sich von der ISO 27001 ab und ist damit kompatibel zu dieser. Der IT-Grundschutz stellt Standardmaßnahmen und -methoden zur Verfügung, die auf die Bereiche Personal, Gebäude, Software, Hardware, Organisation und Kommunikationsnetze angewendet werden können, wodurch sich dieser von der ISO 27001 unterscheidet, die eine individuelle Betrachtung der zu schützenden Assets vorsieht[23]. Weiterhin formuliert das BSI in seinen Standards nicht nur die Anforderungen an ein ISMS, sondern gibt diesbezüglich Methoden, Anleitungen, Empfehlungen und Hinweise zur Einführung und dem Betreiben eines ISMS[24] und führt diese beispielhaft aus. Nach Umsetzung der Kern- oder Standardabsicherung kann eine Zertifizierung „ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz“ erfolgen. Die Basis-Absicherung wird durch ein Testat bestätigt[25]. Der Standard wird im Folgenden näher betrachtet.

Ergänzende Dokumente

Das BSI veröffentlichte zum Thema IT-Sicherheitsmanagement vier Standards und das IT-Grundschutzkompendium, wie das Bild 2.1 zeigt. Die Abbildung wird voraussichtlichen im Jahr 2023 veraltet sein, da die Norm „BSI-Standard 100-4 Notfallmanagement“ durch die zur Zeit in der Entwicklung befindliche Norm „BSI-Standard 200-4 Business Continuity Management“ ersetzt wird. Der Standard ist kostenfrei abrufbar. Im Folgenden wird die Norm BSI 200-1 ausführlicher behandelt.

Inhalt

Der BSI-Standard 200-1[26] ist in zehn Kapitel zuzüglich Anhang aufgeteilt.

Kapite 1 Einleitung Das erste Kapitel steckt den Rahmen für den Standard ab. Neben der Zielsetzung wird die Zielgruppe und die Anwendungsweise themati-

[22] BSI18, Anleitung zur Migration von IT-Sicherheitskonzepte mit einer Auflistung der Unterschiede zwischen 100-x und 200-x.
[23] Vgl. LS17a.
[24] Vgl. BSIoJd.
[25] Vgl. BSIoJc.
[26] Abrufbar unter BSI17a.

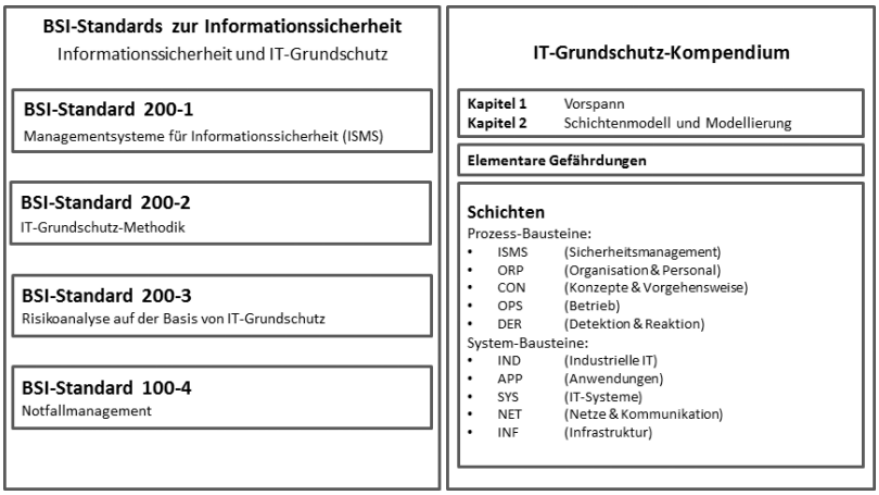

Bild 2.1: Übersicht über BSI Publikationen zum Sicherheitsmanagement[28]

siert. Das Ziel der Norm ist es, IT-Sicherheit als „integralen Bestandteil von Planung, Konzeption und Betrieb von Geschäftsprozessen und der Informationsverarbeitung“[27] zu etablieren. Dabei wird ein systematisches Vorgehen angestrebt, das auf organisatorischen Maßnahmen fußt und mit technischen Maßnahmen ausgebaut wird. Der Standard richtet sich dabei in erster Linie an die Verantwortlichen für die Informationssicherheit in einer Organisation und unterstreicht, dass die Umsetzung durch die Hinweise bedarfsgerecht angepasst werden kann. Abschließend umreißt das Kapitel die Anwendungsweise des Standards. Demnach dient die 200-1 als Management-Standard, der die wichtigsten Aufgaben des Sicherheitsmanagements abbildet. Die Methodik zur Umsetzung des IT-Grundschutzes wird im BSI 200-2 ausgeführt.

Kapitel 2 Einführung in die Informationssicherheit Das zweite Kapitel setzt den theoretischen Grundstein und klärt zunächst die Frage, was Informationssicherheit ist:„Informationssicherheit hat das Ziel, Informationen jeglicher Art und Herkunft zu schützen.“[29] Gleichwohl wird der Unterschied zwischen IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit erklärt, der bereits im Kapitel 2.1.1 ausgeführt wurde. Darauffolgend wird ein Überblick über die Standards und Normen der Informationssicherheit gegeben.

Kapitel 3 ISMS-Definitionen und Prozessbeschreibung Das dritte Kapitel widmet sich der theoretischen Ausarbeitung eines ISMS, wobei zunächst die Komponenten eines ISMS aufgeführt werden. Laut BSI besteht ein ISMS grundlegend

[27] BSI17a, S. 6.
[28] [Quelle: Ebd., S. 11]
[29] Ebd., S. 8.

aus den im Bild 2.2 dargestellten Komponenten. Der Sicherheitsprozess wird

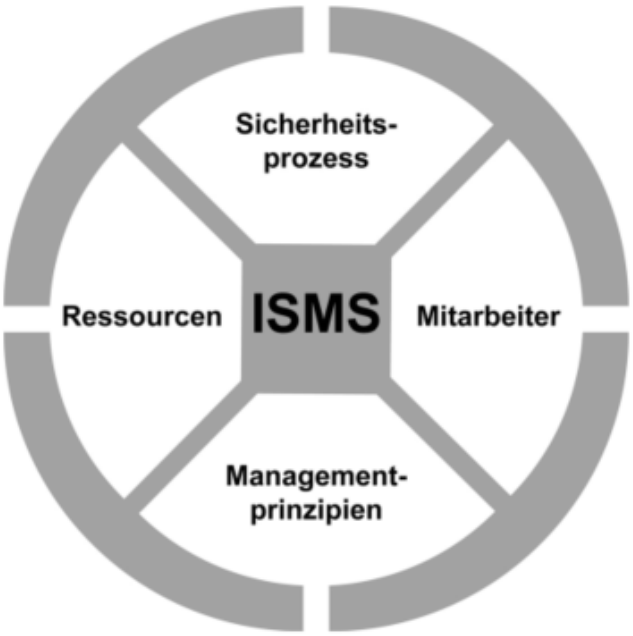

Bild 2.2: Bestandteile eines ISMS[30]

weiterführend aufgeteilt in die Leitlinie zur Informationssicherheit, das Sicherheitskonzept und die Sicherheitsorganisation. In der Leitlinie gibt die Leitungsebene die Sicherheitsstrategie vor, die sich aus den Rahmenbedingungen und den Geschäftszielen ergibt. Zur Umsetzung dieser Leitlinie dienen laut BSI das Sicherheitskonzept und die Sicherheitsorganisation.[31] Die Bestandteile der beiden Elemente werden in dem Bild 2.3 zusammengefasst.

Bild 2.3: Werkzeuge zur Umsetzung der Sicherheitsstrategie[32]

[30] [Quelle: BSI17a, S. 15]
[31] Vgl. ebd., S. 16.
[32] [Quelle: Ebd., S. 16]

Der zweite Teilabschnitt des Kapitels befasst sich mit der Prozessbeschreibung und dem Lebenszyklus-Modell von Informationssicherheit. Die Informationssicherheit unterliegt demnach einem kontinuierlichen Anpassungsbedarf, der sich unter anderem durch die ständige Weiterentwicklung der Technik, neuen Angriffsmethoden, den sich ändernden Geschäftsprozessen, aber auch durch neue Anforderungen an das Unternehmen durch neue Gesetze und Vertragsbedingungen begründet. Deshalb muss ein Unternehmen einen Prozess etablieren, der die Ausgangssituation ständig neu bewertet und auch die Wirksamkeit von getroffenen Maßnahmen prüft. Als Lebenszyklus-Modell verwendet das BSI hier den

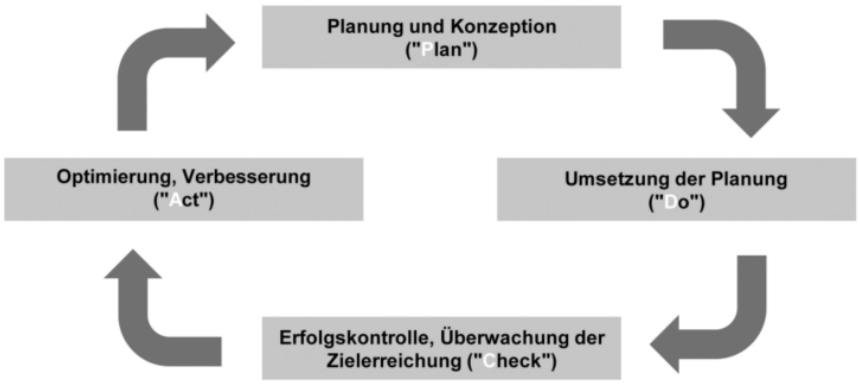

Bild 2.4: PDCA-Zyklus[33]

PDCA-Zyklus oder auch Deming-Kreis. **P**lan **D**o **C**heck **A**ct (PDCA) ist, wie das Bild 2.4 zeigt, in vier Phase aufgeteilt, die kontinuierlich durchlaufen werden. In der ersten Phase „Plan“ werden die Ausgangslage erfasst, die Sicherheitsziele bestimmt und eine Sicherheitsstrategie ausgearbeitet. Im Anschluss erfolgt die Umsetzung der Strategie über die Sicherheitsorganisation und das Sicherheitskonzept in der zweiten Phase „Do“. Der Erfolg, bzw. die Wirksamkeit der Maßnahmen und die Erreichung der Zielsetzung wird in der dritte Phase „Check“ evaluiert. Zum Abschluss eines Zyklus werden in der vierten Phase „Act“ die Mängel an der Umsetzung festgehalten und Optimierungen formuliert, die in den nächsten Zyklus mit einfließen. Der Zyklus beginnt dann erneut mit der Planungsphase, in der die zuvor getroffene Strategie ggf. überarbeitet wird und die Kritik aus der vierten Phase verarbeitet wird.

Kapitel 4 Management-Prinzipien Im vierten Kapitel werden die Management-Prinzipien behandelt. Laut dem BSI findet ein großer Teil der Umsetzung von Informationssicherheit nicht durch die Einführung kostenintensiver Technik und der Umsetzung von technischen Maßnahmen statt,

[33] [Quelle: BSI17a, S. 18]

wenngleich diese durchaus notwendig und wichtig sind, sondern durch die Umsetzung von organisatorischen Maßnahmen und Management-Prinzipien. Entsprechend ausführlich werden im Standard verschiedene Prinzipien vorgestellt und thematisiert. Der erste Block umfasst die Aufgaben und Pflichten des Managements, die in der Tabelle Aufgaben und Pflichten des Managements zusammengefasst wurden und im Anhang A.1 nachzuschlagen sind. Der zweite Block fokussiert auf das Thema Kommunikation und Wissen. Dem Management ist in geeigneter Form die aktuelle Sicherheitslage regelmäßig zuberichten, bspw. durch die Informationssicherheitsbeauftragter (ISB). Mitarbeiter:innen müssen im Sicherheitsprozess mit einbezogen werden, in der Form, dass ihnen der Zweck der Sicherheitsmaßnahmen erklärt wird und dass sie sich durch die Einbringung ihrer Ideen und Einschätzungen beteiligen können. Um das Verständnis und die Kommunikation im Prozess aber auch nach außen zu erleichtern, sollten Informationen klassifiziert werden. Durch des Festhalten der Prozessschritte, der Entscheidungen und Absprachen in Dokumentationen wird die Kontinuität und Konsistenz über den gesamten Sicherheitsprozess in seinen vielzähligen Iterationen sichergestellt. Der dritte Teil thematisiert die Erfolgskontrolle im Sicherheitsprozess. Zur Kontrolle sollte der Erfolg des Sicherheitskonzeptes und der Sicherheitsorganisation beurteilt werden. Der letzte und vierte Abschnitt wurde der kontinuierlichen Verbesserung des Sicherheitsprozesses gewidmet. Zuvor ermittelte Mängel und Verbesserungspotentiale müssen Maßnahmen nach sich ziehen, die je nach Umfang umgehend oder im nächsten Zyklus eingebracht werden.

Kapitel 5 Ressourcen für Informationssicherheit Im fünften Kapitel führt das BSI die Problematik der Ressourcen in der Informationssicherheit an. Dabei spielen „finanzielle, personelle und zeitliche Ressourcen, die von der Leitungsebene ausreichend bereitgestellt werden müssen“[34] eine Rolle. Die Ressourcen müssen sowohl bei der Planung durch eine Kosten-Nutzen-Schätzung, als auch in späteren Phasen stets berücksichtigt werden, damit sie nicht verschwendet oder die Ziele aufgrund unzureichende Ressourcen nicht erreicht werden können. Das BSI unterstreicht dabei, dass die Investitionen in personelle Ressourcen häufig effektiver sind als in Sicherheitstechnik. Dies ließe sich damit begründen, dass die beste Technik nur wenig wirkt, wenn das Personal nicht hinreichend geschult ist und die Technik nicht richtig anwendet. Weiterhin sei die Zeit eine wichtige Ressource, die im IS-Prozess oft zu wenig Beachtung findet. Darüber hinaus wird der gut funktionierende Betrieb als Grundvoraussetzung für den sicheren Betrieb

[34] BSI17a, S. 26.

von Informationstechnik angeführt. Die Informationssicherheit ist nicht dafür gedacht marode Infrastrukturen zu reparieren, sondern diese nach der Reparatur abzusichern.

Kapitel 6 Einbindung der Mitarbeiter:innen in den Sicherheitsprozess Das sechste Kapitel thematisiert die Beteiligung der Belegschaft am Sicherheitsprozess: jede(r) „Einzelne kann durch ein verantwortungs- und qualitätsbewusstes Handeln Schäden vermeiden und zum Erfolg beitragen“[35]. Die Beschäftigen sollen durch Schulungen und Sensibilisierungsmaßnahmen im Bereich Informationssicherheit unterstützt werden. Damit die Sicherheitsmaßnahmen auch erfolgreich umgesetzt werden können, müssen die Mitarbeiter:innen die Maßnahmen verstehen und mittels der Sicherheitsmechanismen anwenden können. Förderlich ist es auch, wenn Informationssicherheit im Unternehmen durch die Unternehmenskultur, die gemeinsamen Wertevorstellungen und das Arbeitsklima gelebt werden. Gleichsam müssen Prozesse etabliert werden, das Personal beim Übernehmen neuer Aufgaben oder Aufgabenbereiche auch im Bereich IS einführen und sensibilisieren. Ebenso muss ein Prozess beim Ausscheiden von Angestellten die informationssicherheitsrelevanten Aspekte, wie den Entzug von Rechten oder das Sperren von Accounts, berücksichtigen. Abschließend hält das BSI fest, dass Mitarbeiter:innen „zur Einhaltung aller im jeweiligen Umfeld relevanten Gesetze, Vorschriften und Regelungen verpflichtet werden“[36] müssen und vom Unternehmen über diese und den Meldeweg informiert werden sollten.

Kapitel 7 Der Sicherheitsprozess Im siebten Kapitel beschreibt das BSI den Sicherheitsprozess in 5 Unterkapiteln, wobei dem Sicherheitskonzept ein eigenes Kapitel gewidmet wurde. Anfangs werden die Bausteine des Prozesses in Zusammenhang gesetzt: „Die Leitungsebene muss die Sicherheitsziele [..] festlegen und die Voraussetzungen für deren Umsetzung schaffen. Mit einer Sicherheitsstrategie wird das Vorgehen geplant, um einen kontinuierlichen Sicherheitsprozess zu etablieren. Umgesetzt wird die Strategie mithilfe eines Sicherheitskonzepts und einer Sicherheitsorganisation.“[37]. Es folgt die Planung des Sicherheitsprozesses, bei der zunächst die Rahmenbedingungen ermittelt werden. Die Vorbereitung wird auch von daher als wichtig eingeschätzt, da hier Konfliktpotentiale und unzureichende Wissenspunkte aufgedeckt werden können. Gemäß der allgemeinen Ziele des Unternehmens und der erarbeiteten Rahmenbedingungen werden die Sicherheitsziele abgeleitet und die Sicherheitsstrategie zur Umsetzung dieser ausgearbeitet, deren

[35] BSI17a, S. 27.
[36] Ebd., S. 27.
[37] Ebd., S. 28.

Kernaussagen wieder in der Sicherheitsleitlinie[38] dokumentiert werden. Laut BSI sollte die Sicherheitsleitlinie folgende Themen umfassen[39]:

- Stellenwert der Informationssicherheit und Bedeutung der wesentlichen Informationen, Geschäftsprozesse und der IT für die Aufgabenerfüllung,
- Bezug der Informationssicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
- Sicherheitsziele und die Kernelemente der Sicherheitsstrategie für die Geschäftsprozesse und die eingesetzte IT,
- Zusicherung, dass die Sicherheitsleitlinie von der Institutionsleitung durchgesetzt wird, sowie Leitaussagen zur Erfolgskontrolle und
- Beschreibung der für die Umsetzung des Informationssicherheitsprozesses etablierten Organisationsstruktur.
- opt.: Nennung von Gefahren für Geschäftsprozesse, wichtige Regelungen und Rahmenbedingungen
- opt.: Aufzeigen der Wesentlichen Aufgaben und Zuständigkeiten im Sicherheitsprozess
- opt.: Nennung von Organisationseinheiten und Rollen, die als Ansprechpartner für Sicherheitsfragen fungieren
- opt.: Ankündigung von Programmen zur Förderung von Informationssicherheit, bspw. Schulungs- und Sensibilisierungsmaßnahmen

Ist die Sicherheitsleitlinie formuliert, schließt sich die Bestimmung des angemessenen Sicherheitsniveaus für Geschäftsprozesse an, die auch als Vorarbeit zum Sicherheitskonzept dient. Hierbei können bestimmte Bereiche oder Prozesse mit besondere Anforderungen an Vertraulichkeit, Integrität oder Verfügbarkeit festgelegt werden. Darauffolgend wird der Geltungsbereich des ISMS festgelegt, der im BSI IT-Grundschutz auch „Informationsverbund“ genannt wird und das gesamte Unternehmen oder Teilbereiche umfassen kann. Allerdings sollten die Aufgaben und Prozesse innerhalb des Verbundes im wesentlich und inhaltlich abgeschlossen sein, so dass keine Kernteile außerhalb des Verbundes liegen. Das BSI bietet für die Absicherung drei Modelle an, bei der der Geltungsbereich der Basis- und Standard-Absicherung häufig das gesamte Unternehmen umfasst und sich die Kern-Absicherung auf einige herausragende, besonders kritische Assets (sogenannte „Kronjuwelen“) bezieht.
Das zweite Unterkapitel widmet sich dem Aufbau einer Sicherheitsorganisation, die aus dem Festlegen von Organisationsstrukturen und dem Definieren von

[38] auch Leitlinie für Informationssicherheit, englisch: „Information Security Policy“ oder „IT Security Policy“[Vgl. BSI17a, S. 29]
[39] Ebd., S. 29, optionale Themen wurden mit einem vorangestellten „opt.“ gekennzeichnet.

Rollen und Aufgaben besteht. Dabei sollte der Aufwand und Umfang stets der Organisation und deren Ressourcen entsprechen und die Definition der Rollen die folgenden Regeln erfüllen[40]:

- Die Gesamtverantwortung für die Informationssicherheit verbleibt bei der Leitungsebene.
- Es muss mindestens eine Person benannt werden, die den Informationssicherheitsprozess fördert und koordiniert, typischerweise als Informationssicherheitsbeauftragter (ISB).
- Jeder Mitarbeiter ist gleichermaßen für seine originäre Aufgabe wie für die Aufrechterhaltung der Informationssicherheit an seinem Arbeitsplatz und in seiner Umgebung verantwortlich.

Die Aufrechterhaltung der Informationssicherheit ist das Thema des vierten Unterkapitel. „Die Schaffung von Informationssicherheit ist kein zeitlich begrenztes Projekt, sondern ein kontinuierlicher Prozess“[41], unterstreicht das BSI. So müssen nicht nur alle Sicherheitsmaßnahmen, sondern auch die Sicherheitsstrategie regelmäßig geprüft und ggf. angepasst werden. Es empfiehlt sich interne Audits zur Prüfung der Maßnahmen zu nutzen, um so auch interne Praxiserfahrungen im Bewertungsprozess miteinzubeziehen. Gleichwohl helfen Sensibilisierungsmaßnahmen und Schulungen das Wissen aktuell zu halten und Notfallsituationen und -verhalten zu simulieren, zu vergegenwärtigen und zu erproben. Durch Änderungen bspw. in Geschäftsprozessen oder in der Infrastruktur können die gewonnenen Erkenntnisse mit einfließen und so proaktiv Fehlerquellen geschlossen werden.
Das letzte Kapitel reißt kurz die kontinuierliche Verbesserung der Informationssicherheit an. Die aus der Überprüfung gewonnenen Erkenntnisse dienen der Verbesserung des Prozesses, sodass die Wirksamkeit und die Effizienz der gewählten Sicherheitsstrategie beurteilt und ggf. angepasst werden kann. Doch auch eine Änderung an den Sicherheitszielen und Rahmenbedingungen sollte zu einer Überprüfung und eventuellen Anpassung der Sicherheitsstrategie führen.

Kapitel 8 Sicherheitskonzept Das achte Kapitel führt das Sicherheitskonzept in vier Unterkapiteln aus. Das Sicherheitskonzept beschreibt die Vorgehensweise zur Umsetzung der geplanten Sicherheitsziele und stellt die zentrale Dokumentation des Sicherheitsprozesses dar[42]. Dabei muss zunächst der Zusammenhang der Elemente im Anwendungsbereich für sich und deren Abhängigkeit von den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit der Information verstanden

[40] BSI17a, S.30.
[41] Ebd., S. 30.
[42] Vgl. BSIoJb.

und dokumentiert werden. Gleichwohl müssen die Schadensursachen erhoben und ein Umgang mit den Risiken festgelegt werden. Anschließend werden die IT-Grundschutzbausteine aus dem IT-Grundschutzkatalog für Asset-Gruppierungen verwendet, die bereits vom BSI einer Risikoanalyse unterzogen wurden und bei denen entsprechende Bewertungen und Maßnahmen formuliert sind. Eine separate Risikoanalyse und -behandlung muss durchgeführt werden, wenn die Zielobjekte des betrachteten Informationsbundes

- „einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.“[43]

Die Durchführung der Analyse und Behandlung von Risiken ist im BSI-Standard 200-3[44] beschrieben. Die Festlegung fließt in das ISMS mit ein, muss entsprechend dokumentiert werden und es müssen die Ressourcen zur Behandlung der Risiken eingeplant, bzw. zur Umsetzung der Maßnahmen zur Verfügung gestellt werden. Diese Maßnahmen leiten sich aus den Sicherheitszielen und -anforderungen ab. Dabei gilt es die Kosten-Nutzen-Aspekte, die Auswirkungen auf das Sicherheitsniveau und die Praxistauglichkeit zu berücksichtigen. Die Sicherheitsmaßnahmen können sowohl technischer als auch organisatorischer Art sein. In der Dokumentation muss nachvollziehbar festgehalten werden, warum die ausgewählten Maßnahmen die Sicherheitsziele und -anforderungen unterstützen oder warum ein Risiko durch nicht Umsetzung der Maßnahmen akzeptiert wird.
Das zweite Unterkapitel widmet sich der Umsetzung des Sicherheitskonzepts. Die ausgewählten Sicherheitsmaßnahmen werden in einem Realisierungsplan organisiert, der die Priorität, die Verantwortlichkeit zur Initiierung, Bereitstellung der Ressourcen durch das Management und die Umsetzungsplanung der einzelnen Maßnahmen regelt. Anschließend wird der Realisierungsplan ausgeführt. Dabei sollten anfallende Probleme möglichst zeitnah durch Kommunikationswege, Rechtezuweisung oder Änderung der technischen Verfahren behoben werden. Sowohl während der Durchführung als auch im Anschluss sollten die Einhaltung der Zielvorgaben geprüft werden. Kommt es hier zur Nichteinhaltung sollte dies umgehend kommuniziert werden, um so Folgeschäden zu vermeiden.
Das dritte Unterkapitel thematisiert die Erfolgskontrolle des Sicherheitskonzeptes. Um die Effektivität und Effizienz des Sicherheitskonzeptes zu beurteilen rät

[43] BSI17a, S. 32.
[44] BSI17c.

das BSI zu regelmäßigen internen Audits, bzw. zu externen Audits, wenn keine internen Ressourcen zur Verfügung stehen. Die Audits umfassen dabei einen technischen Check der IT-Systeme, eine Aktualitätsprüfung vorhandener Dokumentationen und Workshops, bei denen Erfahrungen und Probleme mit dem Sicherheitskonzept ausgetauscht werden können. Über die Audits hinaus sollten weitere Aktionen durchgeführt werden, wie Beispielsweise die Überprüfung der Einhaltung der Vorgaben oder die Dokumentation festgestellter Sicherheitsvorfälle, die im BSI-Standard[45] nachgeschlagen werden können.
Im letzten und vierten Unterkapitel wird die kontinuierliche Verbesserung des Sicherheitskonzeptes angeführt. Die aus der regelmäßigen Überprüfung resultierenden Maßnahmen sollten zur Optimierung und Ausbesserung des Konzeptes beitragen. Das BSI unterstreicht, dass auch die Praxistauglichkeit von TOMs beleuchtet werden sollte, um so die Akzeptanz der Sicherheitsmaßnahmen zu erhöhen. Gleichwohl können die Ergebnisse der Internviews dazu führen, das Maßnahmen umformuliert werden müssen, um deren Verständlichkeit und Nachvollziehbarkeit zu verbessern.

Kapitel 9 Zertifizierung des ISMS Das neunte Kapitel widmet sich den Zertifizierungsmöglichkeiten nach erfolgreichem Aufbau eines ISMS. Die Umsetzung sollte nach innen und außen dokumentiert werden und die Bemühungen sollten transparent gemacht werden[46]. Die daraus resultierenden Vorteile werden vorgestellt und decken unter anderem die potentiellen Wettbewerbsvorteile oder auch das Erfüllen von gesetzlichen Richtlinien ab. Anschließend wird das zweistufige Zertifizierungsverfahren bei der ISO/IEC 27001 kurz angeführt, dass eine Prüfung durch eine erfahrene, geschulte und qualifizierte Person aus dem Auditorenkreis vorsieht und bei dem die Zertifikate durch unabhängige Zertifizierungsstellen ausgestellt werden. „Die Standard- und Kernabsicherung des IT-Grundschutzes bilden die Anforderungen der ISO/IEC 27001 ab“[47]. Folglich kann die erfolgreiche Einführung eines ISMS durch die Umsetzung des IT-Grundschutzes durch den BSI zertifiziert werden. Auch hier wird durch externe beim BSI registrierte Auditor:inne eine Prüfung vorgenommen, die in einen Audit-Bericht beim BSI endet, der dann über die Vergabe des Zertifikates entscheidet.

Kapitel 10 Das ISMS auf Basis von BSI IT-Grundschutz Im letzten und zehnten Kapitel beschreibt das BSI das ISMS auf Basis der IT-Grundschutz-Methodik. Das erste Unterkapitel führt in die IT-Grundschutz-Methodik des BSIs

[45] Vgl. BSI17a, S. 36-38.
[46] Vgl. ebd., S. 39.
[47] Ebd., S. 39.

ein. Dabei wird ausgeführt, dass sowohl der BSI Standard als auch die ISO-Normen eine generische Schilderung haben, sodass der Gestaltungsspielraum in der Praxis groß ist. Ferner bestehe die Herausforderung darin, „in der eigenen Institution ein ISMS zu etablieren, das nicht nur hilft, die gesteckten Sicherheitsziele zu erreichen, sondern auch noch kostengünstig und somit wirtschaftlich ist“[48]. Die Kernelemente der Sicherheitskonzeption sind die Risikoanalyse und die Auswahl der Sicherheitsmaßnahmen. Das BSI rät zur Anwendung der IT-Grundschutz-Methodik. Diese bietet verschiedene Vorgehensweisen, die je nach angestrebtem Schutzniveau, der verarbeiteten Informationen und verfügbaren Ressourcen genutzt werden können. Abseits dessen führt die Methodik zusammen mit dem IT-Grundschutz-Kompendium durch die Erstellung eines ISMS und die Umsetzung der Maßnahmen. Die erste und einfachste Umsetzungsform ist die Basis-Absicherung. Diese etabliert die kostengünstigste Form eines ISMS, die durch die Kern-Absicherung ergänzt oder vollständig zur Standard-Absicherung ausgebaut wird. Die Vorgehensweisen hat das BSI im „BSI-Standard 200-2 IT-Grundschutz-Methodik“[49] ausgeführt, wobei die Thematik durch das IT-Grundschutz-Kompendium[50] praxisnah vertieft werden kann.
Im zweiten Unterkapitel beschreibt das BSI die wesentlichen Elemente der Methodik und somit den Sicherheitsprozess nach IT-Grundschutz. Das BSI reduziert dieses Kapitel auf die grundsätzliche Vorgehensweise zur Erstellung eines Sicherheitskonzeptes, da die größten Unterschiede bei einem ISMS in der Art und Weise, wie ein Sicherheitskonzept konkret erstellt wird, also bei der Ausgestaltung der Risikobeurteilung und der Auswahl der Sicherheitsmaßnahmen, bestehen. Nach der Einführung in die integrierte Risikobewertung[51] wird die Sicherheitskonzeption vorgestellt. Wie bereits weiter oben beschrieben, bietet das BSI drei Herangehensweisen an, wie ein Unternehmen entsprechend der eigenen Anforderungen und Ressourcen ein ISMS aufbauen und betreiben kann: die Basis-, Kern- und Standardabsicherung. Die Basisabsicherung bietet das geringste Schutzniveau bei einer vergleichsweise günstigen Implementierung. Die Kernabsicherung beschränkt sich auf besonders wichtige Assets des Unternehmens und die Standardabsicherung bietet den umfangreichsten Schutz. Das Bild 2.5 zeigt dabei die Schritte die zum Erreichen der Standardabsicherung durchlaufen werden müssen. Die beiden anderen Herangehensweisen unterscheiden sich in sofern von dieser Darstellung, als dass sie Schritte auslassen, wie bei der Basisabsicherung, oder sich in der Definition des Informationsverbundes auf besondere Assets beschrän-

[48] BSI17a, S. 40.
[49] BSI17b.
[50] BSI22.
[51] Mehr dazu in BSI17a, S. 41 - 43.

ken und den IT-Grundschutz-Check zwei auslassen, wie bei der Kernabsicherung. Nachfolgend werden die einzelnen Schritte kurz erklärt.

Um ein Sicherheitskonzept erfolgreich umsetzen zu können, muss im ersten

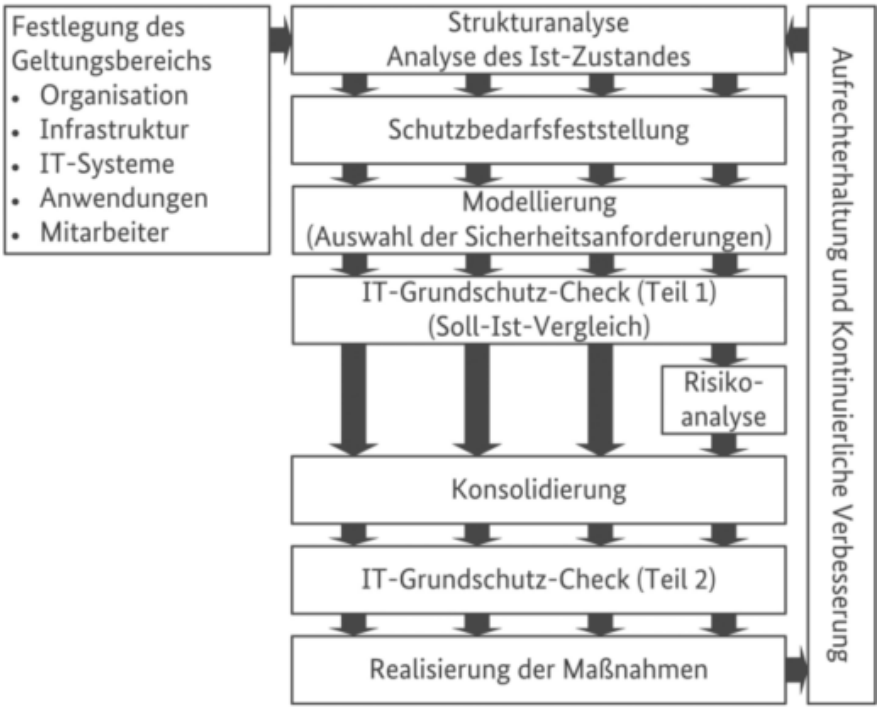

Bild 2.5: Erstellung der Sicherheitskonzeption bei der Standard-Absicherung

Schritt der *Informationsverbund definiert* werden. Im Rahmen der Standardabsicherung wird dies in der Regel die gesamte Organisation betreffen. In der Kernabsicherung werden hingegen nur hoch relevante Assets betrachtet, wie bspw. bestimmte Prozesse oder Fachaufgaben. Dem schließt sich die *Strukturanalyse* an, in der „die für den betrachteten Informationsverbund, also Geltungsbereich oder Geschäftsprozess relevanten Schutzobjekte wie Informationen, Anwendungen, IT-, ICS-, oder IoT-Systeme, Netze, Räume und Gebäude, aber auch zuständige Mitarbeiter ermittelt [werden].“[52]. Weiterhin müssen die Verbindungen der Schutzobjekte untereinander festgehalten werden, um so Ausfallketten oder Abhängigkeiten zu identifizieren. Damit bei der Erfassung der Objekte keine Überforderung eintritt und die Komplexität reduziert wird, empfiehlt das BSI im BSI-Standard 200-2, ähnliche „Objekte sollten deshalb sinnvoll zu Gruppen zusammengefasst werden.“[53] Darauf folgt die *Schutzbedarfsfeststellung*, die in Form von Schutzbedarfskategorien die Auswirkungen eines Sicherheitsvorfalls auf einen Geschäftsprozess abstrahiert und festhält. Um den Schutzbedarf der

[51] [Quelle: BSI17b, S. 76]
[52] BSI17a, S. 43.
[53] BSI17b, S. 79.

Schutzobjekte zu ermitteln, wird hier ein Top-Down-Ansatz genutzt, der bei den Geschäftsprozessen beginnt. Der Schutzbedarf der Anwendungen bestimmt sich aus den verarbeiteten Informationen und den Geschäftsprozess, den sie bedienen. Dieser Schutzbedarf überträgt sich auf die IT-Systeme, die zur Verarbeitung der Informationen und zum betreiben der Anwendungen genutzt werden. „Der Schutzbedarf der Räume leitet sich aus dem Schutzbedarf der Anwendungen und IT-Systeme, die dort betrieben werden, ab.“[54] Sind die Schutzobjekte erfasst und die Schutzbedarf bestimmt, folgt die *Modellierung*. Bei der Modellierung werden den Schutzobjekten passende Bausteine aus dem IT-Grundschutz-Kompendium zugeordnet. Die Bausteine decken unter anderem Bereiche wie Betrieb, IT-Systeme, Organisation und Personal oder Konzeption und Vorgehensweise ab. Anhand der zugeordneten Bausteine resultieren Sicherheitsanforderungen, die gemäß dem Schutzbedarf und der gewählten Absicherungs-Methode ausgewählt werden. Durch dieses Verfahren spart das Unternehmen die aufwendige Betrachtung jeder einzelnen Komponente, deren Gefährdung und die daraus resultierenden Sicherheitsziele und kann auf bereits erhobene und erprobte Erfahrungen zurückgreifen. Das Resultat dieses Prozesses ist eine Liste mit Sicherheitsmaßnahmen, die zum Erreichen des geplanten Schutzniveaus, bzw. der Erfüllung der Sicherheitsanforderungen der Schutzobjekte umgesetzt werden sollte und im Folgenden mit dem aktuellen Stand abgeglichen werden muss. Diesen Schritt bezeichnet das BSI als *IT-Grundschutz-Check*. Hierbei wird mittels Interview und Überprüfungen der Systeme der IST-Stand erhoben und mit dem SOLL-Stand abgeglichen, so dass sich der Umsetzungsgrad der Anforderungen ergibt. Dieser wird nach BSI mit entbehrlich, ja, nein, oder teilweise erfasst. Die Anforderungen, die nicht oder nur teilweise umgesetzt sind, führen durch eine erfolgreiche Umsetzung zur Verbesserung des Sicherheitsniveaus im gesamten Informationsverbund. Wie bereits weiter oben beschrieben, sind die Bausteine für ein gewöhnliches Anwendungsfeld formuliert und decken den normalen bis hohen Schutzbedarf ab. Ist der Schutzbedarf eines Objektes hoch oder sehr hoch oder wird das Objekt nicht hinreichend mit dem Baustein abgebildet, muss eine Risikoanalyse durchgeführt werden. Maßnahmen, die aus der Risikoanalyse resultieren, müssen in den Katalog mitaufgenommen werden, sodass der Umsetzungsgrad bestimmt und ggf. umzusetzende Maßnahmen erhoben werden können. Der letzte Schritt des Prozesses ist die *Umsetzung der Maßnahmen*. Die Umsetzung sollte geplant werden, sodass die Reihenfolge der umzusetzenden Maßnahmen, der Zeitpunkt und die verantwortliche Person definiert sind. Anschließend gilt es die Maßnahme durchzuführen, zu begleiten und zu überwachen. Nach Abschluss des Sicherheitsprozesses wird die-

[54] BSI17a, S. 43.

ser in regelmäßigen Abständen wiederholt, sodass Änderungen eingepflegt werden und stets ein aktuelles Bild des Sicherheitsniveaus vorliegt.

Fazit

Das BSI hat mit seiner 200-Reihe einen umfangreichen, anwendungsfreundlichen Standard veröffentlicht, der ergänzt mit dem IT-Grundschutz-Kompendium eine flexible Möglichkeit zum Aufbau eines ISMS im Unternehmen verschiedenster Größen bietet. Die Ausführung des Kapitels 2.2.3 zeigt bereits, dass der Standard umfassend formuliert ist und mit praxiserprobten Erfahrungen die Umsetzung unterstützt. Gleichwohl ist eine ISMS-Implementierung nach BSI durch die Anlehnung an die ISO/IEC 27001 Norm mit dieser kompatibel und zertifizierbar. Hervorzuheben ist auch, dass der gesamte Standard 200-X inklusive der ergänzenden Dokumente kostenlos abrufbar und verfügbar ist.

2.2.4 VdS 10000

Die VdS 10000 ist die jüngste Norm und wurde im November 2018 als Nachfolger der VdS 3473 von dem Verband der Sachversicherer e.V (VdS) veröffentlicht. Bei der strukturellen Umsetzung von IT-Sicherheit mittels der ISO 27001 oder dem IT-Grundschutz stoßen Kleine und mittelständische Unternehmen (KMU) und kleinere Organisationen an ihre kapazitiven Grenzen. Eben diesem Umstand begegnet die VdS 10000. „Mit ca. 20 % des Aufwandes im Vergleich zu ISO 27001 können KMU aus den VdS-Richtlinien Maßnahmen und Prozesse ableiten, mit denen sie im IT-Bereich ein angemessenes Schutzniveau erreichen.“[55]. Der VdS bietet die Möglichkeit für Unternehmen und Organisationen die Umsetzung der VdS 10000 zertifizieren zu lassen. Gleichsam ist die Norm so aufgebaut, dass es eine aufwärtskompatibilität zur ISO 27001[56] und folglich auch zum BSI IT-Grundschutz bietet. Die nachfolgende Ausführung hat das Ziel den Aufbau und den Inhalt der Richtlinie zu erfassen und zusammen zufassen. Dabei wird nicht auf jede Maßnahme eingegangen.

Ergänzende Standards

Die VdS 10000 beschreibt anhand der Anforderungen ein ISMS für klein und mittelständische Unternehmen. Dieses Dokument wird ergänzt oder branchenspezifisch präzisiert durch weitere Standards, die in der Tabelle 2.2 zusammengetragen wurden. Nachfolgend wird ausschließlich die VdS 10000 näher beschrieben.

[55] VdS21.
[56] Vgl. ebd.

Inhalt

Norm /Richtlinie	Titel / Untertitel
VdS 10001	VdS Quick-Audit, Verfahren
VdS 10002	Zertifizierung von Managementsystemen für KMU (Informationssicherheit und Datenschutz), Verfahren
VdS 10003	Richtlinien für die Anerkennung von Beratern für Cyber-Security
VdS 10005	Mindestanforderungen an die Informationssicherheit von Klein- und Kleinstunternehmen, Anforderungen
VdS 10005LF	Leitfaden zur Umsetzung der Richtlinien VdS 10005
VdS 10006	Testierung der Informationssicherheit von Klein- und Kleinstunternehmen, Verfahren
VdS 10010	VdS-Richtlinien zur Umsetzung der DSGVO, Anforderungen
VdS 10020	Cyber Security für kleine und mittlere Unternehmen (KMU), Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme

Tabelle 2.2: Ergänzende Normen zur VdS 10000[57]

Die Richtlinie[58] ist in 18 Kapitel und zwei Anhänge aufgeteilt. Die Kapitel werden im Folgenden beschrieben und zusammengefasst.

Kapitel 1 Allgemeines Nach einer kurzen Einleitung vermittelt das erste Kapitel das Ziel dieser Richtlinie: „Die vorliegenden Richtlinien legen Mindestanforderungen an die Informationssicherheit fest und beschreiben ein auf kleine und mittlere Unternehmen (KMU) zugeschnittenes Informationssicherheitsmanagementsystem (ISMS).“[59] Es wird darauf hingewiesen, dass Fachwissen im Bereich IT-Sicherheit zur Umsetzung notwendig ist. Anschließend werden die Schlüsselbegriffe für die empfohlenen und verpflichtenden Maßnahmen angeführt. Der VdS empfiehlt die Umsetzung der VdS 10000 zusammen mit der „Richtlinie zur Umsetzung der DSGVO“ (VdS 10010)[60] und dem „Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme“ (VdS

[57] Quelle: selbst erstellte Zusammenfassung
[58] VdS18, Erwerbbar unter https://shop.vds.de/publikation/vds-10000.
[59] Ebd., S. 6.
[60] Siehe hierzu VdS22.

10020)[61]. Gleichwohl sei angemerkt, dass die VdS 10000 nicht auf Unternehmen für industrielle Automatisierungssysteme beschränkt ist. Abschließend wird der Anwendungs- und Geltungsbereich auf KMU, den gehobenen Mittelstand, Verwaltung, Verbände und sonstige Organisationen eingegrenzt und die Gültigkeit ab dem 01.12.2018 datiert.

Kapitel 2 und 3 Normative Verweise und Begriffe Das zweite Kapitel führt die Quelle auf, auf die sich die Richtlinie bezieht. Darunter fallen bspw. die BSI-Standards 100-4 und 200-2 oder die ISO/IEC 27001, aber auch andere bisher noch nicht erwähnte Standards wie die DIN En ISO 9001. Das dritte Kapitel stellt das Glossar dar und erklärt grundlegende und in der Richtlinie verwendete Begriffe der IT-Sicherheit.

Kapitel 4 Organisation der Informationssicherheit Das vierte Kapitel führt die Maßnahmen an, die zum Anfang der Einführung eines ISMS ausgeführt werden sollten. Dabei geht es in erster Linie um die Organisation des ISMS. Wie wichtig und essentiell dieser Teil ist, suggeriert bereits der Gebrauch des Umsetzungslevels „MÜSSEN“, dass bei 12 der 14 Maßnahmen angewendet wird. Im ersten Teil werden dabei die Anforderungen an die Verantwortlichkeiten definiert. Diese müssen „eindeutig und widerspruchsfrei zugewiesen werden.“[62] Gleichsam müssen die Beschaffenheit der Verantwortung, also bspw. das angestrebte Ziel, die Berechtigung und die Ressourcen definiert und dokumentiert werden. Bei der Verteilung der Verantwortung ist auf eine Funktionstrennung zu achten, die eine Kollision der Interessen ausschließt. Sowohl die Verantwortung als auch die Funktionstrennung gilt es, regelmäßig auf Wirksamkeit und Erfüllung zu prüfen. Die Verantwortlichen können ihre Aufgabe nur wahrnehmen, wenn sie für die Tätigkeit von anderen Tätigkeiten freigestellt werden. Um einer Überlastung vorzubeugen, kann die verantwortliche Person Aufgaben delegieren, wobei die Verantwortung jedoch bei der delegierenden Person verbleibt.
Wie auch bei den anderen Richtlinien muss sich die Geschäftsführung hier zur Übernahme der Gesamtverantwortung für die Informationssicherheit bekennen, ausreichend Ressourcen zur Verfügung stellen und die Informationssicherheit als integralen Bestandteil der Unternehmenskultur und -prozesse etablieren. Um das Erreichen der Ziele aus der Leitlinie für Informationssicherheit zu ermöglichen, muss das Management einer Person die Verantwortung der / des ISB zuweisen, die die Koordination und Prüfung der Umsetzung und Einhaltung der TOMs überwacht, zur Verbesserung des ISMS beiträgt und Anpassungen an die Informations-

[61] Siehe hierzu VdS20.
[62] VdS18, S. 12.

sicherheit durch rechtliche oder betriebliche Änderungen einführt und umsetzt. Ferner muss diese einen jährlichen Bericht zum aktuellen Stand der Informationssicherheit dem Informationssicherheitsteam (IST) vorlegen. Die Richtlinie führt anschließend weitere Organisationseinheiten des Unternehmens und deren Verantwortlichkeit an, die in Tabelle Organisationseinheiten des ISMS nach VdS 10000 im Anhang A.2.1 zusammengefasst wurden.

Kapitel 5 Leitlinie zur Informationssicherheit (IS-Leitlinie) Das fünfte Kapitel widmet sich den Anforderungen an die Leitlinie zur Informationssicherheit (IS-Leitlinie). Sie wird von dem VdS als „das zentrale Dokument für die gesamte Informationssicherheit“[63] ausgewiesen und von der Geschäftsführung verabschiedet und in Kraft gesetzt. In ihr werden die Ziele und die Verantwortlichkeiten bzgl. der IT-Sicherheit und der Stellwert dieser in der Organisation definiert. Sie muss jährlich auf Gültigkeit geprüft und ggf. aktualisiert und zeitnah publiziert werden.

Kapitel 6 Richtlinien zur Informationssicherheit (IS-Richtlinien) Da die IS-Leitlinie generelle Formulierungen zum Umgang mit IT-Sicherheit im Unternehmen enthält, führt der VdS zur Konkretisierung eine Zusammenstellung von Dokumenten ein, die Richtlinien zur Informationssicherheit (IS-Richtlinien). Diese muss nach VdS von der / dem ISB in Kooperation mit dem IST erstellt und von der Geschäftsführung in Kraft gesetzt oder widerrufen werden. Gleichwohl müssen auch diese Dokumente jährlich auf Aktualität geprüft und ggf. aktualisiert werden. Im Anschluss gilt es, das aktualisierte Dokument der entsprechenden Zielgruppe in geeigneter Form zugänglich zu machen. In jeder Richtlinie müssen die Zielgruppe, der Grund zur Erstellung, das beabsichtigte Ziel und die Konsequenzen bei nicht einhalten festgehalten werden. Bei der Erstellung ist darauf zu achten, dass sie weder gegen anderen Richtlinien noch die Leitlinie verstößt. Unter „6.3 Regelung für Nutzer“[64] definiert der VdS dann Regellungen, die für alle Mitarbeiter:innen gelten und den Umgang mit IT festlegen. Dabei wird unter anderem auf die Privatnutzung, den Umgang mit den Informationen der Organisation und die Missbrauchskontrolle eingegangen. Abschließend wird vermerkt, dass ggf. themenspezifische IS-Richtlinien erarbeitet werden müssen, die bspw. die Bereiche mobile IT-Systeme oder Sicherheitsvorfälle betreffen. Auf diese wird weiter unten eingegangen.

[63] VdS18, S. 15.
[64] Siehe ebd., S. 16.

Kapitel 7 Mitarbeiter Das siebente Kapitel hält die Anforderung der IT-Sicherheit in Bezug auf Mitarbeiter:innen fest. Das Kapitel deckt die drei Bereiche „Vor der Aufnahme der Tätigkeit“, „Aufnahme der Tätigkeit“ und „Beendigung oder Wechsel der Tätigkeit“ ab, wobei es weniger um die Tätigkeit geht, als viel mehr darum, welche Prozesse existieren müssen, um Mitarbeiter:innen in die Lage zu versetzen, die IT-Sicherheit im Unternehmen zu fördern oder zumindest nicht zu stören. So wird bspw. die Eignung und Vertrauenswürdigkeit der Person für die Besetzung einer IS-relevanten Position verlangt oder, dass Mitarbeiter:innen „in die IS-Leitlinie und in sämtliche für sie relevante Regelungen zur Informationssicherheit (wie z. B. in die Inhalte entsprechender Richtlinien und Verfahren) eingewiesen“[65] werden.

Kapitel 8 Wissen Das achte Kapitel behandelt den Umgang mit Wissen. Hierbei geht es darum, dass das vorhandene Wissen zum Thema IT-Sicherheit transferiert, aktualisiert und verständlich präsentiert wird. Aktualisiertes Wissen muss als Faktor zur Beurteilung der Aktualität der Richtlinien, Maßnahmen, Gefahreneinschätzung und Leitlinie dienen und muss an die Mitarbeiter:innen im Unternehmen in verständlicher Form vermittel werden. Dies kann durch Schulungs- oder Sensibilisierungsmaßnahmen erfolgen, die Inhalte vermitteln, welche auf die Zielgruppe angepasst sind und mit Erfolgskontrollen den Lernerfolg messen. Der VdS empfiehlt, die Maßnahmen durch die Teilnehmer:innen bewerten zu lassen, um so ggf. eine Verbesserung der Maßnahmen zu erzielen.

Kapitel 9 Identifizieren kritischer IT-Ressourcen Im Kapitel neun vermerkt der VdS, dass die / der ISB die kritischen Assets der Organisation identifizieren und jährlich aktualisieren muss. Als Verfahren wird die „Informationsklassifizierung auf Basis eines anerkannten Standards wie ISO/IEC 27001 oder eine Schutzbedarfsanalyse gemäß BSIStandard 200-2“[66] vorgeschlagen. Andere Verfahren werden akzeptiert, wenn diese dokumentiert werden und die in Tabelle Identifikation kritischer IT-Ressourcen aus Anhang A.2.2 zusammengefassten Anforderungen erfüllen. Es bleibt anzumerken, dass die Erhebung der Prozesse und die Dokumentation der kritischen Informationen von der Geschäftsführung freigegeben werden muss, wohingegen die Dokumentation der IT-Ressourcen durch die IT-Verantwortliche freigegeben wird.

Kapitel 10 IT-Systeme Das zehnte Kapitel widmet sich den Kernkomponenten der elektronischen Datenverarbeitung, den IT-Systemen, und hält die anzuwen-

[65] VdS18, S. 17.
[66] Ebd., S.19.

denden Maßnahmen fest. Die IT-Systeme gilt es in einem Inventar zu erfassen und über den gesamten Lebenszyklus, beginnend bei der Inbetriebnahme und endend mit der Ausmusterung, dokumentiert zu betreuen. Dazu gehört unter anderem das Erfassen der Kritikalität bei der Inbetriebnahme und das Anwenden des Basisschutzes, aber auch das Sichern von Daten bei der Ausmusterung und die Sicherstellung, dass Informationen vor unrechtmäßigem Zugriff geschützt sind bei der Ausmusterung. Der Basisschutz muss auf jedem Gerät im Informationsverbund angewendet werden. Er enthält verschiedene Maßnahmen bspw. zur installierten Software, zur Protokollierung oder zum Verwenden externer Schnittstellen und Laufwerke. Der VdS sieht zusätzliche Maßnahmen für mobile oder kritische IT-Systeme als erforderlich und führt diese entsprechend ergänzend zum Basisschutz auf. Bei den mobilen IT-Systemen ist eine zusätzliche IS-Richtlinie erforderlich, die die unternehmensweiten Regelungen im Umgang mit den Geräten für die Mitarbeiter:innen festlegt. Darüber hinaus müssen besondere Maßnahmen für die Geräte ergriffen werden, die das Ausmaß an Folgen bei Verlust reduzieren und auch bestimmen, wer bei Verlust benachrichtigt wird. Auch kritische IT-Systeme erfahren zusätzlich zum Basisschutz besondere Maßnahmen. Werden diese nicht umgesetzt, fordert der VdS, dass dem „entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet“[67] wird. Die angewendeten Maßnahmen sind restriktiver als noch im Basisschutz und das IT-System und dieses betreffende Prozesse müssen deutlich ausführlicher dokumentiert werden. Gleichwohl gilt es das System speziell zu härten und für ein Ersatzsystem zu sorgen oder eine angemessene Wiederherstellungsform zu etablieren.

Kapitel 11 Netzwerke und Verbindungen Damit die Informationen an die IT-Systeme übertragen werden können, werden Verbindungen und Netzwerke benötigt, die es entsprechend abzusichern gilt. So wie die IT-Systeme in einem Inventar erfasst werden müssen, muss auch das Netzwerk für Fachpersonal nachvollziehbar in einem Netzwerkplan dokumentiert werden. Dieser muss sowohl die logische als auch die physikalische Struktur wiedergeben. Alle aktiven Netzwerkkomponenten müssen analog zu den IT-Systemen abgesichert werden. Der VdS führt weiterhin spezielle Maßnahmen für Netzübergänge in weniger vertrauliche Netzwerke ein und einen Basisschutz, der Maßnahmen wie bspw. die Netzwerk-Segmentierung oder den Fernzugang thematisiert. Ergänzend muss bei kritischen Verbindungen eine Risikoanalyse und -behandlung durchgeführt werden.

[67] VdS18, S. 25.

Kapitel 12 Mobile Datenträger Für die Behandlung von mobilen Datenträgern, wie Festplatten oder USB-Sticks, muss das Unternehmen eine weitere IS-Richtlinie einführen, die bspw. festlegt, welche Informationen der Organisation auf derartigen Medien gespeichert und transportiert werden dürfen. Um den Verlust der Vertraulichkeit oder der Integrität der Informationen auf den Datenträgern vorzubeugen, sollten die Geräte mit besonderen Maßnahmen, wie bspw. der Verschlüsselung, gesichert werden. Ergänzend muss auch bei kritischen mobilen Datenträgern eine Risikoanalyse und -behandlung durchgeführt werden.

Kapitel 13 Umgebung Um die Kompromittierung von IT-Systemen und Datenleitungen durch negative Umwelteinflüsse, wie Blitzschlag, Luftfeuchtigkeit oder Vandalismus zu schützen, müssen geeignete Absicherungen etabliert werden, die im Kapitel 13 thematisiert werden. Der VdS empfiehlt die Absicherung nach der VdS 2007[68], wobei auch andere Vorgehensweisen akzeptiert werden, wenn diese bestimmte Anforderungen wie bspw. das Absichern von Servern vor unberechtigten Zugriff, das Bewerten und Behandeln von bestimmten Bedrohungen für IT-Systeme oder die Installation von Datenleitungen nach gängigen Standards, erfüllen. Abschließend werden ergänzende Maßnahmen aus der Risikoanalyse und -behandlung von kritischen IT-Systemen abgeleitet, wobei in dieser zumindest die folgenden Bedrohungen betrachtet und behandelt werden müssen: „ungeeignete Umgebungsbedingungen, negative Umwelteinflüsse, unzuverlässige Stromversorgung, Beschädigung und Verlust, unautorisierter Zutritt und Ausspähen vertraulicher Informationen“[69].

Kapitel 14 IT-Outsourcing und Cloud Computing Das Thema IT-Outsourcing und Cloud Computing wird im Kapitel 14 behandelt. Hierbei muss das Unternehmen sicherstellen, dass die im Unternehmen geltenden Richtlinien und Ansichten bzgl. IT-Sicherheit auch beim Auslagern weiterhin gewährleistet und erfüllt werden. Es gilt daher eine weitere ergänzende IS-Richtlinie zu erstellen, in der Kriterien festgelegt werden, unter denen die Auslagerung ausgeführt werden darf. Über diese Punkte hinaus müssen zusätzliche Maßnahmen ergriffen werden, wenn kritische IT-Ressourcen ausgelagert werden. Es muss eine Risikoanalyse durchgeführt werden und bestimmte Punkte der Leistungen, der Kommunikation, der Leistungsänderung und der Vertragsauflösung schriftlich festgehalten werden[70].

[68] Kostenlos abrufbar unter VdS16.
[69] VdS18, S. 31.
[70] Mehr hierzu auf ebd., S. 32.

Kapitel 15 Zugänge und Zugriffsrechte Das 15. Kapitel widmet sich den Zugängen und Zugriffsrechten auf IT-Systeme. Der VdS verlangt die Etablierung von Prozessen für das Hinzufügen und das Entfernen von Zugängen und Zugriffsrechten. Dabei sollen die Vorgänge beantragt, geprüft und genehmigt werden. Es gilt das Prinzip, dass nur so viele Rechte eingeräumt werden, wie zur Erfüllung der Aufgabe notwendig sind. Administrative Freigaben müssen begründet und durch IT-Verantwortliche entschieden werden. Der VdS fordert weiterführend, dass die jeweiligen Prozesse dokumentiert werden. Auch für die Zugänge und Zugriffsrechte auf kritische Informationen und Zugänge zu kritischen IT-Systemen werden gesonderte Maßnahmen angelegt. Diese Zugänge und Zugriffsrechte müssen jährlich und auf bestehende Notwendigkeit überprüft werden. Fallen dabei Zugänge und Zugriffsrechte auf, die nicht ordnungsgemäß angelegt wurden, muss dies als Sicherheitsvorfall laut VdS behandelt werden.

Kapitel 16 Datensicherung und Archivierung Das Thema des 16. Kapitels ist die Datensicherung und Archivierung, die gemäß eines anerkannten Standard wie dem BSI-Standard 200-2 durchgeführt werden soll. Gleichwohl kann aber auch eine andere Vorgehensweise gewählt werden, wenn sie die aufgelisteten Anforderungen[71] erfüllt. Anschließend führt der VdS den Basisschutz für die betroffenen IT-Systeme aus. Dieser besagt, dass eine Komponente so gesichert werden muss, dass ihr vollständig wiederherstellbarer Zustand nicht älter als eine bestimmte Zeit ist: bspw. müssen Server so gesichert werden, „dass ihr letzter vollständig wiederherstellbarer Zustand (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.) nicht älter als 24 Stunden ist“[72]. Der VdS hat über den Basisschutz hinaus Maßnahmen für kritische IT-Systeme formuliert. Bei diesen muss eine Risikoanalyse und -behandlung durchgeführt und der maximal tolerierbare Datenverlust (MTD) bestimmt werden. Darüber hinaus müssen die Systeme vollständig gesichert werden und die Einhaltung der maximal tolerierbaren Ausfallzeit (MTA) wird im Falle einer Wiederherstellung ohne Ersatzsysteme oder -Verfahren garantiert.

Kapitel 17 Störungen und Ausfälle Alle Maßnahmen dienen dem Reduzieren von Risiken, doch diese lassen sich nicht gänzlich vermeiden und so widmet sich das 17. Kapitel den Störungen und Ausfällen. Um bei derartigen Ereignissen angemessen zu reagieren, empfiehlt der VdS die Implementierung eines Business Continuity Management (BCM) nach anerkannten Standards wie dem BSI-Standard

[71] Siehe hierzu VdS18, S.33.
[72] Ebd., S.35.

100-4[73]. Doch auch hier kann das Unternehmen eine eigene Vorgehensweise wählen, wenn diese den Kriterien[74] genügen. Unter anderem müssen in einer ergänzenden IS-Richtlinie Regeln zum Umgang mit Störungen und Ausfällen definiert werden, die festlegen, wann die Unternehmensführung über einen Vorfall informiert wird und wie und wann intern und nach außen ein Vorfall gemeldet wird. Für kritische IT-Systeme werden auch hier weitere Maßnahmen gefordert, wie bspw. dass für jedes System ein Wiederanlaufplan existieren muss, der die Arbeitsschritte zur Wiederherstellung enthält.

Kapitel 18 Sicherheitsvorfälle Das letzte und 18. Kapitel widmet sich dem Umgang mit Sicherheitsvorfällen. Zusätzlich zu den bereits vorhandenen Richtlinien muss für den Umgang mit Sicherheitsvorfällen eine weitere IS-Richtlinie erstellt werden, die unter anderem den Begriff Sicherheitsvorfall definiert und festlegt, dass alle Mitarbeiter:innen einen möglichen Sicherheitsvorfall an den / die ISB melden und diese:r dann mit den Verantwortlichen den Vorfall untersucht und ggf. einen Sicherheitsvorfall feststellt. Weiterhin wird die Kommunikation definiert, das heißt wann die Unternehmensführung zu informieren ist und wann und wie die interne und externe Meldung erfolgt. Abschließend fordert der VdS die Etablierung eines Verfahrens zur Reaktion auf einen Sicherheitsvorfall, das unter anderem die Eindämmung des Schadens durch Sofortmaßnahmen, die Dokumentation des Schadens und Sicherung des Beweismaterials umfasst.

Anhang A und Anhang B Der Anhang A beschreibt im ersten Teil, dass die Umsetzung der Maßnahmen aus den Richtlinien durch Verfahren geprüft, gesteuert und stetig verbessert werden muss. Für diesen Zweck biete sich eine Prüfung im Rahmen eines Qualitätsmanagementsystem an oder eine eigene Vorgehensweise die bestimmten Anforderungen[75] genügt. Im zweiten Teil des Anhangs wird die Risikoanalyse und -behandlung, wie auch die Kriterien zur Wiederholung und Anpassung dieser beschrieben. Der Anhang B enthält ein Register der Änderungen zur Vorgängerversion, die hier nicht weiter ausgeführt werden[76].

Fazit

Die VdS 10000 hat den Anspruch durch eine unkomplizierte und direkte Vorgehensweise die Ressourcenknappheit kleiner und mittelständischer Unternehmen zu berücksichtigen und diesen die Möglichkeit zur Etablierung eines ISMS zu

[73] Abrufbar unter BSI08.
[74] Siehe dazu VdS18, S. 35ff.
[75] Siehe hierzu ebd., S. 29.
[76] Siehe hierzu ebd., S. 41.

geben. Dabei wird ein Basisschutz etabliert, der sich durch andere Normen und Standards auch sukzessive ausbauen lässt. Wo das BSI und die ISO / IEC mit ergänzenden Normen die konkrete Umsetzung thematisieren und somit im Hauptdokument eher generisch bleiben, fasst die VdS 10000 sowohl die Begriffserklärung als auch die Umsetzungsrichtlinie in einem Dokument zusammen. Die ergänzenden Richtlinien sind branchenspezifisch gehalten. Alle hier erwähnten Richtlinien des VdS müssen jedoch kostenpflichtig als Abo oder als Einmalzahlung erworben werden.

3 Vorstellung des konzeptionell überarbeiteten ISMS

Nachdem im Kapitel 2 die Vermittlung der Grundlagen und die theoretische Aufarbeitung zum ISMS stattgefunden hat, wird im Folgenden das Konzept des überarbeiteten ISMS vorgestellt. Dazu werden die Gemeinsamkeiten der drei Standards ausgeführt. Anschließend erfolgt die Darstellung des Konzeptes. Abschließend werden die Anforderungen der Firma dargelegt und die vorhandene Vorarbeit angeführt.

3.1 Gemeinsamkeiten der verglichenen Standards und der Richtlinie

Alle drei ausgewählten Dokumente beschreiben auf ihre Art und Weise die Anforderungen an ISMS. Wenngleich diese sich in der Umsetzung unterscheiden, haben sie doch auch Gemeinsamkeiten, die es im Folgenden herauszuarbeiten gilt, da diese als Fundament für das überarbeitete ISMS genutzt werden können.

Erhebung der Ausgangsbasis Allen voran fordern alle drei Standards die Definition des Anwendungsbereiches. Dabei gilt es sowohl die Anforderungen und Ansprüche des Unternehmens festzuhalten, aber auch eine Inventarisierung, bzw. eine Übersicht über die Systemlandschaft des Unternehmens zu erstellen. Ersteres dient unter anderem dazu, dass die IT-Sicherheit im Einklang mit dem Unternehmen und nicht an diesem vorbei etabliert wird. So werden bspw. Schadensgrenzen und Schutzkategorien definiert und der Rahmen, in dem die IT-Sicherheit verbessert werden soll, festgelegt. Dies kann ein gesamtes Unternehmen umfassen, aber auch nur einzelnen Bereiche oder Prozesse. Im zweiten Teil werden dann bspw. die Prozesse, IT-Systeme, Programme, Netzwerkelemente und Räumlichkeiten erfasst und gruppiert und zusammen mit ihren Kerneigenschaften und dem Schutzbedarf dokumentiert. Daraus ergibt sich eine solide Basis, die für weitere Schritte zur Verfügung steht, aber auch ständig erneuert werden muss.

Verantwortlichkeiten und Organisation Die drei Standards fordern die Übernahme der Hauptverantwortung von der obersten Leitung, bzw. von der Geschäftsführung. Gleichwohl räumen sie dieser die Möglichkeit zur Delegation von Aufgaben ein. Die Einführung einer / eines ISB wird empfohlen. Die Person, die diese Aufgabe wahrnimmt, dient als Vermittler:in zwischen der Geschäftsführung und den restlichen Verantwortlichen und steht darüber hinaus beratend der Geschäftsführung und informativ und aufklärend der Belegschaft zur Seite. Um eine praxisnahe Umsetzung zu bewirken, wird ebenso angeraten die Einführung und Betreuung der Umsetzung von Maßnahmen an bestimmte verantwortliche Personen, wie bspw. der Teamleitung zu übertragen. Wichtig ist zudem, dass die IT-Sicherheit mit der Unternehmenskultur einhergeht und dadurch die Akzeptanz und effektive Umsetzung begünstigt wird. Insbesondere durch das Vorleben der IT-Sicherheit durch leitende Personen wird dieses Vorhaben maßgeblich mitbestimmt.

Technische und organisatorische Maßnahmen Der Sinn und Zweck eines ISMS ist es, die Informationssicherheit im Unternehmen zu verbessern. Die drei vorliegenden Normen verbessern die IT-Sicherheit schlussendlich mittels Maßnahmen. Die IT-Systeme werden dabei mittels technischer Maßnahmen unterstützt. Den Umfang bestimmt dabei der Schutzbedarf der Systeme. Die drei Standards sind sich in der Anzahl der empfohlenen Kategorien uneins. Die ISO / IEC empfiehlt eine angemessene Anzahl, das BSI drei und der VdS zwei Kategorien. Die Maßnahmen umfassen bspw. eine Protokollierung von Zugängen und Zugriffen bei IT-Systemen oder die Umsetzung von Firewalls zum Schutz des internen Netzwerks. Nebst den technischen müssen organisatorische Maßnahmen umgesetzt werden. Diese umfassen bspw. die Definition und Dokumentation von Prozessen, wie der Umgang mit Benutzerkonten nach dem Ausschied oder die Einführung und regelmäßige Durchführung von Schulungs- und Sensibilisierungsmaßnahmen. Beide Maßnahmenarten sind entscheidend für den Erfolg eines ISMS.

Risikoanalyse und -behandlung Eine weitere Übereinstimmung in den Standards zeigt sich im Umgang mit dem Risiko. Überschreitet der Schutzbedarf eine bestimmte Grenze oder zählen die betrachteten Assets zu den kritischen Komponenten, muss die Risikoanalyse und -behandlung durchgeführt werden, um den speziellen Anforderungen nachzukommen.

Kontinuierlicher Prozess Keine der drei Ausführungen verspricht ein abgeschlossenes und vollendetes ISMS nach dem Abarbeiten der Anforderungen. Sind die Anforderungen erfüllt, ist viel mehr das Konstrukt erstellt, dass im weiteren

Verlauf kritisiert, angepasst und verbessert werden muss. Am Anfang vermehrt und im weiteren Verlauf weniger werden diese Änderungen durch noch nicht umgesetzte Maßnahmen notwendig. Doch auch durch den Wandel des Unternehmens, der internen Strukturen oder durch neue äußere Einflüsse in Form von Gesetzen oder Kund:innenanforderungen muss das ISMS ständig überarbeitet werden. Hinzu kommt, dass der Stand der Technik bei den System etabliert sein sollte, so dass eben auch diese Entwicklungen zum ständigen Anpassen der Systeme führt. Somit kann der aktuelle Zustand eines ISMS stets nur als vorübergehend tauglich aber niemals als vollendet angesehen werden.

3.2 Das konzeptionell überarbeitete ISMS

Nachdem im Kapitel 2.2 drei weitverbreitete Standards zusammengefasst und deren Gemeinsamkeiten im Kapitel zuvor erfasst wurden, gilt es nun die Essenz dieser mit Verbesserungsvorschlägen anzureichern, um so ein konzeptuell überarbeitetes ISMS zu erstellen, dass dann im Anschluss anhand einer Praxisumsetzung auf Realisierbarkeit und Praxistauglichkeit geprüft wird. Dabei wird zunächst der vorgeschlagene Aufbau erläutert, dem sich die Erklärung der einzelnen Komponenten anschließt. Abschließend wird das Phasenmodell vorgestellt.

3.2.1 Der Aufbau

Ein ISMS besteht in allen drei Standards aus einem kontinuierlich voran schreitenden Prozess, der den Stand der IT-Sicherheit und die Anforderungen im Unternehmen erfasst und durch die Einführung von technischen und organisatorischen Maßnahmen zur Verbesserung der IT-Sicherheit beiträgt. Das Bild 3.1

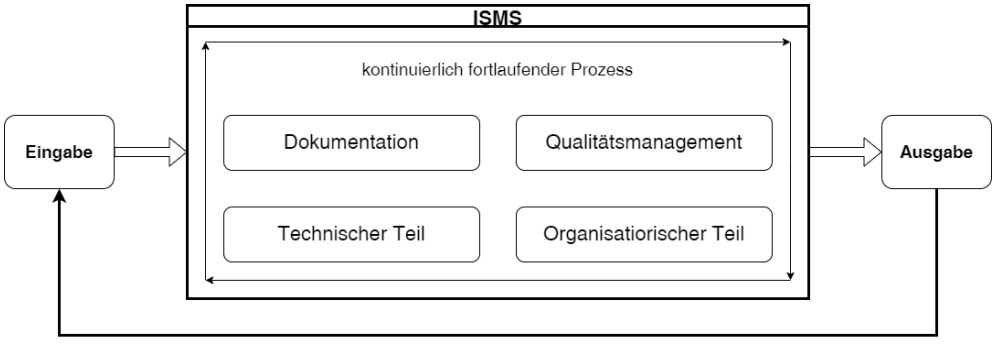

Bild 3.1: Aufbau ISMS[1]

stellt den grundsätzlichen Aufbau des ISMS dar. Durch den Input kommen stets

[1] Selbsterstellte Grafik

neue Anforderungen und die Ausgabe aus dem letzten Durchlauf hinzu, wodurch sich das ISMS in einem ständigen Wandel befindet und kein statisches Konstrukt darstellt. Dieser Anforderung wird durch den kontinuierlich fortlaufenden Prozess Rechnung getragen, der sich im Inneren des ISMS vollzieht. Dabei werden die Anforderungen und der aktuelle Stand mit einander im Qualitätsmanagement abgeglichen und resultieren ggf. in einer Anpassung oder Ergänzung der technischen und organisatorischen Maßnahmen. Um den Prozess in kontrollierte Bahnen zu lenken, müssen Verantwortungen definiert und Stellen besetzt werden, was unter anderem in dem organisatorischen Teil des ISMS fällt. Der technische Teil des ISMS erstreckt sich unter anderem über die Inventarisierung der IT-Systeme und das Anwenden von technischen Maßnahmen im Anwendungsbereich. Um einen übersichtlichen und nachvollziehbaren Überblick über das ISMS zu erhalten, werden bspw. die einzelnen Prozesse, Festlegungen und Entscheidungen dokumentiert. Die Form und der Inhalt der Dokumentation, wird im Teil Dokumentation festgelegt. Das ISMS verfolgt keinen Selbstzweck, sondern begegnet Anforderungen mit Lösungen und Umsetzungen, die zur Generierung eines Outputs führen. Wenngleich im Folgenden die einzelnen Bestandteile eines ISMS getrennt beschrieben und dargelegt werden, ergeben sich doch oft Überschneidungen insbesondere mit dem Kernbestandteil Dokumentation.

Die Eingabe

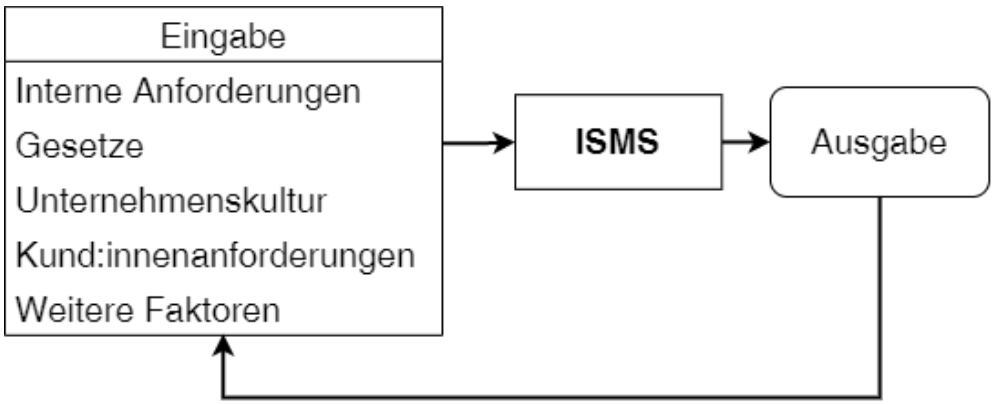

Bild 3.2: Bestandteile der Eingabe[2]

Das ISMS muss so gebaut sein, dass es auf spontane wie auch längerfristige Entwicklungen reagieren kann. Durch den Input aus verschiedenen Quellen kann es dazu kommen, dass zuvor getroffenen Maßnahmen als obsolet oder unzureichend eingeschätzt, oder neue Maßnahmen eingeführt werden müssen. Beispiele

[2]Selbsterstellte Grafik

der verschiedenen Quellen werden nachfolgend beschrieben. Die Quellen wie auch die Einreihung der Eingabe in den Prozess wurden in dem Bild 3.2 dargestellt.
Ein großer Teil der Anforderungen, die auf ein ISMS eintreffen können, werden aus dem Unternehmen selbst stammen. Dies umfasst bspw. die Architektur von Unternehmensflächen, die technische Ausstattung des Unternehmens oder die finanziellen und personellen Ressourcen. Um die erfolgreiche Umsetzung eines ISMS auch längerfristig zu ermöglichen, sollten eben diese Anforderungen stets in die Weiterentwicklung des ISMS mit einfließen, sodass es zu keinen Engpässen oder der Umsetzung unangemessener Maßnahmen kommt.
Jedes Unternehmen steht unter dem Druck **Gesetze und Regularien** wie bspw. die Rechte von Kund:innen oder den Datenschutz zu berücksichtigen und wahrzunehmen. Ein Verstoß kann einen beträchtlichen finanziellen, wie auch Ruf schädigenden Schaden nach sich ziehen. Daher ist es ratsam eine juristische Betrachtung und Bewertung in den Entwicklungsprozess mit einzubeziehen.
Die Unternehmenskultur ist die „Grundgesamtheit gemeinsamer Werte, Normen und Einstellungen, welche die Entscheidungen, die Handlungen und das Verhalten der Organisationsmitglieder prägen.“[3]. Um die Akzeptanz des ISMS zu erhöhen und die Mitarbeiter:innen nicht vor einem Bruch mit ihrem gewohnten Umfeld zu stellen, muss die Unternehmenskultur als relevanter Faktor mit einbezogen werden. Diese kann sich auch zum Beispiel durch die Expansion des Unternehmens wandeln und sollte daher stets neu bewertet werden.
Um am Markt bestehen zu können, muss sich ein Unternehmen stets um neue Aufträge und das Pflegen von bestehenden Kund:innenbeziehungen bemühen. Dies kann dazu führen, dass die (potentiellen) Kunden:innen mit Forderungen im Zusammenhang mit IT-Sicherheit an das Unternehmen herantreten, um so die eigenen IT-Systeme vor Schaden zu bewahren. Dementsprechend können **Kunden:innenanforderungen** als einflussreicher Input bewertet werden und in der Einführung oder Durchsetzung von Maßnahmen resultieren. Gleichwohl sollte das Unternehmen hierbei stets die anderen Faktoren, wie Unternehmenskultur und interne Anforderungen, mit in die Betrachtung einbeziehen.
Wie bereits erwähnt, ist das ISMS ein kontinuierlicher Prozess, der stets wiederholt wird. Am Ende eines Durchlaufs wird eine Ausgabe erzeugt, die im Kapitel 3.2.1 näher thematisiert wird. **Die Ausgabe** kann Einfluss auf den nächsten Durchlauf nehmen und fließt daher in die Eingabe mit ein. Bspw. können unzureichende Schutzmaßnahmen festgestellt worden sein, die im nächsten Durchlauf erst verbessert werden und folglich als Verbesserungsmöglichkeit einfließen.
Abseits dessen seien hier noch weitere unbestimmte Faktoren angegeben, die nicht

[3] Lie18.

in die vorherigen Kategorien fallen. Dazu zählen bspw. Entwicklungen der Gesellschaft oder Entwicklungen, die durch neue oder vorangetriebene Technologien entstehen. Das Unternehmen und die Verantwortlichen sollten diese Entwicklungen soweit möglich verfolgen und entsprechend der Relevanz in den Prozess einfließen lassen.

Der organisatorische Teil

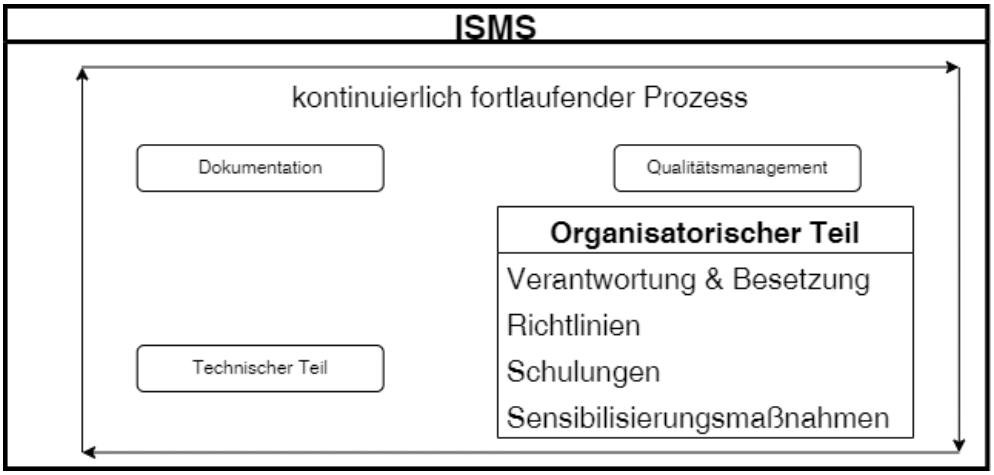

Bild 3.3: Bestandteile des organisatorischen Teils[4]

Die Betrachtung der Standards im Kapitel 2.2 machte deutlich, dass ein großer Teil des Erfolgs und der Tauglichkeit eines ISMS von der Organisation abhängt. Es müssen Verantwortlichkeiten definiert, Stellen besetzt, Prozesse festgelegt und weitere organisatorische Maßnahmen, wie bspw. Schulungen und Sensibilisierungsmaßnahmen, eingeführt und weiterentwickelt werden. Das Bild 3.3 stellt die wichtigsten Kernelemente des organisatorischen Teils dar, die nachfolgend beschrieben werden.

Die Verantwortung für die IT-Sicherheit muss von der Geschäftsführung übernommen werden. Dies stellt den initialen Schritt zum Erstellen des ISMS dar. Durch das offizielle Bekenntnis muss die Führung geeignete Maßnahmen ergreifen, um die Sicherheit der Informationen im Unternehmen zu gewährleisten. Dabei muss sie finanzielle und personelle Ressourcen für das Vorhaben zur Verfügung stellen. Diese Ressourcen werden durch interne und / oder externe Mitarbeiter:innen genutzt, um das ISMS zu betreiben, zu warten und weiter zu entwickeln. Der aktuelle Stand der IT-Sicherheit sollte in regelmäßigen Berichten an die Geschäftsführung kommuniziert werden. Die Geschäftsführung sollte ein Team abstellen, dass die Einführung und Pflege des ISMS aber auch die Berichterstat-

[4]Selbsterstellte Grafik

tung übernimmt. Gleichwohl ist auch die Delegation der Aufgabe auf eine Person, wie der / dem ISB, möglich, dem die Unterstützung von Mitarbeiter:innen des Unternehmens eingeräumt wird. Die Aufgabe des Teams, bzw. der / des ISB, ist es, die IT-Sicherheit im Unternehmen zu strukturieren und fortlaufend sicherzustellen und zu verbessern, indem sie den IST-Zustand bspw. durch interne Audits erfassen und ggf. durch die Einführung von geeigneten Maßnahmen verbessern. Weiterhin stehen die Beauftragten für Auskünfte zur IT-Sicherheit und den Meldungen von Sicherheitsvorfällen zur Verfügung und koordinieren bei letzteren das weitere Vorgehen. Um angemessene und praxistaugliche Maßnahmen zu erstellen und umzusetzen, können die Beauftragten die Maßnahmen mit Vertreter:innen der betroffene Bereiche abstimmen und diese an sie übergeben. Es bietet sich an, dauerhafte Besetzungen für diese Prozesse in den Bereichen festzulegen.
Ein weiterer wichtiger Punkt bei der Sicherung der IT-Sicherheit sind **die Richtlinien**. Richtlinien legen im Generellen den Umgang mit IT-Sicherheit im Unternehmen fest. Sie können sich bspw. auf den Umgang mit mobilen Endgeräte beziehen aber auch auf das Verhalten bei einem Besuch von externen Personen. Die Geschäftsführung muss die Richtlinien wirksam machen und auf die Konsequenzen bei nicht Einhaltung hinweisen. Die Richtlinien müssen in verständlicher Form für alle Mitarbeiter:innen zugänglich gemacht werden. Um die Verständlichkeit zu begünstigen sollten sie über die klare Handlungsanweisung hinaus auch einen erklärenden Anteil beinhalten, der das Sicherheitsziel beschreibt. Durch eine kontinuierliche Überprüfung und ggf. der Anpassung der Richtlinien wird zeitgemäße Tauglichkeit sichergestellt. Das Unternehmen sollte für alle notwendigen Handlungsanweisungen kategorisch getrennte Richtlinien erstellen. Über vertraute Kanäle sollten die Mitarbeiter:innen über Änderungen an Richtlinien oder neu verabschiedete Richtlinien informiert werden.
Schulungen stellen eine interaktive Möglichkeit zur Wissensaneignung der Mitarbeiter:innen dar. Hierbei wird von externem oder auch internem Schulungspersonal auf wichtige Punkte im Bezug auf Informationssicherheit hingewiesen. Ein Teil der Schulungen verarbeitet das Wissen aus den Richtlinien für die Teilnehmer:innen und offeriert damit auch die Möglichkeit Fragen im direkten Austausch zu klären. Gleichwohl bietet diese Form der Schulung aber auch die Möglichkeit die Verständlichkeit des Inhalts der Richtlinie zu hinterfragen und Verbesserungspotential aufzudecken. Die Schulungen sollten mit einer Bewertung des Kurses und einer Feedback-Runde enden, um so kontinuierlich an der Verbesserung des Kurses mit zu wirken und die Akzeptanz zu erhöhen. Darüber hinaus sollte das Unternehmen Ressourcen für die Verantwortlichen zur Verfügung stellen, damit diese sich auch extern weiterbilden können. Der Kerngedanke von **Sensibilisie-**

rungsmaßnahmen ist, durch kontinuierliches Einwirken die Mitarbeiter:innen zu sensibilisieren, sodass diese reflektierter agieren und somit bestimmte Angriffsarten nicht funktionieren. Dabei müssen die Mitarbeitenden über die bestehenden Gefahren aufgeklärt und und über wirksame Gegenmaßnahmen informiert werden. Dies kann durch Workshops im interaktiven Rahmen, durch Schulungen oder durch fortlaufendes Informieren auf den vertrauten Kanälen bewirkt werden. Bei den Maßnahmen sollte stets die Verständlichkeit und die Kommunikationsbereitschaft im Vordergrund stehen, sodass sich die Mitarbeiter:innen abgeholt fühlen und im Falle eines Vorfalls auch vertrauensvoll an die Verantwortlichen wenden.

Der technische Teil

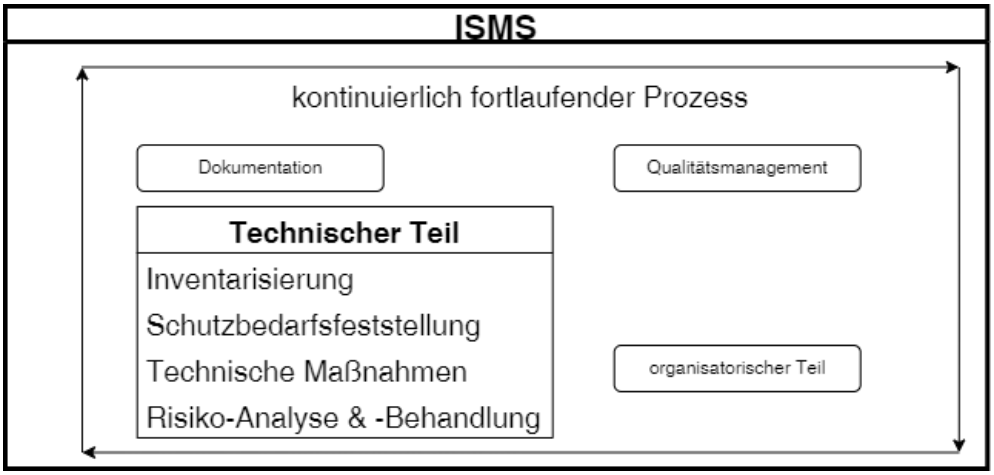

Bild 3.4: Bestandteile des technischen Teils[5]

Viele der notwendigen Maßnahmen müssen und können maschinell umgesetzt werden. Das Bild 3.4 zeigt die Einordnung des technischen Teils im Gesamtbild und mit seinen Bestandteilen.
Um einen angemessenen Schutz der Informationen auf technischer Seite zu ermöglichen, muss **das Inventar** erstellt werden. Dieses sollte die Komponenten der Firma wieder spiegeln. Dabei geht es darum, eine Übersicht der IT-Systeme und deren Abhängigkeit zu erstellen. Technische Komponenten, die eine gleiche Konfiguration und Verwendung aufweisen, sollten dabei zweckdienlich zusammengefasst werden, um so die Übersichtlichkeit zu bewahren und einen angemessenen Detailgrad abzubilden. Wenngleich initial ein generelles Schutzniveau - oder auch ein Basisschutz nach BSI 200-2[6] - angesetzt werden sollte, muss eine Unterscheidung der Komponenten stattfinden, wozu sich ein Top-Down- oder Button-

[5]Selbsterstellte Grafik
[6]Vgl. BSI17b, S. 29.

Up-Ansatz anbietet, wie es im BSI 200-2[7] in der Strukturanalyse beschrieben wird. Das Inventar sollte die Bezeichnung der Komponente oder der Gruppe, die Verwendung und die Abhängigkeit zu anderen Komponenten und die angesetzte Kritikalität wiederspiegeln. Anhand der Kritikalität kann dann der Schutzbedarf festgelegt werden.
Um einen adäquaten Schutz für die IT-Systeme zu etablieren, ist es notwendig deren **Schutzbedarf festzulegen**. Dafür werden die Konsequenzen einer Kompromittierung eines Assets anhand der von der Geschäftsführung festgelegten Kriterien aus dem Qualitätsmanagement eingeordnet. Eine zweistufige Einordnung gilt hierbei als Mindestanforderung. Im Generellen sollte zwischen schutzbedürftigen Assets und kritischen schutzbedürftigen Assets unterschieden werden.
Wenn die Inventarisierung abgeschlossen ist, kann die Einschätzung und Umsetzung von **technischen Maßnahmen** erfolgen. Dabei werden entsprechend des Schutzbedarfs des Assets geeignete Maßnahmen ausgewählt und ggf. umgesetzt. Die Maßnahmen sollten sich am Stand der Technik orientieren, weshalb sich das IT-Grundschutzkompendium[8] des BSIs als solide Informationsbasis anbietet. Sollten Maßnahmen nicht oder teilweise umgesetzt werden, muss dies dokumentiert und begründet werden. Es ist zunächst ein solider Basisschutz zu etablieren, der die absolut notwendigen und grundlegenden Maßnahmen auf den IT-Systemen vorsieht und dann in weiteren Durchläufen weiter ausgebaut wird. Somit verteilt sich bspw. die Last der Umsetzung einer Standardabsicherung nach BSI 200-2[9] auf mehrere Iterationen, wobei zugleich die IT-Sicherheit stetig steigt.
Eine **Risiko-Analyse und -Behandlung** sollte immer dann zum Einsatz kommen, wenn die IT-Systeme nicht mit den vorhandenen Elementen des Grundschutzkompendium abzubilden sind oder die Assets in einer untypischen Umgebung genutzt werden. Hierbei ist die Vorarbeit des BSI in Form der Bausteine als unzureichend zu bewerten und somit eine ergänzende oder neue Analyse durchzuführen. Als Vorgehensweise sollte auf die erprobte Methodik aus dem BSI Standard 200-3[10] zurückgegriffen werden.

Das Qualitätsmanagement

Das ISMS ist durch äußere Einflüsse oder durch interne Entwicklungen einem ständigen Wandel unterworfen. Das Qualitätsmanagement fasst die Transformation in den Fokus und hat die Aufgabe die Tauglichkeit und die Angemessenheit der Maßnahmen zur Steigerung der IT-Sicherheit im Unternehmen zu bewerten

[7] Vgl. BSI17b, S. 78 ff.
[8] BSI22.
[9] Mehr hierzu unter BSI17b, S. 76 ff.
[10] Mehr dazu in BSI17c.

und zu kritisieren.

Bei der **Bewertung der Ausgangslage** durch die Geschäftsführung werden

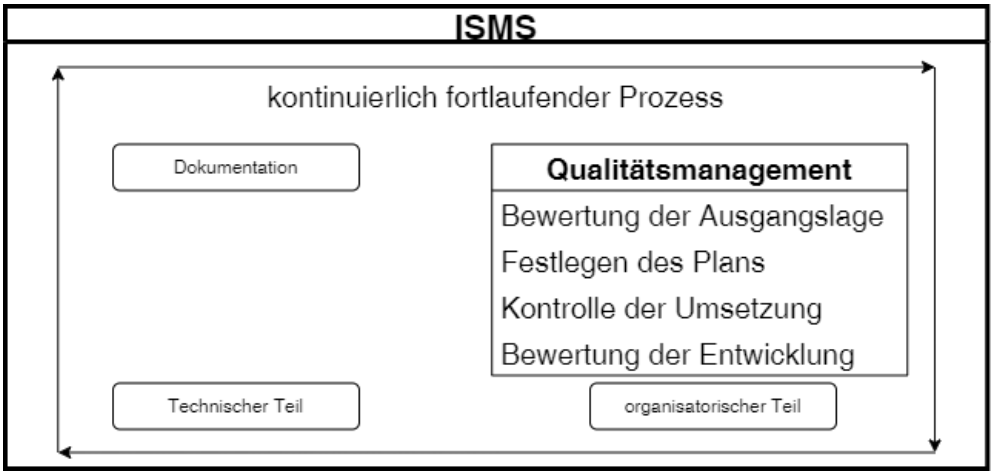

Bild 3.5: Bestandteile des Qualitätsmanagement[11]

der Anwendungsbereich und wichtige Kriterien für die Einschätzung des Schutzbedarfs von Assets festgelegt. Zur Erstellung der Kriterien, bzw. zur Definition der Kategorien, empfiehlt sich der BSI Standard 200-2[12]. Zusätzlich müssen alle relevanten Faktoren für das ISMS ermittelt und geprüft werden. Bei nachfolgenden Durchläufen muss der Stand des ISMS mit den neuen oder geänderten Anforderungen abgeglichen werden.

Nach der initialen oder erneuten Bewertung der Ausgangslage muss im Anschluss das **Festlegen des Plans** für den Durchlauf erfolgen. Dabei werden die Aktualität der Strukturanalyse geprüft und ggf. Anpassungen vorgenommen. Infolge dessen muss auch der Schutzbedarf der Assets geprüft werden. Am Ende entsteht eine Liste mit umzusetzenden Maßnahmen. Diese gilt es in einem reflektierten Plan zu überführen, wobei die zur Verfügung stehenden Ressourcen berücksichtigt werden müssen. Im Plan wird festgehalten, welche Maßnahmen im derzeitigen Durchlauf umgesetzt werden sollen und welche begründet nicht oder später umgesetzt werden.

Ist der Plan ausgeführt, erfolgt die **Kontrolle der Umsetzung** und die Dokumentation. Es kann durch Umstände dazukommen, dass angedachte Maßnahmen nicht umgesetzt wurden, sodass diese in einem späteren Durchlauf erneut einfließen müssen. Gleichwohl kann sich bei der Umsetzung zeigen, dass die abgeschätzte Paxistauglichkeit nicht gegeben ist und somit auf die Umsetzung verzichtet wird. Dies gilt es zu Dokumentieren, um die Entscheidung in späteren Durchläufen ver-

[11] Selbsterstellte Grafik

[12] Mehr zur Schutzbedarfsfestellung, bzw. Definition der Schutzbedarfskategorieren in BSI17b, S. 104.

ständlich zu halten und ggf. auch neu bewerten zu können.
Ein Kernargument für die Einführung und Verwendung eines ISMS ist, dass die IT-Sicherheit im Unternehmen messbar wird. Die **Bewertung der Entwicklung** obliegt dem Qualitätsmanagement, dass durch interne Audits die Erfüllung der Anforderungen an das ISMS überprüft. Im Bezug auf das ISMS können dabei Messwerte, wie das Einhalten zur Verfügung gestellter Ressourcen, aber auch die Anzahl von nicht, teilweise oder komplett umgesetzten Maßnahmen herangezogen werden. Auch die Anzahl an Verstößen gegen in Richtlinien festgelegte Handlungsanweisung stellen wichtige Werte dar. Zusätzlich sollten auch die Rückmeldungen aus dem Unternehmens in Form von Kritiken der Mitarbeiter:innen oder Kund:innen verwertet werden. Diese, wie auch die Verstöße, bieten das Potential die Akzeptanz und das Verständnis durch Anpassungen oder Ergänzungen zu erhöhen, was sich wiederum begünstigend auf die IT-Sicherheit im Unternehmen auswirkt. Nicht zuletzt stellt die Anzahl Sicherheitsvorfälle oder Ausfälle von Diensten einen Vergleichswert für die Bewertung der Effektivität des ISMS dar. Die Auswertung sollte stets kritisch erfolgen und in einer konstruktiven Auseinandersetzung mit den bereits etablierten Einschätzungen und Maßnahmen münden. Abschließend sollte regelmäßig ein Bericht an die Geschäftsführung erfolgen.

Die Dokumentation

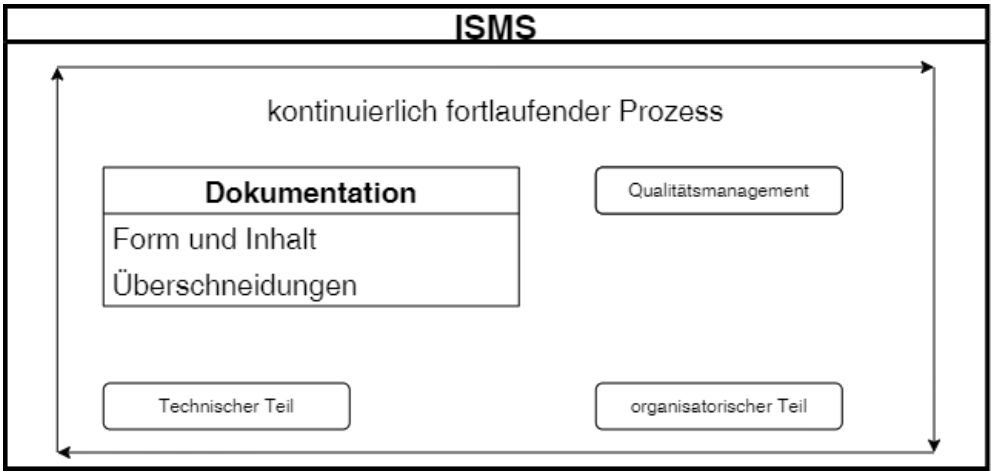

Bild 3.6: Bestandteile der Dokumentation[13]

Die Dokumentation bildet das Gerüst und das Fundament des ISMS. In ihr werden sämtliche Entscheidungen, Festlegungen, Definitionen und Richtlinien hinterlegt. Dies dient zum Einen der Nachvollziehbarkeit, damit zu einem späteren Zeitpunkt getroffene Entscheidungen verständlich bleiben. Zum Anderen ist diese

[13]Selbsterstellte Grafik

aber auch für Zertifizierungen essentiell.

Die Form der Dokumentation variiert je nach Bereich, in dem diese angefertigt und verwendet wird. Dennoch sollten alle Dokumentationsanteile übersichtlich arrangiert werden, so dass der Zugriff auf die benötigten Informationen jeder Zeit schnell erfolgen kann. Grundsätzlich sollte die Dokumentation die notwendigen Sachverhalte beinhalten. Dabei ist die Übersichtlichkeit und der Aufwand wie auch der Mehrwert zu berücksichtigen.

Die Dokumentation zieht sich durch alle anderen Bereiche und sorgt damit für eine **Überschneidung** mit bereits vorhandenen Informationen. Im organisatorischen Teil müssen bspw. die Inhalte der Schulungen, die Regelmäßigkeit und die Teilnehmer:innen dokumentiert werden. Im technischen Bereich müssen bspw. die IT-Systeme in Form des Inventars und die Umsetzung der Maßnahmen dokumentiert werden. Im Qualitätsmanagement müssen bspw. die Entscheidungen der Geschäftsführung für die Schutzkriterien, der Plan für den nächsten Durchlauf oder der aktuelle Stand und die Vorfälle dokumentiert werden. Eine Dokumentation im ISMS erfüllt oft über den Zweck des Festhaltens von Sachverhalten und Entwicklungen hinaus weitere Aufgaben. Um überflüssige Aufwände zu sparen, ist es wichtig, bereits aufgearbeitete und vorhandene Informationen für die Dokumentation zu nutzen.

Die Ausgabe

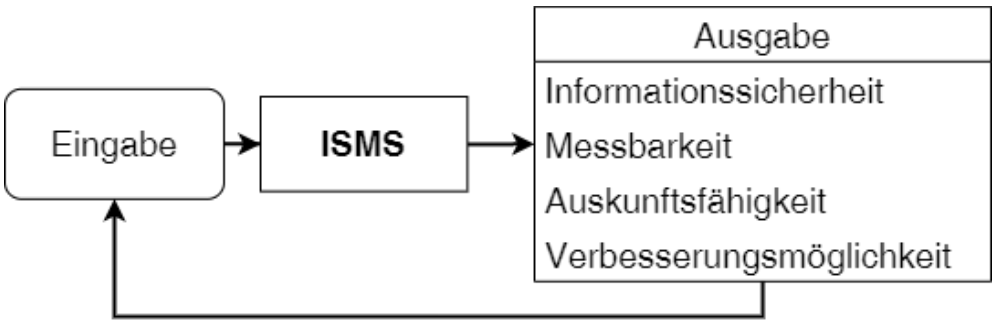

Bild 3.7: Bestandteile der Ausgabe[14]

Ein Durchlauf bei einem ISMS endet mit der Ausgabe, bevor es bei der Eingabe erneut startet. In der Ausgabe werden Werte erzeugt, die für das Unternehmen zweckdienlich sind oder zumindest Potential besitzen in weiteren Durchläufen zweckdienliche Werte zu erzeugen.

[14]Selbsterstellte Grafik

Der Sinn und Zweck eines ISMS ist es, **Informationssicherheit** für ein Unternehmen messbar und wirksam umzusetzen. In der ersten Iteration wird ein Basisschutz angestrebt und die notwendigen Maßnahmen werden umgesetzt, sodass dies bereits zur flächendeckenden Steigerung der IS führt. In weiteren Iterationen wird dann durch die Schutzbedarfsfeststellung ein Bedarf für die Assets festgelegt und entsprechende weiterführende Maßnahmen appliziert. Zusätzlich werden besondere IT-Systeme durch die Risikoanalyse und -behandlung speziell betrachtet und mit angepassten Maßnahmen abgesichert. Durch diese dreistufige Entwicklung, die in weiteren Iteration reflektiert, kritisiert und ggf. angepasst wird, steigt die Informationssicherheit kontinuierlich an.
Wie bereits weiter oben angeführt, resultiert die Etablierung eines ISMS in der **Messbarkeit** von IS. Wenn diese zuvor mit bestem Wissen und Gewissen umgesetzt wurde, verfolgt das ISMS einen strukturierten Ansatz. Durch die Dokumentation des Umsetzungszustands von Maßnahmen wird bereits eine breite Datenbasis angelegt. Dies fördert die bereits zuvor erwähnten Messwerte hervor, die das Umsetzungslevel, bzw, Umsetzungsverhältnis des ISMS anzeigen. Durch das Einführen von Maßnahmen wie dem Monitoring von IT-Systemen oder dem Bewerten von Schulungen, werden weitere Messwerte erzeugt. Ersteres ermöglicht das Nachvollziehen der Verfügbarkeit von den Diensten. Letzteres gibt Einblick in die Akzeptanz der Veranstaltung und dem Verbesserungspotential. Zuletzt sei noch die Dokumentation von Sicherheitsvorfällen erwähnt, deren Anzahl ebenso als Messwert für die IT-Sicherheit herangezogen werden kann.
Wie eingehens im Kapitel 1.2 beschrieben, verlangen immer mehr Auftraggeber:innen eine Auskunft zur IT-Sicherheit im Unternehmen. Die Umsetzung des ISMS begünstigt die **Auskunftsfähigkeit** und die Beantwortung der Fragenkataloge, da diverse Maßnahmen, wie bspw. die Formulierung eines Disaster Recovery Plan (DRP), eingeführt wurden. Darüber hinaus bietet ein ausgebautes ISMS die Möglichkeit zur Zertifizierung, die dann wiederum Kund:innen zur Verfügung gestellt werden kann.
Am Ende eines jeden Durchlaufs steht eine Übersicht mit Maßnahmen. Nicht oder nur teilweise umgesetzte Maßnahmen stellen ein **Verbesserungspotential** dar und sollten im darauffolgenden Zyklus wieder mit aufgenommen werden. Gleichwohl gilt es aber auch, umgesetzte Maßnahmen ggf. neu zu beurteilen. Abseits dessen wurden im Durchlauf auch Erfahrungen gesammelt. Ähnlich einer Retrospektive aus dem Projektmanagement-Framework SCRUM[15], sollte die Arbeit am Durchlauf von allen Akteur:innen kritisch beurteilt und reflektiert werden, um so die gewonnenen Erfahrung im nächsten Durchlauf mit einbringen zu können.

[15]Mehr dazu unter: https://www.scrum.org/resources/what-is-scrum

3.2.2 Die Phasen des ISMS

Die drei Normen stellen das ISMS als ein sich stets im Ausbau und in der Verbesserung befindendes Konstrukt dar. Doch wenngleich dieses den Handlungsspielraum für ein unvollständiges Konstrukt nach dem ersten Durchlauf bietet, wird es nicht ausgeführt. Viel mehr werden die Anwender:innen mit einer Reihe von Aufgaben überfrachtet und finden ein vermeintlich enttäuschendes Resultat vor. Insbesondere beim initialen Durchlauf kann dies zu unbefriedigenden Ergebnissen führen, die erst in weiteren Durchläufen ausgeglichen werden. Daher erscheint es zweckdienlich den Aufbau, die Umsetzung und die Wartung eines ISMS in Phasen einzuteilen, die jeweils eigene Ziele verfolgen. Durch diese Einteilung entsteht zum einen ein aussagekräftigeres Bild vom Zustand des ISMS und zum anderen können Projektplanungen genauer erfolgen. Es sei an dieser Stelle angemerkt, dass der BSI mit der IT-Grundschutzmethodik eine Vorgehensweise vorschlägt, die jedoch generalisiert ist und auf alle Iterationen angewendet wird. Im Folgenden sollen daher die Phasen des überarbeiteten ISMS vorgestellt werden.

Phase I: Initialisierung des Prozesses

In der ersten Phase wird das ISMS initialisiert. Wie bereits weiter oben ausgeführt, erfolgt der initiale Schritt durch die Übernahme der Verantwortung für IT-Sicherheit im Unternehmen von Seiten der Geschäftsführung. Dies bewirkt, dass nun Prozesse, Maßnahmen und Verantwortlichkeiten festgelegt werden müssen und somit das ISMS eingeführt wird.
Die Geschäftsführung sollte als ersten Schritt eine Person als ISB bestellen. Dies kann eine geeignete interne oder externe Person sein. Wenn die Komplexität des Unternehmens durch eine:n ISB allein nicht verwaltbar ist, sollte mindestens eine weitere Fachkraft zur Unterstützung beschäftigt werden. Gemeinsam bilden diese beiden Stellen das IS-Management-Team. Gleichwohl sollten in den einzelnen Abteilungen des Unternehmens Personen bestimmt werden, die das IS-Management-Team bei der Einführung und Umsetzung von Maßnahmen unterstützen.
Sind die Verantwortlichkeiten festgelegt und das IS-Management-Team[16] bestellt, müssen die Rahmenbedingungen festgelegt werden. Dabei gilt es, zum einen den Anwendungsbereich zu definieren und zum anderen die Anzahl an Schutzbedarfskategorien festzulegen. Der Anwendungsbereich kann auch für den Start enger gefasst werden, sollte dann aber bei darauffolgenden Iterationen auf weitere Bereiche ausgedehnt werden. Die Ausweitung bleibt aus, wenn das Unternehmen bspw. einer Kernabsicherung anstrebt und nur bestimmte Teile oder Prozesse

[16] Im weiteren Verlauf wird nur noch das IS-Management-Team benannt, womit gleichsam der oder die ISB gemeint ist, wenn kein Team einberufen wurde.

absichern möchte. Gleiches gilt für die Festlegung der Kategorien. Anfänglich sollten mindestens zwei Kategorien definiert werden, wie es auch die VDS 10000 ausführt, sodass zwischen normalem und kritischem Schutzbedarf unterschieden werden kann.
Die Prozesse und Festlegungen sind zu dokumentieren und vor jedem folgenden Durchlauf zu prüfen. Am Ende der ersten Phase steht der organisatorische Rahmen für die weitere Bearbeitung und die Verantwortlichkeiten sind festgelegt.

Phase II: Erfassung des IST-Zustands

Das Hauptziel der zweiten Phase ist die Erhebung des IST-Zustands. Der IST-Zustand besteht aus den Bestandteilen der Eingabe, den Kernprozessen und Anwendungen, den IT-Systemen und den bereits vorhandenen organisatorischen und technischen Maßnahmen im definierten Anwendungsbereich.
Damit die Entwicklung des ISMS nicht am Unternehmen vorbei geht und damit ein angemessener Schutzbedarf eingeschätzt werden kann, müssen die Bestandteile der Eingabe erfasst werden. Die gesammelten Daten werden bei der weiteren Bearbeitung als Entscheidungsgrundlage genutzt. Beispielsweise hat die Unternehmenskultur maßgeblichen Einfluss auf die IT-Sicherheitsleitlinie und die Anforderungen der Kund:innen. Die Gesetze wirken bei der Abgrenzung der Schutzbedarfskategorien in Form der Schutzszenarien mit.
Anschließend wird die Struktur der Firma erfasst. Es bietet sich an, einen Top-Down-Ansatz zu nutzen. Zweckdienlich ist die Strukturanalyse des BSI Standards 200-2[17]. Damit können relevante Strukturelemente und deren Abhängigkeiten zielgerichtet erfasst werden. Das Resultat dieser Analyse ist eine abstrakte Übersicht des Unternehmens, in dem die Elemente, wie bspw. Räume, Prozesse und IT-Systeme, und deren Abhängigkeiten abgebildet werden.
Zuletzt sollten technische und organisatorische Maßnahmen festgehalten werden. Bei den technischen Maßnahmen sollte auf ein angemessenes Abstraktionsniveau geachtet werden, sodass unnötiger Aufwand beim Sammeln von Detail-Informationen vermieden wird. Bei den organisatorischen Maßnahmen werden bspw. vorhandene Richtlinien, Meldewege oder Schulungsangebote festgehalten.
Am Ende der zweiten Phase ist das Fundament und das Gerüst für die weitere Bearbeitung gelegt. Der Rahmen ist durch die Leitlinie, den Anwendungsbereich und die definierten Schutzbedarfskategorien gegeben und der Bezugsraum liegt durch die Erhebung des IST-Zustands vor.

[17] Mehr dazu in BSI17b, S. 104 ff.

Phase III: Fortlaufende Verbesserung

Nachdem die Vorarbeit geleistet ist, kann der fortlaufende Prozess zur Verbesserung des IST-Zustands umgesetzt werden. Anfangs sollte die Umsetzung des Basisschutzes angestrebt werden und anschließend in weiteren Iterationen durch entsprechende Maßnahmen erweitert werden. Dadurch wird ein Grundniveau an IT-Sicherheit etabliert, das entsprechend den Anforderungen und Entwicklungen ausgebaut wird und somit zu einer kontinuierlich verbesserten Informationssicherheit führt.
Zur Realisierung des Basisschutzes in der ersten Iteration des ISMS, nachdem die ersten beiden Phasen durchlaufen sind, bietet sich die Umsetzung der VDS 10000 als Einstieg an. Durch die eingeführten Richtlinien und umgesetzten Maßnahmen wird das Grundschutzniveau erreicht. Ergänzend sollte die Basisabsicherung des BSI Standard 200-2[18] in Erwägung gezogen werden, die einen verbesserten Grundschutz etabliert. Bei der Einführung der Maßnahmen sollten bereits umgesetzte Maßnahmen aus der Analyse des IST-Zustands berücksichtigt werden. Diese müssen ggf. angepasst oder überarbeitet werden.
In weiteren Iterationen gilt es das etablierte Grundschutzniveau auszubauen. Die Standardabsicherung aus dem BSI Standard 200-2[19] bietet sich für dieses Vorhaben an. Insbesondere die Schutzbedarfsfeststellung, die Modellierung, der IT-Grundschutzcheck und Realisierung der Maßnahmen etablieren ein höheres Schutzniveau, als es die VDS 10000 oder Basisabsicherung ermöglichten. Die Maßnahmen von schutzbedürftigen Objekten aus dem Bereich Basisabsicherung werden mit den Maßnahmen aus dem Bereich Standardabsicherung aus dem IT-Grundschutzkompendium ergänzt. Gleiches gilt auch für schutzbedürftige, kritische Objekte wobei diese auch die Maßnahmen bei erhöhtem Schutzbedarf erhalten. Sollten Assets nicht angemessen modelliert werden können, muss eine Risikoanalyse und -behandlung erfolgen.
Nach den vorangegangen Schritten wurde ein Schutzniveau etabliert, das auf die Firma angepasst ist und dem Stand der Zeit entspricht. Um diesen Zustand beizubehalten, muss eine kontinuierliche Überprüfung stattfinden. Bei dieser werden die Zuständigkeiten, die Einschätzungen der Schutzbedarfskategorien, die Anforderungen, die Prozesse, die Struktur und die etablierten Maßnahmen geprüft und bewertet. Die daraus resultierenden Anpassungen werden erneut umgesetzt und führen zum Aktualisieren des ISMS.

[18] Mehr dazu in BSI17b, s. 61 ff.
[19] Mehr dazu in ebd., S. 76.

3.3 Anforderungen der Firma

[...]

3.4 Vorhandene Vorarbeit

[...]

3.5 Evaluation und Testen geeigneter Softwarelösungen zur Realisierung des ISMS

Nachdem in den vorherigen Kapiteln das überarbeitete ISMS ausgeführt und die Anforderungen und die Vorarbeit der Firma festgehalten wurden, gilt es im Folgenden eine geeignete Softwarelösung auszuwählen. Dabei werden drei Ansätze genauer betrachtet und abschließend eine Empfehlung für das Management ausgestellt.

3.5.1 Vorstellung der Lösungsansätze

Am Markt existiert eine Vielzahl an Softwarelösungen zur Realisierung eines ISMS. Wenngleich sich auch Tabellenkalkulationsprogramme wie Microsoft Excel in Kombination mit Microsoft Word zur Umsetzung einsetzen lassen, bieten Softwarelösungen im Bereich ISMS einen erheblich übersichtlicheren Aufbau und Funktionalitäten, die die Dokumentation des ISMS deutlich vereinfachen. Da dies sowohl in der Einrichtung als auch in der Wartung des ISMS mit einer deutlichen Reduzierung des Aufwands einhergeht, sollte eine Softwarelösung stets bspw. einer Office-Suite vorgezogen werden. Die Tabelle „Vergleich der Softwarelösungen“ im Anhang A.4 stellt eine erste grobe Auswahl des Angebots dar, das bei der Recherche erschlossen wurde. Drei Ansätze wurden anhand folgender Kriterien verglichen: das Herkunftsland der Firma, die Art des Betriebes, unterstützte Standards, die finanziellen Kosten, Möglichkeiten zur Integration in die bestehende Systemlandschaft und die Quellcodeoffenheit, die Flexibilität und der Reifegrad der Software.

SerNet Vernice.

Das Produkt „Verinice.“ ist eine Softwarelösung, die von der deutschen Firma SerNet GmbH[20] entwickelt und 2007 zum ersten Mal veröffentlicht wurde. Seit-

[20] Link: https://verinice.com/

dem wurde die Software kontinuierlich weiterentwickelt, aktualisiert und befindet sich seit Mai 2022 in der Version 1.24.1. Zur Zeit arbeitet die Firma die zweite Generation des Produktes unter des Namen „Verinice.Veo“ als SaaS-Lösung und On-Premise-Lösung aus, bei dem jedoch aktuell nur das Datenschutzmodul verfügbar ist. Das ISMS-Modul wird im Laufe des Jahres 2023 veröffentlicht. Mittels „Verinice.“ lassen sich unter anderem der BSI IT-Grundschutz, ein ISMS nach ISO 27001 und seine Selbstauskunft nach VDA-Vorgaben realisieren[21]. Dabei bietet das Produkte sowohl Hilfestellungen als auch Bausteine zur Realisierung an, die ein manuelles Einpflegen deutlich reduzieren. Zusätzlich arbeitet SerNet GmbH mit dem BSI zusammen. In Folge dessen wurde bspw. das IT-Grundschutz-Kompendium lizenziert, das nun über die Homepage des BSI bezogen und im „Verinice.“ importiert werden kann, sodass die Modellierung der Assets mittels der Bausteine erfolgen kann.

Technische Betrachtung Das Produkt „Verinice.“ steht unter GPLv3 quellcodeoffen zur Verfügung[22]. „Verinice.“ wird als Einzelplatzversion betrieben und kann durch den Erwerb von „Verinice.PRO“ in eine Server-Client-Version umgewandelt werden. Bei der Server-Client-Version wird auf einem CentOS oder Red Hat Enterprise Linux der Server-Teil installiert, der das Server-Modul und das Datenbank-Modul umfasst. Die Datenbank wird mittels PostgreSQL oder Oracle bedient. Auf dem Client wird eine „Vernice.“-Instanz installiert, die über HTTPS mit dem Web-Server der „Verinice.PRO“-Installation kommuniziert. Wird ausschließlich das Produkt „Vernice.“ verwendet, handelt es sich um eine Einzelplatz-Version, bei der der Server-Anteil entfällt und die Datenbank lokal mittels Apache Derby verwaltet wird. Beide Produkte wurden in der Programmiersprache Java umgesetzt und der Client kann unter allen gängigen Betriebssystemen betrieben werden. Zum Import von Daten oder zur Kommunikation mit anderen Systemen steht eine XML- und CSV-Schnittstelle zur Verfügung. Die Systemanforderungen und die Softwarearchitektur können unter [SeroJa] eingesehen werden.

Finanzielle Betrachtung Neben den Kosten für den Aufwand zur Einrichtung und dem Betreiben der Software, bestimmen sich die Kosten aus der gewählten Arbeitsplatzlizenz und den hinzu gebuchten Unterstützungsmodulen. Die Einzelplatzversion „Verinice.“ kann über den Shop von SerNet bezogen werden. Beim Kauf kann zwischen einer Laufzeit von ein, zwei oder drei Jahren entschieden werden. Zusätzlich muss das Betriebssystem des Arbeitsplatzes für die spätere Installation festgelegt werden. Ein nachfolgender Wechsel zu einem anderen Be-

[21] Vgl. SeroJb.
[22] Link: https://github.com/SerNet/verinice

triebssystem ist laut Vertrieb nicht ohne weiteres möglich. Die Lizenzkosten bei einer Laufzeit von einem Jahr liegen bei Brutto 595,00 € und steigen auf bis zu Brutto 1606,50 € bei drei Jahren Laufzeit an. Wird die Laufzeit erhöht, wird bei zwei Jahren Laufzeit ein Rabatt von 5 % und bei drei Jahren Laufzeit ein Rabatt von 10 % gegeben. Das Produkt „Verinice.Pro“ kann über den Shop nicht bezogen werden und muss separat angefragt werden. Zudem vertreibt SerNet über den Shop ergänzende Module, die weitere Inhalte für den Import in das Produkt zur Verfügung stellen. Diese Module unterstützen bei der Arbeit am ISMS und stellen zusätzliche Informationen und Funktionen für die Anwender:innen zur Verfügung. Einige der Module sind kostenfrei erhältlich, wie bspw. das IT-Grundschutz-Kompendium oder der Demodatensatz zum IT-Grundschutz. Andere Module müssten kostenpflichtig erworben werden, wobei auch hier die Laufzeit ausgewählt werden kann. Zur Unterstützung der Anwender:innen bei der Risiko-Analyse oder Risiko-Behandlung und der Umsetzung des Datenschutzes bietet SerNet bspw. das Modul „verinice. Risikokatalog inkl. Datenschutzmodul 3 (ISO/ISM)“ an, das bei einer Laufzeit von einem Jahr für Brutto 1130,50 € erworben werden kann. Wurden bei den Softwarelizenzen noch Rabatte bei einer längeren Laufzeit gegeben, wurden diese bei den überprüften Beispielen nicht festgestellt. Es bleibt anzumerken, dass der Support von SerNet GmbH über ein Support-Budget abgerechnet wird, das im Shop erworben werden kann. Eine Einheit Support-Budget umfasst zehn Stunden Dienstleistungen und kostet Brutto 1666,00 €. Das Budget hat eine Gültigkeit von 24 Monaten und verfällt danach ersatzlos. Zur Umsetzung des überarbeiteten ISMS genügt die Einzelplatzversion „Vernice.“ mit dem Content-Modul „IT-Grundschutz-Kompendium 10.0 Edition 2022“.

Atlassian Confluence und Jira

Das australische Unternehmen Atlassian[23] bietet unter anderem die Projektverwaltungssoftware Jira und das Dokumentationssystem Confluence an. Die Firma ist seit 2002 am Markt und wird international genutzt. Beide Systeme zeichnen sich durch einen hohen Grad an Flexibilität aus, so dass Anpassungen gemäß den Anforderungen der Kund:innen weiterreichend umgesetzt werden können. Atlassian stellt dabei die Kernfunktionalität, bzw. das Gerüst, innerhalb dessen die Anpassungen erfolgen können. Beide Softwarelösungen befinden sich bereits seit längerem im betrachteten Unternehmen im Einsatz, so dass bereits umfangreiches Wissen mit der Software gesammelt werden konnte und durch die Nutzung dieser keine zusätzlichen Lizenzkosten entstehen, sofern keine weiteren Apps be-

[23] Link: https://www.atlassian.com/

nötigt und gekauft werden. Allerdings steht hier die Gefahr des Vendor-Locks im Raum. Atlassian hat die Entwicklung von den Server-Versionen der Produkte, die auch im betrachteten Unternehmen zum Einsatz kommen, eingestellt und fokussiert sich nun ausschließlich auf die Data Center oder Cloud Versionen. Zum 15.02.2024[24] wird der Support für die Server-Versionen auslaufen, so dass hier mit keinen weiteren Updates zu rechnen ist. Das Unternehmen steht dann vor der Wahl die Cloud-Produkte wahrzunehmen oder zu einem anderen Anbieter zu wechseln.

Technische Betrachtung Die Produkte werden innerhalb der betrachteten Firma bereits in der Server-Variante betrieben. Atlassian bietet darüber hinaus eine SaaS-Lösung und eine Datacenter-Version für den On-Premise Betrieb an, die auch in Zukunft weiterhin vom Anbieter unterstützt werden. Zur Zeit verwenden circa 1000 Mitarbeiter:innen und Kund:innen die Produkte, Projekte zu verwalten oder zu dokumentieren. Die Produkte wurde in zwei virtuellen Maschinen installiert. Darüber hinaus existieren Demo-Instanzen der Produkte, die kontinuierlich aktualisiert und für Tests und Einarbeitungen genutzt werden. Beide Produkte wurden in Java geschrieben und verwenden als Datenbankmanagement-System MySql. Das Frontend wird durch den Web-Server Nginx zur Verfügung gestellt, sodass der Dienst über HTTPS angesprochen werden kann. [..] Jira und Confluence können mit einander verbunden werden, was den Workflow der Mitarbeiter:innen unterstützt. Darüber hinaus bieten beide Systeme verschiedene Schnittstellen zur uni- oder bidirektionalen Interaktion mit anderen Systeme an, darunter eine API-Schnittstelle und Import- und Export-Funktionen für bspw. JSON- und CSV-Dateien.

Finanzielle Betrachtung Da das Produkt bereits im Unternehmen genutzt wird, fallen zumindest für die Nutzung der Kerninstanz keine zusätzlichen Kosten an. Nebst der Kern-Instanz bieten Atlassian und andere Unternehmen über den Marketplace[25] eine Vielzahl an zusätzlichen kostenfreien und kostenpflichtigen Apps an. Diese ergänzen den Funktionsumfang und stellen auch Mustervorlagen für bestimmte Prozesse zur Verfügung. Die Automation-App zum Automatisieren von ausgeführten Aktionen im Jira oder die Draw.IO Integration zur Nutzung von Draw.IO im Confluence sind zwei Beispiele aus dem Marketplace. Die Addons können ggf. für zusätzliche Kosten sorgen jedoch auch für eine Reduzierung des Aufwands, bspw. zur Einrichtung und Wartung des ISMS. Als zweckdienliche und unterstützende Applications haben sich die in Tabelle 3.1 aufgelisteten

[24] Mehr dazu unter AtloJc.
[25] Link: https://marketplace.atlassian.com/

Produkte bei der Recherche herausgestellt. Insbesondere das Add-On „Automation for Jira“ kann die Aufwände auch längerfristig reduzieren und wird in der Lite-Version bereits im Unternehmen eingesetzt. Um die Änderungen an Dokumenten im Confluence durch einen definierten Workflow an die Verantwortlichen zur Revision und später zur Kontrolle weiter zuleiten, ist die Erweiterung „Comala Document Management“ hilfreich. Die restlichen aufgeführten Erweiterungen stellen Vorlagen und etablierte Workflows zur Verfügung, sodass die manuelle Erstellung entfällt oder zumindest reduziert wird.

Name / Link	System	Preis	Beschreibung /Funktion
Comala Document Management	Confluence	10000 € / Jahr	Dokumenten-Verwaltung mit Abnahmen- und Review-Funktionen
Automation for Jira	Jira	kostenlos	Automatisierung von wiederkehrenden Tätigkeiten mittels Triggers, Conditions und Actions
ISMS for Confluence	Confluence	auf Anfrage	Space mit individualisierbaren ISMS-Vorlagen nach ISO 27001
Instant 27001 for Confluence	Confluence	3995 €	Vorgefertigter Space mit Vorlagen, Makros und Seiten für ISMS nach ISO 27001
Jira Companion	Jira	995 €	Drei Jira Projekte zur Unterstützung von ISO 27001 mittels angepassten Asset-Typen, Workflows und Boards, arbeitet mit Instant 27001 for Confluence zusammen

Tabelle 3.1: Atlassian Apps[26]

HiScout GRC-Suite

Das deutsche Unternehmen HiScout GmbH[27] ist seit 2009 am Markt und entwickelt die Software „HiScout GRC-Suite“. Die Software und das Unternehmen unterstützen bei der Umsetzung bspw. eines ISMS nach ISO 27001 oder dem BSI IT-Grundschutz nach BSI Standard 200-1. Die Software ist modular aufgebaut und wird entsprechend der Kund:innenwünsche mit den notwendigen Modu-

[26] Quelle: selbst erstellt
[27] Link: https://www.hiscout.com/

len ausgestattet. Durch das Hinzufügen der Module werden vorgefertigte Inhalte, Vorlagen und Workflows den Anwender:innen zur Verfügung gestellt. Zudem werden vom BSI lizenzierte Inhalte angeboten und aktuell gehalten. Die eingepflegten Daten können in anderen Modulen wieder verwendet werden, sodass ein erneutes Einpflegen nicht notwendig ist. Damit kann die Realisierung eines ISMS sukzessive ausgebaut und erweitert werden. Die Software wird grundsätzlich als On-Premise-System angeboten und kann darüber hinaus auf Wunsch auch als SaaS-Lösung genutzt werden. Das gesonderte Modul „DataExchange“ ermöglicht zudem den Import und Export von Daten über das XML-Format.

Technische Betrachtung Das Produkt „HiScout GRC-Suite“ wird nicht quelloffen angeboten und besteht aus drei Komponenten: dem Web, bzw. Anwendungs-Server, dem Datenbank-Server und dem Client. Der Anwendungs-Server und der Datenbank-Server werden unter Microsoft Windows Server betrieben. Die Software basiert auf dem .Net Framework und nutzt einen MYSQL-Server als Datenbankmanagementsystem. Mittels Web-Server wird der Service über HTTPS angeboten. Die Nutzung eines Zertifikats wird vom Hersteller empfohlen und stellt die verschlüsselte Kommunikation sicher. Der Client kann mit allen gängigen Web-Browsern auf den Dienst zugreifen. Da HiScout in seiner Dokumentation[28] außer Microsoft Windows keine weiteren Betriebssysteme aufführt, ist es fraglich, ob MaOS oder Linux im vollen Funktionsumfang unterstützt werden. Die konkreten Systemanforderungen wurden beim Vertrieb von HiScout angefragt und können im Anhang HiScout Systemanforderungen eingesehen werden. Der Zugriff auf die Dienste wird über die Benutzerauthentifizierung geregelt, wobei der Anwendungs-Server mit einem Active-Directory verbunden werden kann. Die Software wird grundsätzlich als On-Premise-Lösung angeboten. Auf Nachfrage beim Vertrieb können aber durch Sonderabstimmungen auch SaaS-Lösungen umgesetzt werden.

Finanzielle Betrachtung Der Kauf des Produktes gliedert sich in drei Elemente: den Lizenzkauf, die Wartung und Softwarepflege und die Workshops. Die Lizenzen für die Module und die Erweiterungen werden einmalig berechnet und hängen von der Anzahl der Mitarbeiter:innen ab. Zur Zeit sind im Unternehmen ungefähr 500 Mitarbeiter:innen beschäftigt, wodurch die „Größenklasse bis max 1000 Mitarbeiter[sic]“ vom Vertrieb angesetzt wurde. In dieser Klasse betragen die Kosten für die Module [..] Die Tabelle 3.2 stellt die möglichen Module und deren Bedeutung dar. Zu den Lizenzkosten kommen zumindest einmalig „Software

[28] Vgl. HiS22, auch im Anhang unter HiScout Systemanforderungen eingepflegt.

und Wartungspflege“. Diese werden prozentual anhand der ausgestellten Gesamtlizenzkosten berechnet und mit einer Vertragslaufzeit von 12 oder 36 Monaten gebucht, wobei die Kosten bei einer Vertragslaufzeit von 36 Monaten einmalig oder jährlich beglichen werden können. Die angeführten Optionen bieten jeweils unterschiedliche Prozentsätze zur Berechnung der Kosten an und liegen zwischen [..] Eine weitere Beispielberechnung mit den verschiedenen Laufzeiten und Zah-

Name HiScout	Typ	Verwendung
ISM	Modul	ISMS Module zur Umsetzung von ISO 270001 oder BSI IT-Grundschutz
BCM	Modul	Umsetzung von Business Continuity Management
DS	Modul	Umsetzung von Datenschutz, bspw. Verarbeitungsverzeichnis
DataExchange	Erweiterung	Import und Export von Daten mittels XML-formatierter Datensätze
Questionaire	Erweiterung	Ermöglicht Befragungen für Mitarbeiter:innen im Portal oder mittels PDF
DocGen	Erweiterung	Ermöglicht das Erstellen von angepassten Berichten
Business Logic Engine	Erweiterung	Ermöglicht Automatisierung komplexer Prozesse mit frei konfigurierbaren Workflows

Tabelle 3.2: Übersicht Module und Erweiterungen HiScout[29]

lungsoptionen wurde im Anhang A.6 aufgeschlüsselt. Die Wartung und Softwarepflege beinhaltet Updates, Patches und Upgrade des genutzten System, eine freie Lizenz für ein Testsystem und den In-House-Customer-Support. Wird diese Position nicht gebucht, kann das erworbene System weiterhin genutzt werden, jedoch wird es nicht aktualisiert. Entscheidet sich das Unternehmen dafür zu einem späteren Zeitpunkt die Wartung und Softwarepflege in Anspruch zu nehmen müssen gesonderte Abstimmungen mit dem Vertrieb von HiScout erfolgen. Zuletzt stehen die optionalen Workshops als möglicher Kostenpunkt auf der Liste. Diese können Leistungen wie die Installation und Einrichtung umfassen, aber auch Leistungen wie die Beratung und Einführung. Generell werden die Workshops über Projekt-Tage (PT) abgerechnet [..].

[29] Quelle: selbst erstellt

3.5.2 Auswertung der Tests

Die Vorbetrachtung der Lösungen sind abgeschlossen. Um einen Eindruck der Softwarelösung zu erhalten und essentielle Funktionalitäten zu prüfen, wurden diverse Tests mit den Teststellungen ausgeführt. Im Anhang Kapitel „Auswertung der Testcases“ ist die Beschreibung der Testsysteme und die Auswertung tabellarisch hinterlegt. Diese werden nachfolgend ausgeführt.

SerNet Vernice.

Über den SerNets Shop konnte eine Evaluations-Version[30] von Verinice. kostenfrei bezogen werden. Zum Testen wurde die Version 1.24.1. Darüber hinaus wurde der Demodatensatz zum IT-Grundschutz[31] und der Datensatz für das IT-Grundschutz-Kompendium[32] heruntergeladen und import. Beide Erweiterungen sind kostenfrei im Shop abrufbar. Das Programm wurde über den Installer auf einem lokalen Arbeitsplatz installiert und getestet.
Wie bereits auf der Shop-Seite zu lesen war, ist die Evaluationsversion in ihren Funktionen eingeschränkt und bietet keine Report-Erstellung und nur eingeschränkte Import und Export-Möglichkeiten an[33]. Daher konnten diverse angedachte Testfälle nicht geprüft werden. Darüber hinaus sind weitere Funktionen ausschließlich im Verinice.Pro verfügbar, das als Evaluationsversion nicht erhältlich ist. Dies betraf bspw. die Benachrichtigung von Verantwortlichen oder die Rechteverwaltung innerhalb der Software. Abseits dessen bietet Verinice. bereits in der unbearbeiteten Version die Möglichkeit eine Scope für eine VDA-Selbstauskunft auszuführen oder ein ISMS nach ISO 27001 aufzubauen. Nach dem Import der aufgeführten Erweiterungen kann auch eine geführte Umsetzung des BSI IT-Grundschutzes erfolgen. SerNet hat zudem eine Hilfe im Programm integriert, die die Anwender:innen jederzeit bei der auszuführenden Tätigkeit unterstützt. Wenngleich das Produkt sowohl in der Basis-Version als auch nach dem Import der Erweiterungen mit zweckdienlichen Inhalten und Vorlagen aufwartet, können Benutzer:innen auch eigene Anforderungen an das Datenmodell einführen[34]. Dies geschieht über die Bearbeitung der Datei „SNCA.xml“ aus dem Java-Archiv „sernet.gs.server_<Versionsnummer_Datum>.jar“, das sich im Plugins-Verzeichnis der Application befindet. In ihr ist das Datenmodell beschrieben und kann entsprechend ergänzt oder angepasst werden. Dies stellt keine komfortable dafür aber eine weitreichende Handlungsmöglichkeit dar. Ob die Anpassungen

[30] Link: https://shop.verinice.com/ -> Software -> verinice.EVAL (1.24.1)
[31] Link: https://shop.verinice.com/ -> Content -> Demodaten
[32] Link: https://shop.verinice.com/ -> Content -> IT-GS-Kompendium
[33] Vgl. SeroJc.
[34] Vgl. Ser22, S. 111ff.

auch bei neuen Updates übertragen werden, ist sowohl in der Datei als auch im Handbuch nicht dokumentiert.

Atlassian Confluence und Jira

Zum Testen der Lösung von Atlassian wurde die Test-Systeme der Firma genutzt. In den Testsystemen ist Jira als Jira-Server in der Version 9.2.0 und Confluence als Confluence-Server in der Version 7.19.1 installiert. Beide Testsysteme befinden sich in separaten virtuellen Maschinen. Zum Prüfen der Testfälle wurde das Jira Projekt „ISMS“ und der Confluence Space „ISMS“ angelegt. Weiterhin ist im Jira-Testsystem das Add-On „Automation for Jira lite“ installiert, das in der Firma auch produktiv bereits genutzt wird. Es wurden keine weiteren Add-Ons installiert.
Atlassian bietet von Haus aus keine Vorlagen und Workflows zur Umsetzung eines ISMS an. Damit verbleibt ein großer Teil des Einrichtungsaufwands bei den Anwender:innen. Dieser steht, wenn Atlassian Produkte bereits im Unternehmen genutzt werden, den Kosten für den Kauf anderer ISMS-Produkte mit vorgefertigten Lösungen gegenüber. Dennoch bieten Confluence und Jira die Werkzeuge, um ein ISMS zu realisieren. Dokumente können revisions-sicher verfasst werden. Assets können im Jira eingepflegt und deren Maßnahmen verwaltet werden. Durch das Zusammenspiel der beiden Produkte können Verlinkungen und Übersichten schnell gebaut werden. Soll der Aufwand für die manuelle Einrichtung von Workflows und Dokumenten-Vorlagen reduziert werden, können Applikationen aus dem Marketplace kostenpflichtig erworben werden. Weiterhin ragen Jira und Confluence durch ihre komfortable und hohe Anpassungsfähigkeit hervor. Ticket-Typen und Confluence-Seitenvorlagen können entsprechend der Bedürfnisse der Anwender:innen gebaut und schnell angepasst werden. Gleichwohl können Benutzer:innenberechtigungen sowohl Projekt- und Space-seitig eingeführt, aber auch feingranular auf Seiten in Spaces eingeschränkt werden. Die Kernfrage, die sich bei dieser Lösung stellt, ist: Wie viel Aufwand ist ein Unternehmen bereit zu investieren um die längerfristigen Kosten zu reduzieren? Abseits dessen ist der Punkt des Vendor-Locks entscheidend. Atlassian hat das Ende der Server-Versionen seiner Produkte bereits angekündigt und wird den Support im Februar 2024 beenden. Daher ist das Unternehmen gezwungen auf die Datacenter- oder die Cloud-Version umzusteigen. Dies sollte vor der Investition der Aufwände zum Einrichten des ISMS im Jira und Confluence in Betracht gezogen werden.

HiScout GRC-Suite

Zum Testen der HiScout GRC-Suite wurde der Vertrieb von HiScout kontaktiert, da eine kostenfreie herunterladbare Version zum Evaluieren nicht existiert. Die Teststellung kann sowohl On-Premise als auch als SaaS-Lösung erfolgen. Für den Testlauf wurde die SaaS-Lösung gewählt. Nach der Abwicklung der Vertragsbedingungen wurden die Zugangsdaten für die Teststellung zugestellt. Mittels der Zugangsdaten konnte auf die bei 1und1 betriebene SaaS-Lösung zugegriffen werden, in der die HiScout GRC-Suite in der Version 3.10.0 mit den Modulen HiScout ISM und HiScout Grundschutz und der Erweiterung HiScout Questionaire betrieben wurde.
HiScout bietet mit der GRC-Suite ein Produkt, das durch die verschiedenen Module und Erweiterungen ergänzt, nahezu alle geprüften Testfälle erfolgreich besteht. Die Module ergänzen die Basissoftware mit Vorlagen und Hilfestellungen zur Umsetzung der geforderten Standards und Normen. Die Hilfetexte führten zum einen durch die Standards, konnten aber auch auf den einzelnen Seiten kontextbezogene Unterstützung geben. Abseits dessen konnten eigene Klassen mit Eigenschaften oder auch eigene Webseitenlayouts über die Weboberfläche komfortabel integriert und vorhandene Objekte individualisiert werden. Das zentrale Datenmodell des Produktes ermöglicht die Nutzung von erfassten Informationen in den aktivierten Modulen. So können bspw. im Rahmen der Strukturanalyse eingepflegte IT-Systeme auch in der ISO 27001 Umsetzung genutzt werden und müssen nicht erneut erfasst werden. Die generische Export- und Importfunktion im XML-Format ermöglicht die Anbindung von externen Systemen, die bspw. bei der Inventarisierung von Assets genutzt werden können. Zusätzlich konnten Reports mittels etablierter Vorlagen oder auch in angepasster Form erstellt werden. In der Teststellung wurde E-Mailversand aus sicherheitsgründen seitens HiScout nicht aktiviert. Daher konnten die Möglichkeiten der Benachrichtigung nicht geprüft werden. Auch die Funktionalität des Questionaire konnte innerhalb der Teststellung nicht vollends erprobt werden.

3.5.3 Fazit und Empfehlung zu den Lösungsansätzen

Die Evaluation der geeigneten Softwarelösungen ist abgeschlossen und mündet in drei Lösungsansätze mit unterschiedlichen Vor- und Nachteilen. Diese bewegen sich von einem kostengünstigen Ansatz mit sehr hohem Einrichtungsaufwand bis hin zu einem vergleichsweise teuren Ansatz mit geringem Einrichtungsaufwand. Die nachfolgende Ausführung wie auch die Tabelle 3.3 fasst die aus der Evaluation gesammelten Erkenntnisse und Erfahrungen zusammen, vergleicht die Lösungs-

ansätze und dient darüber hinaus der Geschäftsführung des Unternehmens als Entscheidungsgrundlage.

Kategorie	Lösung I	Lösung II	Lösung III
Software	Atlassian Jira und Confluence	HiScout GmbH GRC-Suite	SerNet GmbH Verinice.
Kosten	ohne zusätzliche Apps nur bereits vorhandene	sehr hoch	gering
Einrichtungsaufwand	ohne zusätzliche Apps sehr hoch	normal	normal
Flexibilität	sehr hoch und komfortabel	sehr hoch und komfortabel	hoch und unkomfortabel

Tabelle 3.3: Zusammenfassung der Lösungsansätze[35]

Lösung I: geringe Kosten und sehr hoher Einrichtungsaufwand Als kostengünstigster Lösungsansatz hat sich Atlassian Jira und Confluence herausgestellt, was nicht zuletzt daran liegt, dass es bereits im Unternehmen genutzt wird und somit die Lizenzkosten entfallen, bzw. der Kauf der Software keine zusätzlichen Kosten aufwirft. Dem entgegen steht der Aufwand zum Einrichten des ISMS der vergleichsweise hoch ausfällt, da keine Vorlagen und Workflows von Haus aus für diesen Zweck integriert sind, was auch den größten Nachteil darstellt. Allerdings können die Aufwände durch den Kauf von Applikationen aus dem Marketplace reduziert werden, wobei hierbei die Kosten von einmalig rund 4000 € und jährlich 10000 € im Raum stehen. Ein entscheidender Vorteil ist die hohe Flexibilität der Software, die eine vergleichsweise komfortable Anpassung an die Anforderungen der Kund:innen ermöglicht. Es bleibt anzumerken, dass durch die Umsetzung des ISMS durch diesen Lösungsansatz eine weitere Abhängigkeit zum Betreiber Atlassian aufgebaut wird, was im Zuge des Endes des Support für die Server-Version im Frühjahr 2024 relevant ist.

Lösung II: sehr hohe Kosten und normaler Einrichtungsaufwand Der dritte Lösungsansatz ist der mit Abstand teuerste. Sowohl die einmaligen Anschaffungskosten als auch die fortlaufenden Kosten für Softwarepflege und Wartung fallen sehr hoch aus. Dafür bietet die Software einen hohen Komfort und wartet mit Vorlagen, Automatismen und Workflows auf. Zudem eignet sich die Software durch

[35] Quelle: selbst erstellt

die hohe Anpassungsfähigkeit der Objekte und Übersichten auch zur Umsetzung von Lösungen abseits der Standards. Das zentrale Datenmodell reduziert dabei auch den Aufwand bei Umstellung oder Ergänzung auf gängige Standards.

Lösung III: moderate Kosten und normaler Einrichtungsaufwand Der Lösungsansatz für die Mitte wird durch SerNets Verinice. ausgefüllt. Die Software ist vergleichsweise günstig und wartet mit geführten Vorlagen für gängige Standards oder Selbstauskünfte auf. Das Datenmodell der Software ist anpassbar, wenngleich dies vergleichsweise unkomfortabel gelöst wurde. Dennoch wird ermöglicht die Software somit eine Anpassung an die individuellen Anforderungen der Kund:innen. Abseits dessen steht die Veröffentlichung der zweiten Generation der Software im kommenden Jahr an, die jedoch nicht vorab getestet werden konnte.

Die Empfehlung mit Fokus auf das konzeptionell überarbeitete ISMS Alle drei Lösungsansätze bieten die Möglichkeit ein ISMS nach gängigen Standards, Normen und Richtlinien umzusetzen. Für die Realisierung des im Kapitel 3.2 beschriebenen konzeptionell überarbeiteten ISMS ist der Lösungsansatz I der Geeignetste. Eben durch die hohe Flexibilität des Systems können eigene Anforderungen an Vorlagen, Workflows und Automatisierungen implementiert werden. Gestützt durch weitere mögliche Applikationen aus dem Marketplace, kann der Einrichtungsaufwand reduziert werden. Darüber hinaus steigert dies auch die Akzeptanz der Mitarbeiter:innen, da diese bereits langjährige Erfahrung mit der Software haben. Alternativ ist der zweite Lösungsansatz zu wählen, sofern die finanziellen Ressourcen dafür vorhanden sind. Die zweite Lösung bietet sowohl eine hohe Flexibilität als auch die Umsetzung der gängigen Standards. Dennoch sind die Anschaffungs-, Softwarepflege- und Wartungskosten signifikant höher als bei den anderen beiden Lösungsansätzen. Eine beispielhafte Berechnung für HiScout wurde im Anhang A.6 „HiScout Beispiel Kostenrechnung“ eingefügt. Lösungsansatz II bietet für die Umsetzung des überarbeiteten ISMS und auch für zukünftige Entwicklungen der Firma einen zu geringen Mehrwert. Wohl möglich bietet die zweite Generation der Software einen Anlass zur erneuten Evaluation und Bewertung der Software.

4 Einführung des überarbeiteten ISMS mittels Atlassian Jira und Confluence

Im Kapitel 3 wurde die Ausarbeitung des überarbeiteten ISMS vorgestellt und die Evaluation einer geeigneten Softwarelösung zur Realisierung des ISMS durchgeführt. Das Kapitel schloss mit der Empfehlung für den Lösungsansatz I „Atlassian Jira und Confluence“ ab, den das Unternehmen angenommen hat. Der Lösungsansatz II wurde aufgrund der finanziellen Belastung ausgeschlossen und der Lösungsansatz III wurde wegen eines geringen Mehrwerts und geringer Flexibilität abgelehnt. Dementsprechend wird im Folgenden die Realisierung des ISMS durch den Lösungsansatz I für das Unternehmen ausgeführt. Dabei wird zunächst die Umsetzung in den beiden Softwarekomponenten beschrieben[1]. Anschließend wird ein Fallbeispiel zur Umsetzung von Maßnahmen ausgeführt. Das Kapitel schließt mit der Auswertung der Realisierung des überarbeiteten ISMS und des Lösungsansatzes I, sowie dem Vorschlagen von Verbesserungsvorschlägen ab.

4.1 Einführung des Spaces ISMS für die Dokumentation im Confluence

Als erstes wurde die notwendige Basis im Atlassian Confluence der Firma aufgebaut. Dazu wurde ein neuer Space „Informationsecuritymanagementsystem“ mit dem Space Key „ISMS“ in der Instanz erstellt, der ausschließlich für das ISMS genutzt werden soll. Der Bild 4.1 zeigt den Space kurz nach der Erstellung. Um den Space vor ungewollten Zugriffen zu schützen, wurden die Berechtigungen in den Grundeinstellungen angepasst, sodass nur bestimmte Personen und Gruppen auf den Space zugreifen konnten. Das Bild „Berechtigungen im Confluence“ im Anhang A.8.1 zeigt die gewählten Einstellungen an, die sich, abseits von den

[1] Der Name des Spaces und des Projektes ist „Informationsecuritymanagementsystem“. Für eine bessere Lesbarkeit wird im Folgenden der Space- und Projekt-Key „ISMS“ zur Referenzierung verwendet.

Standardberechtigungen für die Administratoren:innen, auf das Management und die Space-Verantwortlichen beschränken. Anonyme Zugriffe werden komplett unterbunden. Im Anschluss an die Einführung des Spaces und die Rechteanpassung wurden Werkzeuge zur strukturierten Arbeit innerhalb des Spaces gebaut und die ersten Seiten erstellt.

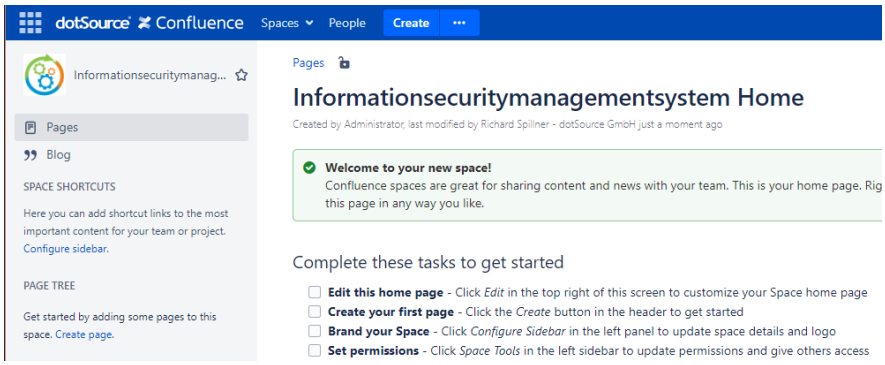

Bild 4.1: Confluence Space ISMS[2]

4.1.1 Vorlagen für die Arbeit im Space

Um die Arbeit innerhalb des ISMS zu vereinheitlichen und zu vereinfachen, wurden zunächst Vorlagen erstellt, die bei der Erstellung neuer Seiten ausgewählt werden können. Im Bild 4.2 sind die aktuell erstellten Vorlagen zu sehen, die im Anhang A.8.2 einzeln abgebildet sind. Diese wurden je nach Funktion mit spe-

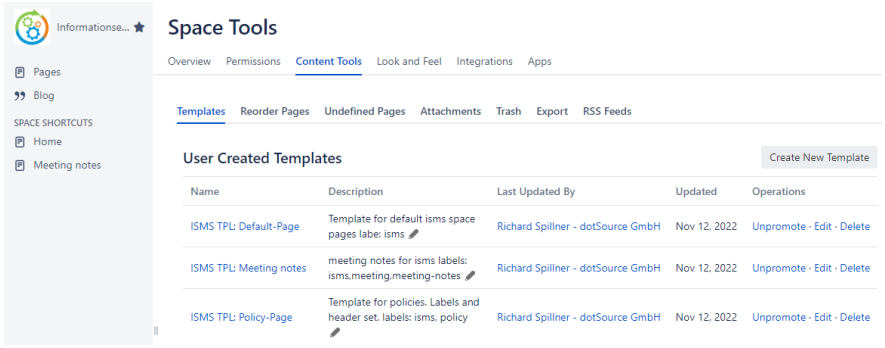

Bild 4.2: Confluence Space Vorlagen[3]

ziellen Labels definiert, sodass anhand der Labels die Erstellung von Übersichten oder Filterungen auf anderen Seiten möglich sind. Darüber hinaus enthält jede Vorlage das Makro „Page properties“. Dieses ermöglicht das Zuweisen von Eigenschaften zu der Seite durch das Einfügen einer Tabelle, die ein- oder ausgeblendet werden kann. Diese Eigenschaften können nachfolgend über das Makro

[2]Quelle: interner Space ISMS
[3]Quelle: Space ISMS: Space tools: Content Tools: Templates

„Page properties report“ zur Erstellung einer detaillierten Übersicht genutzt werden. In den Vorlagen wurden als Eigenschaften die verantwortliche Person, das letzte Update und der aktuelle Status der Seite vordefiniert. Diese Maßnahmen unterstützen bei der Erfüllung der Anforderung die Form der Dokumentation eines ISMS. Abschließend wurden die Vorlagen auf „promoted“ gesetzt, wodurch diese bei der Erstellung neuer Seiten im Space an erster Stelle stehen, wie im Bild 4.3 zu sehen ist. Somit wird der Workflow vereinfacht. Die aufgeführten

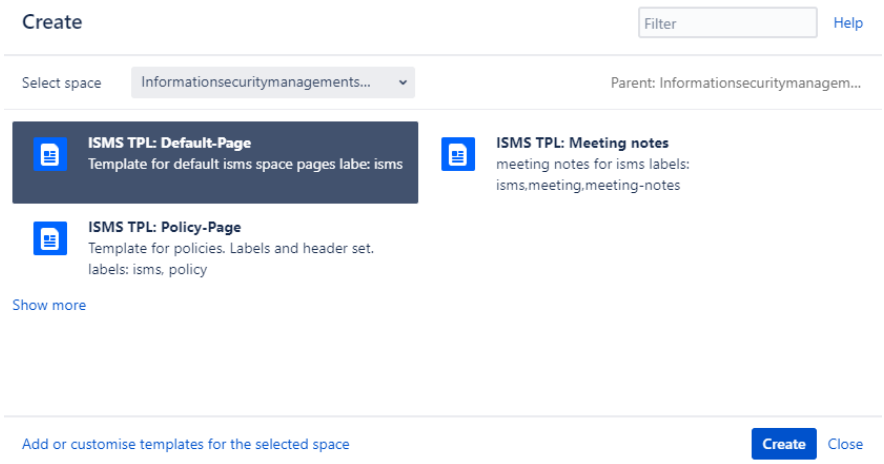

Bild 4.3: Dialog: Erstellen einer neuen Seite im ISMS-Space[4]

Vorlagen sind ausschließlich im Space ISMS verfügbar. Darüber hinaus können auch leere Seiten oder Seiten mittels anderer Vorlagen über den Button „Show more“ erstellt werden.

4.1.2 Die ersten Seiten im ISMS

Als erstes wurde die **Home-Page** der Spaces überarbeitet. Die Space-Activity und die Seiten-Historie wurden beibehalten und es wurde ein Inhaltsverzeichnis eingefügt. Die Hauptaufgabe der Seite ist es, den Zustand das ISMS übersichtlich darzulegen und wichtige Kontaktinformationen anzubieten. Daher wurde eine Tabelle mit Details zu verantwortlichen Personen erstellt. Die Übersicht über den Zustand des ISMS wird durch die Anzahl und den Status von Jira-Tickets in Form von Kreisdiagrammen und durch eine Tabelle mit detaillierten Informationen abgebildet. Die Tabelle wurde so eingerichtet, dass sie ausschließlich die Tickets aus dem Projekt ISMS anzeigt, dessen Einrichtung in Kapitel 4.2 beschrieben wird. Zusätzlich wurde eine Tabelle „Reports and Policies“ eingeführt, die wie weiter oben angeführt, die Eigenschaften von Unterseiten durch das Makro „Page properties report“ sammelt und darstellt. So kann ein schneller Überblick gewonnen

[4]Quelle: Space ISMS: „...“-Button in der Kopfzeile

werden, welche Tickets noch offen sind und welche Seite sich noch im Zustand „DRAFT“ befindet, wie Bild 4.4 zeigt. Die komplette Homepage ist im Anhang A.8.3 hinterlegt.

Des Weiteren wurden Sammelseiten für Meeting-Notes und Policies angelegt.

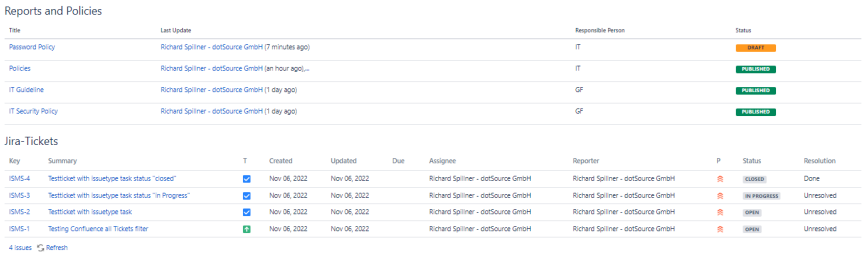

Bild 4.4: ISMS Home-Page Part 3[5]

Die **Meeting-Notes-Seite** enthält Protokolle zu Meetings, die im Rahmen des ISMS stattgefunden haben und ist im Bild „ISMS Seite: Meeting Notes“ im Anhang A.8.4 dargestellt. Die Seite wurde mit der Vorlage „ISMS TPL: Default Page“ erstellt und enthält folglich den definierten Kopf. Zusätzlich wurde ein Button „Create Default Meeting Note“ integriert, der bei Ausführung eine neue Seite nach der Vorlage „ISMS TPL: Meeting notes“ unterhalb der Meeting-Notes-Seite erstellt. Dies vereinfacht den Prozess, steigert die Akzeptanz zur Protokollierung von Meetings und sorgt für einen einheitlichen Aufbau der Protokolle. Die **Policies-Seite** dient als Oberseite zur Verwaltung von Richtlinien und Leitlinien und wurde analog zur Meeting-Notes-Seite entworfen, wie Bild 4.5 zeigt.

Auf der Seite wird ein Überblick über die vorhandenen Richtlinien mit Hilfe

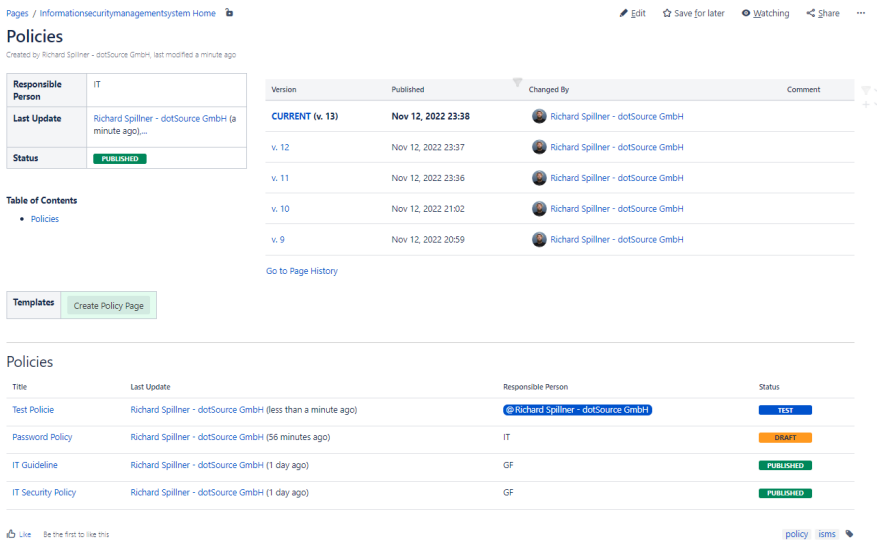

Bild 4.5: ISMS Seite: Policies[6]

[5]Quelle: Space ISMS Landing Page

des Makros „Page properties report“ erstellt, der die Richtlinie, die letzte Bearbeitung, die verantwortliche Person, den Status und ggf. ein mit der Richtlinie verbundenes Vorgang aus dem Jira Projekt wiedergibt. Ebenso wurde ein Button „Create Policy Page“ eingeführt, der eine schnelle Erstellung von weiteren Unterseiten mit der Vorlage „ISMS TPL: Policy Page“ ermöglicht. Da in der Firma bereits Richtlinien und Leitlinien vorhanden sind, sollten diese auch längerfristig im ISMS eingepflegt werden. Anschließend können sie über die Makros „Include Page“ oder „Excerpt Include“ auf anderen Seiten in anderen Spaces dargestellt werden. Dadurch können öffentliche Teile des ISMS den Mitarbeiter:innen und Kund:innen zur Verfügung gestellt werden, ohne direkten Zugriff auf das Dokument zu riskieren. Die bereits erstellten IT Guideline und IT Security Policy wurden auf diese Weise in den ISMS Space eingebunden, da sie zur Zeit noch im Company Space der Firma abgelegt sind.
Als letztes wurden die ersten Kerninformationsseiten des ISMS erstellt, so dass diese mit den notwendigen Informationen und Kriterien befüllt werden können. Dazu gehört die „Scope“-Seite, die den Anwendungsbereich für das ISMS definiert, die „Structure analysis“-Seite, die die Prozess- und Infrastruktur des Unternehmens festhält und die „Protection needs“-Seite, auf der der Schutzbedarf definiert und die Kategorien festgelegt werden. Die Struktur-Analyse wurde mit den bereits vorhandenen Informationen befüllt und auf englisch übersetzt. Auf der Definitions-Seite für den Schutzbedarf wurden die initialen Kategorien „normal“ und „critical“ angelegt. Die erstellten Seiten sind im Anhang A.8.6 bis A.8.8 beigefügt.

4.2 Einführung des Projekt ISMS zur Projektverwaltung im Jira

Nach der Einrichtung der grundlegenden Struktur im Confluence wurde das neue Projekt „Informationsecuritymanagementsystem“ mit dem Projekt-Key „ISMS“ in der Jira Instanz der Firma erstellt, wie Bild 4.6 nachweist. Das Jira-Projekt unterstützt bspw. bei der Umsetzungsprotokollierung von Maßnahmen oder Verwaltung des Review-Prozesses von Dokumenten oder Richtlinien. Da auch in diesem Projekt kritische Daten gepflegt werden, wurde der initiale Zugriff auf die notwendigen Personen reduziert, wie das Bild „Benutzer und Rollen im Jira“ im Anhang A.9.1 zeigt. Zusätzlich wurde der Autor als Projektleiter eingefügt. Um das Projekt für die weitere Arbeit am ISMS vorzubereiten, wurden weitere

[6] Quelle: Space ISMS Policies

Einstellungen angepasst und neue Schemes erstellt, die nachfolgend exemplarisch ausgeführt werden.

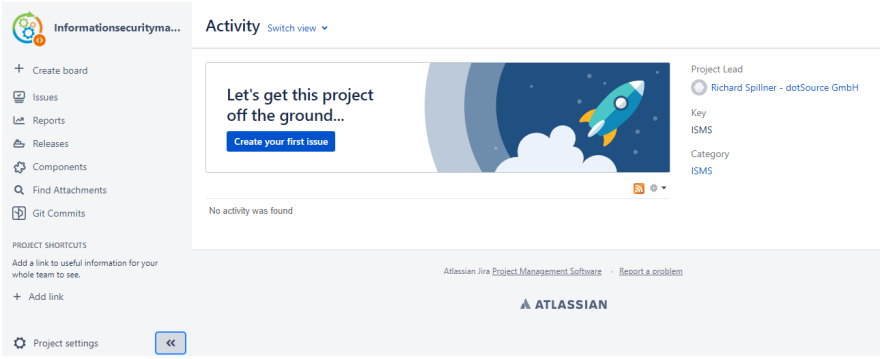

Bild 4.6: Jira Projekt: ISMS[7]

4.2.1 Berechtigungen in Jira

Die Berechtigungsverwaltung in Atlassian Jira wird durch „Permission Schemes“ festgelegt. Im Schema ist definiert, welchen Projekt-Rollen, Personen oder Gruppen konkrete Rechte eingeräumt wurden. Die Projekt-Rollen werden über die Projekteinstellung „Users and Roles“ Benutzer:innen oder Gruppen zugewiesen. Zusätzlich können unter „Issue Security“ Sicherheitslevel definiert werden, die einem Issue oder auch Vorgang zugewiesen werden können. Dadurch können ausschließlich definierte Benutzer:innen, Gruppen oder Projekt-Rollen den Vorgang sehen und bearbeiten. Sicherheitslevel werden in der Regel bei Vorgängen mit hoch kritischen Informationen angewendet. Da der Zugriff auf das Projekt ISMS zur Zeit ausschließlich auf die Verantwortlichen beschränkt ist, wurde kein neues Vorgangssicherheitsschema eingeführt. Sowohl Berechtigungsschemata als auch Vorgangssicherheitsschemata werden global definiert und anschließend den Projekten zugeordnet. Für das Projekt ISMS wurde das separate Berechtigungsschema „ISMS Permission Scheme“ als Klon des Schemas „ITAM[8] Permission Scheme“ erstellt und ausschließlich diesem Projekt zugewiesen, um ungewollte Rechteanpassungen aufgrund von Anforderungen aus anderen Projekten im Schema zu vermeiden. Das vollständige Schema ist im Anhang A.9.2 abgedruckt. Standardmäßig kann die Projektrolle Administrators nahezu alle Tätigkeiten durchführen. Diese Rolle wird dem Kernpersonal des Projektes zugewiesen, um diese möglichst weit von der Betreuung durch die IT zu entkoppeln. Zusätzlich wurden in dem Schema zwei bereits definierte Rollen wiederverwendet: Project Editor und Project Reader. Diese werden weiteren Benutzer:innen zugeteilt. Benötigt die Person

[7] Quelle: internes Projekt ISMS
[8] IT Asset Management (ITAM)

ausschließlich lesenden Zugriff auf das ISMS, wie es bspw. bei Vertreter:innen des Managements oder Auditor:innen sein kann, wird die Rolle Project Reader vergeben. Arbeitet die Person mit an der Umsetzung, wie bspw. der oder die ISB, wird die Rolle Project Editor vergeben. Durch diese reduzierte Rollen- und Rechteverwaltung bleibt die Übersicht erhalten und die Komplexität begrenzt sich auf ein notwendiges Maß.

4.2.2 Issue Types

In Atlassian Jira werden die Informationen in Vorgängen erfasst. Diese durchlaufen verschiedene Status und können durch Kommentierung den Prozess der Vorgangsabwicklung protokollieren. Durch Konfiguration eines Vorgangstypen können sowohl die Maske für die Informationssammlung als auch die Prozessschritte definiert werden. Für das Projekt wurden zusätzliche Vorgangstypen angelegt: Der Typ „Review“ wird als Kontrollvorgang für Dokumente oder Maßnahmen genutzt; der Typ „Incidents“ dient zum Erfassen von Vorfällen und der Typ „New Measure“ wird bei der Erstellung neuer Maßnahmen eingesetzt. Jira bietet zudem die Möglichkeit durch „Issue Type Schemes“ eine Kollektion von möglichen Vorgängen zu erstellen. Diese Kollektion wird dann mit dem Projekt verknüpft. Das Schema „dotSource ISMS Issue Type Scheme“ wurde für das Projekt neu angelegt und enthält die notwendigen Vorgangstypen, wie im Bild 4.7 zu sehen ist. Dabei wurden Standardvorgangstypen entfernt und die zuvor neu erstellten Ty-

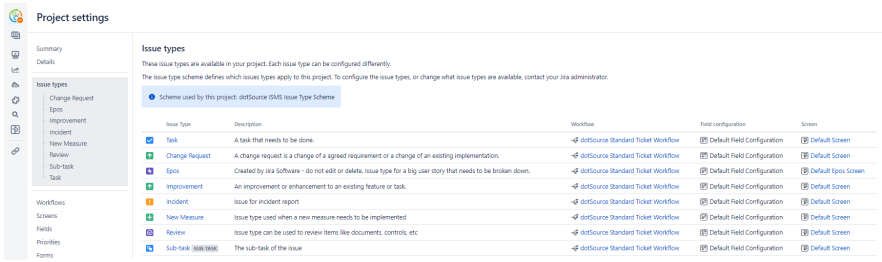

Bild 4.7: dotSource ISMS Issue Type Scheme[9]

pen hinzugefügt. Dies soll die ungewollte Nutzung von Vorgangstypen innerhalb des Projektes durch die Anwender:innen unterbinden und ermöglicht gleichzeitig das Hinzufügen neuer Vorgangstypen ohne andere Projekte zu beeinflussen.

4.2.3 Workflow

Wie bereits weiter oben beschrieben, können Vorgänge verschiedene Status durchlaufen. Welcher Status in welchen übergehen kann, ist im Workflow definiert.

[9]Quelle: Projekt ISMS: Project Settings: Summary: dotSource ISMS Issue Type Scheme

Zusätzlich können hierbei weitere Anpassungen wie das Einblenden besonderer Masken oder das automatische Setzen von Werten festgelegt werden. Über das Workflow Scheme wird ein Workflow einem oder mehreren Vorgängen zugewiesen. Dieses Schema wird dann über die Projekteigenschaften mit dem Projekt verknüpft. Für das Projekt ISMS wurde der neue Workflow „dotSource ISMS

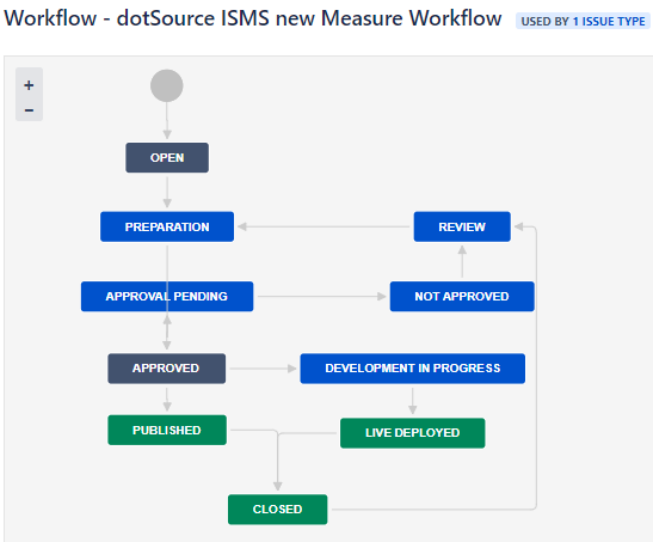

Bild 4.8: dotSource ISMS new Measure Workflow[10]

new Measure Workflow“ eingeführt. Zur Erstellung des Workflows wurde der Status „Published“ eingeführt und ein separates Workflow-Schema erstellt, über das das Projekt mit dem Workflow verbunden wurde. Durch diese Konstellation können Vorgänge vom Typ „New Measure“ ausschließlich die im Bild 4.8 abgebildeten Zustände annehmen und Übergänge vollziehen, wodurch eine Prozessreihenfolge etabliert wurde. Wird eine neue technische oder organisatorische Maßnahme im Unternehmen eingeführt, wird dies innerhalb des ISMS über diesen Vorgang bearbeitet. Dabei wird zunächst eine Vorbereitung (*Preparation*) durchgeführt. Im Falle einer neuen Richtlinie kann dies bspw. die Ausarbeitung dieser sein. Anschließend muss der Entwurf von den verantwortlichen Personen genehmigt werden (*Approval pending*). Ist dies erfolglos (*Not approved*), gilt es die Kritik einzuarbeiten (*Review* und *Preparation*) und den neuen Entwurf zur Bewilligung einzureichen (*Approval pending*). Kommt es zu Genehmigung (*Approved*), wird der Entwurf publiziert (*Published*) und der Vorgang abgeschlossen (*Closed*). Diverse Übergänge wurden mit speziellen Screens konfiguriert, sodass die Benutzer:innen ausschließlich die notwendigen Felder für den Übergang sehen. Wechselt ein Vorgang bspw. von „Published“ zu „Closed“, wird die im Anhang A.9.4 im

[10] Quelle: Projekt ISMS: Project Settings: Workflow: dotSource ISMS new Measure Workflow
Detailliert im Anhang A.9.3 Bild A.1

Bild A.2 angezeigte Maske ausgelöst, bei der die Anwendenden die Lösung auswählen und einen Kommentar einfügen sollen. Anschließend ist der Vorgang im Zustand Closed. Durch diese Möglichkeiten bietet Jira eine hohe Flexibilität an Prozessgestaltung und Fehlerreduzierung.

4.3 Exemplarische Betrachtung der Umsetzung einer Maßnahme am Beispiel der Kennwort-Richtlinie

[...]

4.3.1 Beschreibung der Ausgangssituation

[...]

4.3.2 Die Anforderungen an die neue Kennwort-Richtlinie

[...]

4.3.3 Erstellung der Kennwort-Richtlinie im Arbeitsablauf

[...] Nach der Beschreibung des IST-Zustandes und der Anforderungen für die Kennwortrichtlinie wird im Folgenden der Prozess zur Erstellung der neuen Richtlinie mit den eingeführten Wegzeugen dargelegt. Dabei wird zuerst das Ticket im Projekt ISMS angelegt. Anschließend werden die Informationen aufbereitet, die verbunden Aufgaben und der erste Entwurf der Richtlinie formuliert. Der Entwurf wird zur Kontrolle an die verantwortliche Person zur Freigabe übergeben. Die Aufgaben werden parallel dazu vorbereitet und ggf. umgesetzt. Kommt es zur Freigabe wird das Dokument für die Mitarbeiter:innen zur Verfügung gestellt. Abschließend werden die offenen Aufgaben protokolliert und ggf. für weitere Durchläufe zur Realisierung vorgemerkt.
[...]

4.3.4 Zusammenfassung der exemplarischen Umsetzung

Die Einführung der Passwort-Richtlinie konnte im Zuge der vorliegenden Arbeit nicht abschließend umgesetzt werden. Der Prozess wurde durch den neu erstellten Ticket Typ "New Measure"gestartet und führte zu einer Aufteilung der Aufgaben auf insgesamt vier Tickets. Dabei verblieb die organisatorische Maßnahme der

Formulierung, Kritik und Veröffentlichung der Maßnahmen beim Haupt-Ticket und die Anpassung der Dienste, wie auch die Handhabung der aktuellen Kennwörter wurde auf Unteraufgaben aufgeteilt. Dies förderte ein strukturiertes Bild zu Tage, dass auch im Confluence auf der Landing Page nachvollzogen werden konnte. Anschließend wurden die notwendigen Informationen zusammengetragen und im Ticket zur Verfügung gestellt.
Die neue Passwort-Richtlinie wurde auf englisch und deutsch formuliert und ist zur Zeit im Zustand „Approval pending“, sodass der nächste Schritt die Kritik oder Freigabe seitens des Managements ist. Nach der Freigabe kann die Seite oder auch nur ein Teil der Seite durch das Confluence Makro „Include Page“ im öffentlichen Bereich des Unternehmens zur Verfügung gestellt werden. Daraufhin wird das Ticket in den Zustand „Published“ überführt. Die Anpassung der Dienste wurde beleuchtet und entsprechend protokolliert. Die Maßnahmen wurden soweit vorbereitet, dass Testläufe nach der Zuarbeit von der Fachabteilung durchgeführt werden können. Nach den Testläufen steht die Freigabe durch das Management für die Anwendung der Maßnahme an. Sollte es hierbei zur Kritik an der Umsetzung kommen, werden die kritisierten Punkte ausgeräumt und das Ticket wird erneut zur Freigabe vorgelegt. Erfolgt hierbei eine Freigabe, werden die Maßnahmen umgesetzt, im Ticket protokolliert und das Ticket auf „Closed“ gesetzt. Abschließend bleibt vor allem der Umgang mit den bestehenden Kennwörtern zu klären. Sind alle relevanten Tätigkeiten abgeschlossen, wird das Ticket in den Status „Closed“ überführt und ist damit geschlossen.
Die exemplarische Betrachtung der Umsetzung gab einen Einblick, wie die eingeführten Werkzeuge zur Umsetzung von Maßnahmen im überarbeiteten ISMS genutzt werden können. Im Anhang A.11.3 wurden Auszüge aus der Home-Page des Confluence Spaces ISMS nach der Bearbeitung der neuen Passwort-Richtlinie dargestellt. Diese geben, wie angedacht, einen Überblick über die aktuellen Zustand des ISMS.

4.4 Auswertung der Realisierung des überarbeiteten ISMS

Die Einführung des ISMS und die Betrachtung der exemplarischen Umsetzung von Maßnahmen im Rahmen der vorliegenden Arbeit sind abgeschlossen und münden nachfolgend in eine Bewertung der Nutzbarkeit des konzeptionell überarbeiteten ISMS und der Softwarelösung Atlassian Jira und Confluence.

4.4.1 Bewertung der Nutzbarkeit des überarbeiteten ISMS

Das überarbeitete ISMS wurde im Kapitel 3 beschrieben. Dabei wurden der Aufbau und die Phasen des ISMS ausgeführt. Diese wurden auch bei der Umsetzung in der Softwarelösung und bei der Realisierung der Maßnahme genutzt. Nachfolgend wird die Anwendung reflektiert.

Die Umsetzung des beschriebenen Phasenmodells bei der Einführung des ISMS Das Phasenmodell des überarbeiteten ISMS aus Kapitel 3.2.2 besteht aus drei Phasen und wurde im Rahmen der Möglichkeiten als Ablaufplan für die Einführung und den Ausbau des ISMS im Unternehmen genutzt.
Im Rahmen der Arbeit wurde die erste Phase des ISMS als Einstiegspunkt für den Aufbau des ISMS genutzt und konnte erfolgreich durchlaufen werden. Das Bekenntnis der Geschäftsführung zur IT-Sicherheit lag bereits durch die Veröffentlichung der IT-Richtlinie und die Berufung des ISBs vor. Zusätzlich wurden der Autor und weitere Personen aus der internen IT mit der Einführung und Wartung des ISMS und die Unterstützung des ISBs betraut. Entsprechend wurde das IS-Management-Team gebildet und im Space ISMS auf der Homepage unter „Verantwortlichkeiten“ dokumentiert. Nach dieser Festlegung folgte die Definition des Anwendungsbereiches und der Schutzbedarfskategorien. Zu diesem Zweck wurden im ISMS die Seiten „Scope“ und „Protection needs“ eingeführt. Auf der ersten Seite wurde das gesamte Unternehmen als Anwendungsbereich definiert. Dieses umfasst den Haupt- wie die Nebenstandorte, die gesamte Infrastruktur, Applikationen, IT-Systeme und alle im Unternehmen Beschäftigte. Dies folgt auch den Anforderungen, die im Bezug auf die TISAX-Auskunft gefordert wurden. Auf der zweiten Seite werden zur Zeit die Schutzbedarfskategorien und deren Abgrenzungen ausgearbeitet. Im Rahmen der Arbeit und der Ausarbeitung aus Kapitel 3.2.2 folgend, wurden zwei Kategorien, „normal“ und „kritisch“, angenommen. Damit schloss die erste Phase des ISMS erfolgreich ab.
In der zweiten Phase des ISMS ist der IST-Zustand zu ermitteln. Der IST-Zustand wurde 2019[11] im Rahmen einer Strukturanalyse unvollständig erhoben. Dennoch bietet diese eine nutzbare Ausgangsbasis, die übernommen und formatiert in das ISMS integriert wurde. Die Auflistung muss im Nachgang aktualisiert und vervollständigt werden, sodass eine Abbildung des Unternehmens dokumentiert ist. Weiterhin fehlen zur vollständigen Umsetzung der zweiten Phase die Erhebung der aktuellen technischen und organisatorischen Maßnahmen und der Eingabefaktoren. Die zweite Phase konnte daher nicht abschließend durchlaufen werden. Im der dritte Phase soll durch fortlaufende Verbesserung des IST-Zustands das

[11] Als Resultat der Ausarbeitung in Spi19.

Schutzniveau angehoben werden. Als erstes ist dabei ein flächendeckender Basisschutz zu etablieren. Durch die Einführung der Kennwort-Richtlinie wird diesem Vorhaben nachgekommen. Die Verbindlichkeiten der Richtlinie heben das Schutzniveau im Ganzen und durch die Umsetzung der Maßnahmen auf den betroffenen Systemen, werden die Benutzer:innen auch zum Einhalten der Regeln gezwungen. Die neuen Anforderungen an die Kennwörter bewirken deutlich sicherere Passwörter als es zuvor der Fall war, was das Erraten der Zugangsdaten an den öffentlich verfügbaren Diensten deutlich erschwert. Wenngleich die Maßnahme nicht abschließend bearbeitet werden konnte, so erzielt diese nach der vollständigen Umsetzung eine Verbesserung des Schutzniveaus. Weitere Elemente der dritten Phase konnten im Rahmen der vorliegenden Arbeit nicht umgesetzt werden, da sie den Rahmen sprengen würden.
Die Phasen des ISMS stellten für die Umsetzungen einen nutzbaren Ablaufplan dar, der eine nachträgliche Einschätzung der Vollständigkeit des ISMS ermöglichte.

Die Anwendung des beschriebenen Aufbaus bei der Einführung des ISMS
Im Kapitel 3.2.1 wurden die sechs Komponenten des überarbeiteten ISMS beschrieben, die bei der Realisierung im Unternehmen als Leitlinie für den Aufbau genutzt wurden.
Als Eingabe in das ISMS wurden die Anforderungen seitens des Unternehmens und die Vorarbeiten genutzt. Insbesondere die IT-Leitlinie und die Kompatibilitätsforderung zur TISAX-Auskunft waren dabei maßgeblich. Darüber hinaus sollten in den nächsten Iterationen weitere Eingabefaktoren, wie bestehende Gesetze oder Anforderungen der Kund:innen, aufgenommen werden und bspw. in die Erstellung der Schutzbedarfskategorien oder der Schutzbedarfsfeststellung einfließen.
Der organisatorische Teil wurde in der ersten Phase des ISMS und in der Umsetzung der Maßnahme bedient. Bei Ersterem wurden die Verantwortlichkeiten definiert und das Bekenntnis der Geschäftsführung dokumentiert. Bei der Umsetzung der Maßnahme wird die Kennwort-Richtlinie formuliert und zur Prüfung, bzw. zur Freigabe vorgelegt. Beide Vorgänge sind essentielle Bestandteile im Bereich der Organisation. Im weiteren Verlauf müssen weitere Richtlinien verabschiedet werden, um so den Mitarbeiter:innen einen Handlungsrahmen vorzugeben. Zusätzlich sollten weitere Stellen in den Abteilungen festgelegt werden, die bei der Umsetzung der Maßnahmen unterstützen, aber auch bei der Bewertung der Wirksamkeit und Praktikabilität von neuen und alten Maßnahmen dem IS-Management-Team zur Seite stehen. Abseits dessen müssen bereits vorhandene

Schulungen und Sensibilisierungsmaßnahmen im ISMS dokumentiert und protokolliert werden.
Die Umsetzung der Kennwort-Richtlinie führt dazu, dass die Konfiguration von zwei Diensten angepasst werden muss. Dies fällt in den technischen Bereich. Die technische Maßnahme wurde beleuchtet und die Testläufe vorbereitet. Weiterhin wurde die Strukturanalyse aus der Vorarbeit übernommen und in das ISMS integriert. Damit wurde eine Übersicht von Diensten, Prozessen, IT-Systemen und Applikationen erstellt. Die übertragene Übersicht wurde 2019 erstellt und muss dem aktuellen Umfeld entsprechend angepasst werden. Anschließend kann die Übersicht für die Schutzbedarfsfeststellung oder für die Folgenabschätzung bei der Einführung von Maßnahmen verwendet werden. Nach der Umsetzung des Basisschutzes sollte die Risikoanalyse und -behandlung eingeführt werden.
Während der Formulierung und Spezifikation der Kennwort-Richtlinie und während der Ermittlung der Umsetzungsmöglichkeiten bei den Diensten wurden die (Zwischen-)Ergebnisse stets mit den Einscheidungsträger:innen abgestimmt, sodass die Vorgänge stets in Übereinstimmung mit der Prozesswelt des Unternehmens durchgeführt wurden. Diese Abstimmung ist Teil des Qualitätsmanagements, das den vierten Teil des ISMS darstellt. Ebenso fällt auch die Vorlage des Entwurfes der Richtlinie zur Prüfung in diesen Bereich. Zusätzlich können die Übersichten auf der Homepage des ISMS im Confluence zur Bewertung der Qualität genutzt werden. Nach der Umsetzung der Maßnahme sollte im Rahmen des Qualitätsmanagements die Überprüfung dieser nach spätestens einem Jahr durchgeführt werden.
Die Einführung des ISMS in Jira und in Confluence stellen die Kernpunkte der Dokumentation dar. Im Confluence Space werden die Informationen, wie bspw. die Verantwortlichkeiten oder der Anwendungsbereich in aufbereiteter Form zur Verfügung gestellt. Zusätzlich werden Richtlinien und Maßnahmen erfasst und dokumentiert. Für die bessere Bedienung wurden bspw. Vorlagen eingefügt. Im Jira Projekt ISMS findet die Projektverwaltung statt. Aufgaben und neue Maßnahmen, wie die Erstellung der Kennwort-Richtlinie, werden hier koordiniert und deren Umsetzung protokolliert. Beide Dienste greifen auf einander zu und können somit Informationen und Übersichten zur Verfügung stellen. Der Ausbau der beiden Werkzeuge kann die Arbeit mit dem ISMS maßgeblich vereinfachen und strukturieren, sodass eine konsistente und übersichtliche Dokumentation erzeugt wird.
Der letzte Teil des ISMS ist die Ausgabe. Diese fällt im derzeitige Bearbeitungszustand des ISMS gering aus, da es sich im Aufbau befindet und folglich die Aussagekraft zur Informationssicherheit im Unternehmen vergleichsweise schwach

ist. Dennoch können bereits jetzt die Übersichten auf der Homepage des ISMS anzeigen, in welchem Zustand sich eine Maßnahme oder die Richtlinie befinden und wie viele offene Vorgänge es zur Zeit gibt. Zusätzlich verbessert die Kennwort-Richtlinie die Auskunftsfähigkeit des Unternehmens. Diese kann durch weitere Richtlinien oder dokumentierte Maßnahmen weiter ausgebaut werden. Abseits dessen, können angestrebte Verbesserungen und Fehlerkorrekturen durch „Improvements"- oder „Tasks"-Tickets im Jira festgehalten werden, wodurch weitere Metriken generiert werden können.
Die Umsetzung des beschriebenen Aufbaus des überarbeiteten ISMS stellte bei der Konzeption und Einführung des ISMS in Jira und Confluence einen wichtigen Rahmen und konnte weitestgehend integriert werden.

Kritik an dem überarbeiteten ISMS Der Aufbau und die Phasen des ISMS sind im Rahmen der Realisierung praktikabel einsetzbar und bieten den Anwender:innen einen Rahmen sowie einen Ablaufplan für die Umsetzung des ISMS. Es zeigte sich jedoch, dass die strikte Einhaltung der Phasen zwar eine koordinierte und strukturierte Vorgehensweise ermöglicht, jedoch im Rahmen einer flexiblen Unternehmenskultur mit zeitkritischen Anforderungen den Prozessfortschritt hemmt. Es wäre daher die Etablierung einer parallelen Vorgehensweise zweckdienlich. Dies hätte jedoch auch zu Folge, dass die Verwaltung der Vorgänge komplexer ausfällt. Zudem ist zu kritisieren, dass die Definition der Schutzbedarfskategorien auch nach der Etablierung des Basisschutzes ausgeführt werden kann. Die Kategorien, bzw. der Schutzbedarf eines Assets wird erst relevant, wenn das Asset in die Klassifizierung „kritisch" fällt und deswegen über den Basisschutz hinaus weitere Maßnahmen umgesetzt werden müssen. Es wäre daher praktischer, wenn vor der Definition der Schutzbedarfskategorien die Umsetzung des Basisschutzes erfolgt und somit auch das Sicherheitsniveau deutlich früher angehoben wird. Gleichwohl ist hierbei anzumerken, dass bei zu geringen personellen Ressourcen dieses Vorgehen die vollständige Beschreibung des Verbundes (Definition Anwendungsbereich und Schutzkategorien, Strukturanalyse, bzw. Inventarisierung) verzögert. Daher bleibt der Verbesserungsvorschlag, dass die Teilvorgänge im Phasenmodell entsprechend der personellen Ressourcen, sofern nicht auf einander aufbauend, zu parallelisieren sind. Bei geringen personellen Ressourcen sollte die sequentielle Vorgehensweise gewählt werden.

4.4.2 Bewertung der Realisierung mittels Atlassian Jira und Confluence

Das Unternehmen hat sich für den Lösungsansatz I Atlassian Jira und Confluence aufgrund der hohen Flexibilität der Software, der ausbleibenden Anschaffungskosten und der bereits vorhandenen Erfahrung und Nutzung in der Firma entschieden. Im Zuge der Einführung des ISMS wurde im Kapitel 4.1 beschrieben, wie der dazugehörige Space im Confluence und im Kapitel 4.2, wie das dazugehörige Projekt im Jira eingerichtet und konfiguriert wurde. Anschließend wurde im Kapitel 4.3 erläutert, wie eine Maßnahme mit den eingerichteten Werkzeugen weitestgehend umgesetzt werden konnte. Nachdem diese praktischen Erfahrungen gesammelt wurden, folgt im Anschluss eine kritische Nachbetrachtung des ausgewählten Lösungsansatzes.

Auswertung der Nutzung von Confluence zur Dokumentation des ISMS Atlassian weist Confluence als kollaboratives Wissensverwaltungswerkzeug aus[12]. Dieses wird in der Firma zur Projektdokumentation oder zu kollaborativem Arbeiten an Informationen genutzt. Die Einrichtung des ISMS und die exemplarische Umsetzung der Maßnahme haben gezeigt, dass sich die Software zur Dokumentation des ISMS eignet. Die Form der Seiten wurde bspw. durch das Einrichten von Vorlagen standardisiert. Bei der Erstellung neuer Seiten können diese ausgewählt werden und erzeugen damit das gleiche Layout und vergeben auch gleichzeitig die gewünschten Labels. Dadurch können auf der einen Seite die Ansprüche an die Form der Dokumentation seitens des ISMS erfüllt werden und zum anderen sorgt diese Vereinheitlichung für eine bessere Wahrnehmung bei der Navigation durch das ISMS. Darüber hinaus wurden Makros genutzt, um die Informationen auf anderen Seiten in Form von Übersichten oder durch komplettes Einfügen verfügbar zu machen. Soweit möglich wurden die Markos ebenso in die Vorlagen eingebaut. Diese beiden Anpassungen bewirken unter anderem eine erhöhte Akzeptanz des Werkzeugs zur Dokumentation. Weitere Verbesserungen durch Makros oder durch Standardwerkzeuge von Confluence wurden nicht evaluiert, sind aber durchaus denkbar.
Bei der Realisierung wurde auf eine möglichst kostensparende Variante geachtet. Somit wurden ausschließlich die vorhandenen Addons und Plugins verwendet. Wenngleich dadurch keine weiteren Kosten aufgeworfen wurden, führt dieser Ansatz zu einer starken personellen Belastung. Auf dem Marketplace von Atlassian bieten diverse Firmen Vorlagen für ein ISMS an. Die Vorlagen fokussieren in den meisten Fällen eine Zertifizierung nach ISO / IEC 27001. Da dies im Rahmen der

[12] AtloJa.

Arbeit nicht notwendig war, wurde die Struktur des ISMS von der Ausarbeitung innerhalb der Arbeit abgeleitet und umgesetzt. Folglich mussten und müssen Verweise auf und Anforderungen von Normen, Standards oder Richtlinien manuell eingepflegt und nachgeschlagen werden, was in der Summe für den erwähnten hohen Aufwand sorgt. Hier sollte vor der weiteren Bearbeitung der Thematik eine Schätzung des Aufwands der restlichen Umsetzung erfolgen, sodass diese mit den finanziellen Kosten für die Nutzung eines Addons verglichen werden kann. Dabei gilt es zu beachten, dass manche Addons weitere Addons benötigen, wodurch weitere und möglicherweise dauerhafte Kosten entstehen.
Ein weiterer Kritikpunkt ist die Kommentierung beim Editieren von Seiten. Wird eine Seite bearbeitet, ist die Person nicht gezwungen eine Beschreibung der Bearbeitung in das Kommentarfeld einzufügen. Dieser Umstand mag bei einem ISMS an sich trivial erscheinen, jedoch wird dies ein relevanter Punkt, wenn eine Zertifizierung und damit ein Audit ansteht. Viele Standards erwarten eine erneute Abnahme eines Dokumentes durch die verantwortlichen Person, wenn eine Änderung vorgenommen wurde. War die Änderung trivial, ist keine erneute Prüfung und Freigabe erforderlich. Fehlt aber der beschreibende Kommentar für die Änderung, müssen im Zweifelsfall die Änderungen überprüft oder eine erneute Freigabe vergeben werden. Der Marketplace bietet ein Addon „Comala Document Management“[13], das unter anderem diese Verbindlichkeit realisiert. Da das Addon noch weitere praktische Funktionalitäten aufweist, wurde das Thema an die Entscheidungsträger:innen herangetragen und befindet sich zur Zeit in der Abwägung.
Atlassian Confluence ermöglichte die Einführung der Dokumentation des ISMS mit den Standardwerkzeugen. Die Ausarbeitung, Weiterentwicklung und Nutzung des ISMS kann wie bisher weitergeführt werden oder durch die Nutzung von potentiell kostenpflichtigen Vorlagen und Addons verbessert und effizienter gestaltet werden.

Auswertung der Nutzung von Jira zur Projektverwaltung des ISMS Atlassian beschreibt Jira als Werkzeug zur agilen Projektverwaltung[14]. Jira wird im Unternehmen für die Projektverwaltung mittels Ticket-System genutzt. Um die zahlreichen Aufgaben des ISMS zu verwalten wurde daher das Projekt ISMS in Jira eingeführt und konfiguriert. Das Projekt wurde durch die Konfiguration an die Anforderungen des ISMS angepasst. Dabei wurde ein neuer Workflow erstellt, der die Anwender:innen bei der Erstellung einer neuen Maßnahme durch den Prozess führt. Um möglichst viele Aufgaben des ISMS im Projekt abbilden zu können, wurden neue Vorgangstypen eingeführt. Durch die Verwendung potentiell kri-

[13] Link: https://marketplace.atlassian.com/apps/142/comala-document-management
[14] AtloJb.

tischer Informationen in den Tickets mussten die Rechte zur Bearbeitung oder Sichtung eingeschränkt werden. Dies wurde durch die Erstellungen, Anpassung und Zuweisung eines neuen vereinfachten Rechteschema bewirkt. Diese Konfigurationsanpassungen deuten bereits die Möglichkeiten zur Arbeitsablaufverbesserung im Jira an. Zusätzlichen können die Informationen der Tickets, wie bspw. der Status, das Fälligkeitsdatum oder die aktuell bearbeitende Person, durch ein Makro im Confluence visualisiert werden.
Innerhalb der Arbeit konnten die Screens nicht im Detail behandelt werden, wenngleich diese den Workflow weiter vereinfachen und effizienter gestalten können. Ein Screen gibt an, welche Felder auf einer Maske angezeigt werden sollen. Eine Maske wird bei der Erstellung, Bearbeitung oder beim Statuswechsel angezeigt. Für jeden dieser Schritte kann eine separate Maske ausgewählt werden, sodass eine Person ausschließlich die relevanten Felder angezeigt bekommt. Diese Felder können zudem als obligatorisch gekennzeichnet werden. Weiterhin bietet Jira durch das in der Firma bereits genutzte Addon „Automate for Jira-Server lite“[15] die Möglichkeit aufgrund von Ereignissen Aktionen auszuführen. So könnte bspw. der Statusübergang „Ready to approve“ dazu führen, dass das Ticket der für die Freigabe verantwortlichen Person zugewiesen wird. Die Automatisierung könnte auch beim Review-Prozess zum Einsatz kommen, sodass in einem gesetzten Intervall ein Maßnahmen-Ticket wieder geöffnet und einer Person zugewiesen wird, die dann die Maßnahmen prüft und ggf. weitere Schritte einleitet. Trotz der breiten Anwendungsfläche dieses Addons gibt es auch negative Punkte. Die aktuell verwendete Version ist eine Lite-Variante und in einem Funktionsumfang eingeschränkt. Die normale Version[16] ist für die Server-Variante von Jira nicht weiter erhältlich. Weiterhin können ausschließlich Jira-Systemadministrator:innen die Automatisierungen anlegen und verwalten, sodass die Aufgabe für zusätzliche Aufwände in der internen IT sorgt. Die normale Variante bietet die Möglichkeit den Projektadministrator:innen das Recht zum Erstellen von Automatisierungen zuzuordnen.
Die Projektverwaltung des ISMS konnte mittels Jira umgesetzt werden. Die Konfiguration des Projektes sorgte für eine erste Verbesserung des Projektvorgangs, den es im weiteren Verlauf auszubauen und an die aktualisierten Anforderungen anzupassen gilt.

[15] Link: https://marketplace.atlassian.com/apps/1211836/automation-for-jira-server-lite
[16] Link: https://marketplace.atlassian.com/apps/1215460/automation-for-jira

5 Auswertung und Ausblick

Die Ausarbeitung der Master-Thesis ist abgeschlossen und es bleibt ein Fazit aus der Arbeit zu ziehen. Im Folgenden wird zuerst eine kritische Nachbetrachtung vorgenommen und der Ablauf reflektiert. Abschließend wird der Ausblick festgehalten und das Vorgehen für die nächsten Schritte empfohlen.

5.1 Kritische Nachbetrachtung

Die Arbeit konnte im Kern umgesetzt werden und das Ziel, ein konzeptionell überarbeitetes ISMS zu erstellen und dieses in einer Praxisumsetzung mit einer geeigneten Softwarelösung zu prüfen, wurde weitestgehend erfüllt.
Im ersten Kapitel wurden, nach einer kurzen Einleitung, die Beweggründe für die Themenwahl und die Anforderungen bzgl. des Nachweises von Informationssicherheit als Herausforderung der Unternehmen beschrieben. Das Kapitel schloss mit der Zielstellung und der geplanten Vorgehensweise für die vorliegende Arbeit ab.
Das zweite Kapitel diente der Aufarbeitung der Grundlagen und der theoretischen Betrachtung eines ISMS. Dabei wurden zunächst Grundbegriffe erklärt, die für das Verständnis der Arbeit wichtig sind. Anschließend wurden zwei Standards, die ISO / IEC 27001 und der BSI IT-Grundschutz, bzw. BSI-Standard 200-x, sowie die Richtlinie VdS 10000 zur Umsetzung eines ISMS detailliert betrachtet.
Im dritten Kapitel wurde das konzeptionell überarbeitete ISMS vorgestellt und es fand die Evaluation einer geeigneten Softwarelösung statt. Dabei wurden zunächst die Gemeinsamkeiten der drei Normen herausgestellt, worauf folgend der Aufbau und die Phasen des überarbeiteten ISMS ausgeführt wurden. Anschließend wurden die Anforderungen der Firma und die Vorarbeiten festgehalten und drei Lösungsansätze für die Realisierung des ISMS mit einer geeigneten Software ausgearbeitet. Das Kapitel schloss mit einer Empfehlung ab.
Im vierten Kapitel wurde die Einführung des überarbeiteten ISMS und die Umsetzung einer Maßnahme beschrieben und es erfolgte eine kritische Nachbetrachtung des ausgearbeiteten ISMS und der Nutzung der Softwarelösung. Am Anfang wurde die Einführung des überarbeiteten ISMS in das Unternehmen durch den Lö-

sungsansatz I, Realisierung in Atlassian Confluence und Jira, beschrieben. Dabei wurden die Einrichtung und Konfiguration des Projektes und Spaces beschrieben, wie auch die Anpassung der Werkzeuge an die Arbeit im ISMS. Anschließend wurde die Umsetzung der Kennwort-Richtlinie als Fallbeispiel genutzt, um die Realisierung einer Maßnahme zu veranschaulichen und die Praxistauglichkeit des ISMS zu prüfen. Das Kapitel schloss mit einer kritischen Nachbetrachtung ab. In dieser wurde das umgesetzte ISMS mit dem in Kapitel drei ausgeführten ISMS abgeglichen. Anschließend wurde die Nutzbarkeit und das Potential des ausgewählten Lösungsansatzes beleuchtet.
Initial wurde mit der vorliegenden Arbeit die vollständige Umsetzung eines ISMS bis einschließlich Phase drei im Unternehmen angestrebt, sodass eine Selbstauskunft nach TISAX ermöglicht wird. Aufgrund mangelnder Erfahrungen bei der Einführung und Wartung eines ISMS zeigte sich, während der Arbeit am und im ISMS, dass der Aufwand unterschätzt wurde. Daher wurde sich frühzeitig dazu entschieden, dass ISMS im Rahmen der Arbeit reflektiert und nachhaltig aufzubauen, sodass dieses Fundament für den weiteren Ausbau genutzt werden kann. Da die Einführung eines ISMS, gleich welcher Art, für gewöhnlich von mehreren Personen ausgeführt wird, die vorliegende Arbeit jedoch ohne Unterstützung erstellt werden musste, wurde der Aufwand auf diese Art reduziert. Dies hat zur Folge, dass Teile, wie bspw. die Ausgabe des ISMS, in dieser Arbeit nicht vollständig auf Tauglichkeit geprüft werden konnten.
Der Beschäftigung mit den Standards und der Richtlinie im zweiten Kapitel wurde verhältnismäßig viel Raum eingeräumt. Eine kürzere Darstellung der Inhalte wären dem Verständnis nicht abträglich gewesen und hätte für mehr Kapazitäten an anderen Stellen gesorgt. Dennoch konnte so ein detailliertes Verständnis von der Wirk- und Arbeitsweise der Dokumente gewonnen werden, das im weiteren Verlauf der Arbeit hilfreich eingesetzt werden konnte.
Die exemplarische Umsetzung der Maßnahme erfolgte zu spät innerhalb der Arbeit, sodass am Ende die Reaktion der Fachabteilungen und die Freigabe durch die Entscheidungsträger:innen für die Realisierung der Maßnahmen und die Kennwort-Richtlinie nicht mehr rechtzeitig eintrafen. Dies bewirkte, dass die Maßnahmen nur bis zum Prüf-Status und bis zur Testphase bearbeitet wurden und die abschließende Handhabung nur theoretisch beschrieben werden konnte. Gleichwohl dies einen Kritikpunkt darstellt, wurden die restlichen Schritte der Umsetzung so beschrieben, dass der Prozess in Gänze abgebildet und somit eine Vorstellung der Arbeit im ISMS vermittelt werden konnte.
Gleichwohl diese Kritikpunkte bestehen, konnte ein konzeptionell überarbeitetes ISMS erstellt, in einer Praxisumsetzung in der Firma eingeführt, auf Tauglichkeit

geprüft und mit Inhalten befüllt werden, sodass die ersten Schritte zum verbesserten und reflektierten Umgang mit Informationssicherheit gesetzt wurden. Das so gesetzte Fundament stellt eine solide Basis für das weitere Vorgehen dar.

5.2 Ausblick

Das eingeführte ISMS wird im weiteren Verlauf ausgebaut und gegen Ende des ersten Quartals 2023 die Phase drei erreicht haben. Da die weitere Arbeit im ISMS nicht an die Anforderungen einer Master-Thesis gebunden ist, kann die als Verbesserungsvorschlag im Kapitel 4.4.1 angebrachte parallele Bearbeitung von Aufgaben erfolgen, sodass der Fortschritt des ISMS effizienter und beschleunigt umgesetzt wird. Dabei sollte der Verbund vollständig definiert und der Basisschutz etabliert werden. Die Arbeit im ISMS wird weiteres Verbesserungspotential hervorbringen, dass sich durch Anpassungen an der Konfiguration des Projektes oder des Spaces beantworten ließe. Zudem sollte der Erwerb des Addons „Comala Document Management“ thematisiert werden, um die Handhabung im Confluence zu erleichtern und den Anforderungen an das ISMS gerecht zu werden. Ist diese Basis soweit ausgebaut, wird das Qualitätsmanagement und die Ausgabe eine deutlich wichtigere Rolle spielen. Durch die kontinuierliche Arbeit am ISMS und dem voranschreitenden Ausbau der Informationssicherheit ließe sich auch eine erneute Bewertung der Nutzbarkeit des überarbeiteten ISMS vornehmen, die dann auf einem deutlich ausgeweiteten Erfahrungsschatz fußen würde.
Wenngleich dieser Ausblick recht positiv ist, sollte der Aufwand zur Umsetzung des ISMS nicht unterschätzt werden. Ein ISMS muss kontinuierlich bearbeitet, überarbeitet und gewartet werden, damit es der Informationssicherheit auch wirklich nützt. Somit sollten auch für die weitere Einführung, die Betreuung und die Pflege ausreichend Ressourcen in Form von Personal und Zeit zur Verfügung gestellt werden. Denn wie der Volksmund in Kurzform spricht, so wusste auch schon Herr von Grimmelshausen:

> „Gut Ding will Weile haben! Vortreffliche Sachen werden ohne große Mühe und Arbeit nicht erworben, sonst würde jeder Narr ohn[sic] Schnaufens und Bartwischens einen solchen edlen Sauerbrunn zuwege bringen.“
>
> Aus H. J. C. von Grimmelshausen's *Der abenteuerliche Simplicissimus*[1]

[1] Gri17, S. 340.

Literaturverzeichnis

[AtloJa] Atlassian: *Confluence, Accomplish more together*, o. J.
https://www.atlassian.com/software/confluence

[AtloJb] Atlassian: *Jira, Schnelles Vorankommen, gute Koordination und bessere Builds – in Zusammenarbeit*, o. J.
https://www.atlassian.com/de/software/jira

[AtloJc] Atlassian: *Moving to a Cloud future, together*, o. J.
https://www.atlassian.com/migration/assess/journey-to-cloud
Abruf: 15. 10. 2022

[BSI08] BSI: *BSI-Standard 100-4, Notfallmanagement*, 2008,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2
Abruf: 03. 10. 2022

[BSI17a] BSI: *BSI-Standard 200-1, Managementsysteme für Informationssicherheit (ISMS)*, 2017,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2
Abruf: 16. 01. 2022

[BSI17b] BSI: *BSI-Standard 200-2, IT-Grundschutz-Methodik*, 2017,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2
Abruf: 07. 08. 2022

[BSI17c] BSI: *BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz*, 2017,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=

publicationFile&v=2
Abruf: 07. 08. 2022

[BSI18] BSI: *Anleitung zur Migration von Sicherheitskonzepten, Hilfsmittel zum modernisierten IT-Grundschutz*, 2018,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Anleitung_zur_Migration.pdf?__blob=publicationFile&v=1
Abruf: 10. 07. 2022

[BSI22] BSI: *IT-Grundschutz-Kompendium*, 2022,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=3
Abruf: 07. 08. 2022

[BSIoJa] BSI: *4.3 Risiken bewerten*, o. J.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/4_RisikenAnalysieren/2_Risiken%20bewerten/RisikenBewerten_node.html
Abruf: 03. 07. 2022

[BSIoJb] BSI: *Deutschsprachiges Glossar*, o. J.
https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/Functions/glossar.html?nn=520190&cms_lv2=132764
Abruf: 22. 06. 2022

[BSIoJc] BSI: *ISO 27001 Zertifizierung auf Basis von IT-Grundschutz*, o. J.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html
Abruf: 10. 07. 2022

[BSIoJd] BSI: *IT-Grundschutz, Informationssicherheit im System*, o. J.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
Abruf: 05. 07. 2022

[DIN14] DIN: *ISO/IEC 27001 Technical Corrigendum 1, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen*, 2014,
`https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:224185780`
Abruf: 04. 08. 2022

[DIN15] DIN: *ISO/IEC 27001 Technical Corrigendum 2, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen; Korrektur 2*, 2015,
`https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:246061472`
Abruf: 04. 08. 2022

[DIN17a] DIN: *DIN EN ISO/IEC 27001, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*, 2017,
`https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:269670716`
Abruf: 06. 08. 2022

[DIN17b] DIN: *ISO/IEC 27003, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anleitung*, 2017,
`https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:273220362`
Abruf: 07. 08. 2022

[DIN18] DIN: *ISO/IEC 27005, Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement*, 2018,
`https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:293433974`
Abruf: 07. 08. 2022

[DIN20] DIN: *DIN EN ISO/IEC 27000, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020*, 2020,
`https://www.beuth.de/de/norm/iso-iec-27000/286523288`
Abruf: 06. 08. 2022

[DIN22] DIN: *DIN EN ISO/IEC 27002:2022-08 - Entwurf, Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche und Englische Fassung prEN ISO/IEC 27002:2022*, 2022,
`https://www.beuth.de/de/norm-entwurf/din-en-iso-iec-27002/354833769`
Abruf: 06. 08. 2022

[ENXoJ] ENX: *TISAX*, o. J.
`https://www.enx.com/en-US/TISAX/`
Abruf: 16. 01. 2022

[Gri17] Grimmelshausen, H. J. C. v.: *Der abenteuerliche Simplicissimus, Das ist Beschreibung des Lebens eines seltsamen Vaganten*, hrsg. von Kolbenheyer, E. G., 2017,
`https://www.gutenberg.org/files/55171/55171-h/55171-h.htm`
Abruf: 20. 11. 2022

[HiS22] HiScout: *Systemvoraussetzungen, Gültig ab: HiScout 3.8.0*, Wurde im Anhang zur Verfügung gestellt, 18. Mai 2022

[ISO13] ISO: *ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements*, 2013,
`https://www.iso.org/standard/82875.html`
Abruf: 03. 07. 2022

[ISOoJa] ISO: *ISO/IEC 27001, INFORMATION SECURITY MANAGEMENT*, o. J.
`https://www.iso.org/isoiec-27001-information-security.html`
Abruf: 20. 01. 2022

[ISOoJb] ISO: *ISO/IEC FDIS 27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, o. J.
`https://www.iso.org/standard/54534.html`
Abruf: 04. 08. 2022

[Kus22] Kussmann, C.: *Cyberangriffe und Schäden bei KMU*, 2022,
`https://www.experten.de/2022/04/cyberangriffe-und-schaeden-bei-kmu/`
Abruf: 14. 11. 2022

[Lie18] Lies, J.: *Unternehmenskultur*, 2018,
`https://wirtschaftslexikon.gabler.de/definition/unternehmenskultur-49642/version-272870`
Abruf: 20. 09. 2022

[LS17a] Luber, S. und Schmitz, P.: *Was ist der IT-Grundschutz des BSI?, Definition IT-Grundschutz (BSI*, 2017,
`https://www.security-insider.de/was-ist-der-it-grundschutz-des-bsi-a-648864/`
Abruf: 10. 07. 2022

[LS17b] Luber, S. und Schmitz, P.: *Was ist ein Information Security Management System (ISMS)?, Definition ISMS*, 2017,
`https://www.security-insider.de/was-ist-ein-information-security-management-system-isms-a-648735/`
Abruf: 21. 06. 2022

[Ser22] SerNet GmbH: *verinice. Benutzerhandbuch 1.24.1*, Im Lieferumfang der Verinice.EVAL enthalten., 2022

[SeroJa] SerNet GmbH: *Systemanforderungen, für verinice. und verinice.PRO (Server)*, o. J.
`https://verinice.com/support/systemvoraussetzungen`
Abruf: 23. 10. 2022

[SeroJb] SerNet GmbH: *verinice. im Detail, Möglichkeiten und Funktionen des ISMS-Tools*, o. J.
`https://verinice.com/produkte/details`
Abruf: 15. 10. 2022

[SeroJc] SerNet GmbH: *verinice.EVAL (1.24.1)*, o. J.
`https://shop.verinice.com/de/software/19/verinice.eval-1.24.1?c=22`
Abruf: 30. 10. 2022

[Spi19] Spillner, R.: „IT-Sicherheitskonzept, Schutzbedarfsfeststellung“, Freigabe auf Anfrage, Projektarbeit IV, Duale Hochschule Gera-Eisenach, 2019

[TÜVoJ] TÜV Rheinland: *ISO 27001 Zertifizierung – Informationssicherheit*, o. J.
`https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html`
Abruf: 16. 01. 2022

[VdS16] VdS Schadenverhütung GmbH: *VdS 2007 : 2016-03 (04), Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen*, 2016,
`https://shop.vds.de/publikation/vds-2007/1b81f2cc-43e4-4065-a359-a4a1e08a34a8`
Abruf: 09. 09. 2022

[VdS18] VdS Schadenverhütung GmbH: *VdS 10000 : 2018-12 (02), Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), Anforderungen*, 2018,
`https://shop.vds.de/publikation/vds-10000`
Abruf: 25. 09. 2022

[VdS20] VdS Schadenverhütung GmbH: *VdS 10020: Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme*, VdS 10020 : 2020-04 (02), VdS Schadenverhütung GmbH, Köln, 2020

[VdS21] VdS Schadenverhütung GmbH: *Informationssicherheits-Management mit Zertifikat, Informationsverarbeitung für den Mittelstand*, 2021,
`https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10000-informations-sicherheit-fuer-kmu`
Abruf: 10. 07. 2022

[VdS22] VdS Schadenverhütung GmbH: *VdS 10010: VdS-Richtlinien zur Umsetzung der DSGVO, Anforderungen*, VdS 10010 : 2022-07 (02), VdS Schadenverhütung GmbH, Köln, 2022

Bildverzeichnis

Tabellenverzeichnis

Ausgaben

Anhang

A.1 BSI 200-1 Tabellen

A.1.1 Aufgaben und Pflichten des Managements

Aufgabe / Pflicht	**Beschreibung**
Übernahme der Gesamtverantwortung für IS	Die Geschäftsführung trägt die Verantwortung für die Gewährleistung von IS. Die Geschäftsführung und andere Führungskräfte übernehmen Verantwortung und bringen den Mitarbeiter:innen die Bedeutung von IS näher.
IS initiieren, steuern und kontrollieren	• IS-Strategie und Sicherheitsziele verabschieden und kommunizieren • Entscheidung über Umgang mit Risiken treffen • Schaffen organisatorischer Rahmenbedingungen für IS • Zuständigkeiten und Befugnisse zuweisen • Bereitstellung von Ressourcen für IS • Anbieten von Schulungen und Sensibilisierungsmaßnahmen zum Thema IS für Mitarbeiter:innen
IS integrieren	Integration von IS in allen Prozessen und Projekten, bei denen Informationen verarbeitet werden.
Erreichbare Ziele setzen	Ziele sollten entsprechend der Möglichkeiten und Ressourcen gesetzt werden, sodass bspw. eine Vollabsicherung das langfristige Ziel ist, das durch Umsetzen kleiner Kernabsicherungen und der Basisabsicherung iterativ erreicht wird.
Sicherheitskosten gegen Nutzen abwägen	Evaluation der Abhängigkeiten von Geschäftsprozessen und Informationsverarbeitungen als Basis für eine fundierte Auswahl an Sicherheitsmaßnahmen. Es sollten stets die organisatorischen Maßnahmen bei der Einführung von technischen Maßnahmen beachtet werden.
Vorbildfunktion	Die Geschäftsführung zeigt ihr Bekenntnis zur und ihre Wahrnehmung der IS durch eigene Teilnahme an Schulungen und Maßnahmen und durch die Einhaltung von Sicherheitsregeln.

Tabelle A.1: Aufgaben und Pflichten des Managements[1]

[1] Quelle: selbst erstellte Zusammenfassung von [BSI17a, S. 20-22]

A.2 VdS 10000 Tabellen

A.2.1 Organisationseinheiten des ISMS nach VdS 10000

Einheit	**Verantwortung**
IST	setzt sich aus Vertreter:innen der anderen Einheiten zusammen und unterstützt ISB durch: • Erkennen und Bewerten neuer Bedrohungen und Schwachstellen • Entwickeln und Bewerten von Maßnahmen zur Informationssicherheit • organisationsweites Steuern und Koordinieren der Maßnahmen zur Informationssicherheit
IT-Verantwortliche	setzen die Richtlinie im Verantwortungsbereich um und stimmen Verbesserungsvorschlägen und Maßnahmen mit ISB ab.
Administrator:innen	implementieren technische Maßnahmen nach Abstimmung mit der IT-verantwortlichen Person.
Vorgesetzte	stellen sicher, dass Mitarbeiter:innen die TOMs für Informationssicherheit umsetzen und einhalten.
Mitarbeiter:innen	müssen Maßnahmen umsetzen und einhalten und melden Störungen, Sicherheitsvorfälle und Ausfälle.
Projektverantw.	konsultieren ISB in Bezug auf sicherheitsrelevante Aspekte bei ihren Projekten.
Externe	werden verpflichtet die in der Organisation geltenden Sicherheitsanforderungen durch Einhalten und Umsetzen der angeordneten Maßnahmen zu wahren, sofern sie Zugriffe auf IT-Strukturen oder kritische Informationen des Unternehmens haben.

Tabelle A.2: Organisationseinheiten des ISMS nach VdS 10000[2]

[2][selbst erstellte Zusammenfassung nach VdS18, S. 14-15]

A.2.2 Identifikation kritischer IT-Ressourcen nach VdS 10000

Asset	**Anforderung**
Prozesse	Identifikation und Dokumentation von zentralen Prozessen und Prozessen mit hohem Schadenspotential, wobei folgendes Dokumentiert werden muss • Beschreibung des Prozesses • Begründung der Einordnung • Prozessverantwortliche Person • maximal tolerierbare Ausfallzeit (MTA) des Prozesses
Informationen	Prüfung und Dokumentation der Speicherung, Verarbeitung oder Übertragung von kritischen Informationen. Kritische Informationen führen zu katastrophalen Schäden bei der Verletzung der Vertraulichkeit, der Integrität, der Verfügbarkeit oder dem Überschreiten des maximal tolerierbaren Datenverlustes, die mit weniger als 24h festgelegt wurde. Die Dokumentation muss die Entscheidungskriterien für die Einstufung der Kritikalität und die Begründung zur Einstufung der Information enthalten.
IT-Ressourcen	Identifikation und Dokumentation kritischer IT-Ressourcen. Kritische IT-Ressourcen verarbeiten, speichern oder übertragen kritische Informationen oder sind zur Umsetzung eines zentralen Prozesses oder eines Prozesses mit hohem Schutzbedarf zwingend notwendig. Die Dokumentation muss die Beschreibung der Ressource, die Begründung der Einordnung und die MTA der Ressource umfassen.

Tabelle A.3: Identifikation kritischer IT-Ressourcen[3]

[3][selbst erstellte Zusammenfassung nach VdS18, S. 19-21]

A.3 Vergleich der Standards und der Richtlinien

Standard, Norm, Richtlinie / Kriterium	**ISO / IEC 27001**	**BSI Standard 200-2**	**VdS 10000**
Herausgeber	International Organization for Standardization	Bundesamt für Sicherheit in der Informationstechnik	Verband der Sachversicherer e.V
Erstveröffentlichung	2013	2017	2018
Aktuelle Edition, Veröffentlichungsjahr	2, 2017	1.0, 2017	1, 2018
Reviewzyklus	5 Jahre	unbekannt	unbekannt
Seitenanzahl (Gesamt)	35	48	43
Ergänzende Dokumente	✔	✔	✔
Einstiegsfreundlich	✘	✔	✔
Zertifizierbar	✔	✔	✔
Verbreitung	international	europaweit, vermehrt in Deutschland	deutschlandweit
Kostenlos (Preis)	✘ (98,30 €[4])	✔	✘ (83,18 €)[5]

Tabelle A.4: Vergleich der Standards / Richtlinien[6]

[6] selbst erstellte Zusammenfassung

A.4 Informationssammlung zu Softwarelösungen für ISMS

Name	Link	OpenSource	Kosten	Kommentar
Atlassian Jira / Confluence	• Atlassian | Software Development and Collaboration Tools • Jira | Issue & Project Tracking Software | Atlassian • Confluence | Your Remote-Friendly Team Workspace | Atlassian	✗	für Server-Version nicht mehr einsehrbar	• Aktuell in Verwendung • dadurch keine zusätzlichen Anschaffungskosten für Basissoftware • Mögliche zusätzliche Kosten durch Plugins • hoher Einrichtungsaufwand
Eramba	• https://www.eramba.org/	✓	2500 € / Jahr	• eingeschränkte Community-Edition verfügbar • Automatisierung, Benachrichtigung und weiter Funktionen nur in Enterprise-Edition enthalten
Verinice	• The Open Source ISMS Tool | verinice. • Verinice - IT Internal Services - Confluence dotSource GmbH	✓	mind. 595,00 € /Jahr	• aktuell nur als AP-Lizenz vorhanden • Weitere Kosten fallen durch Content-Erweiterungen an • Support kostet extra • Führen zur Zeit ein Rebuild aus Verinice.Veo • ISMS für .Veo erst 2023 • unterstützt viele Standards
CertVision NormTracker	• CertVision	✗	ab 2400 € / Jahr	• Deutsches Unternehmen, • Teil von TeccleGroup • 2018 gegründet • vermutlich kleines Unternehmen • SaaS-Lösung
ibi systems iris	• ISMS- und GRC-Management - ibi systems GmbH (ibi-systems.de)	✗	ab 400 € / Monat 1 User, keine API	• Deutsches Unternehmen • On-Premise, SaaS,,Webanwendung
HiScout	• ISMS-Tool für Informationssicherheitsmanagement nach ISO 27001/2 (hiscout.com) • HiScout GRC Suite: Software mit gemeinsamer Datenplattform	✗	ungewiss	• Deutsches Unternehmen aus Berlin • Modularer Aufbau
SwissGRC	• Swiss GRC AG | Governance, Risikomanagement und Compliance (GRC)	?	?	• Viele Auskünfte nur auf Anfrage • wenig Informationen auf der HP
I-doIT	• i-doit - Die 360°- IT-Dokumentation & CMDB	✗	ab 1881€ jährlich für 5k Objekte	• Aus Düsseldorf • self-hostable • Tests auf Anfrage Online möglich
QSec	• QSEC - Die Software für GRC, ISMS und Datenschutz - WMC (wmc-direkt.de)	✗	?	• Online Demo auf Anfrage möglich • Keine Preise gefunden
Risma	• https://www.rismasystems.com/	✗	Auf anfrage	• Dänemark • ISO27001 abdeckung
InterValid	• Intervalid - Datenschutz- & Informationssicherheitsmanagement Software	✗	?	• ISO 27001 | BSI IT- Grundschutz | VdS 10000 | TISAX | B3S | ISIS12/CISIS12 • HQ in Österreich, Nebenstandort in Deutschland • Deutschland

A.5 HiScout Systemanforderungen

[..]

A.6 HiScout Beispiel Kostenrechnung

[..]

A.7 Auswertung der Testcases

Testcases

	Vernice.	Confluence Jira	GRC-Suite
Testsystem	lokale Installation	Unternehmens Testsystem	SaaS-Lösung
Version	EVAL 1.24.1	Confluence: Server 7.19.1 Jira: Server 9.2.0	HiScout GRC-Suite 3.10.0
Erweiterungen (Version)	Recaplast Demodaten IT-GS-Kompendium (10)	Automation for Jira Lite (8.0.4)	HiScout ISM HiScout Grundschutz HiScout Questionaire

	Bezeichnung	Vernice. EVAL	Confluence Jira	GRC-Suite
1	Anpassung von Vorlagen	✓	✓	✓
2	Anpassung von Workflows	sind nur in Pro-Version vorhanden	✓	✓
3	Anwendungsbereich definieren	✓	✓	✓
4	Benachrichtigungen von Verantwortlichen	ist nur in Pro-Version möglich	✓	✗
5	Berichtserstellung	✗		✓
6	Dokumente revisionssicher verwalten	✓	✓	✓
7	Erinnerungen für wiederkehrende Ereignisse	✗		✗
8	Export von Daten (Format)	✗	✓ (pdf,csv,word)	✓ (xml)
9	Import von Daten (Format)	✓ (csv,xml, vna)	✓ (pdf,csv,word)	✓ (xml)
10	Inventarisierung pflegen	✓	✓	✓
11	Rechteverwaltung innerhalb ISMS	✗	✓	✓
12	Schutzkategorien definieren	✓	✓	✓
13	Templates, Workflows vorhanden	sind nur in Pro-Version vorhanden	ohne Apps: ✗ mit Apps: ✓	✓
14	Übersichten für den Umsetzungsprozess	✗	✓	✓
15	Verantwortlichkeiten definieren	✓	✓	✓

A.8 Einrichtung Confluence Space ISMS

A.8.1 Berechtigungen im Confluence

[..]

A.8.2 Templates im Confluence

[..]

A.8.3 Confluence ISMS Pages: Homepage

[..]

A.8.4 Confluence ISMS Pages: Meeting notes

[..]

A.8.5 Confluence ISMS Pages: Policies

[..]

A.8.6 Confluence ISMS Pages: Scope

[..]

A.8.7 Confluence ISMS Pages: Structure analysis

[..]

A.8.8 Confluence ISMS Pages: Protection needs

[..]

A.9 Einrichtung Jira Project ISMS

A.9.1 Berechtigungen im Jira

[..]

A.9.2 Jira ISMS Permission Scheme

[..]

A.9.3 Jira ISMS Workflow

dotSource ISMS new Measure Workflow

From	Transition		To
OPEN	Prepare measure No Screen	→	PREPARATION
APPROVAL PENDING	Approving measure Select Assignee Screen	→	APPROVED
	Not approved No Screen	→	NOT APPROVED
APPROVED	Document published Resolve Issue Screen	→	PUBLISHED
	Preparing deployment No Screen	→	DEVELOPMENT IN PRO...
NOT APPROVED	Starting Review Assignee-Fix	→	REVIEW
PUBLISHED	Closed Close Issue Screen	→	CLOSED
LIVE DEPLOYED	Closed Close Issue Screen	→	CLOSED
REVIEW	Start preparing No Screen	→	PREPARATION
DEVELOPMENT IN PRO...	Measure deployed Resolve Issue Screen	→	LIVE DEPLOYED
CLOSED	Reopen Reopen Issue Screen	→	REVIEW
PREPARATION	Ready to approve Select Assignee Screen	→	APPROVAL PENDING

Close

Bild A.1: dotSource ISMS new Measure Workflow detailliert[7]

A.9.4 Jira ISMS Test Workflow

[7] Quelle: Project ISMS: Project Settings: User and Roles
[8] Quelle: Projekt ISMS

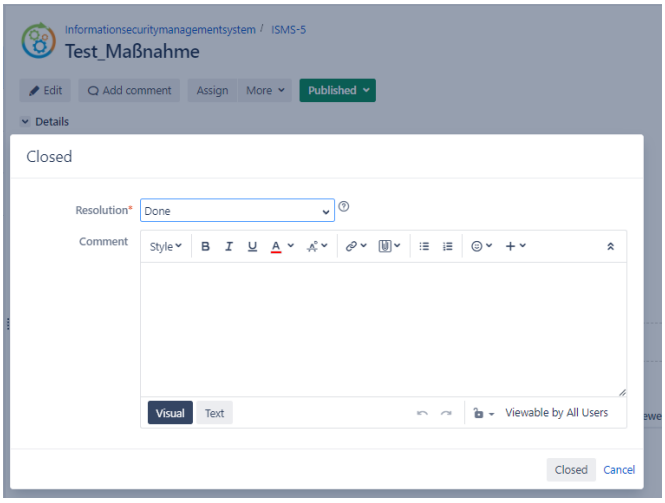

Bild A.2: Übergangsmaske Published zu Closed[8]

A.10 Erstellung der Passwortrichtlinie

A.10.1 Passwortanforderungen

[..]

A.10.2 Jira Ticket Ablauf

[..]

A.10.3 Passwortrichtlinie im Confluence Space Kopfteil

[..]

A.10.4 Passwortrichtlinie im Confluence Space Inhaltsteil

[..]

A.11 Anpassung der Dienste

A.11.1 Erstellung Sub-Tasks

[..]

A.11.2 Pasword Self-Service-Portal

[..]

A.11.3 Confluence Landing Page Ansicht nach Bearbeitung der Maßnahme

[..]

Abkürzungsverzeichnis

BCM Business Continuity Management

BSI Bundesamt für Sicherheit in der Informationstechnik

bspw. beispielsweise

DRP Disaster Recovery Plan

IS Informationssicherheit

IS-Leitlinie Leitlinie zur Informationssicherheit

IS-Richtlinien Richtlinien zur Informationssicherheit

ISB Informationssicherheitsbeauftragter

ISMS Informationssicherheitsmanagementsystem

ISO International Organization for Standardization

IST Informationssicherheitsteam

ITAM IT Asset Management

KMU Kleine und mittelständische Unternehmen

MTA maximal tolerierbare Ausfallzeit

MTD maximal tolerierbarer Datenverlust

PDCA **P**lan **D**o **C**heck **A**ct

PT Projekt-Tage

VdS Verband der Sachversicherer e.V

Glossar

Plan Do Check Act ist ein vier Phasen-Modell aus dem Wirtschaftsbereich zur kontinuierlichen Qualitätsprüfung und -verbesserung.

Cyber-Sicherheit Cyber-Sicherheit weitet das Aktionsfeld klassischer IT-Sicherheit auf den Cyber-Raum aus[9].„Dieser [- der Cyber-Raum -] umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein“[10].

Informationssicherheit hat nach BSI das Ziel „Informationen jeglicher Art und Herkunft zu schützen“[11]. Dabei umfasst die Begrifflichkeit sowohl die verarbeitenden Systeme, als auch die informationstragenden Elemente.

Informationsverbund Der Informationsverbund umfasst auch alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen.[12]

IT-Sicherheit IT-Sicherheit beschäftigt sich mit der Sicherheit von informationsverarbeitenden Systemen.

Kronjuwel Als Kronjuwelen werde im IT-Grundschutz des BSI besonders geschäftskritische Assets bezeichnet. Der Geltungsbereich der Kernabsicherung bezieht sich auf die Kronjuwelen.

Risikobewertung bewertet das Risiko nach dem zu erwartenden Schaden und der Eintrittwahrscheinlichkeit.[13]

Sicherheitskonzept Das Sicherheitskonzept stellt das zentrale Element der Dokumentation im Sicherheitsprozess dar. Es beschreibt die geplante Vorge-

[9] Vgl. BSI17a, S. 8.
[10] Ebd., S. 8.
[11] Ebd., S. 8.
[12] Ebd., S. 29.
[13] für mehr Informationen empfiehlt sich die Ausführung des BSI BSIoJa.

hensweise zur Erfüllung der festgelegten Sicherheitsziele und setzt damit die Sicherheitsstrategie um.[14]

[14]Vgl. BSIoJb.

Thesen

1. Die etablierten Normen zur Erstellung eines ISMS bieten durch Symbiose und Ergänzung die Möglichkeit ein verbessertes ISMS zu erstellen.

2. Durch Einteilung der Entwicklung eines ISMS in Phasen wird der Einstieg und die Einführung eines ISMS erleichtert.

3. Die kürzeste Umsetzung eines ISMS dauert mit begrenzten personellen Ressourcen ohne weitere finanzielle Investitionen länger als ein halbes Jahr.

4. Die Bestandteile eines ISMS lassen sich schwer von einander abgrenzen, da diese oft multifunktional sind.

5. Mittels Atlassians Confluence und Jira kann ein gängiges oder individuelles ISMS realisiert werden.

6. Für eine Effizienzsteigerung oder Vereinfachung der Arbeit in Jira und Confluence sind die Standardwerkzeuge ausreichend.

7. Durch das Anpassen von Workflows, Screens und Issue-Types kann die Verwendung von Vorgängen in Jira anwendungsfreundlich gestaltet werden.

8. Atlassians Confluence bietet, abseits vom Marketplace, keine Möglichkeiten, um die Anforderungen an die Form der Dokumentation eines ISMS vollständig umzusetzen.