INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Masterthesis

Dokumentation in einem Informationssicherheits-Managementsystem (ISMS)

Peter Anton Werner

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Masterthesis

Dokumentation in einem Informationssicherheits-Managementsystem (ISMS)

Peter Anton Werner

Aufgabensteller:	Prof. Dr. Helmut Reiser
Betreuer:	Dr. Michael Brenner, LRZ (michael.brenner@lrz.de) Stefan Metzger, LRZ (stefan.metzger@lrz.de) Bastian Kemmler, LRZ (bastian.kemmler@lrz.de)
Abgabetermin:	29. Oktober 2017

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 29. Oktober 2017

. . . . . .

Peter Anton Werner

Abstract

Die vorliegende Masterarbeit befasst sich mit der Erstellung eines Dokumentationskonzepts für ein Informationssicherheits-Managementsystem (ISMS) gemäß der ISO/IEC 27000 Reihe.

Dabei fand eine Analyse unterschiedlicher, am Markt befindlichen Dokumentationstools statt, die Anhand eines entwickelten Kriterienkatalogs verglichen und evaluiert wurden. Die daraus resultierten Ergebnisse bildeten unter Berücksichtigung der führenden Literatur im Bereich des Dokumenten- und Informationssicherheits-Managements ein konkretes Informations- und Datenmodell, wodurch eine Umsetzungsempfehlung für eine wirksame und nachhaltige Dokumentationsstruktur für ein ISMS entwickelt werden konnte. Um die Wirksamkeit auch im praktischen Einsatz bestätigen zu können, wurde das Konzept abschließend exemplarisch im Kontext des IT-Dienstes Sync & Share am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) implementiert und den etablierten Dokumentationstools gegenübergestellt.

Die Basis dieser Masterarbeit bilden Studien von Reiss (2015), Kersten (2013) und Brenner (2017). Der Autor erhofft sich durch diese Arbeit einen Erkenntnisgewinn in Form einer praxisnahen Implementierungsempfehlung für die Dokumentation eines solchen Managementsystems mit Fokus auf den normativen Anhang A der ISO/IEC 27001 innerhalb einer beliebigen Organisationsstruktur und unabhängig eines expliziten Dokumentationstools.

Inhaltsverzeichnis

1 Einleitung

Immer mehr Unternehmen und Organisationen im staatlichen sowie privaten Bereich verfolgen das Ziel einer Zertifizierung zum Nachweis der Dienst- oder Produktionsqualität. Sie basieren auf Normen, die sich in verschiedensten Branchen wie beispielsweise der Elektronik-, Lebensmittel- aber auch in der IT-Industrie etabliert haben und bauen auf den Grundgedanken der Herstellung einer nachhaltigen Produktion bzw. eines effektiven und konformen Managementsystems auf. Die Anstrebung einer Konformität bezüglich eines akkreditierten Standards liegt dabei in den Händen der jeweiligen Organisation und ist, sofern keine gesetzlichen Vorgaben existieren, freiwillig.

Im Bereich der IT-Sicherheit und der Informationssicherheit sind unter anderem die grundlegenden Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität definiert. Die Maßnahmen zum Schutz dieser Ziele werden innerhalb eines Informationssicherheits-Managementsystems (Informationssicherheits-Managementsystems (ISMS)) behandelt, welches aus Leitlinien, Verfahren, Anleitungen und weiteren zugehörigen Betriebsmitteln, die zur Einhaltung der Schutzziele benötigt werden, besteht. Die Mindestanforderungen an ein solches ISMS sowie empfohlene Vorgehensweisen werden innerhalb der internationalen Norm DIN ISO/IEC 27001:2014-02 (ISO/IEC 27001) aufgeführt.

Die Realität zeigt jedoch, dass Organisationen mit zunehmender Anzahl geschäftskritischer Dienste und dem steigenden Anspruch eine sichere, wirksame und systematisch-gemanagte IT-Infrastruktur zu schaffen, einem erheblichen Verwaltungsaufwand gegenüberstehen. Der komponentenartige Aufbau eines ISMS sowie die Zusammenhänge mit anderen bereits etablierten Managementsystemen sowie der Forderung an Mitarbeiter, dem prozessorienterten Ansatz zum Zwecke messbarer und wiederholbarer Ergebnisse zu folgen, schlussfolgert die Notwendigkeit eines wohlstrukturierten und belastbaren Dokumentationskatalogs.

Die Art und Weise, in der eine solche Dokumentation vorliegen kann, ist innerhalb des Standards nicht eindeutig definiert und es obliegt daher dem Unternehmen, eine für sich geeignete und zweckmäßige Form der Dokumentation zu wählen. Eine digitale Dokumentation ermöglicht viele Vorteile und auch die für eine effektive und wirksame Dokumentenlenkung, unerlässliche Funktionalitäten wie beispielsweise Automatismen zur Archivierung obsoleter Dokumente oder auch die Unterstützung individueller Workflows.

1.1 Motivation

Ein ISMS besteht aus mehreren miteinander verknüpften Komponenten. Zu den wichtigsten Komponenten gehören Informationswerte, Risiken und Schutzmaßnahmen. Diese Komponenten stehen in einem gewissen Zusammenhang zueinander und können auch Verknüpfungen zu anderen Normen wie beispielsweise des ISO/IEC 20000 im Bereich des IT-Service Managements oder dem Qualitätsmanagement (ISO/IEC 9000) besitzen.

Unternehmen, die bei der Realisierung und Zurverfügungstellung von Diensten auf der Grundlage solcher Normen aufbauen, sind auf ein integriertes und effektives Dokumentationsmanagement angewiesen, um die Nachhaltigkeit durch Nachweisbarkeit auch über einen längerfristigen Zeitraum zu gewährleisten. In der Praxis gestaltet sich dies bei der Realisierung eines ISMS überwiegend als problematisch, da zwar auf die elementaren Inhalte mit Hinblick auf eine Zertifizierung geachtet, aber die parallele Umsetzung einer regelmäßig gepflegten Dokumentation oftmals vernachlässigt wird. Meist wird von Unternehmen erst zu einem späteren Zeitpunkt festgestellt, dass eine frühzeitig strukturierte Dokumentation bei dynamischen Organisationsumgebungen zu einer langfristig gesteigerten Funktionstüchtigkeit und einem allgemeinen Mehrwert hätte führen können.

Ein weiteres Extrem stellen Unternehmen dar, die die Idee einer grundlegenden Überwachung von Geschäftsprozessen verfolgen, deren Durchführung zu einem Übermaß an Formalismen und Bürokratie führen. Verantwortlich hierfür sind nicht zwangsläufig die Formulierungen der Mindestanforderungen innerhalb der Norm, sondern eher die Verantwortlichen des anwendenden Unternehmens.

Heinrich Kersten et. al. [KRS13] haben aus Gesprächen mit Zertifizierern und aus ihrer eigenen Praxis erfahren, dass 60% bis 90% der Beanstandungen bei Zertifizierungsaudits im Bereich der Dokumentation liegen. Nach Ihrer Auffassung sei vielen Unternehmen nicht bewusst, dass die Mindestanforderungen bereits durch eine angemessene und zweckmäßige Dokumentation erfüllt wären.

Tatsächlich wird ein solches Dokumentationsmanagement zur zentralen Steuerung von Dokumenten durch das Kapitel 7.5 des ISO/IEC 27001 explizit gefordert. Die Anforderungen umfassen unter anderem Richtlinien zur Erstellung, Aktualisierung, Verteilung, Speicherung und Überwachung dokumentierter Informationen. Was der Standard nicht vorgibt, ist ein konkretes Informations- und Datenmodell, wie die Implementierung einer ISMS-Dokumentation in der Realität stattzufinden hat. Hier fehlen Frameworks und Modelle, die Unternehmen einen beispielhaften Ansatz oder eine Vorgabe zur Umsetzung eines Dokumentationsmanagements aufzeigen und zur Implementierung und Pflege innerhalb dieses Bereichs unterstützen.

Diese Situation führt dazu, dass die Realisierung eines anforderungsgerechten und nachhaltigen Dokumenationsmanagements schon bei der Umsetzung übergeordneter Managementprozesse scheitert und die Anstrengungen innerhalb dieses Managementbereichs oftmals über einen längeren Zeitraum vernachlässigt werden. Selbst in der Literatur finden sich nur wenig Ansätze, die sich mit dem Bereich der Dokumentation eines ISMS beschäftigen.

1.2 Zielsetzung

Ziel dieser Masterthesis ist es, ein Informationsmodell zur Darstellung der Zusammenhänge der verschiedenen Komponenten eines ISMS zu modellieren und dieses nutzbringend innerhalb eines geeigneten digitalen Dokumentationssystems prototypisch zu implementieren. Hierdurch sollen später die Anwender des Systems aktiv bei der Pflege von sensiblen und infrastrukturellen Informationen im Kontext des ISO/IEC 27000 Standards unterstützt werden. Darüber hinaus soll eine strukturierte Dokumentation auch im Hinblick auf zukünftige Zertifizierungsanstrebungen, einen übersichtlichen, transparenten und belastbaren Nachweis liefern können.

Die Erhebung einer Anforderungsanalyse auf Grundlage der bereits etablierten Dienste, soll dazu dienen, definierte Informationswerte, mögliche Sicherheitsrisiken und diesbezügliche Schutzmaßnahmen zu identifizieren, zu kategorisieren und zu strukturieren. Dies soll stets unter Berücksichtigung des ISO/IEC 27000 Anforderungskatalogs geschehen. Darüberhinaus lassen sich unter Umständen bereits mögliche funktionale und nicht-funktionale Anforderungen für das zu realisierende Dokumentationskonzept ableiten. Weiterhin existieren auf dem Markt bereits verfügbare Dokumentationstools mit Spezialisierung auf IT-Informationssicherheit aber auch allgemeine Tools im Rahmen des Qualitätsmanagements, die durch eine Analyse einen Beitrag zum Erkenntnisgewinn bezüglich einer Herstellung einer ISMS-Dokumentation liefern können.

Im zweiten Schritt steht die Modellierung eines der Norm entsprechenden Informationsmodells, dass die Zusammenhänge der einzelnen Komponenten innerhalb eines ISMS darstellt. Der Detailgrad sollte dabei zweckmäßig und organisationsspezifisch gewählt werden, um eine unnötige Formalisierung zu verhindern. Außerdem sollten die erarbeiteten Anforderungen in Form eines Kriterienkatalogs zur Kategorisierung der Inhalte innerhalb der Komponenten dienen.

Aus dem Informationsmodell entsteht anschließend ein konkretes Datenmodell, bestehend aus Objekten mit definierten Attributen. Das Datenmodell soll als Grundlage einer Implementierung innerhalb eines Produktivsystems im Bereich des Dokumentationsmanagements dienen. Für die prototypische Implementierung des konzeptionierten Modells würden die im Vorfeld betrachteten Dokumentationstools in Frage kommen. Da es wahrscheinlich ist, dass durch das IT-Service Management, dem Risikomanagement und dem Informationssicherheitsmanagement bereits relevante und dokumentierte Informationen existieren, würde sich eine Berücksichtigung bereits vorhandener Inhalte in Form einer logischen Verknüpfung anbieten, da Zusammenhänge besonders schnell erkannt werden könnten und die Konsistenz der zum Teil überlappenden Inhalte erhöht werden könnte.

Die Erkenntnisse aus den erarbeiteten Modellen sowie der Analyse möglicher Dokumentationstools, soll abschließend als Grundlage für eine prototypische Implementierung einer wirksamen ISMS-Dokumentation innerhalb eines beispielhaften Dienstes dienen. Auf lange Sicht, sollen die Erkenntnisse aus dieser Arbeit den prozessorientierten Ansatz einer strukturierten und nachhaltigen Dokumentation organisationsweit optimieren und einen hilfreichen Ansatz zur Realisierung eines Dokumentenmanagementsystems im Bereich der Informationssicherheit bieten.

1.3 Vorgehensweise

Zu Beginn wird der Leser in die für diese Arbeit erforderliche Thematik eingearbeitet. Hierzu zählen insbesondere Grundlagen zu den Themen des Informationssicherheitsmanagements aber auch des Dokumentationsmanagements. Ergänzend zu den Grundlagen eines ISMS und des Dokumentationsmanagements wird in Bezug auf die im Anschluss folgende Anforderungsanalyse, der Status-Quo des Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) vorgestellt, um sich ein Bild über das Tätigkeitsumfeld und den vorherrschenden Stand des Dokumentationsmanagement machen zu können.

Basierend auf dieser Grundlage, bildet das vierte Kapitel die Anforderungsanalyse. Sie definiert konkrete Kriterien, die an das zu entwickelnde Informationsmodell zur Dokumentation eines ISMS gestellt werden und für den Vergleich zwischen etablierter Dokumentationstools im Bereich des Informationssicherheitsmanagements und der prototypischen Implementierung herangezogen werden.

Das fünfte Kapitel umfasst den Vergleich zwischen bereits am Markt erhältlichen Dokumentationstools im Bereich der IT-Informationssicherheit, welche anhand des Kriterienkatalogs evaluiert werden. Während der Analyse lassen sich so unter anderem auch Erkenntnisse sammeln, die bei der Modellierung eines Informationsmodells berücksichtigt werden.

Das sechste Kapitel nimmt die Erkenntnisse aus den vorhergehenden Kapiteln als Basis für die Herstellung eines allgemeinen Informationsmodells. Der Fokus hierbei liegt auf der Dokumentation des normativen Anhangs A der ISO/IEC 27001, der die Bestandteile Informationswerte, Risiken und Schutzmaßnahmen behandelt.

Aus dem Informationsmodell entsteht anschließend im siebten Kapitel eine prototypische Implementierung innerhalb des Dokumentationstools Confluence. Confluence wird aus dem Grund gewählt, da es durch das LRZ bereits organisations- und abteilungsübergreifend zur Dokumentation von Servicemanagementprozessen erfolgreich eingesetzt wird und sich somit durch geeignete Schnittstellen eine Berücksichtigung bereits vorhandener Inhalte finden lässt.

Kapitel Acht beinhaltet eine Zusammenfassung der Erkenntnisse dieser Arbeit und stellt Ansätze zur Weiterführung der Arbeit in Form eines Ausblicks vor.

2 Grundlagen

Um ein Dokumentationsmodell für ein ISMS zu entwickeln, bedarf es an Definitionen und der Erschließung notwendiger Zusammenhänge, die in Verbindung mit der Informationssicherheit und der Herstellung eines solchen Managementsystems stehen.

In Kapitel 2.1 werden die Grundlagen zum Themenbereich des Informationssicherheitsmanagements beschrieben. Dabei geht es zunächst darum ein grundlegendes Verständnis für die Sinnhaftigkeit eines ISMS und dessen Ursprungs herzustellen. Besonders in den Bereichen der Finanz- und Versicherungsindustrie sind seit Ende der 1990er Jahre unterschiedliche Ansätze zum Schutz von Informationen im Rahmen des Risikomanagements etabliert worden. Viele legten den Grundstein für die Richtlinien und Maßstäbe des ISO/IEC 27001 Standards und dem Bedürfnis eines international anerkannten Zertifizierungsmodells. Weiterhin gilt es, Definitionen für wichtige Fachbegriffe zu erläutern und danach, den Aufbau eines ISMS zu beschreiben.

Kapitel 2.2 befasst sich mit dem Aufbau und der Struktur eines ISMS. Dabei stehen insbesondere Themen des Risikomanagements und der Methodik bei der Herstellung sowie der Aufrechterhaltung eines ISMS durch einen kontinuierlichen Verbesserungsprozess (KVP) im Mittelpunkt.

Kapitel 2.3 befasst sich mit den Themen des Dokumentenmanagements und der Dokumentenlenkung. Beschrieben wird der Umgang mit Dokumenten und Aufzeichnungen. Die typischen Kernfunktionalitäten umfassen die Genehmigung und Veröffentlichung von Dokumenten sowie ihrer Überprüfung und Kennzeichnung. In Abschnitt 7.5 des ISO/IEC 27001 wird eine solches Dokumentenmanagement explizit gefordert, um die Sicherstellung der Verfügbarkeit von Dokumenten und ihrer kontrollierten Verteilung gewährleisten zu können.

2.1 Informationssicherheits-Managementsystem (ISMS)

2.1.1 Historische Entwicklung

Die ersten Entwicklungen rund um den ISO/IEC 27001 Standard finden sich Anfang der 1990er Jahre wieder. Dem *ISO 27000 Directory* [iso16] nach, wurde das sog. Commercial Computer Security Centre (CCSC) der zuständigen Abteilung für Handel und Industrie der britischen Regierung damit beauftragt, sowohl Sicherheitsevaluierungskriterien als auch empfohlene Vorgehensweisen im Bereich der IT-Sicherheit zusammenzustellen. In Folge dessen, entstanden die beiden Dokumente der IT Security Evaluation and Certification (ITSEC) und Delivering Information Solutions to Customers (DISC) *(PD003)*, die bereits zum damaligen Stand, zehn Regelungsbereiche für Maßnahmen und Maßnahmenziele für Informationssicherheit darlegten.

Im Jahr 1995 wurden die Dokumente nach regelmäßiger Weiterentwicklung zum BS7799 Standard erhoben. Die Ausarbeitung des BS7799 wurde jedoch in zweierlei Bereiche aufgeteilt. Der erste Bereich (BS7799-1) befasste sich weiterhin mit dem ursprünglich angedachten Zielen, während der zweite Bereich (BS7799-2) die Überführung in ein übergeordnetes, abstrahiertes und minimalistisches Model konzipierte. Das Modell, das hieraus entstand, war das ISMS, dessen Norm 1998 vom BS7799-2 Standard in den Bereich der Mindestanforderungen des ISO/IEC 27001 umbenannt wurde. Der BS7799-1 Standard ging später im Jahr 2000 auf den ISO/IEC 17799 über, welcher Ende 2007 zugunsten der Einhaltung innerhalb des Nummerierungssystems zum ISO/IEC 27002 Standard umbenannt wurde.

Neben der internationalen Norm wurden auch weitere sowohl optionale als auch obligatorische Rahmenbedingungen zum Schutz von Informationssicherheit entwickelt. 1998 trat mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ein Gesetz in Kraft, durch das für die Informationssicherheit relevante Änderungen im Aktiengesetz aber auch im Handelsgesetzbuch herbeigeführt wurden. So werden im Aktiengesetz (AktG § 91 Abs. 2)) geeignete Maßnahmen gefordert, die das Einrichten eines Überwachungssystems umfassen, um für den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig zu erkennen.

Ein weiteres Rahmenwerk, dass den Schutz von Informationen zum Ziel hat, stellt der IT-Grundschutz dar. Der IT-Grundschutzkatalog wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und stellt in mehreren Katalogen sowohl Vorgehensweisen zur Identifizierung möglicher Gefährdungen aber auch Schutzmaßnahmen dagegen vor. Der Umfang des Grundschutzkatalogs ist deutlich größer als der, der ISO-Norm und umfasst noch detailliertere Informationen zu Vorgehensweisen und Gefahren im Rahmen der Informationssicherheit. Seit 2006 wird der Grundschutzkatalog durch das BSI in regelmäßigen Abständen an die internationale Norm angeglichen.

2.1.2 Gesetzliche Anforderungen

National hat sich die Forderung eines ISMS auch rechtlich durchgesetzt. So wurden auf Basis des Art. 108 Abs. 7 (GG) im Bereich des Steuerrechts 2001 die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) erlassen, die Regeln zur Aufbewahrung digitaler Unterlagen und Sorgfaltspflichten bei Bereitstellung, Nutzung und Übertragung vorschreiben. Die Regelung wurde am 1. Januar 2015 durch die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GOBD) abgelöst. Innerhalb dieser Grundsätze wird die Einrichtung eines internen Kontrollsystems (IKS) gefordert, dessen Definition wie folgt beschrieben wird [Bun95]:

Als IKS wird grundsätzlich die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen bezeichnet, die die folgenden Aufgaben haben: Sicherung und Schutz des vorhandenen Vermögens und vorhandener Informationen vor Verlusten aller Art [...].

Die Definition des Internes Kontrollsystem (IKS) schließt die Realisierung eines ISMS mit ein. Auch das Bundesdatenschutzgesetz (BDSG) fordert im § 9 die Errichtung eines ISMS insbesondere für Unternehmen, die mit dem Umgang von personenbezogenen Daten zu tun haben[Bun90]:

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Insbesondere im Zusammenhang zwischen staatlicher oder auch privatwirtschaftlicher Organisationen, die an der Grundversorgung der Bevölkerung mittels maßgeblicher Dienstleistungen beteiligt sind und dem Schutz dieser wird von dem Begriff KRITIS gesprochen. Der Begriff Kritische Infrastrukturen (KRITIS) umfasst im Sinne der EU-Richtlinie 2008/114/EG [Rat] den Ausfall oder auch die Beeinträchtigung von Infrastrukturen, die zu einer erheblichen Störung der öffentlichen Sicherheit führen und somit dramatische Folgen nach sich ziehen können. Aufbauend auf dieser EU-Richtlinie, wurde am 17. Juli 2015 das IT-Sicherheitsgesetz [Bun15] durch die Bundesregierung beschlossen, nach dem dem BSI zusätzliche Befugnisse zum Schutze der Infrastrukturen zugesprochen werden. Das BSI unterteilt hierbei Organisationen und Einrichtungen des Landes in neun Sektoren, durch die die Widerstandsfähigkeit der wichtigsten kritischen Infrastrukturen wie beispielsweise Energieversorgung, Wasser, Ernährung und Verkehr durch aktiven Förderung der Robustheit kritischer Prozesse, dem Austausch über aktuelle Vorkommnisse oder dem Auf- und Ausbau von Krisenmanagementstrukturen erhöht und langfristig stabilisiert werden soll.

Für die eingetragene Aktiengesellschaften an der US-Börse sind zudem das amerikanische Sarbanes-Oxley Gesetz (S-Ox) zu berücksichtigen, dass 2002 in Kraft getreten ist. In Artikel 404 wird ein Kontrollsystem gefordert, dass dem vorher genannten IKS entspricht, jedoch mit einem größeren Bezug auf das Management und zu tragenden Konsequenzen bei Verstößen.

Das Committee of the Sponsoring Organizations of the Treadway Comission Enterprise Riskmanagement (COSO ERM) stellt ein weiteres international anerkanntes Framework im Bereich des Risikomanagements in Unternehmen dar. Der Fokus liegt hier auf dem Design und der Implementierung interner Kontrollen. Kersten et. al. [KRS13] beschreiben wie im Finanzsektor durch Wirtschaftsprüfer im Rahmen des International Standard on Assurance Engagements (ISAE) 3402 Kontrollstrukturen zur Überwachung gefordert werden sollen, die sich mit einer Zertifizierung nach ISO/IEC 27001 erfüllen ließen. Weiterhin erklären sie, dass durch Gesetze wie die Kapitaladäquanzrichtlinie für Banken (Basel II) oder dem Kreditwesengesetz zwar grobe Anforderungen an das Risikomanagement vorgegeben werden, diese aber lediglich einen rudimentären Bezug auf IT-Themen besitzen und nicht allübergreifend sind.

2.1.3 Informationssicherheit

Bei der Informationssicherheit hat die Sicherstellung der wichtigsten Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit oberste Priorität. Vertraulichkeit umfasst den Schutz von Informationen vor der Offenlegung durch unberechtigte Personen. Verfügbarkeit stellt den Zugriff von Informationen für berechtigte Nutzer sicher und Integrität bezieht sich auf den Schutz von Informationen vor unberechtigter Modifikation.

Weitere Teilaspekte für Informationssicherheit können folgende Parameter sein:

- Authentizität
- Zurechenbarkeit (Verantwortlichkeit)
- Verbindlichkeit (Nicht-Abstreitbarkeit)
- Verlässlichkeit

Für das Maß an ausgeübter Informationssicherheit existiert keine allgemeine Einheit, da sich die gewählten Schutzmaßnahmen stets im Individualfall mit Hilfe einer Risikoanalyse ergeben müssen.

Innerhalb der individuellen Risikoanalyse spricht man dann vom sogenannten Schutzbedarf und der Wertigkeit bzw. dem Schutzziel. Das BSI [fSidI96] definiert den Schutzbedarf in Form von qualitativen Werten, die den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit zugeordnet werden können. So ist es beispielsweise möglich, dass der Schutzbedarf bei Systemen mit einer geringen Nutzergruppe deutlich geringer ist und somit bereits durch wenig Anstrengung ein hohes Maß an Informationssicherheit gewährleistet werden kann. Im Gegensatz dazu steht ein System, das mehrere tausend Nutzer umfasst und bei dem jeder Nutzer für sich ein potentielles Sicherheitsrisiko darstellen würde.

Weiterhin führt das BSI den Begriff der Wertigkeit von Informationen im Zusammenhang mit der Konzeption und Planung des Sicherheitsprozesses auf, wodurch ein Anhaltspunkt bezüglich des finanziellen Schadens bei Ausfall oder Beeinträchtigung eines Vermögenswerts bzw. Verletzung eines oder mehrerer Schutzziele und die dazugehörige Wiederherstellungszeit zu bewerten ist.

Nach dem DIN ISO/IEC 27002:2014-02 (ISO/IEC 27002) dient die Sicherstellung der Schutzziele im weitesten Sinne dazu, die Kontinuität eines Geschäfts aufrecht erhalten zu können [Int15b]:

Informationssicherheit bedeutet Schutz von Informationen vor Angriffen, mit dem Ziel, die Kontinuität des Geschäfts (Geschäftsfortführung) zu sichern, Geschäftsrisiken zu minimieren und den Return on Investment (ROI), Profit sowie die Geschäftsopportunitäten und Geschäftschancen zu maximieren.

2.1.4 Zusammenhänge der Managementsysteme

Ein Managementsystem stellt eine Ansammlung von Komponenten dar, die durch wechselseitige Beziehungen miteinander verbunden sind. Es dient dazu, den Prozess zur Gestaltung,

Lenkung und Entwicklung eines zweckorientierten Systems zu fördern und durch Bereitstellung von Leitlinien, Verfahren und Anleitungen die ausführende Organisation bei der Erreichung ihrer Ziele zu unterstützen.

Die Komponenten eines solchen Systems können selbst weitere Systeme umfassen oder Schnittmengen mit anderen Systemen bilden.

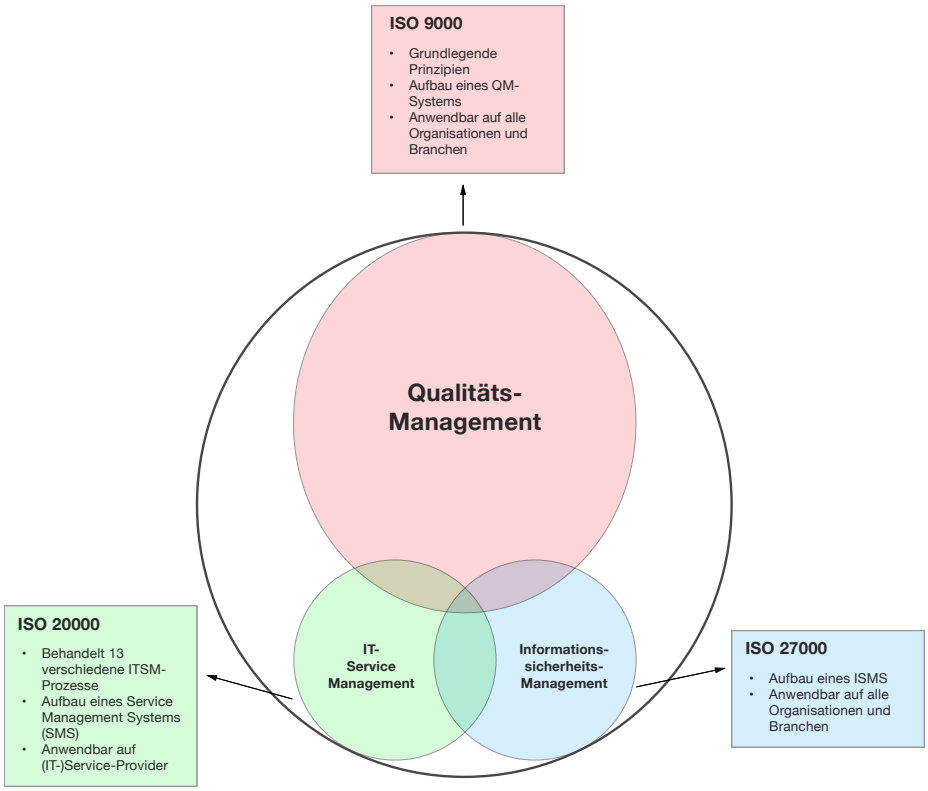


Abbildung 2.1: Schnittmengen der für ein ISMS relevanten Managementsysteme

Wie in Abbildung 2.1 zu sehen ist, teilt das Managementsystem für Informationssicherheit eine Schnittmenge mit dem übergeordneten Qualitätsmanagementsystem aber auch mit dem hauptsächlich in der IT angesiedelten IT-Servicemanagement (ITSM).

So finden sich im Bereich des IT-Service-Managements 13 unterschiedliche ITSM-Prozesse, deren Ziel es ist, einen prozessorientierten Aufbau eines Service Management Systems (SMS) herzustellen. Der zugehörige ISO/IEC 20000 Standard basiert dabei auf der Bücherreihe Information Technology Infrastructure Library (ITIL), die insgesamt 37 Kernprozesse, grundlegende empfohlene Vorgehensweisen zur strikten Aufgabentrennung in IT-Abteilungen und Ansprechstellen sowie Eskalationsstufen definieren. Der Prozess des *Information Security Management* (ISM) wird im ITSM eigenständig behandelt und liefert wichtige Schnittstellen zu den angrenzenden Managementprozessen wie dem Change Management (CHM) oder dem Configuration Management (CONFM).

Laut Buchsein [Buc07] werden so insbesondere Leistungswerte der Informationssicherheit

aufgenommen und protokolliert, die Aufschluss über die Funktionstüchtigkeit der Informationssicherheit innerhalb der Organisation geben sollen.

Die ISO/IEC 9000 Serie, die sich mit dem Qualitätsmanagement befasst, stellt neben dem ISO/IEC 27000 und dem ISO/IEC 20000 einer der bekanntesten und erfolgreichsten Normen dar und liefert wichtige Bestandteile zum Thema Dokumentation und Prozessorientierung im Allgemeinen. Historisch gesehen beruhen die Wurzeln des ISO/IEC 9000 ebenso auf den Ansätzen britisch-militärischer Beschaffungsämter, deren Grundgedanke eines elementeartigen Aufbaus später durch einen Paradigmenwechsel in einen prozessorienterten Aufbau überging. Ertl-Wagner et. al. [EWSW13] beschreiben dabei, welchen Stellenwert die sog. *Dokumentenlenkung* besitzt und welche Merkmale ein Dokument aufweisen sollte, um Ergebnisse auch langfristig zur Verfügung stellen zu können und die Auffindbarkeit gewährleisten zu können.

Weiterhin beschreiben die Autoren, dass sich unterschiedliche Modelle in Bezug auf Zielgruppe und Kundenorientierung etabliert haben. So stellt der Deming-Kreis, der in Abschnitt 2.2.6 in Bezug auf ISO/IEC 27001 genauer beschrieben wird, ein mögliches Verfahren vor. Alternativ existiert beispielsweise noch die Reaktionskette nach Deming, welche unter anderem die Produktivitätsverbesserung und Preisreduktion in den Fokus setzt. Ziel eines nachhaltigen Qualitätsmanagement ist es in jedem Fall die Optimierung von Prozessen zum Zwecke der Kosteneinsparung und Erhöhung der Effizienz.

2.2 ISMS nach ISO/IEC 27000

2.2.1 Definition

Ein ISMS ist nach ISO/IEC 27001 wie folgt definiert [Int15a]:

Teil des gesamten Managements, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt. Das Managementsystem enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.

Dabei wird das ISMS, wie bereits im Abschnitt über Managementsysteme beschrieben, als Komponente eines übergreifenden Managementsystems angesehen. Die Voraussetzung zur Etablierung eines zweckmäßigen ISMS liegen im Bereich des Risikomanagements. Geschäftsrisiken müssen vor der Herstellung eines ISMS erkannt werden. Darunter fallen sowohl die operativen Risiken sowie die für die weitere Entwicklung eines Unternehmens notwendigen strategischen Risiken.

Ein ISMS sollte stets individuell auf eine Organisationsstruktur zugeschnitten werden, da sich die konkreten Ausprägungen der Informationssicherheit sowie der dazugehörigen Schutzmaßnahmen und die Art und Weise, wie dieser Grad an Informationssicherheit herzustellen ist, im Einzelfall unterscheiden können.

Da ein ISMS wie alle Managementsysteme den Anspruch eines prozessorienterten Ansat-

zes verfolgt, ist es in der Lage, den erreichten Stand der Informationssicherheit sichtbar, nachvollziehbar und durch regelmäßige Pflege über einen längerfristigen Zeitraum zu erhalten.

Hinsichtlich des Aufbaus der ISO/IEC 27000 Normenreihe grenzt Abbildung 2.2 die einzelnen Dokumente voneinander ab. Der Fokus dieser Arbeit wird sich auf die ISO/IEC 27001 beschränken, da innerhalb dieses normativen Dokuments die Mindestanforderungen an ein ISMS und alle umzusetzenden Maßnahmen und Maßnahmenziele (Anhang A) aufgeführt werden. Neben der ISO/IEC 27006 besitzen die weiteren Dokumente der ISO/IEC 27000 Normenreihe lediglich einen informativen Charakter.

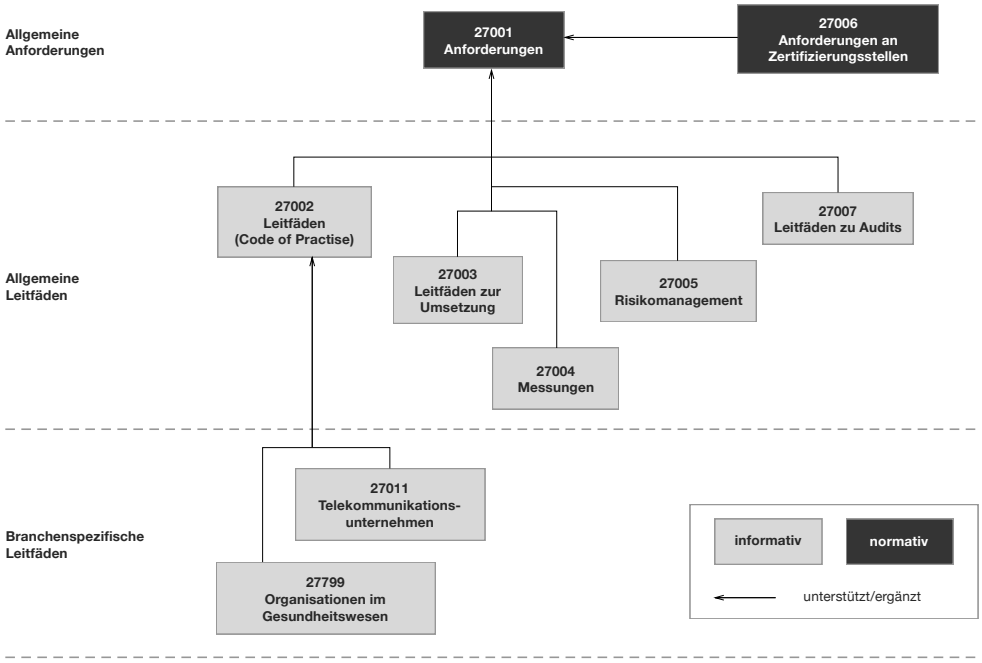


Abbildung 2.2: Die Familie der ISMS-Standards[Gmb13]

2.2.2 Aufbau und Struktur

Eine der ersten Notwendigkeiten, die bei dem Aufbau eines ISMS zu berücksichtigen sind, stellt die Herstellung einer einheitlichen Terminologie dar. Dies ist wichtig, um ein konsistentes Verständnis über die einzelnen Elemente eines ISMS über alle beteiligten Rollen und Verantwortlichkeiten zu erhalten. Vor der Herstellung eines Dokumentationskonzepts ist es empfehlenswert, eingesetzte Begriffe in einem organisationsweiten Begriffsglossar zu sammeln und bereitzustellen.

Da es bei der Umsetzung eines internationalen Standards in einem dem ursprungsfremden Land auch zu Missverständnissen durch Übersetzungen kommen kann, empfiehlt es sich im Zuge der Herstellung eines Dokumentationskonzepts, die eingesetzten Begriffe in einem organisationsweiten Begriffsglossar zu sammeln und bereitzustellen.

2.2.3 Informationswerte und unterstützende Assets

Der Fokus bei der Definition eines Informationswertes (engl. Informationasset) hat sich im Laufe der Entwicklung der ISO/IEC 27001 verändert. Brenner et. al. [BOH+17] definieren Informationswerte als einen Bestandteil eines jeden Unternehmens, der für das Unternehmen schützenswert ist und dem entsprechend auch ein gewisser Schutzbedarf zuzuschreiben ist. Informationswerte können Informationen und Daten unabhängig ihrer Form aber auch Gegenstände (z.B. Festplatten, Akten, Rechner, Infrastruktur, ...) und Personen (z.B. Geschäftsführung, Betriebsrat, Administratoren, ...) sein. Der Implementierungsleitfaden der Information Systems Audit and Control Association (ISACA) [Inf16] fügt neben den oben genannten Typen auch noch immaterielle Werte, Reputation und Image als mögliche Informationswerte-Kategorien hinzu. Auch die ISO/IEC 27001 fordert in Anhang A.8 die Verwaltung solcher Werte.

Kai Jendrian [Kai] weißt jedoch darauf hin, dass die Betrachtung von Informationswerten differenzierter zu betrachten ist und man eine Unterscheidung zwischen konkreten IT-Assets und tatsächlichen Informationassets durchführen müsse. Auch die Norm unterstützt diese Behauptung, da im Teil Annex B der DIN ISO/IEC 27005:2014-02 [Int15d] von sogenannten *supporting Assets* oder auch unterstützenden Assets die Rede ist. Die Version 2013 der Norm unterstützt diesen Gedanken durch Einführung des Begriffs *primary Assets.*

2.2.4 Risikomanagement

Der Schutz von Informationswerten ist abhängig von den potentiellen Gefährdungen für diese Werte und der dazugehörigen definierten Schutzmaßnahmen. Um eine Aussage darüber treffen zu können, in wie weit eine Schutzmaßnahme in Bezug auf eine gewisse Gefahr einzustufen ist, muss durch eine Einschätzung und Bewertung des Risikomanagements stattfinden.

Die ISO/IEC 27005 [Int15d], die sich mit dem Risikomanagement befasst, definiert jedes potentielle Risiko als Kombination der Eintrittswahrscheinlichkeit und dem Schadenspotential eines Ereignisses. Die möglichen Ereignisse müssen durch das Unternehmen erkannt werden und können beispielsweise gezielte Angriffe, fahrlässige Handlungen oder höhere Gewalt einschließen. Das Schadenspotential kann sowohl rein finanzieller Natur sein oder aber einen Imageverlust nach sich ziehen.

Für die Feststellung einer geeigneten Kombination zwischen dem Schadenspotential und der Eintrittswahrscheinlichkeit existieren zwei Ansätze:

- **Probabilstischer Ansatz**

  Bei dem probabilistischen Ansatz wird das Schadenspotential ggü. der Eintrittswahrscheinlichkeit höher bewertet. Dies entspricht beispielsweise dem Grundgedanken von Versicherungen.

- **Possibilistischer Ansatz**

  Beim possibilistischen Ansatz wird lediglich das Schadenspotential betrachtet, unabhängig von der Eintrittswahrscheinlichkeit.

Bedrohungen und Eintrittswahrscheinlichkeiten gilt es grundsätzlich abzuschätzen. Kersten et. al. [KRS13] empfehlen auf Statistiken zurückzugreifen, sofern für relevante Störfälle entsprechende Aufzeichnungen existieren aus denen man ein Risiko für zukünftige Ereignisse ableiten kann. Bei gezielten Angriffen stellt sich dies jedoch als problematisch dar. Auch Klipper [Kli15] sieht statistische Daten, die sich naturgemäß auf die Vergangenheit beziehen in einem Umfeld, in dem sich Angriffsvarianten, Schwachstellen und Möglichkeiten von Verteidigern und Angreifern rasend schnell verändern, als keine gute Basis für eine aussagekräftige Entscheidungsgrundlage an.

Um in diesem Fall dennoch eine Aussage über das potentielle Risiko treffen zu können, wird eine Analyse des Angriffspotenzials und der Stärke von Sicherheitsmaßnahmen erhoben, deren Ergebnisse in einem sog. Risikoindex bzw. in Risikoklassen eingeteilt werden.

Kersten et. al. [KRS13] geben für das Angriffspotential eines Angreifers drei Faktoren vor:

- Fachkentnisse
- Verfügbare Ressourcen
- Gelegenheiten

Abbildung 2.3 stellt die einzelnen Bestandteile des Risikomanagements graphisch vor.

- Risiko-Identifikation

  Identifikation von Bedrohungen, Schwachstellen und bereits vorhandenen Gegenmaßnahmen

- Risikoabschätzung

  Abschätzung des Risikos durch Berücksichtigung von Angriffspotential und Stärke der Schutzmaßnahmen für jede Bedrohung

- Risikobewertung

  Klassifizierung des Risikos anhand der Eintrittswahrscheinlichkeit und des Schadenspotentials

2.2.5 Maßnahmen und Maßnahmenziele

Maßnahmen oder auch Controls sind im Annex A der ISO/IEC 27001 und dienen dem Schutz der Informationswerte vor Risiken. Brenner et. al. [BOH+17] beschreiben, dass die in Anhang A des ISO/IEC 27001 geführten Maßnahmen einen deutlichen Schwerpunkt der Norm darstellen und als normativer Bestandteil und Teil der verbindlichen Mindestanforderungen entsprechend spezifiziert werden müssen. Zur Kategorisierung der Maßnahmen, werden diese unter Berücksichtigung des zu Grunde liegenden Maßnahmenziels zusammengefasst. Da der Begriff der Maßnahme im deutschen eher mit konkreten Risikobehandlungsmaßnahmen in Bezug gebracht wird, welche es ebenfalls zu betrachten gilt, wird im weiteren Verlauf dieser Arbeit der englische Begriff *Control* verwendet.

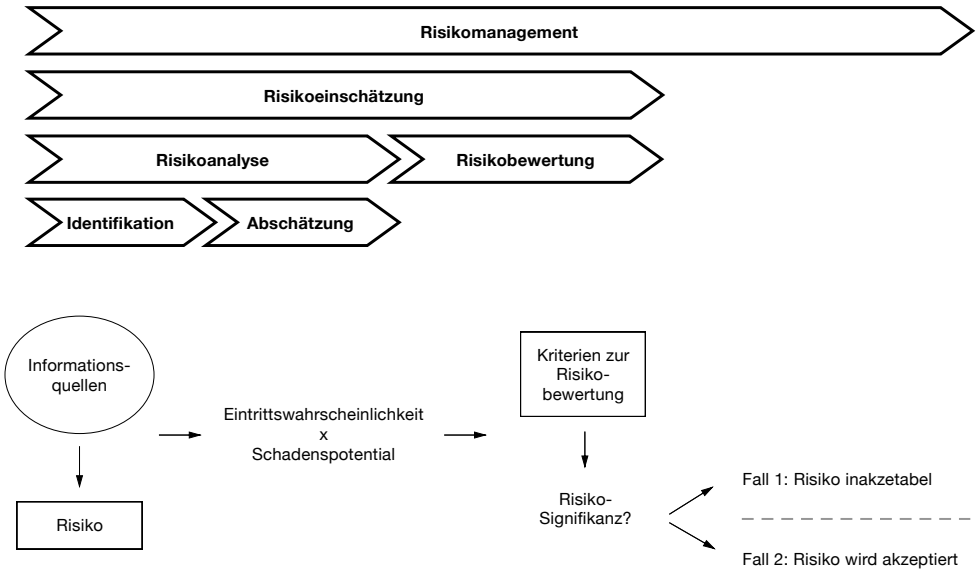


Abbildung 2.3: Bestandteile des Risikomanagements[Gmb13]

Im Zusammenhang mit Controls des Anhangs A ist ebenfalls die Erklärung zur Anwendbarkeit (Statement of Applicability (SoA)) zu erwähnen. Kersten et. al. [KRS13] beschreiben, dass die Erklärung zur Anwendbarkeit neben der ISMS-Leitlinie ein grundlegendes Dokument eines ISMS darstellt, da es alle ausgewählten Maßnahmen und Maßnahmenziele inklusive der dazugehörigen Begründungen für die Auswahl wiedergibt. Auch Maßnahmen, die nicht ausgewählt wurden müssen entsprechend begründet werden, da so gewährleistet werden kann, das auch wirklich alle notwendigen Maßnahmen berücksichtigt wurden.

2.2.6 PDCA-Methodik

Der Aufbau eines ISMS erfolgt in definierten Phasen, die den Schritten des Demingkreises entsprechen (vgl. Sowa [Sow17]). Die einzelnen Phasen bilden einen Prozess, der sich iterativ anwenden lässt und somit eine kontinuierliche Verbesserung oder auch Weiterentwicklung von Systemen fördert. Die einzelnen Schritte lauten entsprechend der Abkürzungen:

Plan - **D**o - **C**heck - **A**ct

Im Hinblick auf die Herstellung eines wirksamen ISMS ergeben sich daher folgende Grundarbeitsschritte während der einzelnen Phasen.

Plan-Phase

In der Planungsphase des PDCA-Zyklus sollen grundlegende Vorbereitung zur Herstellung eines ISMS oder zur Anpassung eines ISMS an neue organisationale Anforderungen getroffen werden. Da die Inhalte eines ISMS auf Erkenntnisse und Einschätzungen des Risikomanagements aufbauen, finden sich wichtige Bestandteile zur Risikoeinschätzung bereits in der Planungsphase.

Zu Beginn steht allerdings die Festlegung des Anwendungsbereichs und den Grenzen des ISMS. Kersten et. al [KRS13] unterstreicht weiterhin die Wichtigkeit dieses Arbeitsschrittes, da das ISMS auf die Bedürfnisse der Organisation zugeschnitten und darüber hinaus möglichst losgelöst von anderen Managementsystemen aufgebaut werden sollte. Als konkreten Anwendungsbereich können Abteilungen einer Organisation, die beispielsweise logisch oder geographisch getrennt sind, dienen. Im Kapitel 6 des ISO 27003 [Int15c] finden sich weitere Hilfen, wie der Anwendungsbereich eines ISMS festgelegt werden kann.

Sobald die Festlegung des Anwendungsbereichs durchgeführt wurde, sollte die Definition der ISMS- und der Informationssicherheitsleitlinie stattfinden. Die Informationssicherheitsleitlinie ist in der ISO/IEC 27002 [Int15b] klar definiert und umfasst Geschäftserfordernisse und gesetzliche sowie vertragliche Anforderungen und Verpflichtungen aller Mitarbeiter der Organisation. Die ISMS-Leitlinie wird von Kersten et. al [KRS13] als separate Richtlinie beschrieben, die zusätzliche Rahmenbedingungen, die zur Erreichung der Informationssicherheit gegeben sein müssen, festlegt.

Anschließend ist die Methode der Risikoeinschätzung festzulegen. Dazu gehören insbesondere die Art und Weise, wie Risiken analysiert und bewertet werden sollen. Darüber hinaus müssen für Risiken bestimmte Akzeptanzkriterien festgelegt werden, die je nach Risikoklasse anzuwenden sind. Die Norm stellt in Bezug auf die Methode zur Risikoeinschätzung keine Anforderungen außer, dass die gewählte Methode zu vergleichbaren und wiederholbaren Ergebnissen führen muss (vgl. ISO/IEC 27001 [Int15a]).

Sobald die Methode zur Risikoeinschätzung definiert wurde und man entsprechende Risikoakzeptanzkriterien vorliegen hat, kann die Identifikation von Risiken beginnen. Zur Identifikation von Risiken ist es notwendig, sämtliche Informationswerte des zu betrachtenden Anwendungsbereichs zu kennen und laut Kersten et. al. [KRS13] im Vorfeld innerhalb eines Asset-Verzeichnisses aufzulisten. Das Asset-Verzeichnis sollte, so Kersten et. al., mindestens die Informationswerte und ihre zugehörigen Eigentümer (Assetowner) identifizieren. Bezüglich jedes aufgelisteten Tupels werden dann Bedrohungen und Schwachstellen angegeben.

Nach Klipper [Kli15] werden neben der betrachteten Bedrohungen und der Schwachstellen anschließend in der Risikoabschätzung und Bewertung für jedes erkannte Risiko Schadenspotential und Eintrittswahrscheinlichkeit geschätzt.

Weiter, so Klipper, schließen die Bereiche der Risikoidentifizierung und der Risikoabschätzung die Risikoanalyse ab, die in Kombination mit dem Abschluss der Risikobewertung, die Risikoeinschätzung umfasst (vgl. Abbildung 2.3). Sollten zum Einschätzungszeitpunkt unbekannte Risiken existieren, so können diese weder abgeschätzt noch bewertet werden und können nur durch bereits festgelegte Schutzmaßnahmen anderer Risiken abgewehrt werden. Sämtliche Restrisiken müssen entweder akzeptiert oder durch Einführung weiterer Risikobehandlungsmaßnahmen entweder übertragen, vermieden oder modifiziert werden.

Nachdem sämtliche Risiken und die dazugehörigen Informationswerte analysiert sind, werden Schutzmaßnahmen ausgewählt, die den Schutz der Informationswerte gewährleisten sollen. Die Norm unterscheidet nochmals zwischen Maßnahmenzielen und Maßnahmen. Viele davon

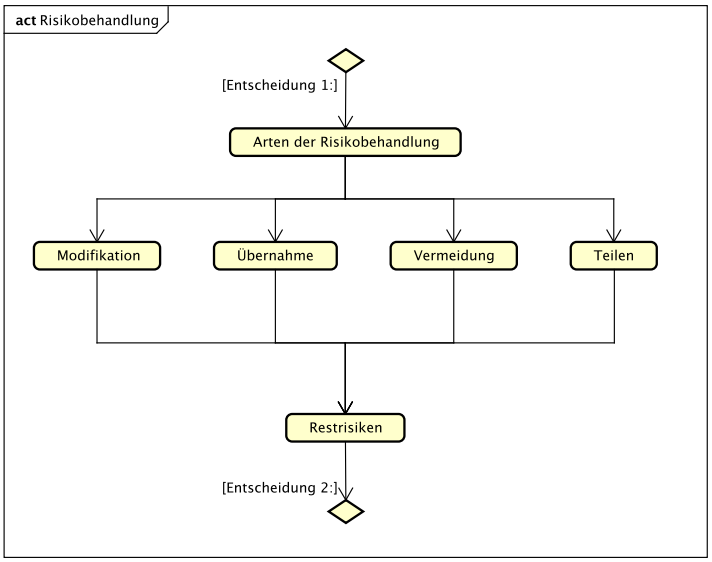


Abbildung 2.4: Arten der Risikobehandlung[Kli15]

werden bereits in Anhang A des ISO/IEC 27001 aufgelistet und können zur Risikosteuerung verwendet werden. Es obliegt der Organisation, noch weitere Maßnahmen einzuführen, die nicht im Anhang A angegeben sind (vgl. ISO/IEC 27001 [Int15a]). Der *Code of Practise* im Teil ISO/IEC 27002 [Int15b] beschreibt zudem zu jeder Maßnahme konkrete Anwendungsbeispiele. Im Zusammenhang mit den Maßnahmen sollte eine Erklärung zur Anwendbarkeit (SoA) gefertigt werden, die sämtliche Maßnahmen unabhängig davon, ob sie realisiert wurden oder nicht, mit einer entsprechenden Begründung auflistet. Kersten et. al [KRS13] führt aus, dass die SoA sicherstellen soll, dass wirklich alle aufgeführten Maßnahmen umgesetzt wurden, die für ein bestimmtes Risiko relevant sein könnten.

Die Planungsphase wird abschließend mit dem Einverständnis des Managements unter Berücksichtigung der zu erwartenden Kosten, des benötigten Personaleinsatzes und dem Ressourcenbedarf in Auftrag gegeben.

Do-Phase

Nach Zusammentragung sämtlicher für ein ISMS relevanten Informationen, der Analyse von Risiken, der Festlegung von Risikoakzeptanzkriterien und der Freigabe durch das Management, findet in der zweiten Phase des PDCA-Zyklus die eigentliche Herstellung des ISMS statt. Der erste Schritt bei der Umsetzung eines ISMS besteht nach Kersten et. al [KRS13] aus der Formulierung eines Risikobehandlungsplans.

Der Risikobehandlungsplan erfüllt zwei grundlegende Funktionen. Er soll die geeigneten Aktionen des Managements und die dafür benötigten personellen und materiellen Ressourcen unter Berücksichtigung der Priorität beschreiben. Zu den Aktionen des Managements zählen ein Großteil der Punkte, die in der Planungsphase aufgelistet wurden. Darunter die Durchführung sämtlicher Schritte der Risikoeinschätzung oder auch die Erstellung einer Er-

klärung zur Anwendbarkeit (Statement of Applicability, SoA, vgl. [KRS13]).

Die Idee hinter dem Risikobehandlungsplan liegt darin, das Management bei dem Aufbau des ISMS stets einzubeziehen und auch die Kommunikation zur Einhaltung der Leitlinien zu fördern und zu unterstützen. Für Mitarbeiter bieten sich regelmäßige Schulungs- und Sensibilisierungsphasen an. Eine Möglichkeit zur Feststellung einer wirksamen Umsetzung stellen interne Audits und Managementbewertungen dar. Klett et. al. [KSK11] beschreiben, dass im Rahmen interner Audits sowohl technische Tests, Inspektionen administrativer und infrastruktureller Maßnahmen aber auch Arbeitsplatzbegehungen zur Prüfung der Einhaltung von Sicherheitsvorgaben geeignete Prüfmethoden darstellen.

Neben dem Aufbau des Risikobehandlungsplans gilt es die formal festgehaltenen Maßnahmenziele und Schutzmaßnahmen umzusetzen und anschließend auf ihre Wirksamkeit hin zu prüfen (vgl. Klett et. al. [KSK11]). Hier ist darauf zu achten, dass eine einheitliche Methode verwendet wird, die bei gleichen Bedingungen über unterschiedliche Maßnahmen hinweg auch vergleichbare Ergebnisse zulässt.

Kersten et. al. [KRS13] führen aus, dass es wichtig ist, nach einer initialen Einrichtung der Schutzmaßnahmen, diese auch zu verwalten. Dies bedeutet, dass die Einhaltung und Wirksamkeit von Schutzmaßnahmen kontrolliert und bei sich ändernden Verhältnissen angepasst werden muss. Die Verwaltung eines ISMS über einen längeren Zeitraum schließt auch das Ressourcenmanagement ein, dessen Aufgabe es ist, einen Ressourcen-Plan für das ISMS zu führen und regelmäßig zu aktualisieren.

Neben der Prävention von Sicherheitsvorfällen spielt die Detektion und Reaktion eine große Rolle, da somit auch neue Risiken erkannt und entsprechend gesteuert werden können. In der Regel wird nach Kersten et. al [KRS13], im Rahmen des Incident Managements ein Incident Management Plan erstellt, der eine Klassifizierung, die empfohlene Vorgehensweise und Eskalationsstufen vorgibt. Für Notfälle existieren nochmals gesonderte Vorgehensweisen, die innerhalb eines Notfallhandbuchs (vgl. Klett et. al. [KSK11]) beschrieben werden sollen. Sämtliche Vorfälle werden mit dem Ziel einer vollständigen Wiederherstellung bearbeitet. Unabhängig vom Auslöser sollten Konsequenzen in Form von beispielsweise strafrechtlicher Maßnahmen oder Optimierungen der Schutzmaßnahmen gezogen werden.

Check-Phase

In der Check-Phase gilt es, die laufende Aktivitäten zu beobachten und so frühzeitig Fehler zu erkennen. Hierbei bietet sich die Einführung von Indikatoren (Key Performance Indicator, KPI) zur Früherkennung von Sicherheitsvorfällen an. Breiter und Fischer [BF11] beschreiben, dass durch regelmäßige Prüfung der Wirksamkeit von Schutzmaßnahmen in Verbindung mit der Prüfung des verbundenen Aufwands und des potentiellen Schadens, den eine unzureichende Wirksamkeit nach sich zieht, ein kontinuierlicher Verbesserungsprozess (KVP) erreicht werden kann.

Um eine stetige Optimierung zu erreichen, ist eine regelmäßige und anlassbezogene Dokumentation der Wirksamkeitsmessungen notwendig. Diese kann laut Kersten et. al. [KRS13] beispielsweise auch im Rahmen interner Audits stattfinden, bei denen entweder unabhängige

Mitarbeiter oder extern engagierte Auditoren mit der Überprüfung der eigenen Managementsysteme beauftragt werden. Neben der Prüfung der Funktionalität des ISMS empfiehlt es sich auch regelmäßige Managementbewertungen durchzuführen, die dafür Sorge tragen, dass der Anwendungsbereich in einem angemessenen Rahmen bleibt und notwendige Verbesserungen im Zusammenhang mit Geschäftsprozessen herausgearbeitet werden können.

Act-Phase

In der Act-Phase werden die aus der vorangegangenen Phase (z.B. aus Managementbewertungen oder Audits) erkannten Verbesserungen umgesetzt. Kersten et. al [KRS13] unterstreichen die Wichtigkeit, die Erwartungshaltung bei allen Beteiligten der umzusetzenden Maßnahmen in Grenzen zu halten, da durch die Umsetzung von Maßnahmen zwar eine positive Entwicklung erwartet werden würde - diese aber auch negative Folgen nach sich ziehen könnten. Weiterhin beschreiben sie, dass für den Fall, dass mehrere Optimierungen auf ein gemeinsames Ziel hinarbeiten würden, die ressourcenschonendere zu wählen sei. Verbesserungsvorschläge, die für eine Umsetzung nicht ausgewählt wurden, sollten für den späteren Gebrauch dokumentiert werden.

2.3 Dokumentation in einem Managementsystem

Unternehmen, die eine Zertifizierung im Bereich der ISO/IEC 27001 Norm anstreben, müssen neben der Herstellung eines ISMS auch die zweckmäßige Dokumentation der einzelnen Komponenten und Mindestanforderungen berücksichtigen. Allgemein gilt, dass eine strukturierte und regelmäßig gepflegte Dokumentation die dynamische Organisationsstruktur mit sich wechselnden Rollen, Verantwortlichkeiten und Geschäftsbereichen über einen langfristigen Zeitraum unterstützen soll. Innerhalb der Norm finden sich konkrete Anforderungen an dokumentierte Informationen im Kapitel 7.5.

2.3.1 Definitionen

Andenmatten [And08] definiert in seinem Praxisbuch das Dokumentationsmanagement als Werkzeug, welches das vollständige und lückenlose Steuern und Regeln aller Dokumente und Daten zur Abwicklung des Geschäfts sicherstellt und weiterhin Dokumente und Daten den Systemen zur sachgerechten Abwicklung und Ordnung der Ablage zugewiesen werden sollen. Ein solches System kann über ein firmeninternes Speichermedium (Intranet) gesteuert, verwaltet und aktualisiert werden.

In der Realität muss man zwischen den beiden Begriffen des Dokumentenmanagements und des Dokumentationsmanagements unterscheiden. Manuela Reiss [Rei16] definiert diese Begriffe:

Dokumentationsmanagement

Dokumentationsmanagement ist die Summe aller Aktivitäten und Funktionen für die Steuerung und Verwaltung von dokumentierten Informationen, die gewährleistet, dass alle erforderlichen dokumentierten Informationen aktuell, vollständig und in ausreichender Qualität verfügbar sind.

Dokumentenmanagement

Dokumentenmanagement beschreibt die meist datenbankgestützte Verwaltung von Dokumenten. Im Fokus stehen die operativen Aktivitäten im Rahmen des Dokumenten-Lifecycle. In Abgrenzung zum Dokumentationsmanagement werden hier übergeordnete Steuerungs- und Kontrollfunktionen durch das Management nicht betrachtet.

Die ISO/IEC 9001 [eur08] unterscheidet weiterhin zwischen den Begriffen der *Dokumentation* und der *Aufzeichnung*. Kersten et. al. [KRS13] definiert Aufzeichnungen als Protkolle, Mitschriften, Berichte, Log-Dateien und ähnliches, die während einer Maßnahme oder als dessen Resultat entstehen können - also Schriftstücke, die der Nachweispflicht ordnungsgemäßer Geschäftsführung entsprechen.

Dokumentationen stellen dagegen Zusammenstellungen von Dokumenten dar, die zum Verständnis oder Festlegung von Regelungen eine abteilungs- oder organisationsweite Relevanz besitzen. Darunter können beispielsweise Richtlinien und Leitlinien aber auch Verfahrens- und Prozessbeschreibungen fallen. Dokumentation können sich über einen bestimmten Zeitraum verändern und besitzen somit einen Revisionsstand.

2.3.2 Dokumentationstypen

Bei der Dokumentation komplexer Managementsysteme sind oftmals mehrere Zielgruppen involviert, die einen unterschiedlichen Kenntnisstand bzw. unterschiedliche Interessen in Bezug auf einen Geschäftsprozess besitzen. Daher empfiehlt es sich, je nach Geltungsbereich eine unterschiedliche Dokumentation anzufertigen oder die Inhalte pro Zielgruppe zu begrenzen (vgl. Kersten et. al. [KRS13]). Im Bereich des Projektmanagements des ISO 21500 [Int15] haben sich die Bereiche aus Abbildung 2.5 bewährt.

In Bezug auf das Informationssicherheitsmanagement zählen die dokumentierten Richtlinien zum Bereich der betreiberbezogenen Dokumentation. Die Freigabe von anwenderbezogenen Dokumentation in diesem Bereich zur Erhöhung der Transparenz gegenüber Kunden bleibt dem auszuführenden Unternehmen überlassen. Teile der servicebezogenen Dokumentationen können bei der Festlegung von Informationswerten relevant sein.

2.3.3 Lesergruppe

Abbildung 2.5 veranschaulicht, dass Dokumentationen für unterschiedliche Adressatenkreise bestimmt sein können. Es ist deshalb wichtig, dass der Detailierungsgrad der Dokumentation auch dem Verständnis und der Berechtigungsstufe der Zielgruppe entsprechend angepasst wird. Die Abstufungen des Detailgrades finden sich innerhalb der Anwendbarkeitskriterien der Dokumente. Reiss und Reiss [RR09] listen mögliche Anwendbarkeitskriterien:

- Technische oder organisatorische Dokumente
- Anleitung oder Dienstbeschreibung
- Sicherheitsberechtigungen (Schreib-/Lesezugriffe)
- Sprache

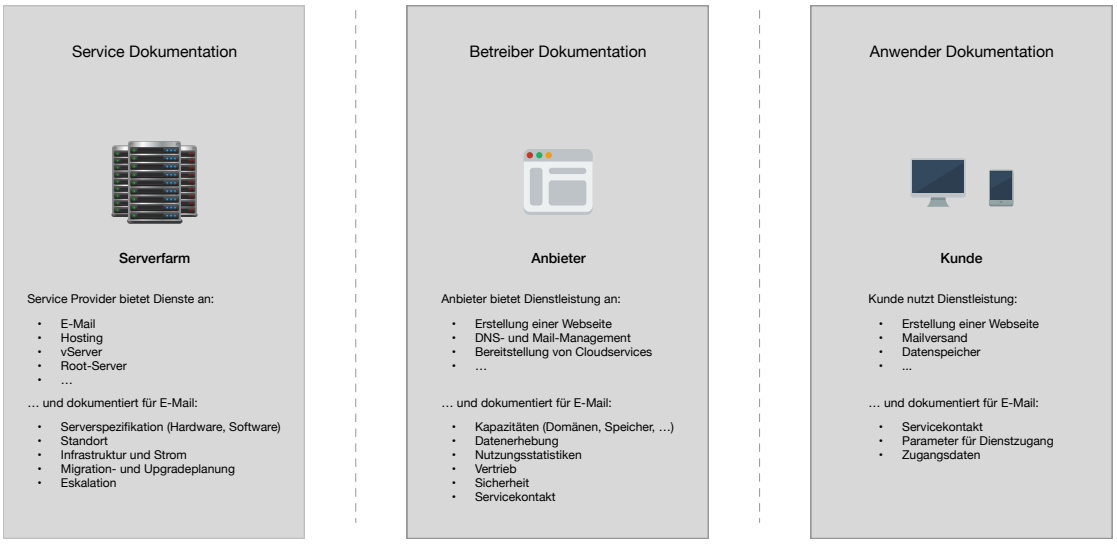


Abbildung 2.5: Dokumententypen im Projektmanagement

Die Autoren [RR09] führen aus, dass Dokumentationen nicht nur zur schriftlichen Festhaltung fortwährender Tätigkeiten, sondern auch als Nachschlagewerk bei Problemstellungen und zur Konsolidierung von Vorgehensweisen dienen. Weiterhin bieten digitale Dokumentationssysteme mehrere Möglichkeiten, um einen schnellen Zugriff auf relevante Daten zu gewährleisten wie beispielsweise eine Suchfunktion, das Tagging von Dokumenten oder die Illustration einer transparenten Ablagestruktur.

2.3.4 Dokumentationsmanagementsysteme (DMS)

Das Dokumentationsmanagementsystem (DMS) dient nach Reiss [RR09] dazu, die für die Dokumentationsmanagementprozesse notwendigen Ziele zu erreichen. Zu den Zielen zählen die Möglichkeiten im Rahmen der Dokumentenlenkung. Die Dokumentenlenkung umfasst die Erstellung, Überprüfung, Genehmigung, Verteilung und den Einzug alter Versionen von Dokumenten. Diese Teilaspekte müssen für jedes Dokument nachvollziehbar festgelegt werden und dienen der Sicherung des Schutzes vor unberechtigter Veränderung, Kenntnisnahme und Vorenthaltung. Zur Realisierung dieser Teilaspekte sind Managementaufgaben festgelegt, die im Folgenden vorgestellt werden und durch Kersten et. al. [KRS13] beschrieben werden:

Dokumenten-Freigabe

Bei der Dokumenten-Freigabe sind Berechtigungsstufen zu berücksichtigen. Berechtigungsstufen stellen ein Mittel zur Steuerung des Informationsflusses dar. Die Autoren Reiss [RR09] definieren neben der grundsätzlichen Steuerung von Berechtigungen einen mehrstufigen Freigabeprozess, der die Prüfung der formalen und inhaltlichen Vollständigkeit, die sachliche

Richtigkeit und die Übereinstimmung mit den in der Dokumentationsrichtlinie definierten formalen Anforderungen umfasst.

Aktualität, Revisionierung und Archivierung

Dokumente müssen während der Durchführung des PDCA-Zyklus kontinuierlich aktualisiert werden. Dies kann entweder ereignisorientiert oder in regelmäßigen Abständen geschehen. Ereignisorientierte oder auch anlassbezogene Anpassungen können durch Änderungen der Geschäftsstrategie oder der Risikolage, aber auch durch Änderungen der Technologie entstehen. Regelmäßige interne Audits als Kontrollwerkzeug können hier Ergebnisse zur tatsächlichen Aktualität der Dokumente liefern.

Neben der Aktualität, ist es wichtig auf Änderungen der Dokumentation aufmerksam zu machen. Der Revisionsstand wird dabei durch eine Versionsnummer und einer Datumsangabe kenntlich gemacht, die einen Vergleich mit alten Dokumenten ermöglicht. Veraltete Dokumente sollten dann nur noch innerhalb eines Archivs gesammelt und zum Zweck der Nachvollziehbarkeit aufgerufen werden können.

Lesbarkeit und Identifizierbarkeit

Bei Dokumenten, die Aussage darüber treffen, wie bestimmte Komponenten eines Systems aufgebaut sind, hat die Lesbarkeit und Identifizierbarkeit eine besonders große Bedeutung. So kann die Lesbarkeit durch Ergänzung geeigneter Grafiken und Illustrationen das Verständnis komplexer Zusammenhänge erhöhen. Die Identifizierbarkeit von Dokumenten kann darüber hinaus über eindeutige Dokumentenbezeichnungen und Metadaten erhöht werden. Solche Dokumentenbezeichnungen lassen sich aus der Klassifikation der betrachteten Dokumente ableiten.

Prozessorientertes Dokumentationsmanagementsystem

Reiss [Rei16] bezeichnet die Steuerung der Dokumentation als zentrale Aufgabe. Abbildung 2.6 illustriert den Zyklus dokumentierter Informationen.

Die Dokumentenerstellung stellt den ersten Schritt im Lebenszyklus eines Dokuments dar. Als Grundlage dienen nach Reiss [Rei16] sowohl die vorherige Festlegung von Berechtigungsstufen und Richtlinien zur Verfassung von Dokumenten.

Anschließend folgt die Freigabe oder auch Bereitstellung der Dokumente innerhalb einer geeigneten Ablagestruktur. Dieser Schritt stellt laut Reiss [RR09] einen der größten Herausforderungen bei der Herstellung eines DMS dar, da sichergestellt werden muss, dass alle Beteiligten Zugriff auf sämtliche für sie relevanten Dokumente erhalten und darüber hinaus die Attribute der einzelnen Dokumente einsehen können.

Dem Grundsatz, welchem zu folge Informationen lediglich in einem Dokument auftauchen dürfen, schreiben Reiss und Reiss einen hohen Stellenwert zu. Durch die Referenzierung von Dokumenten anstatt dem Kopieren einzelner Informations-Teilstücke über mehrere Dokumente hinweg lassen sich Inkonsistenzen, die einen erhöhten Pflegeaufwand verursachen, vermeiden.

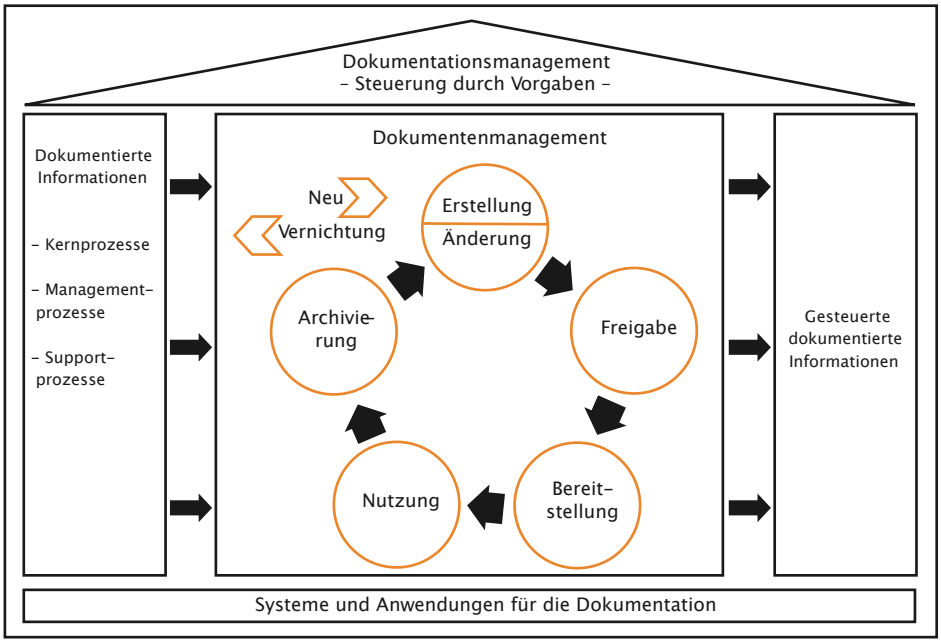


Abbildung 2.6: Aufbau eines prozessorientierten Dokumentationsmanagementsystems[RR09]

2.4 Zusammenfassung

Das Grundlagenkapitel hat die Thematik des Informationssicherheitsmanagements beginnend mit einem historischen Einblick über die Entwicklung der internationalen Norm sowie den Zusammenhang zwischen unterschiedlichen Managementsystemen vorgestellt.

Der zweite Abschnitt behandelt die Vorgehensweise bei der Herstellung eines ISMS mit konkretem Bezug auf die vier Phasen des PDCA-Zykluses, der dem Ziel der kontinuierlichen Verbesserung eines prozessorientierten Managementsystems dient.

Das Dokumentenmanagement, dass eher dem Bereich des Qualitätsmanagements zuzuordnen ist, findet sich auch bei der Dokumentation im Bereich des ISMS wieder, da Organisationen mit dem Anspruch einer Zertifizierung entsprechende Nachweispflichten haben, denen sie nachkommen müssen. Vor dem Hintergrund der erarbeiteten Grundlagen zum Thema Informationssicherheitsmanagement wird im anschließenden Kapitel der Status-Quo des LRZ beschrieben.

3 Allgemeine Informationen zum LRZ

Das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften ist das gemeinsame Rechenzentrum für die beiden Münchner Universitäten sowie der Bayerischen Akademie der Wissenschaften (BAdW) dar und bietet durch wissenschaftliche Nähe zur Forschung und Lehre vielseitige Ressourcen und Dienstleistungen an. Der Dienstleistungskatalog umfasst die Nutzung der Netzinfrastruktur des Münchner Wissenschaftsnetzes (MWN), die Nutzung von Rechnern und Speicher in Form von Attended Housing, Hosting, Data-Science-Storage und Online-Speicher, Mail- und Groupwarefunktionalitäten, Supercomputing sowie die Herstellung und Verwaltung von IT-Infrastrukturen im Münchner Einzugsgebiet.

Abschnitt 3.1 stellt einen Überblick über den Dienstleistungskatalog des LRZ anhand der erhobenen Statistiken aus dem öffentlich publizierten Jahresbericht 2015 [lrz16] vor. Im Zuge dessen werden potentiell relevante Informationswerte, die die Dienste betreffen können, herausgestellt. Die Vorstellung des Dienstleistungskatalogs soll außerdem auf die Komplexität und Diversität der zu erfassenden Infrastruktur aufmerksam machen.

Anschließend folgt in Abschnitt 3.2 die Beleuchtung der derzeitigen Ausgangslage bezüglich des Dokumentations- und Informationssicherheitsmanagements am LRZ - insbesondere in welcher Form die Dokumentationsprozesse am LRZ derzeit gestaltet sind. Aus der Betrachtung der Ausgangslage lassen sich bereits wichtige Ansprechpartner und Verantwortliche identifizieren, deren Interessen es bei der Umsetzung einer ISMS-Dokumentation zu berücksichtigen gilt.

3.1 Dienstleistungskatalog

Das LRZ verpflichtet sich mit speziellen Verträgen zur Auftragsdatenverarbeitung zu einem hohen Maß an Informations- und Datensicherheit. Die Dienstleistungen des LRZ werden durch die Münchner Universitäten und Hochschulen aber auch durch den Bibliotheksverbund Bayern (BVB), der Staatlichen Naturwissenschaftlichen Sammlungen Bayerns (Staatliche Naturwissenschaftliche Sammlungen Bayerns (SNSB)) und der Akademie der Bildenden Künste (Akademie der Bildenden Künste (AKDB)) genutzt.

Die nachfolgende Aufstellung gibt einen detaillierteren Einblick über das Dienstleistungsangebot.

3.1.1 E-Mail und Groupware

Das LRZ bietet das Hosting von E-Mailpostfächern auf OpenSource Basis (z.B. Postfix) oder der auf Windows Server basierenden Groupware Microsoft Exchange an. Die Anzahl der Nutzer von herkömmlichen IMAP-Postfächern betrug 2015 rund 96.000 Nutzer und die Nutzerzahl des Exchange-Dienstes lag bei rund 66.000 Nutzern mit steigender Tendenz.

Als Schnittstelle zwischen dem Internet und der Infrastruktur des MWN ist ein gesteuerter und kontrollierter Versand von Mails zwingend notwendig, weshalb dieser ausschließlich über die 133 dedizierten Mailserver, die über alle wissenschaftlichen Einrichtungen verteilt sind, empfangen werden können. Dies erscheint sinnvoll, weil das durchschnittliche E-Mail-Aufkommen 2015 bei rund 710.000 E-Mails pro Tag lag und durch gezielte Sicherheitsmaßnahmen zur Prävention von Spam- und Virenmails bereits zwei Drittel des E-Mailverkehrs direkt abgewiesen werden konnten.

Hier stellen insbesondere die Serverinfrastruktur, Benutzerauthentifizierungsdaten aber insbesondere die Nutzdaten (E-Mails, Anhänge, Metadaten) informationskritische Elemente dar, die es zu schützen gilt.

3.1.2 Server- und Webhosting

Neben Mailhosting bietet das LRZ auch Server- und Webhostingdienstleistungen auf Basis der Betriebssysteme Linux oder Windows an. Das Angebot umfasst Managed Server, den Betrieb persönlicher Webseiten und Webservices, wie das beispielsweise kürzlich gestartete Gitlab, aber auch Videostreaming und Konferenzfunktionalitäten.

Da die Bereitstellung freier Webhostingmöglichkeiten durch die Divergenz der eingesetzten Anwendungen viele verschiedene Angriffsvektoren ermöglicht, sind Schulungen und eine gehärtete IT-Infrastruktur unabdingbar. Das Webhostingangebot wird durch die Dienstleistung der Administration von Client- und Serverdeployment ergänzt. Windows Betriebssysteme werden über den Microsoft System Center Configuration Manager (SCCM) verteilt. Insgesamt umfasst dieser Teilbereich rund 2000 Clientsysteme und 160 Serversysteme.

Die für die Universitäten zur Verfügung gestellten Rechnerpools werden ebenfalls von dem LRZ verwaltet. Fasst man die Rechner sämtlicher Mandanten zusammen, ergibt sich eine Menge von rund 8240 Light Desktop Systemen.

Zur Nutzung dieser Dienste werden innerhalb einer zentralen Benutzerverwaltung, dem LRZ-SIM (LRZ-Identity-Managementsystem (LRZ-IDM)), sog. Benutzerkennungen generiert, von denen jedem individuellen Nutzer eines Mandanten eine zugeordnet wird. Alleine bei den Münchner Universitäten belaufen sich die eingesetzten Kennungen auf rund 200.000, da jeder immatrikulierte Student ein Kennung zur Nutzung der IT-Infrastruktur erhält. Abbildung 3.1 zeigt die Verteilung der unterschiedlichen Datenbankservern innerhalb der Bereiche so wie deren Schnittstellen untereinander.

Mögliche Informationswerte im Bereich des Server- und Webhostings sind erneut Nutzdaten (Webseiten, Dienstanwendungen, Datenbanken, ...) aber auch Konfigurationen sowie die Daten der Benutzerverwaltung.

3.1.3 Virtuelle Realität und Visualisierung

Das Zentrum für Virtuelle Realität und Visualisierung (V2C) bietet sowohl in Kooperation mit studentischen Projekten als auch in Zusammenarbeit mit führenden Wirtschaftsunter-

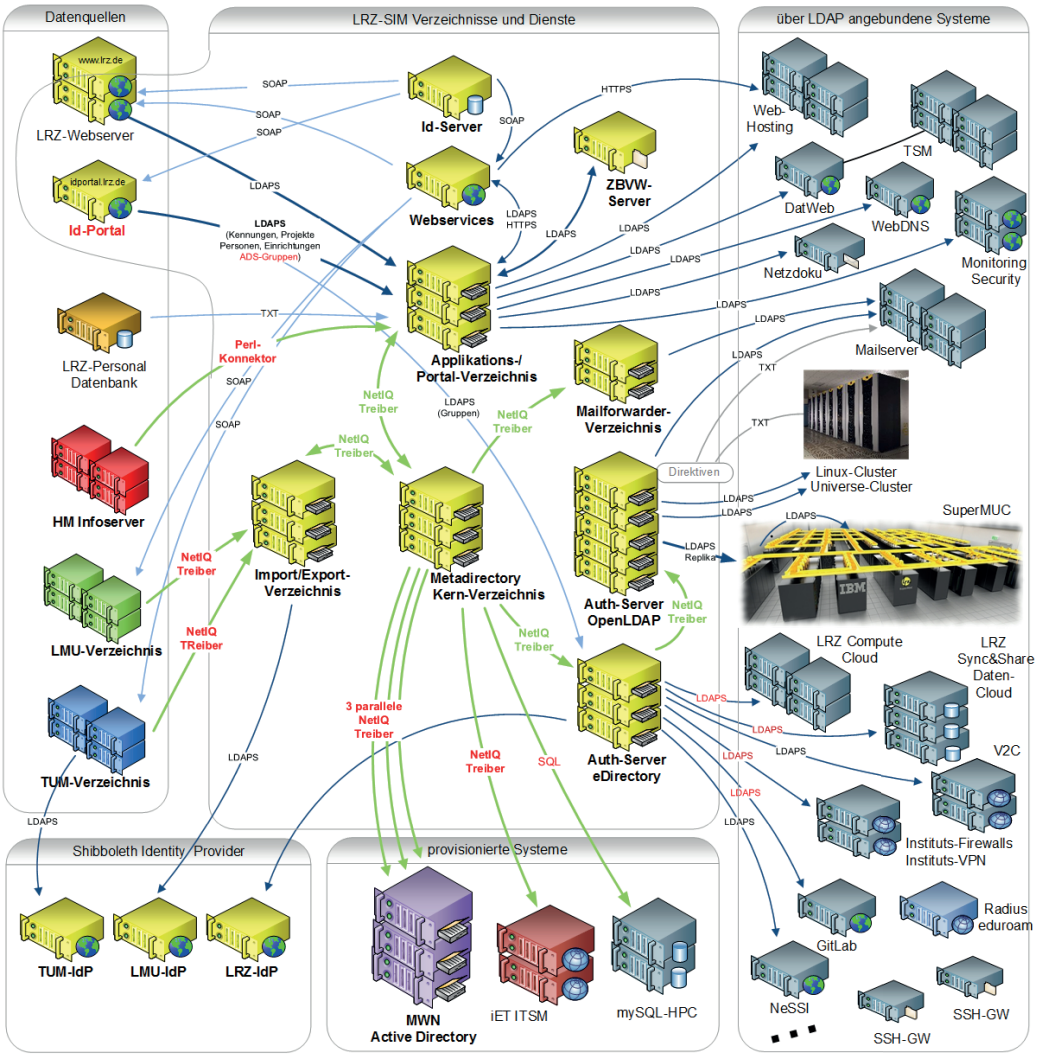


Abbildung 3.1: LRZ-SIM Benutzerverwaltung und Abhängigkeiten [lrz16]

nehmen, Möglichkeiten zur Darstellung stereoskopischer Inhalte. Hierfür ist das LRZ mit einer 5-seitigen Projektionsumgebung, genannt CAVE (CAVE Audio Visual Environment) ausgestattet, die es ermöglicht 3D-Umgebungen in einem Würfel mit einer Seitenlänge von 2,7m x 2,7m abzubilden.

Die Projekte, bei der das V2C Anwendung findet, finden sich unter anderem im architektonischen Bereich (Stadt- und Raumplanung), im molekularbiologischen Bereich (Visualisierung von Genomstrukturen) oder auch im Automobilbereich (Visualisierung von Konzepten und Entwürfen).

Forschungsprojekte und Daten die durch Kooperation mit beteiligten Unternehmen durchgeführt werden, müssen entsprechend geschützt werden.

3.1.4 High Performance Computing

Ein wichtiger Bestandteil des Rechenzentrums ist der Hochleistungsrechner SuperMUC. Die Rechenzeit des SuperMUCs verteilt sich auf den Bedarf wissenschaftlicher Einrichtungen. Ergänzt wird der Hochleistungsrechner durch einen Linux-Cluster, deren Anzahl aktivierter virtueller Maschinen (VMs) erstmalig einen Wert von über 1.400 überschritt. Physisch wurde der SuperMUC im Jahr 2015 durch Phase 2 aufgerüstet und besteht nunmehr aus über 85.000 Prozessoren und 194 TB Speicher womit mehr als das doppelte an Spitzenrechenleistung der ersten Phase bei lediglich einem Viertel des benötigten Stellplatzes erreicht werden kann.

Um die Nutzung der Rechenzeit quantitativ einschätzen zu können, stellt das LRZ eine prozentuale Statistik der Gesamtrechenzeit nach Fachgebieten zur Verfügung. Die Gebiete *Computational Fluid Dynamics* und *Astrophysics/Cosmology* erreichen gemeinsam über 47 % und somit fast die Hälfte der Gesamtrechenzeit in 2015. Die Daten aller beteiligten Fachgebiete bilden den zu schützenden Hauptinformationswert für diesen Dienst.

3.1.5 Speicherlösungen

Im Bereich der Speicherlösungen finden sich am LRZ neben herkömmlicher Cloud Storage Optionen auch Möglichkeiten zur Datensicherung und der Archivierung. Die Speichermöglichkeiten umfassen sowohl Bandlaufwerke aber auch moderne Plattenspeicher, deren Gesamtspeichervolumen im Jahr 2015 von 42 auf 52 Petabyte erweitert werden musste.

Die Archivierung auf Bandlaufwerken ist in drei unterschiedliche Systeme aufgeteilt:

- Hochleistungssystem HABS
- LTO-Bandlaufwerksystem (LABS)
- Desaster Recovery System (DRABS)

Zur Erhöhung der Ausfallsicherheit sind die Archivierungsdaten nicht nur logisch in getrennten Speichernetzen (SAN Fabrics) unterteilt, sondern auch geographisch voneinander getrennt, wie in Abbildung 3.2 zu sehen ist.

Neu dazugekommen ist der Dienst Sync & Share, der Wissenschaftlern und Studenten die Möglichkeit bietet, Daten geräteübergreifend zu synchronisieren und mittels Berechtigungen zu teilen. Der Sync & Share Dienst wurde Anfang November 2015 gestartet und umfasste Ende des Jahres über 9.000 aktive Nutzer. Archiv- und Produktivdaten bilden neben den bereits genannten Benutzerauthentifizierungsdaten die Informationswerte für diesen Dienst.

3.1.6 Internetzugang des Münchner Wissenschaftsnetzes (MWN)

Das Münchner Wissenschaftsnetz ermöglicht die Kommunikation und Kooperation zwischen den angeschlossenen Instituten und Universitäten sowie mit Kooperationspartner sowohl auf nationaler aber auch internationaler Ebene.

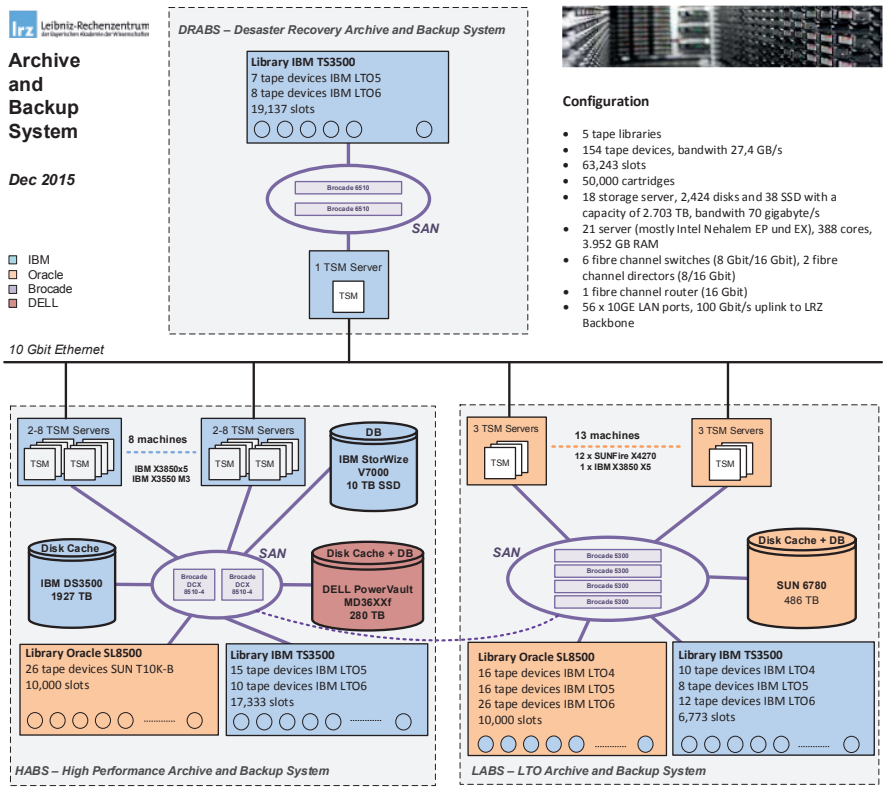


Abbildung 3.2: LRZ Archive and Backup System, Stand Dezember 2015 [lrz16]

Das LRZ ist für das gesamte Backbone-Netz zuständig, das sich aus mehr als 500 Gebäudegruppen zusammensetzt und bis zu 180.000 Geräte versorgt. Die Hauptverbindungspunkte sind mit Glasfaserleitungen (bis zu 100 Gbit/s) verbunden und liefern die Basis für das MWN (vgl. Abbildung 3.3).

Das Routing findet über die beiden Protokolle Open Shortest Path First (OSPF) und Border Gateway Protocol (BGP) statt. Innerhalb der Gebäude, werden modulare Switche eingesetzt mit 1507 Switche in 2015, die zusammen 94.400 Schnittstellen zur Verfügung gestellt haben. Die Aufrechterhaltung eines störungsfreien Betriebs der Netzwerkinfrastruktur an sämtlichen Standorten wird durch mehrere Redundanzmechanismen realisiert, die dem Zweck dienen, das Kernnetz auch bei Ausfall wichtiger Komponenten in einem funktionsfähigen Zustand zu belassen. Um die zur Verfügung gestellte Netzwerkinfrastruktur auch nutzbar machen zu können, bietet das LRZ die Dienste DHCP und DNS/DNSSEC an. Der DNS-Dienst, der zur Namensauflösung von Domänen zu IP-Adressen genutzt wird, umfasste im Jahr 2015 insgesamt 791 Second-Level-Domains. Der DHCP-Dienst, der seit 11 Jahren eingesetzt wird, verwaltet 999 Subnetze mit insgesamt 386.743 dynamisch vergebenen IP-Adressen, die überwiegend von den Münchner Hochschulen und institutseigenen Rechnern genutzt werden.

Die Herstellung einer Netzwerkverbindung über Wireless Local Area Network (WLAN) stellt eine gesonderte Serviceklasse dar, da der großflächige Netzzugang auf dem Campus der Münchner Universitäten insbesondere durch *Eduroam* gewährleistet wird, wodurch be-

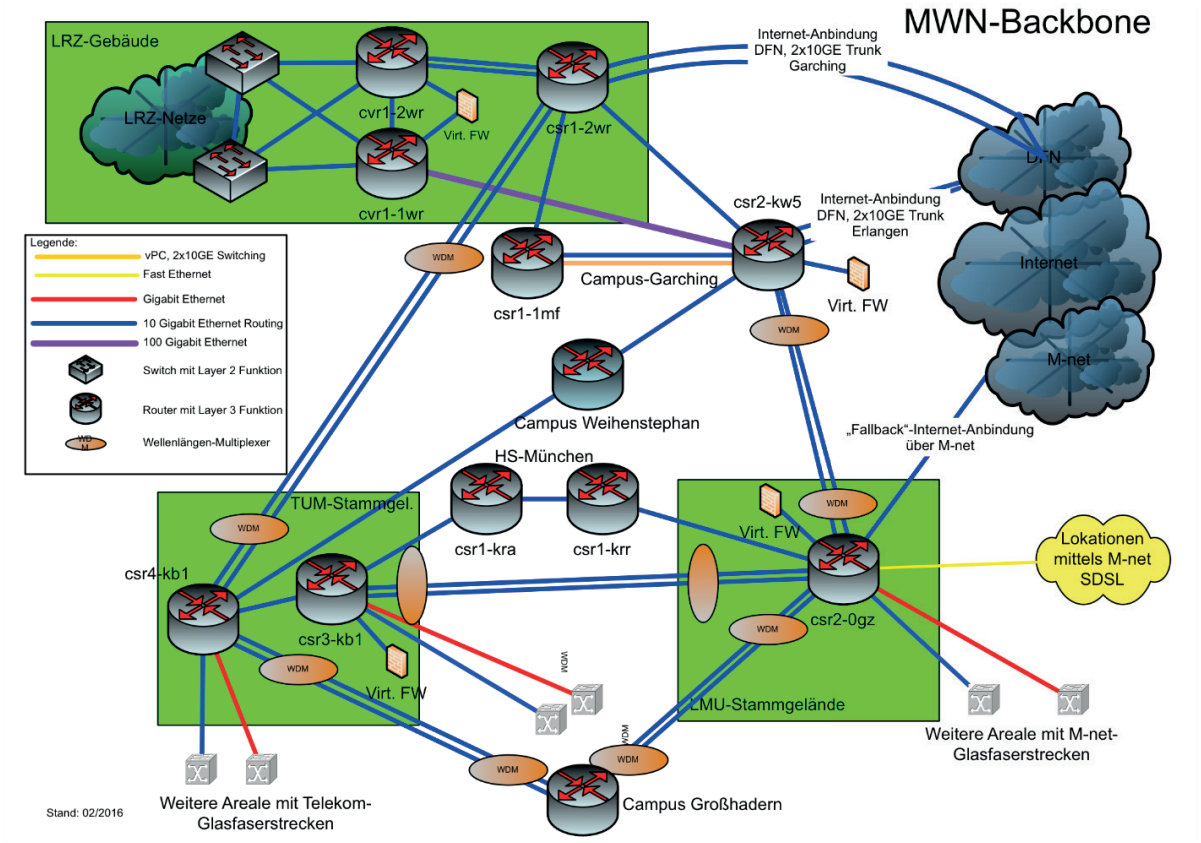


Abbildung 3.3: LRZ Münchner Wissenschaftsnetz Backbone [lrz16]

rechtigten Personen der Zugriff über deren persönliche Hochschulkennung gewährt werden kann. Zur flächendeckenden Versorgung werden insgesamt 354 AccessPoints eingesetzt, über die im Jahr 2015 eine Spitzenanzahl von 33.184 gleichzeitigen Verbindungen aufgebaut wurden.

Die zu schützenden Netzzugangsdaten (preshared keys, RADIUS-Authentifizierungsdaten) aber auch Zertifikate (private Schlüssel) stellen die schützenswerten Informationswerte in diesem Dienst dar.

Nach der Darstellung des grundlegenden Dienstleistungskatalogs sowie der Komplexität und Quantität eingesetzter IT-Systeme, ist es notwendig die derzeitigen Vorgehensweisen und Verfahren zur Erstellung von Dokumenten im Detail genauer zu analysieren. Nachfolgend wird der Status-Quo des Dokumentenmanagements am Leibniz-Rechenzentrum erläutert und damit die Grundlage für die zu etablierende Dokumentation des Informationssicherheits-Managementsystems geschaffen.

3.2 Dokumentenmanagement am LRZ

Das Dokumentationsmanagementsystem des LRZ definiert in der Prozessbeschreibung zwei Kategorien, die die Klassifikation von Dokumenten vorgeben.

Die erste Kategorie definiert sog. *gesteuerte Dokumente*, die einem geordneten Prozess zur Dokumentensteuerung unterstehen und deren spezifischer Dokumententyp anhand der hierarchischen Dokumentationsstruktur (siehe Abbildung 3.4) festzulegen ist. Ungesteuerte Dokumente hingegen, sind von diesen Prozessen ausgeschlossen und unterstehen keinem geordneten Dokumentensteuerungsprozess.

Für die Dokumentenablage existieren unterschiedliche digitale Ablagesysteme. In der Vergangenheit wurden Dokumente überwiegend als Microsoft Word Datei innerhalb des LRZ-Webservers sowohl zur internen Nutzung von Mitarbeitern aber auch zur externen Verbreitung an Nutzer und Kunden hinterlegt. Zur Herstellung einer optimierten und zentralen Dokumentationsstruktur wurde das digitale Dokumentationstool Confluence der Firma Atlassian organisationsweit eingeführt.

3.2.1 Dokumentationshierarchie

Um die Dokumentation im Bereich des ISMS neu zu konzeptionieren, ist es notwendig, die aktuell vorherrschenden Bedingungen und Verfahren zur Erstellung und Veröffentlichung eines Dokuments am LRZ zu betrachten. So können Prozesse unter Berücksichtigung der Norm optimiert und Dokumentationsverfahren entsprechend angepasst werden. Abbildung 3.4 stellt die Hierarchie der spezifischen Dokumentationstypen und deren Zuständigkeiten sowie Änderungsfrequenzen dar.

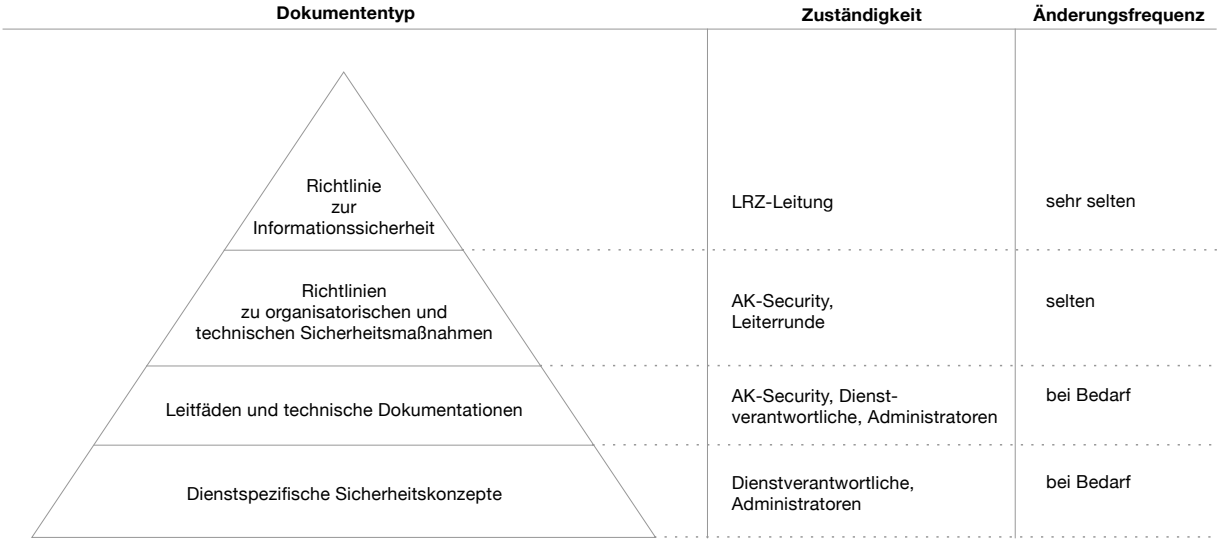


Abbildung 3.4: LRZ-Dokumentationshierarchie mit Zuständigkeiten

Richtlinien zur Informationssicherheit und organisatorischen/technischen Sicherheitsmaßnahmen

Eine Richtlinie umfasst maßgebliche obligatorische Regelungen, die sowohl technischer als auch organisatorischer Art sein können und durch das Top-Management (LRZ-Leitung) unter Genehmigungsvorbehalt in Kraft gesetzt werden. Es ist zu beachten, dass bei der Übersetzung des englischen Begriffs aus der Norm (Policy), geforderte Dokumente wie die Informationssicherheitsleitlinie zwar formal dem Dokumentationstyp *Leitlinie* zugeordnet, allerdings organisationsübergreifend zur Richtlinie erhoben werden. Leitlinien können ebenfalls, wie Richtlinien, Regelwerke darstellen, die jedoch formal schwächer anzusehen sind und eher eine empfohlene Handlungsweise ohne bindenden Charakter vorgeben. Nachdem die Inkraftsetzung einer Leitlinien ihren Zweck verfehlt, wenn sich die Mitarbeiter nicht daran halten, sind die Grenzen zwischen Richtlinien und Leitlinien eher fließend, wodurch sich diese beiden Dokumente trotz der unterschiedlichen Terminologie zusammenfassen lassen können.

Zu den wichtigsten Richtlinien zählt die Informationssicherheitsrichtlinie. Die Informationssicherheitsrichtlinie legt nach Klipper [Kli15] den Anwendungsbereich (Scope) und Grenzen sowie die Verantwortlichkeiten für das anzuwendende ISMS fest. Darüber hinaus gilt es, Basiskriterien für die Nutzung von Systemen sowie bei der Etablierung eines wirksamen Risikomanagementprozesses zu definieren.

Leitfäden und technische Dokumentation

Die Verfahrens- und Prozessbeschreibungen stellen konkrete Informationen dar, die den Umgang mit Systemen im Rahmen der Anforderungen an Informationssicherheit beschreiben. Darunter fallen konkrete Parameter zur Nutzung von Software, empfehlenswerte Vorgehensweisen sowie vorgeschriebene Maßnahmen und Zuständigkeiten. Sie werden durch den LRZ-Arbeitskreis Security in Kooperation mit den dienstverantwortlichen Administratoren zusammengestellt und bei Bedarf angepasst. Ein Beispiel für eine konkrete Verfahrensbeschreibung wäre ein Dokument, dass das Vorgehen bei Viren-infizierten Rechnern beschreibt.

Dienstspezifische Sicherheitskonzepte

Das Dienstspezifische Sicherheitskonzept spiegelt den Ist-Zustand eines konkreten Dienstes wieder. Innerhalb des Sicherheitskonzepts werden von dienstverantwortlichen Administratoren höchst sensible Informationen bzgl. abhängiger Systeme, dienstspezifischer Risiken und Informationen zum Umgang mit datenschutzrechtlichen Daten dokumentiert.

Der grundsätzliche Aufbau ist in drei Abschnitte gegliedert:

- Überblick
- Dienstspezifische Risiken
- Datenschutz und Datensicherheit

Das Dienstspezifische Sicherheitskonzept fasst innerhalb des ersten Abschnitts allgemeine Informationen bzgl. des Dienstes zusammen. Dazu gehören die wichtigsten Ansprechpartner sowie die eingesetzte Hard- und Software. In Bezug auf informationssicherheitsrelevante

Themen werden in diesem Bereich auch die Abhängigkeiten zu anderen unterstützenden Diensten und die Kritikalität des Dienstes festgehalten. Letzteres gibt Aufschluss über die für ein ISMS relevanten Parameter wie dem Schutzbedarf oder den Nutzungsinformationen. Der zweite Abschnitt befasst sich mit den dienstspezifischen Risiken. Dazu gehört die Auflistung sämtlicher eingesetzten Sicherheitsmaßnahmen, die im Zusammenhang mit den Möglichkeiten des Zugriffs durch Administratoren und Benutzer eingeführt wurden. Der dritte Abschnitt beschreibt die Bereiche Datenschutze und Datensicherheit, also wie Systeme vor Ausfällen abgesichert sind und wie diese langfristig überwacht werden. Abschließend werden Verweise zu weiteren wichtigen Dokumenten aber auch zu Änderungen und Ergänzungen von Systemen benannt, die im Zusammenhang mit dem zu betrachteten Dienst stehen.

3.2.2 Dokumentationsprozess

Der Dokumentationsprozess definiert für die unterschiedlichen Arten von Dokumententypen unterschiedliche Verfahren. Eines dieser Verfahren ist die Allgemeine Dokumentationssteuerung. Die Allgemeine Dokumentationssteuerung des LRZ benennt drei unterschiedliche Rollen, die es bei der Erstellung eines Dokuments zu definieren gilt:

- Dokument-Eigentümer
- Dokument-Bearbeiter
- Dokument-Empfänger

Die Zuständigkeiten dieser Rollen werden anhand des RACI-Modells (Responsible, Accountable, Consulted, Informed; vgl. [Buc07]) festgelegt. Dokumentenentwürfe durchlaufen vor der Freigabe verschiedene Organisationsgruppen, die Ihren Input zur Verbesserung einbringen und die Entwicklung zukünftiger Revisionen unterstützen.

3.2.3 Rollen und Verantwortlichkeiten innerhalb des ISMS

Die Informationsweitergabe im Bereich der IT-Sicherheit ist am LRZ in zwei Kategorien unterteilt. Die passive Informationsverbreitung betrifft Dokumente, die innerhalb ihrer Ablagesysteme (Wiki, Intranet, etc.) zur Diskussion veröffentlicht werden. Die aktive Informationsverbreitung umfasst geplante Betriebssitzungen oder ungeplante LRZ-interne Treffen, in denen Informationen verbal bekannt gemacht und diskutiert werden.

Zur Ablaufebeschreibung der Informationsweitergabe ist es notwendig, die beteiligten Personengruppen zu definieren und mit den empohlenen Klassen des Implementierungsleitfadens für ISO/IEC 27001:2013 der ISACA [Inf16] zu vergleichen und zu differenzieren:

Top-Level-Management

Das Top-Level-Management umfasst die Mitglieder der Geschäftsleitung einer Organisation. Nach ISO/IEC 27001 [Int15a] ist im Zusammenhang mit einem ISMS deren Aufgabe sicherzustellen, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind. Darüber hinaus ist das Top-Level-Management dafür Verantwortlich, dass das ISMS in die Geschäftsprozesse der Organisation integriert wird und die dafür erforderlichen Ressourcen zur Verfügung gestellt werden.

Informationssicherheitsbeauftragter (ISB)/Chief Information Security Officer (CISO)

Nach Sowa [Sow17], verantwortet der Chief Information Security Officer (CISO) bzw. Informationssicherheitsbeauftragter (ISB) das Informationssicherheitsmanagement. Er ist maßgeblich für das Management aller sicherheitsrelevanten Komponenten des Informationssicherheitsmanagementsystems, sowie der zugehörigen Risiken und Schutzmaßnahmen verantwortlich. Weiterhin obliegt es ihm, Sicherheitsrichtlinien auszuarbeiten und deren Durchsetzung mit Hilfe interner Audits zu überprüfen. Der Implementierungsleitfaden der ISACA [Inf16] unterscheidet explizit zwischen dem Informationssicherheitsbeauftragten und dem IT-Leiter (Chief Information Officer).

Am LRZ bildet der LRZ-Informationssicherheitsbeauftragte eine wichtige Schnittstelle zwischen der Organisations- und Abteilungsleitung und leistet als Koordinator über sämtliche IT-Sicherheitsprozesse einen wichtigen Beitrag.

Risk- und Asset Owner

Die Risiko- und Informationswerteeigentümer (Risk Owner, Asset Owner) werden durch die ISO/IEC 27001 zwingend vorgeschrieben und individuell gehandhabt. Die Festlegung eines Asset Owner findet statt indem die Verantwortlichkeit eines Assets auf einer bestimmten Person oder Personengruppe zugeordnet wird. Der Zweck dieser Rolle besteht darin, einen definierte Verantwortlichkeit für schützenswerte Informationswerte zu erhalten. Der Risk Owner ist hingegen für ein oder mehrere Risiken zuständig. Seine Tätigkeit umfasst die Steuerung des Risikomanagementprozesses des Einzelrisikos durch Anstoß von Risikobehandlungsprozessen.

Die Zuteilung von Verantwortlichkeiten von Risiken und Informationswerten findet meist in Form der RACI- [RR09] oder SoD-Matrix statt, wodurch eine klare Trennung zwischen Umsetzungsverantwortlichkeit, Rechenschaftspflichtigkeit und den unterstützend/beratenden Rollen hergestellt wird.

Das LRZ hat sich hierbei entschieden, das RACI-Modell [Buc07] organisationsweit anzuwenden. Die Verantwortlichkeit für Informationswerte wird durch die Dienstverantwortlichen Beteiligten übernommen. Die Risikoverantwortlichkeit wird durch Beteiligte des übergeordneten Managementsystems verantwortet.

Datenschutzbeauftragter (DSB)

Nach Kersten et. al. [KRS13] sind Datenschutzbeauftragte im ISMS lediglich beim Umgang mit personenbezogenen Daten hinzuzuziehen. Dies umfasst nicht nur die Prüfung von Voraussetzungen bei der Zurverfügungstellung von Diensten, die personenbezogene Daten verarbeiten sondern auch bei Sicherheitsvorfällen, bei denen die Gefahr einer Verletzung von Schutzzielen personenbezogener Daten besteht.

Zu beachten sei weiter, dass weder der Datenschutz noch die Einrichtung und Zertifizierung eines ISMS eine Aussagekraft über die Qualität der zugrunde liegenden Dienste besitzen. Im Gegenteil reguliert der Gesetzgeber durch das BDSG eingesetzte Verfahren zur automatisierten Verarbeitung personenbezogener Daten. Innerhalb Deutschlands und der Europäischen

Union werden viele dieser nationalen Gesetze durch die Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft ist, auch länderübergreifend wirksam.

Das LRZ hat zur Herstellung einer Konformität mit der aktuellen Gesetzgebung einen dedizierten Datenschutzbeauftragten ernannt, der die Einhaltung der aktuellen Gesetzeslage überwacht.

Systemadministratoren

IT-Administratoren sind innerbetriebliche Spezialisten, die meist mehrere IT-Dienste verantworten. Sie haben meist fundiertes Wissen über die Funktionsweise der ihnen zugewiesenen Systeme und können im Rahmen ihrer Befugnisse mögliche Angriffsvektoren vorhersehen und präventive Schutzmaßnahmen einleiten. Für das IT-Management ist eine solche Einschätzung dringend notwendig, da sie maßgeblich bei der Risikoanalyse (Risikoidentifikation und -Abschätzung) mit einwirkt.

Innerhalb des LRZ sind Administratoren technischen Fachbereichen zugeordnet. Im Bereich der IT-Sicherheit ist der sog. LRZ-Arbeitskreis Security (AKSecurity) zuständig, der bei der Umsetzung und Durchführung der Informationssicherheitsprozesse beteiligt ist.

Auditor

Auditoren führen innerhalb eines systematischen, unabhängigen und dokumentierten Prozesses Audits durch, um nachzuweisen und objektiv auszuwerten, inwieweit Auditkriterien erfüllt sind [Gmb16].

Solche Audits können wahlweise im Rahmen eines internen Audits oder als externes Audit durchgeführt werden. Bei internen Audits wird das Audit unter direkter Verantwortung des Unternehmens und innerhalb seiner eigenen, definierten Grenzen und Infrastruktur durchgeführt [Gmb16]. Ein externes Audit verantworten Organisationen wie Zertifizierungsstellen oder Beratungsfirmen [Gmb16].

Kunden

Bei Kunden handelt es sich in der Regel um Vertragspartner mit beispielsweise weiteren Organisationen oder individuelle Personen, die am ISMS beteiligt sind. Die ISO/IEC 27001 schreibt keine explizite Beteiligung von Kunden an Informationssicherheitsprozessen vor. Lediglich zu Versorgungsdienstleistern, die unternehmenseigene Prozesse unterstützen, sind entsprechende Maßnahmen (siehe [Int15a] Anhang A A.15) definiert. Im Sinne der Transparenz und dem Anspruch eines nachweisbaren Qualitätsstandards, sind die Kunden eine dennoch eine wichtige und zu beachtende Perspektive. Durch eine gefilterte Weitergabe von beispielsweise umgesetzter Schutzmaßnahmen für relevante Informationswerte kann das Vertrauen des Kunden in Bezug auf den Service Dienstleister gesteigert werden.

3.3 Zusammenfassung

In Kapitel 3 wird der Dienstleistungskatalog des LRZ beschrieben, um das Tätigkeitsfeld und die Komplexität der eingesetzten Systeme im ISMS zu verdeutlichen. Außerdem wird durch die Komplexität der eingesetzten Systeme und der Menge an zu verarbeitenden Daten die Notwendigkeit eines strukturierten Dokumentenmanagements deutlich.

Abschnitt 3.2 beschreibt die Art und Weise, wie das Dokumentenmanagement im Bereich der Informationssicherheit zum Verfassungszeitpunkt aufgebaut ist. Zwar bieten die bereits etablierten Dokumentationen wie das dienstspezifische Sicherheitskonzept eine grundsätzliche Dokumentation angebotener Dienstleistungen, jedoch mangelt es noch an Einheitlichkeit und Strukturiertheit in Bezug auf die Anforderungen der ISO/IEC 27001.

Im nächsten Kapitel wird auf Basis der bearbeiteten Informationen aus dem Grundlagenteil und den vorherrschenden Bedingungen des LRZ eine Anforderungsanalyse erstellt, die die Grundlage des zu erarbeitenden modifizierten Informationsmodells bildet.

4 Anforderungsanalyse

Der Konzeption eines geeigneten Informations- und Datenmodells zur Strukturierung und Verknüpfung von Inhalten einer ISMS-Dokumentation geht einer Anforderungsanalyse zur Feststellung der aktuellen Dokumentationsstruktur inklusive ihres Zusammenhangs mit der Norm und ihrer Schnittstellen zu anderen teilhabenden Managementsystemen voraus.

Um eine realistische Aussage über die Anwendbarkeit und Anforderungen einer ISMS-Dokumentation am LRZ zu treffen, basiert die Anforderungsanalyse auf den Status-Quo der Dokumentationsverwaltung, wie sie in Abschnitt 3.2 beschrieben wurde. Die Anforderungsanalyse wird in Form der von Grande [Gra14] beschriebenen Standardanforderungsanalyse durchgeführt.

Das Resultat der Anforderungsanalyse ist ein Kriterienkatalog, der dafür verwendet werden soll, die zu untersuchenden Dokumentationstools voneinander abzugrenzen und Kriterien für die Implementierung einer ISMS-Dokumentation zu definieren.

4.1 Vergleichbare Untersuchungen

Vor der Durchführung einer Anforderungsidentifikation ist es notwendig, bereits durchgeführte Studien, die den Vergleich von Dokumentationstools im Bereich des Informationssicherheitsmanagements durchgeführt haben, zu recherchieren und auszuwerten, um bereits vorab relevante Kriterien für den Vergleich zu erhalten.

Die Computer Sciences Corporation (CSC) hat beispielsweise im September 2015 die Studie *GSTOOL QUO VADIS? - Evaluation von Information Security Management System Tools als Grundschutz Tool Alternativen* [csc15] veröffentlicht, die neun Dokumentationstools untereinander verglichen hat. Die CSC unterstützt seit über 50 Jahren mit derzeit über 70.000 Mitarbeitern Kunden im privaten und öffentlichen Sektor. Das Ziel der Studie des CSC bestand darin, Alternativen, die als Ersatz für das eingestellte Grundschutztool (GSTOOL) des BSI in Frage kommen würden, zu vergleichen und zu prüfen.

4.1.1 Untersuchte Kriterien

Systemvoraussetzungen

QV1 Hardware-Anforderungen Server
QV2 Hardware-Anforderungen Client
QV3 Unterstützte Datenbanken
QV4 Unterstützte Betriebssysteme Server
QV5 Unterstützte Betriebssysteme Client

IT-Grundschutz

QV6 Konnektoren zu GSTOOL
QV7 Dokumentation Basissicherheitscheck möglich
QV8 Optionale Erstellung eigener Bausteine, Maßnahmen, Gefährdungen
QV9 Vorkonfigurierte Importfunktion für Grundschutzkataloge des BSI
QV10 IT-Grundschutz-Kataloge hinterlegen

ISMS-Managementprozesse

QV11 Self-Assessments
QV12 Integation anderer Tools
QV13 IT-Security Management Prozesse
QV14 Versionierung
QV15 Dokumentenmanagement

Benutzbarkeit (Usability)

QV16 Mobile Apps als Client Anwendung
QV17 Modellierung und Verwaltung von komplexen IT-Verbünden
QV18 Mehrsprachigkeit
QV19 Offlinefähigkeit
QV20 Nutzer-/Berechtigungsverwaltung
QV21 Netzwerkfähigkeit
QV22 Mehrbenutzerfähigkeit
QV23 Mandantenfähigkeit

Risikoanalyse

QV24 Ergänzende Maßnahmen
QV25 Unterstützung von Klassischen Bedrohungs- und Risikoanalysen
QV26 Manuelles Anpassen des vererbten Schutzbedarfs
QV27 Vererbungsmechanismen für Schutzbedarf von IT-Objekten
QV28 Konfigurierbare Schutzbedarfsmatrix

ISO 27001

QV29 Unterstützung von ISO 27001:2013 Native
QV30 Switch zwischen IT-Grundschutz und ISO27001

Reporting

QV31 MS Office Kompatible Import-/Exportfunktion
QV32 Darstellung des Implementierungsstatus Maßnahmen/Controls
QV33 Konfigurierbare Reports
QV34 Reportingfunktion

4.1.2 Ergebnisse

Im Ergebnis der Studie werden die Stärken der individuellen Dokumentationstools in den Vordergrund gestellt. Abbildung 4.1 zeigt eine grafische Repräsentation der Ergebnisse, die innerhalb der Studie [csc15] folgendermaßen zusammengefasst wird:

In der Bewertungskategorie Risikoanalysen haben alle Tools die von unseren Experten als Best Case definierte Höchstbewertung erreicht. Beim IT-Grundschutz als Bewertungspunkt sind geringfügige Unterschiede zu erkennen. In den Bewertungskategorien ISMS Managementprozesse, Reporting, Benutzbarkeit, Systemvoraussetzungen und ISO 27001 hingegen sind die Unterschiede zwischen den ISMS-Tools teilweise größer. Opus-i hat u.a. mit seinen niedrigen Hardwareanforderungen die bestmögliche Bewertung in der Kategorie Systemvoraussetzungen erreicht, wohingegen DHC vergleichsweise hohe Anforderungen an die Hardware stellt.

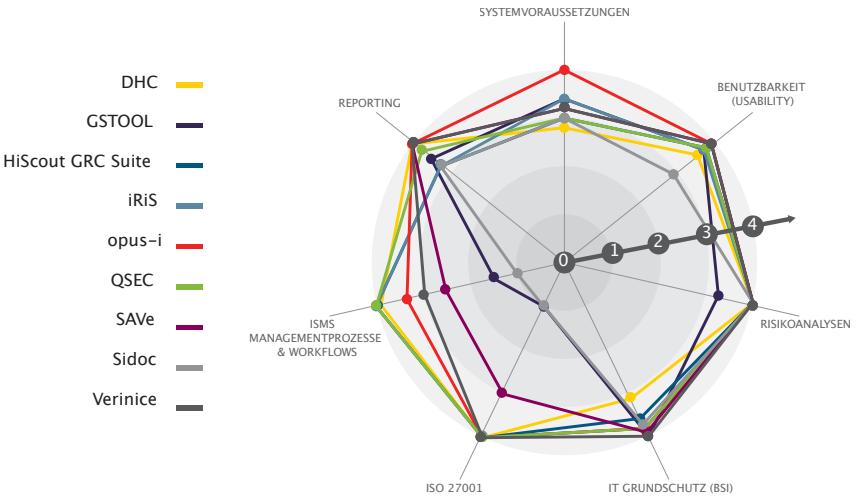


ABBILDUNG 1: ZUSAMMENFASSUNG DER STUDIENERGEBNISSE
Die Detailergebnisse pro Kategorie werden in den folgenden Abschnitten erläutert.

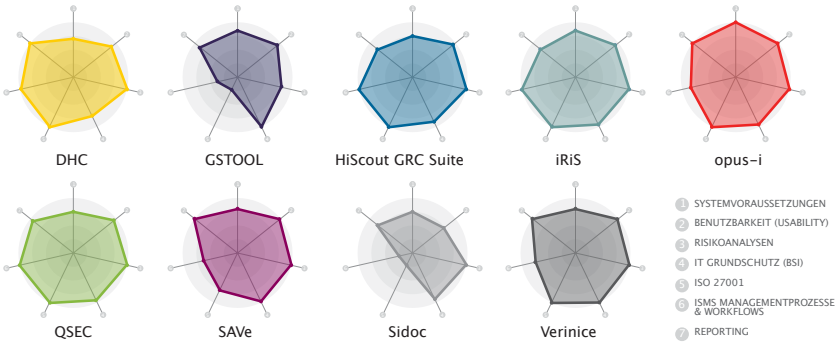


Abbildung 4.1: GSTOOL QUO VADIS? - Ergebnisse [csc15]

4.2 Anforderungsidentifikation

Die Anforderungsidentifikation umfasst eine breit gefächerte Zusammenstellung der Anforderungen, welche aus dem zugrunde liegenden Standard, Interviews mit am Managementprozess beteiligten Personen, den recherchierten vergleichbaren Analysen sowie der Zielsetzung dieser Arbeit gebildet werden.

Sie dient dem Zweck, ein möglichst breites und ungefiltertes Spektrum an zu berücksichtigenden Kriterien zu erfassen. Sämtliche Anforderungen werden bereits vorab in Nichtfunktionale Anforderung (NF) und Funktionale Anforderung (F) unterteilt. Grande [Gra14] definiert Funktionale Anforderungen als Kriterien, die die Funktionalität und das Verhalten des Produkts widerspiegeln - also eine Festlegung, welche Funktionalitäten ein Tool bieten muss. Weiterhin beschreibt er Nicht-funktionale Anforderungen als Qualitätsanforderungen, die sich aus Randbedingungen ergeben. Hierzu passen üblicherweise Kriterien, die die Benutzbarkeit oder Effizienz beeinflussen.

4.2.1 Anforderungen aus der ISO/IEC 27000

Nachstehend finden sich die Anforderungen, die der ISO/IEC 27000 Normenreihe [Int15a] entnommen wurden. Wie in Abschnitt 2.2.1 beschrieben, gibt lediglich die ISO/IEC 27001 inkl. des Anhangs A normative Anforderungen an ein ISMS vor, weshalb auch nur diese als verpflichtend anzusehen sind. Ergänzend dazu, wurden neben der verpflichtenden Anforderungen einige Anforderungen aus den informativen Teilen des Standards ebenfalls berücksichtigt, da diese in Bezug auf die Dokumentation eines ISMS eine sinnvolle Erweiterung darstellen.

Funktionale Anforderungen

F1 Dokumentation des Anwendungsbereichs/Scope des Unternehmens (ISO/IEC 27001 4.3)
F2 Dokumentation der Informationssicherheitspolitik (ISO/IEC 27001 5.2)
F3 Zuweisung von Zuständigkeiten und Bekanntmachung von Rollenzuweisungen/Benutzerverwaltung (ISO/IEC 27001 5.3)
F4 Berichterstellung über die Leistung des ISMS (ISO/IEC 27001 5.3, 9.1)
F5 Dokumentation von Risiken und Chancen sowie Maßnahmen (ISO/IEC 27001 6.1.1)
F6 Klassifizierung von Werten bzgl. Kritikalität und Empfindlichkeit (ISO/IEC 27001 Anhang A 8.2)
F7 Speicherung von IT-Assets (Unterteilung in primary und supporting assets) (ISO/IEC 27002 8.1.2, ISO/IEC 27005)
F8 Dokumentation von Risiko-Assessments zur Festlegung von Bedrohungen und Schwachstellen (ISO/IEC 27005 Annex E.1)
F9 Dokumentation von Risiko-Wahrscheinlichkeiten und Risiko-Auswirkungen (ISO/IEC 27001 6.1.2d)
F10 Dokumentation der Kriterien zur Beurteilung von Risiken sowie der Risikoidentifikation, -analyse und -bewertung (ISO/IEC 27001 6.1.2a)
F11 Dokumentation eines SoA (ISO/IEC 27001 6.1.3)
F12 Dokumentation des Informationssicherheitsziels (ISO/IEC 27001 6.2)

F13 Dokumentenlenkung (ISO/IEC 27001 7.5)
F14 Dokumentation von Audits und Managementbewertungen (ISO/IEC 27001 9.2, 9.3)
F15 Unterstützung eines kontinuierlichen Verbesserungsprozesses (ISO/IEC 27001 4.4)

4.2.2 Ergänzende Anforderungen beteiligter Interessengruppen

Die Anforderungen der beteiligten Interessengruppen (vgl. 3.2.3) lassen sich überwiegend aus den Anforderungen der Norm ableiten, umfassen teilweise aber auch qualitative Kriterien, die sich auf das Ansprechverhalten des jeweiligen Tools beziehen.

Funktionale Anforderungen:

F17 Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen
F18 Modellierung und Verwaltung komplexer IT-Verbünde
F19 Konzeption der Struktur anhand vorhandener Inhalte

Nicht-funktionale Anforderungen:

NF1 Performanz
NF2 Verlässlichkeit
NF3 Usability

4.2.3 Beschreibung der Kernanforderungen

Nachstehend werden die Kernanforderungen den in Abschnitt 3.2.3 definierten Rollen zugeordnet und beschrieben. Die Zuordnung zwischen den jeweiligen Interessengruppen und den gewählten Kernanforderungen findet anhand der sinngemäßen Zuordnung zwischen den Anforderungen der Norm und den beteiligten Interessengruppen statt.

Stakeholder 1: Informationssicherheitsbeauftragter (ISB)/Chief Information Security Officer (CISO)

F5-F11 Maßnahmen, Risiken und Assets dokumentieren

Neben der Herstellung einer Nachweisbarkeit bestehen aufgrund der thematischen Schnittmengen unterschiedlicher Normen wie der ISO/IEC 27001 und ISO/IEC 20000, die Möglichkeit eine allumfassende Dokumentation mit entsprechenden Relationen zu konzeptionieren. Durch eine intelligente Verknüpfung von Inhalten soll es zudem möglich sein, je nach Zugriffsberechtigung einen Austausch von Informationen zwischen unterschiedlichen Parteien zu ermöglichen. Durch die Bereitstellung vieler unterschiedlicher Dienstleistungen durch das LRZ ist die Herstellung einer Übersicht sämtlicher für die IT-Sicherheit relevanten Informationswerte und der dazugehörigen Risiken und Schutzmaßnahmen nur schwer zu gewährleisten. Die Dokumentationsstruktur sollte daher in der Lage sein, Auskunft darüber zu geben, welche Schutzmaßnahmen bereits umgesetzt wurden und welche es noch umzusetzen gilt. Im Rahmen der Norm wird eine Umsetzung des aus dem Abschnitt 2.2.5 genannte SoA zwingend erforderlich und wird daher als funktionale Anforderung F11 aufgeführt.

Unterstützt werden diese funktionalen Anforderungen durch die informativen Teile der ISO-/IEC 27000. ISO/IEC 27002 und ISO/IEC 27005 gehen näher auf die zu dokumentierenden Informationswerte ein und unterteilen diese wie in Abschnitt 2.2.5 beschrieben. Darüber hinaus wird der Risikomanagementprozess erläutert, wodurch sich die Anforderungen F9 und F10 ergeben.

F13 Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen, Performanz und Verlässlichkeit

Das finale Dokumentationstool und das zugehörige Konzept müssen sich in den Arbeitsablauf der verantwortlichen Personen möglichst nahtlos einfügen lassen. Dabei geht es darum, ein möglichst zuverlässiges System zu wählen, dessen Datensätze auch bei einem Versagen der Software gesichert werden oder sich möglicherweise in einem anderen Format exportieren lassen können. Weiterhin sollte das Dokumentationstool in der Lage sein, mit einer steigenden Anzahl an Informationswerten gut zu skalieren. Dazu zählen beispielsweise Reaktions- und Abfragezeiten aber auch die Verknüpfung von Inhalten aus anderen Bereichen. Weiterhin sollte das System möglichst zukunftssicher und plattformunabhängig (Linux, Windows, MacOS, iOS, Android) sein.

F18 Modellierung und Verwaltung komplexer IT-Verbünde

Aufgrund der thematischen Schnittmengen unterschiedlicher Normen wie der ISO/IEC 27001 und ISO/IEC 20000, besteht die Möglichkeit, eine allumfassende Dokumentation mit entsprechenden Relationen zu konzeptionieren. Durch eine intelligente Verknüpfung von Inhalten soll es zudem möglich sein, je nach Zugriffsberechtigung, einen Austausch von Informationen zwischen unterschiedlichen Parteien zu ermöglichen. Die Dokumentation im Bereich der IT-Sicherheit soll im direkten Bezug auf die durch die Norm vorgegebenen Begrifflichkeiten und Terminologien aufbauen. Darüber hinaus sollen nicht nur einzelne Dienste erfasst werden können, sondern die gesamte IT-Sicherheit der Organisation strukturiert dokumentiert werden können. Dazu zählt ebenfalls das Aufgreifen bereits fest integrierter organisationseigener Vorgehensweisen und Bezeichnungen. Die Unterstützung individueller Workflows durch Nutzung von bereits etablierter Software soll zur stetigen Aktualität der Dokumentation beitragen.

F19 Konzeption der Struktur anhand vorhandener Inhalte

Die Dokumentation sollte mit Blick auf Auditprüfungen konzipiert werden. Ein Auditor interessiert sich besonders für eine Übersicht aller relevanten Informationen bzgl. der IT-Informationssicherheit und deren etablierte Schutzmaßnahmen. Unter Umständen bietet sich hier auch ein visueller Überblick in Form von Graphen an, in der die Anzahl und Arten der bereits umgesetzten Sicherheitsmaßnahmen den noch umzusetzenden Sicherheitsmaßnahmen gegenübergestellt werden. Wichtig ist dabei stets die Verknüpfung zwischen bereits umgesetzter Schutzmaßnahmen und der Mindestanforderungen aus der Norm beizubehalten.

F10, F4 Dokumentenlenkung und Berichterstellung

Dokumente müssen eindeutig identifizierbar sein. Dies dient nicht nur dazu, Verantwort-

lichkeiten zu identifizieren, sondern auch eine Unterscheidung zwischen bereits veralteten Revisionen und der aktuellen Version treffen zu können und damit Änderungen nachvollziehen zu können. Im Rahmen der Dokumentenlenkung sollte darüber hinaus eine Möglichkeit zur Berichterstellung existieren (F4) um kontrollierbare und nachweisbare Ergebnisse der Unternehmensprozesse zu erhalten und den kontinuierlichen Verbesserungsprozess (F15) zu fördern.

F1-F3 Anwendungsbereich, Verantwortlichkeiten und Ziele

ISO/IEC 27001 gibt vor, dass der Anwendungsbereich des zu verwaltenden ISMS wie in Abschnitt 2.2.6 beschrieben, festzulegen ist. Weiterhin müssen Verantwortlichkeiten festgelegt werden.

Stakeholder 2: Systemadministratoren

F17 Nutzung visueller Gestaltungsmöglichkeiten und Unterstützung des Workflows

Systemadministratoren sind für die systemnahe Konfiguration von Servicebausteinen verantwortlich und müssen daher bei der Durchführung von Tätigkeiten stets die Dokumentation ihrer zu verwaltenden Systeme pflegen. Nur Sie sind in der Lage konkrete Schwachstellen und Risiken ihrer eingesetzten Soft- und Hardware sowie Infrastruktur zu benennen. Diese müssen jedoch in den Kontext des Informationssicherheitsmanagements auch entsprechend strukturiert werden, weshalb die Dokumentation eine unterstützende Rolle einnehmen soll.

Stakeholder 3: Top-Level-Management

Effizienz und Kosten

Neben den aufgeführten funktionalen und nicht-funktionalen Anforderungen priorisiert das Top-Management vor allem Effizienz und Kosten. Die Einführung neuer Tools, besonders im organisationsübergreifenden Rahmen, ist sowohl mit Anschaffungskosten und Lizenzkosten, Schulungskosten für Weiterbildung der Nutzer sowie kontinuierlichen Produktivkosten verbunden.

Stakeholder 4: Kunden

F1 Benutzerverwaltung mit Zugriffssteuerung

Die Dokumentation der IT-Informationssicherheit soll unterschiedliche Perspektiven abbilden können, um entsprechend der zu betrachtenden Zielgruppe, relevante Inhalte darstellen zu können. So kann eine Auskunft über die Wirksamkeit der Schutzmaßnahmen erbracht werden, ohne diese durch unbeabsichtigte Freigabe sensibler Informationen zu kompromittieren.

Stakeholder 5: Auditoren

siehe F5-F11 Maßnahmen, Risiken und Assets dokumentieren

4.3 Anforderungsspezifikation

Die Anforderungsspezifikation dient dem Zweck, die gesammelten Anforderungen aus der Anforderungsidentifikation zu strukturieren. Dazu werden die Anforderungen in definierten Klassen aufgeteilt. Folgende Klassen werden hierbei betrachtet:

- Obligatorisch/Optional
- Gewichtung
- Relevanz

4.3.1 Definition der Relevanz

Die Kriterien, die aus der Anforderungsidentifikation entstanden sind, stammen von unterschiedlichen Stakeholdern, deren Anforderungen in Bezug auf die Untersuchung von Kriterien unterschiedlich berücksichtigt und gewichtet werden müssen. Dies führt dazu, dass die Basis der hieraus resultierende Arbeit besonders die Meinung der Entscheidungsträger berücksichtigt. Dies bedeutet nicht, dass bestimmte Anforderungen nicht auch zu einem späteren Zeitpunkt dennoch umgesetzt werden könnten. Bei der Relevanz der betrachteten Stakeholder hat man sich auf eine Gewichtung geeinigt, wie sie in Tabelle 4.1 zu finden ist.

Stakeholder	**Gewichtung**	**Quantitativer Wert**
Top-Level-Management (3.2.3)	Ausschlaggebend	4
ISB & CISO (3.2.3)	Hoch	3
Auditoren (3.2.3)	Hoch	3
Systemadministration (3.2.3)	Mittel	2
Kunden (3.2.3)	Gering	1

Tabelle 4.1: Relevanzanalyse

Es sei anzumerken, dass es zwischen der Zuordnung von Kriterien und Stakeholdern zu Überschneidungen der Interessen kommen kann. In diesem Fall sollte jeweils die Interessengruppe mit der höchsten Gewichtung priorisiert werden.

4.3.2 Kriterien-Bewertungsskala

Um die Kriterien untereinander auch unabhängig von der Gewichtung aus der Relevanzanalyse bewerten zu können, ist die Einführung einer weiteren Kennzahl notwendig. Bestimmte Funktionen sind beispielsweise wichtiger bzw. tragen einen höheren Stellenwert als andere Funktionen.

Bewertungsbeschreibung	**Quantitativer Wert**
Zwingend Erforderlich	3
Nice to have	2
Unbedeutend	1

Tabelle 4.2: Kriterien-Bewertungsskala

Gemeinsam mit der Kennzahl aus der Relevanzanalyse ergibt sich so ein Produkt x

$$x = a * b$$

bei dem abhängig von der der Gewichtung einer zugehörigen Interessengruppe a und der Signifikanz eines individuellen Kriteriums b, die Notwendigkeit einer Funktion bewertet werden kann.

4.3.3 Signifikanzbewertung

Für die Bewertung der Signifikanz x wird folgender Schlüssel angewendet:

- $x < 6$: Funktion besitzt geringe Priorität und muss nicht vorhanden sein.
- $x > 6 \wedge x \leq 9$: Funktion sollte vorhanden sein.
- $x > 9$: Funktion muss zwingend vorhanden sein oder implementiert werden

Die Anwendung des Schlüssels findet sich in dem nachstehenden finale Kriterienkatalog (vgl. Tabelle 4.3) wieder. Neben den bereits in der Anforderungsspezifikation definierten Klassifizierung wurde noch eine weitere Kategorisierung der Kriterien zur Abgrenzung der Themenbereiche durchgeführt.

4.3.4 Finaler Kriterienkatalog

Der finale Kriterienkatalog stellt eine Auflistung sämtlicher zu betrachtenden Kriterien dar, an derer die Qualität von Dokumentationstools gemessen wird. Darüber hinaus sind alle Kriterien mit Gewichtungen sowohl in Bezug auf Wichtigkeit aber auch auf die relevante Interessengruppe angegeben, wodurch sich für jedes Kriterium eine individuelle Signifikanz bildet. Die Zuweisung der Interessengruppen wurden aggregiert zu dem jeweils höchsten Wert.

4.4 Zusammenfassung

In diesem Kapitel wurde aus den Erkenntnissen der vorhergehenden Kapitel und der direkten Evaluierung von Anforderungen aus der Norm sowie weiteren Inputs aus bereits durchgeführten Studien von Dokumentationstools einen Kriterienkatalog gebildet. Weiterhin wurden die Kriterien sinnvoll aggregiert und den beteiligten Rollen am Managementprozess zugeordnet und entsprechend erläutert. Die Kernkriterien zur Dokumentation eines ISMS stellen hierbei die Dokumentation von Informationswerten, Risiken und Schutzmaßnahmen/Controls dar. Entsprechend der Wichtigkeit von Kriterien als auch der Nutzergruppe, der das Kriterium zuzuweisen ist, wurde eine Gewichtung eingeführt, um die Kriterien voneinander abgrenzen zu können.

Der finale Kriterienkatalog bildet die Grundlage für die Messung der Tauglichkeit und Differenzierung bezüglich unterschiedlicher Funktionsumfänge für die untersuchten Dokumentationstools innerhalb des nächsten Kapitels.

ID	Anforderung	a	b	x
Systemkompatibilität				
QV4	Client/Server Infrastruktur	3	3	9
QV5	Desktop-Client (nativ)	2	2	6
QV16	Mobile Apps	2	2	6
QV3	Unterstützung für Datenbanksysteme	2	2	6
Risikomanagement-Funktionalitäten				
QV28	Schutzbedarfsmatrix	3	3	9
QV26	Vererbungsmechanismen für Schutzbedarf	3	2	6
QV24	Ergänzende Maßnahmen	3	3	9
QV25	Unterstützung klassischer Bedrohungs- und Risikoanalysen	3	3	9
User Experience und Benutzerfreundlichkeit				
F3	Zuweisung von Zuständigkeiten und Bekanntmachung von Rollenzuweisungen/Benutzerverwaltung (ISO/IEC 27001 5.3)	3	3	9
F13	Dokumentenlenkung (ISO/IEC 27001 7.5)	3	3	9
F15	Unterstützung eines kontinuierlichen Verbesserungsprozesses (ISO/IEC 27001 4.4)	4	3	12
F17	Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen	3	2	6
NF1	Performanz	3	3	9
F18	Modellierung und Verwaltung komplexer IT-Verbünde	3	3	9
F19	Konzeption der Struktur anhand vorhandener Inhalte	3	3	9
NF2	Verlässlichkeit	3	3	9
QV23	Unterstützung mehrerer Anwendungsbereiche/Scopes	3	1	3
QV21	Netzwerkfähigkeit	3	3	9
QV18	Unterstützung mehrerer Sprachen	3	2	6
IT-Grundschutz und ISO27001 Funktionalitäten				
F1	Dokumentation des Anwendungsbereichs/Scope des Unternehmens (ISO/IEC 27001 4.3)	4	3	12
F2	Dokumentation der Informationssicherheitspolitik (ISO/IEC 27001 5.2)	4	3	12
F4	Berichterstellung über die Leistung des ISMS (ISO/IEC 27001 5.3, 9.1)	4	3	12
F5	Dokumentation von Risiken und Chancen sowie Maßnahmen (ISO/IEC 27001 6.1.1)	4	3	12
F6	Klassifizierung von Werten bzgl. Kritikalität und Empfindlichkeit (ISO/IEC 27002 8.2)	4	3	12
F7	Speicherung von IT-Assets (Unterteilung in primary und supporting assets) (ISO/IEC 27002 8.1.2, ISO/IEC 27005)	3	3	9
F8	Dokumentation von Risiko-Assessments zur Festlegung von Bedrohungen und Schwachstellen (ISO/IEC 27005 Annex E.1)	3	3	9
F9	Dokumentation von Risiko-Wahrscheinlichkeiten und Risiko-Auswirkungen (ISO/IEC 27005 Annex E.1)	3	3	9
F10	Dokumentation der Kriterien zur Beurteilung von Risiken sowie der Risikoidentifikation, -analyse und -bewertung (ISO/IEC 27001 6.1.2)	3	3	9
F11	Dokumentation eines SoA (ISO/IEC 27001 6.1.3)	3	3	9
F12	Dokumentation des Informationssicherheitsziels (ISO/IEC 27001 6.2)	4	3	12
F14	Dokumentation von Audits und Managementbewertungen (ISO/IEC 27001 9.2, 9.3)	3	3	9
QV6	Import/Export GSTOOL	3	1	3
QV9	Importfunktion für IT-Grundschutzkatalog und Referenzierung	3	1	3
QV11	Vorgefertigte Self-Assessments	3	1	3
QV29	Importfunktion für ISO-Normentexte	3	2	6
Reporting				
QV31	Microsoft Office Kompatibilität	3	3	9
QV32	Visuelle Darstellung von Status- und Umsetzungsständen	3	2	6
QV33	Konfiguration/Filtermöglichkeiten der Reportingausgabe	3	2	6

Tabelle 4.3: Finaler Kriterienkatalog

5 Evaluierung potentieller Dokumentationstools

In diesem Abschnitt geht es darum, bereits etablierte Dokumentationstools im Bereich des ISO/IEC 27001 und des IT-Grunschutzes auf Ihren Funktionsumfang zu untersuchen. Bei der Analyse stehen die aus der Anforderungsanalyse identifizierten Kriterien im Vordergrund. Neben diesen Kriterien gilt es aber auch allgemeine Qualitätsfaktoren zu betrachten. Dazu gehören beispielsweise Fragestellungen darüber, ob die jeweilige Software auch regelmäßig weiterentwickelt wird, auf welcher Codebasis die Software aufgebaut ist und in welcher Art und Weise die dort hinterlegten Informationen persistent gesichert werden.

Gerade im Bereich der ISMS-Dokumentationstools musste bereits Ende des Jahres 2014 die Entwicklung des weit verbreiteten GSTOOL's, welches 1998 erschienen ist und durch den BSI entwickelt wurde, aufgrund der mangelnden Wirtschaftlichkeit [Rei16] eingestellt werden. Somit waren viele der Kunden gezwungen, über Migrationswerkzeuge zu einer anderen Softwarelösung zu wechseln. Auch das Design und die User Experience (UX) stellen wichtige Qualitätsmerkmale dar, die im Rahmen der derzeitigen Nutzung unterschiedlichster Endgeräte und Betriebssysteme berücksichtigt werden müssen.

5.1 Bewertungsschlüssel

Unabhängig von den festgelegten Kriterien innerhalb der Anforderungsanalyse, gilt es, die Umsetzung bzw. Erfüllung eines Kriteriums pro Anwendung quantitativ zu bewerten, um abschließend einen aussagekräftigen Vergleich präsentieren zu können. Die Bewertung findet wie folgt statt:

- Anforderung ist erfüllt = 2
- Anforderung ist teilweise erfüllt = 1
- Anforderung ist nicht erfüllt = 0

5.2 Dokumentationstools im Bereich IT-Grundschutz und ISO27001

5.2.1 verinice.

Allgemeine Informationen

Verinice. stellt ein Dokumenationstool sowohl im Bereich der ISO/IEC 27000 als auch im Bereich des IT-Grundschutzes nach dem BSI-Grundschutzkatalog dar. Das Tool wurde vom

Unternehmen SerNet Service Network GmbH mit Sitz in Göttingen mit dem Ziel der Bereitstellung eines vom BSI-lizenzierten OpenSource-Werkzeugs zur Dokumentation der IT-Informationssicherheit im Unternehmensbereich entwickelt.

Die nachfolgende Übersicht bezieht sich auf die Version 1.13 vom 27.10.2016.

Systemkompatibilität

Das Dokumentationstool baut auf Basis der Eclipse Rich Client Platform (RCP) auf und erschien im September 2009 in der Version 1.0. Durch die Nutzung der gut dokumentierten Eclipse RCP auf Basis der Programmiersprache Java ist es möglich, die Anwendung plattformunabhängig auf sämtlichen gängigen Betriebssystemen anzubieten, da die Anwendung selbst innerhalb der JVM (Java Virtual Machine) ausgeführt wird.

Als Alternative zur Java Standalone Applikation stellt SerNet als Nutzerschnittstelle zusätzlich ein Webfrontend für verinice.PRO-Kunden zur Verfügung, dass jedoch erst mit der neuen, noch in Entwicklung stehenden Version 1.14 implementiert werden soll. Das Webfrontend ermöglicht, dass die Daten auch von mobilen Endgeräten aus, bearbeitet werden können.

ID	Anforderung	verinice.	Bewertung
Systemkompatibilität			
QV4	Client/Server Infrastruktur	ja	2
QV5	Desktop-Client (nativ)	Linux (ja) MacOS (ja) Windows (ja)	2
QV16	Mobile Apps	nativ (nein) webapp (ja)	1
QV3	Datenbanksysteme Unterstützung	teilweise	1

Lizenzierungsmodelle

Trotz der Tatsache, dass *Verinice.* als OpenSource-Tool zur Verfügung gestellt wurde, sind einige Features lediglich gegen Aufpreis nutzbar. Bei den Softwarepaketen existieren drei unterschiedliche Varianten.

Der Client existiert in zwei unterschiedlichen Ausführungen. Die Evaluierungsversion beinhaltet bis auf die Reporting-Funktion sämtliche Funktionen der Standardvariante und ist nicht mit zusätzlichen Kosten verbunden. Im Rahmen der Nachweisbarkeit und Herstellung wiederholbarer Ergebnisse, sind Berichte über die Umsetzung von Sicherheitsmaßnahmen und dazugehöriger Bedrohungen beispielsweise im PDF- oder Excel-Format unerlässlich. Diese Funktion bleibt der Standardversion vorbehalten, die zum Zeitpunkt der Ausarbeitung ca. 250 EUR kostet.

Da es sich bei der Standardversion des Clients um eine Einzelplatzlizenz handelt, werden sämtliche Daten innerhalb einer lokalen Datenbank festgehalten. Um von mehreren Arbeitsplätzen auf einen Datenpool zugreifen zu können, bietet SerNet mit dem *Verinice.*Pro Paket eine serverseitige Lösung an, die zum einen eine zentrale Datenablage bereitstellt aber auch zusätzliche Serverfeatures wie die Integration einer LDAP-Nutzerverwaltung oder

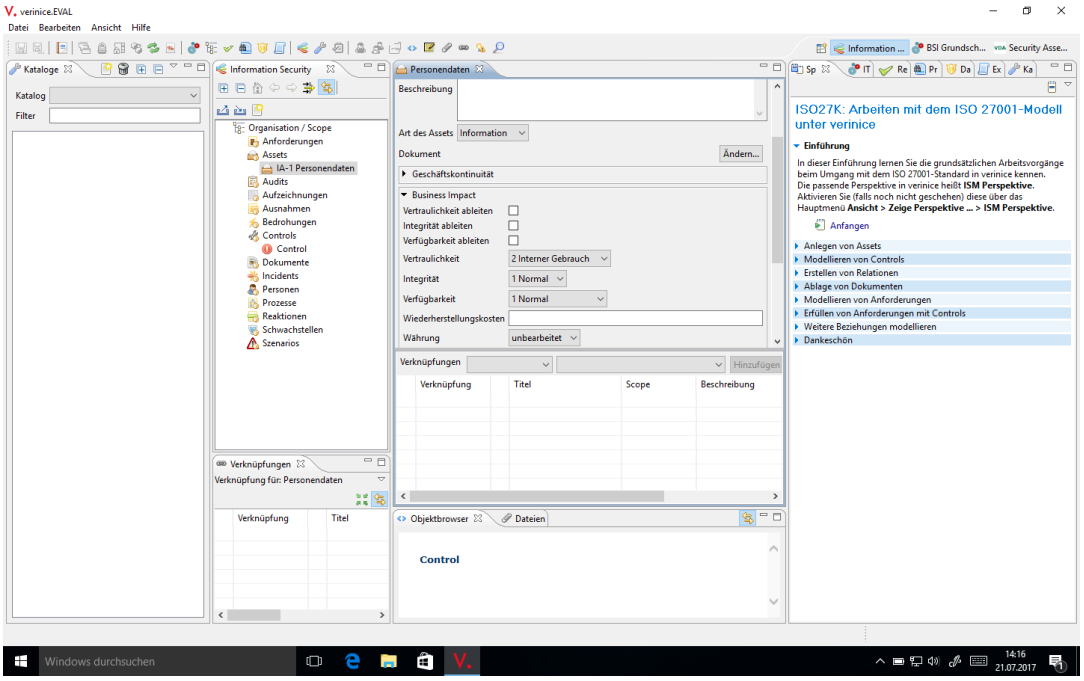


Abbildung 5.1: verinice. Hauptansicht

ActiveDirectory Diensten beinhaltet, um das Dokumenationstool innerhalb der Netzwerkinfrastruktur über Single-Sign-On möglichst nahtlos integrieren zu können.

Funktionsumfang

Verinice. bietet Möglichkeiten zur Dokumentation eines ISMS nach ISO/IEC 27001. Der Fokus liegt trotzdem eher auf dem BSI IT-Grundschutz, dessen Ausrichtung seit 2006 mehr und mehr an der internationalen Norm orientiert ist. Weiterhin bietet das Tool Möglichkeiten zur Risikoanalyse gemäß des ISO/IEC 27005. Dazu gehört die Erfassung von Werten sowie die darauf bezogenen direkten und indirekten Bedrohungen und Schwachstellen.

Die Branchenunabhängigkeit der Norm wird durch die Implementierung von Hilfsmitteln und Empfehlungen zum Zweck des Informationsschutzes durch den Arbeitskreis Integraler Informationsschutz mit IT-Sicherheit, Prototypenschutz und Risk-Management des Verbands der deutschen Automobilindustrie (VDA) verdeutlicht. Diese wurden in Version 1.2 in *Verinice.* integriert wodurch das Tool die Möglichkeit bietet, Information Security Assessments (ISA) anhand der festgelegten Anforderungen durchzuführen.

Darüber hinaus liefert *Verinice.* Schnittstellen zu OpenSource Schwachstellenscannern wie zum Beispiel OpenVAS oder Greenbone GSM, wodurch sich automatisiert Schwachstellen identifizieren und innerhalb eines Berichts zusammenfassen lassen können.

Dateneingabe und -persistenz

Die Eingabe von Informationen bzgl. einzelner Objekte findet innerhalb der Benutzeroberfläche, wie Abbildung 5.2 zeigt, über fest definierte Schaltflächen und Textfelder statt. Durch diese vorbereiteten Formulare erhält man grundsätzlich einheitlich strukturierte Daten, ist jedoch strikt an die Vorgehensweise der *Verinice.*-Entwicklung gebunden, was benutzerdefinierte Attribute oder auch Attributwerte betrifft. Die Beziehungen zwischen Objektklassen wie Assets, Risiken und Schutzmaßnahmen werden über eine tabellarische Darstellung, wie in Abbildung 5.3 gezeigt, abgebildet.

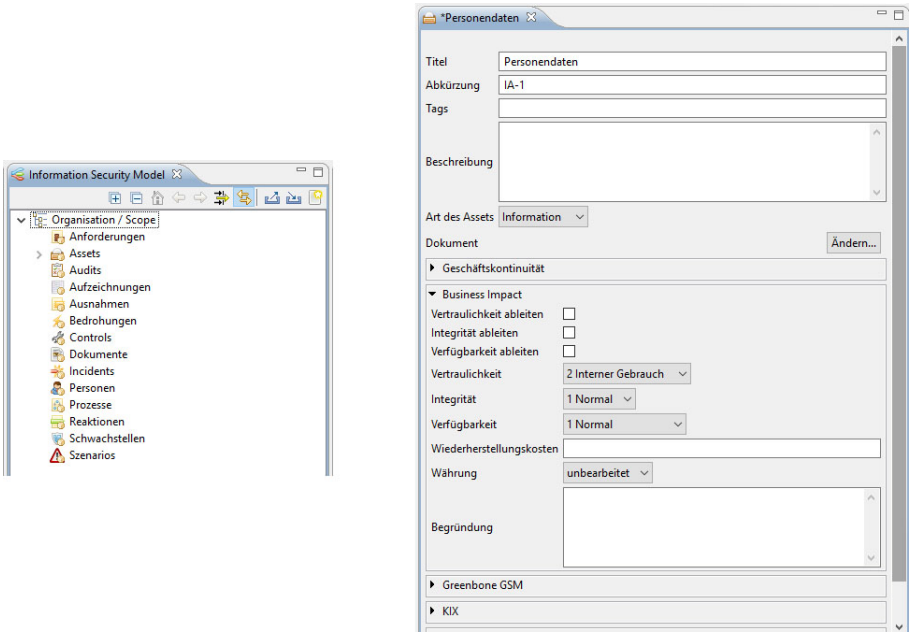


Abbildung 5.2: verinice. Hierarchie und Eingabemaske

Die Persistenz der Daten findet innerhalb einer relationalen Datenbank statt. Unterstützt werden PostgreSQL, Apache Derby oder Oracle DB. Durch die Eclipse RCP liegen sowohl die Datenbank als auch die Client-Konfigurationsdateien innerhalb des Standardworkspace-Pfads im Homeverzeichnis des jeweiligen Nutzers vor und können somit einfach von einem System auf ein anderes übernommen werden.

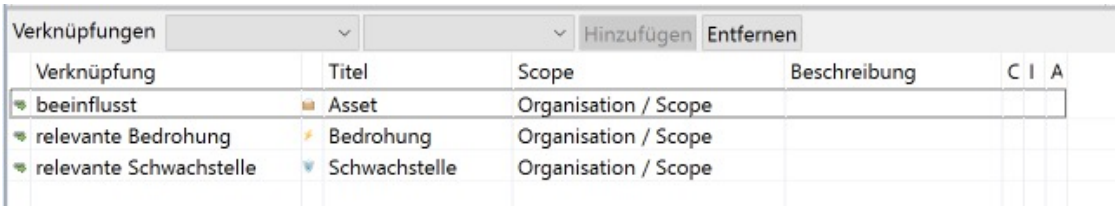


Abbildung 5.3: verinice. Verknüpfungen zwischen Objekten

ID	Anforderung	verinice.	Bewertung
IT-Grundschutz und ISO27001 Funktionalitäten			
F1	Dokumentation des Anwendungsbereichs/Scope des Unternehmens (ISO/IEC 27001 4.3)	ja	2
F3	Dokumentation der Informationssicherheitspolitik (ISO/IEC 27001 5.2)	ja	2
F5	Berichterstellung über die Leistung des ISMS (ISO/IEC 27001 5.3, 9.1)	ja	2
F6	Dokumentation von Risiken und Chancen sowie Maßnahmen (ISO/IEC 27001 6.1.1)	ja	2
F6	Klassifizierung von Werten bzgl. Kritikalität und Empfindlichkeit (ISO/IEC 27002 8.2)	ja	2
F7	Speicherung von IT-Assets (Unterteilung in primary und supporting assets) (ISO/IEC 27002 8.1.2, ISO/IEC 27005)	ja	2
F8	Dokumentation von Risiko-Assessments zur Festlegung von Bedrohungen und Schwachstellen (ISO/IEC 27005 Annex E.1)	ja	2
F9	Dokumentation von Risiko-Wahrscheinlichkeiten und Risiko-Auswirkungen (ISO/IEC 27005 Annex E.1)	ja	2
F10	Dokumentation der Kriterien zur Beurteilung von Risiken sowie der Risikoidentifikation, -analyse und -bewertung (ISO/IEC 27001 6.1.2)	ja	2
F11	Dokumentation eines SoA (ISO/IEC 27001 6.1.3)	ja	2
F12	Dokumentation des Informationssicherheitsziels (ISO/IEC 27001 6.2)	ja	2
F14	Dokumentation von Audits und Managementbewertungen (ISO/IEC 27001 9.2, 9.3)	ja	2
QV6	Import/Export GSTOOL	ja	2
QV9	Importfunktion für IT-Grundschutzkatalog und Referenzierung	ja	2
QV11	Vorgefertigte Self-Assessments	ja	2
QV29	Importfunktion für ISO-Normentexte	ja	2
Risikomanagement-Funktionalitäten			
QV28	Schutzbedarfsmatrix	ja	2
QV26	Vererbungsmechanismen für Schutzbedarf	ja	2
QV24	Ergänzende Maßnahmen	ja	2
QV25	Unterstützung klassischer Bedrohungs- und Risikoanalysen	ja	2
Reporting			
QV31	Microsoft Office Kompatibilität	ja	2
QV32	Visuelle Darstellung von Status- und Umsetzungsständen	teilweise	1
QV33	Konfiguration/Filtermöglichkeiten der Reportingausgabe	ja	2
User Experience und Benutzerfreundlichkeit			
F3	Zuweisung von Zuständigkeiten und Bekanntmachung von Rollenzuweisungen/Benutzerverwaltung (ISO/IEC 27001 5.3)	ja	2
F13	Dokumentenlenkung (ISO/IEC 27001 7.5)	ja	2
F15	Unterstützung eines kontinuierlichen Verbesserungsprozesses (ISO/IEC 27001 4.4)	ja	2
F17	Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen	nein	0
NF1	Performanz	teilweise	1
F18	Modellierung und Verwaltung komplexer IT-Verbünde	ja	2
F19	Konzeption der Struktur anhand vorhandener Inhalte	nein	0
NF2	Verlässlichkeit	ja	2
QV23	Unterstützung mehrerer Anwendungsbereiche/Scopes	ja	2
QV21	Netzwerkfähigkeit	ja	2
QV18	Unterstützung mehrerer Sprachen	ja	2

Tabelle 5.1: Funktionsumfang des Dokumentationstools verinice.

User Experience und Benutzerfreundlichkeit

Die Kompatibilität der Anwendung auf unterschiedlichen Betriebssystemen wie Linux, Windows oder MacOS ist durch die Ausführung innerhalb der Java Virtual Machine (JVM) gewährleistet. Da keinerlei Mobile-Versionen der Anwendung angeboten werden, ist der Einsatz auf Smartphones oder Tablets ohne die Nutzung einer Remote Desktop Verbindung (z.B. RDP oder VNC) nicht möglich.

Im Bereich der User Experience können durch die Nutzung der Eclipse RCP unterschiedliche Workflows unterstützt werden, indem die sog. Views der entsprechenden Ansicht über das Menü beliebig ein- und ausgeblendet werden können. Die eingesetzte Symbolik ist größtenteils selbsterklärend. Eine Schnellstartanleitung führt den Nutzer anhand einfacher Beispiele Schritt für Schritt an die Funktionsweise des Tools heran.

Verknüpfungen zwischen beispielsweise Informationassets und Szenarien, die sich durch Bedrohungen und Schwachstellen ergeben, können per Drag & Drop miteinander verknüpft werden, jedoch kann die Erkennung von Relationen bei einer großen Menge an Daten schnell unübersichtlich werden, da Verknüpfungen zwischen Objekttypen hauptsächlich tabellarisch dargestellt werden (vgl. 5.3).

Zusammenfassung

Die Anwendung wird regelmäßig weiterentwickelt und hat durch die Lizenzierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) keine unbedeutende Relevanz im Bereich der Dokumentation der ISO/IEC 27001 oder des IT-Grundschutzes. Die Unterstützung bei der Umsetzung innerhalb von Unternehmen wird durch den Entwickler selbst gewährleistet, indem dazu regelmäßige Konferenzen und Schulungen angeboten werden.

Die Software selbst vermittelt allerdings im Vergleich mit nativen Systemanwendungen den Eindruck, dass sie nicht mehr zeitgemäß ist. Die Anwendung skaliert auf hochauflösenden Displays nur schlecht, wodurch Schrift und Bilder einen unscharfen Eindruck hinterlassen. Auch bei der visuellen Darstellung von Zusammenhängen zwischen einzelnen Modulen wie Schutzmaßnahmen und zugehörigen Risiken scheint die Software ihre Grenzen zu erreichen. Darüber hinaus ist durch die Ausführung innerhalb der Java Virtual Machine (JVM) zwar eine gewisse Plattformunabhängigkeit gegeben, die aber auch mit Nachteilen einhergeht. Die Ausführung auf mobilen Endgeräten wie Tablets oder Smartphones ist zum Beispiel nicht möglich.

Der Overhead innerhalb des Arbeitsspeichers, der bei der Ausführung der Anwendung entsteht, ist ebenfalls nicht zu vernachlässigen. Bei längerer Nutzungsdauer kann es zu Instabilitäten kommen. Verinice. liefert eine gute und vor allem normnahe Struktur, um die Inhalte eines ISMS gemäß den Anforderungen an ein Audit zu hinterlegen. Darüber hinaus wird die Dokumentation durch nützliche Features wie zum Beispiel einem Assistenten zur Erstellung einer Risikoanalyse und Schwachstellenanalysetools ergänzt. Verbesserungswürdig erscheint insgesamt die visuelle Darstellung wichtiger Zusammenhänge.

5.2.2 opus-i

Allgemeine Informationen

opus-i ist ein weiteres Dokumentationstool im Bereich der IT-Sicherheit. Entwickelt wurde das Tool vom Unternehmen kronsoft, das 1992 als ITSoft gegründet wurde und bis in die frühen 2000er Jahren mit der modular erweiterbaren Anwendung BDAdmin, einem Tool für Datenschutzbeauftragte, hervorstach. Seit 2004 wird BDAdmin neu programmiert und ist unter dem neuen Namen opus-i nach vier Jahren Entwicklungszeit auf den Markt gekommen. Ebenfalls wie bei *verinice.* umfasst opus-i sowohl die Unterstützung für den IT-Grundschutzkatalog des BSI aber auch die Mindestanforderungen des ISO/IEC 27001.

Die nachfolgende Übersicht bezieht sich auf die Testversion 7.2.134.760 vom 14.03.2017.

Systemkompatibilität

Bei opus-i handelt es sich um eine native Windows-Software. Für andere Desktop-Betriebssysteme stellt das Unternehmen keine Alternativen bereit. Um dennoch eine zentrale Nutzung der Inhalte über Server zu ermöglichen, stellt kronsoft eine Web-Applikation, genannt *opus-i WEB* zur Verfügung, mit der betriebssystemunabhängig über den Browser auf die Daten zugegriffen werden kann. Die Software ist proprietär und erlaubt somit keinen Einblick in den Quellcode.

ID	Anforderung	opus-i	Bewertung
Systemkompatibilität			
QV4	Client/Server Infrastruktur	ja	2
QV5	Desktop-Client (nativ)	Linux (nein) MacOS (nein) Windows (ja)	1
QV16	Mobile Apps	nativ (nein) webapp (nein)	0
QV3	Datenbanksysteme Unterstützung	ja	2

Lizenzierungsmodelle

Das Lizenzierungsmodell der Firma kronsoft orientiert sich an der Nutzerzahl. So besteht zumindest die Möglichkeit anhand der Anzahl der tatsächlichen Anwender eine Mietpauschale zwischen 26 EUR und 515 EUR zu entrichten, die Arbeitsplatzlizenzen für einen bis beliebig vielen Nutzern beinhaltet. Hier wird zwischen sog. Modulen unterschieden, die die zu verwaltenden Managementbereiche widerspiegeln sollen. Da die Entwicklung neuer Module zur Erweiterung der Hauptanwendung durch kronsoft durchgeführt wird, ist es möglich, den Funktionsumfang nachträglich zu erweitern. kronsoft arbeitet beispielsweise an Modulen zur Unterstützung des Incident Management Prozesses durch ein Service Desk Modul (Ticketsystem) sowie der Integration zur Dokumentation des Notfallmanagements.

Neben dem Abonnement-Modell bietet kronsoft auch den Erwerb von unlimitierten Lizenzen an. Somit können einzelne der oben genannten Module mit einer einmaligen Arbeitsplatzlizenz erworben und ohne zeitliche Einschränkung genutzt werden. Die Preise skalieren hier

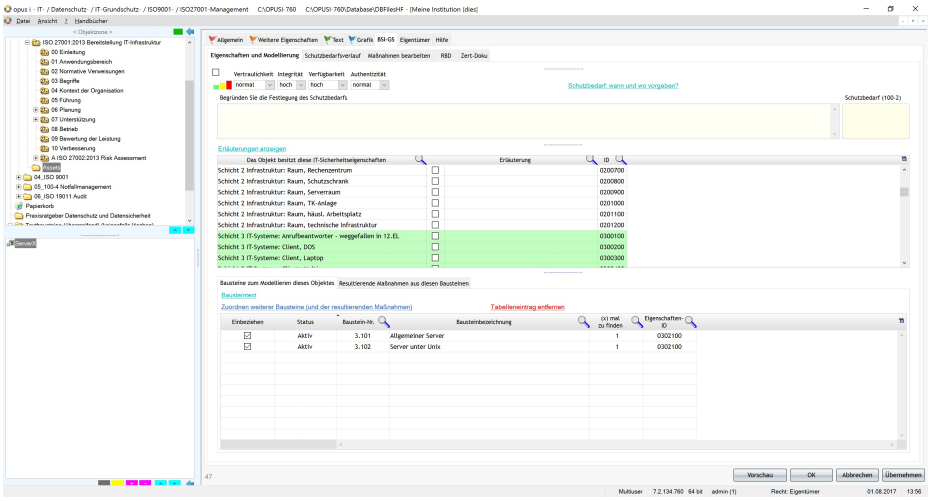


Abbildung 5.4: Opus-i Hauptansicht

vom zweistelligen bis in den drei- und vierstelligen Bereich.

Die Konfiguration mehrerer Mandanten oder auch Anwendungsbereiche ist mit einem Geldbetrag verbunden, wodurch sich die Entwicklung einer Dokumentationsstruktur stark anhand des preislichen Angebots orientiert. Neben den benötigten Softwarepaketen, belaufen sich die Kosten pro User bei der Dokumentation im Bereich der ISO/IEC 27001 für die urheberrechtlich geschützten Normentexte zwischen 100 EUR und 200 EUR.

Abschließend werden noch diverse Supportleistungen sowohl für die Software selbst als auch für das gewählte Datenbanksystem angeboten, deren Preis sich prozentual aus dem Betrag der Lizenzkosten für die Anwendung zusammensetzt.

Funktionsumfang

opus-i setzt sich, wie Eingangs erwähnt, aus mehreren unterschiedlichen Modulen zusammen. Folgende Module werden zur Zeit angeboten:

- Datenschutz
- IT-Grundschutz
- ISO 9001
- ISO 27001

Das Basissystem bietet grundlegende Funktionen wie eine Benutzerverwaltung, Archivierungs- und Backupfunktionalitäten und den Import/Export von Office-kompatiblen Daten. Zusätzlich kann das Basispaket zur Dokumentation von IT-Objekten ähnlich einer Configuration Management Database (CMDB) verwendet werden und den Workflow durch anpassbare Parameter und Wiedervorlage-Funktionen unterstützen.

Zugehörige Dokumente müssen nicht zwangsläufig in das Datenbanksystem von opus-i importiert werden sondern können auch als Uniform Resource Locator (URL) verknüpft werden. Diese Lösung erlaubt, bestimmten Rohdaten wie Formulare, Anleitungen oder Verfahrensbeschreibungen auf einem unabhängigen Netzlaufwerk separat zu sichern, aber dennoch einen Verweis auf das entsprechende Dokument zu hinterlegen.

Die oben genannten Module ergänzen das Basissystem um eine digitale Form der entsprechenden gesetzlichen Regelungen, empfehlenswerte Vorgehensweisen und Normen. So wird beim Datenschutzpaket beispielsweise ein Verfahrensverzeichnis nach dem deutschen Bundesdatenschutzgesetz hinterlegt, dass mit den erstellten Hard- und Softwareobjekten sowohl auf kritische Punkte aufmerksam macht, aber auch in der Lage ist, Strukturen, Prozesse und Datenflüsse mit den entsprechenden Referenzen abzubilden.

Ein Support für VDA Information Security Assessments wird ebenfalls angeboten. Wenn die Module für den IT-Grundschutz und des ISO/IEC 27001 eingebunden wurden, verlaufen die Grenzen zwischen diesen beiden Paketen fließend. So werden die Anforderungen der ISO/IEC 27001 mit den entsprechenden Verantwortlichkeiten und Rollen ausgestattet. Betrachtet man allerdings die einzelnen Informationswerte, so wird auf die bereits sehr detaillierte Zusammenstellung möglicher Gefahren und der dazugehörigen Schutzmaßnahmen des IT-Grundschutzkatalogs zurückgegriffen.

Dateneingabe und -persistenz

Bei der Datenpersistenz ist opus-i vergleichsweise flexibel. Zu den wichtigsten unterstützten Datenbanksystemen zählen Microsoft SQL, MySQL, Oracle und PostgreSQL. Für Microsoft SQL bietet das Unternehmen auch vollen technischen Support an. In der Testversion befindet sich innerhalb des Installationsverzeichnisses ein definierter Ordner namens 'Database', der sämtliche Daten in Form von .mmo und .dat Dateien beinhaltet. Standardmäßig ist der MultiUser-Mode und nicht der Client-/Server Modus aktiviert, wodurch der Zugriff auf das lokale System inkl. einer lokalen Benutzerverwaltung beschränkt wird.

Eine Sicherung und Wiederherstellung der Daten erfolgt über die Anwendung selbst. Die Datei wird als Textdatei und als ZIP-komprimierte Datei innerhalb eines Unterverzeichnisses hinterlegt. Regelmäßige Sicherungen führt opus-i selbstständig in fest definierten Zeiträumen durch.

Nr.	Maßnahmenbezeichnung	Siegel-stufe	Initiierung durch	Umsetzung durch	Lebenszyklus	Umsetzungs-status	ISO
1.28	Lokale unterbrechungsfreie Stromversorgung	B Aufbau			Planung und Konze	unbearbeitet	
2.204	Verhinderung ungesicherter Netzzugänge	A Einstieg			03 UM Umsetzung	unbearbeitet	
2.22	Hinterlegen des Passwortes	Z zusätzlich			04 BT Betrieb	unbearbeitet	
2.273	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	A Einstieg			04 BT Betrieb	unbearbeitet	
2.314	Verwendung von hochverfügbaren Architekturen für Server	Z zusätzlich			Planung und Konze	unbearbeitet	
2.315	Planung des Servereinsatzes	A Einstieg			Planung und Konze	unbearbeitet	
2.316	Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server	A Einstieg			Planung und Konze	unbearbeitet	
2.317	Beschaffungskriterien für einen Server	C Zertifikat			02 BE Beschaffung	unbearbeitet	
2.318	Sichere Installation eines IT-Systems	A Einstieg			03 UM Umsetzung	unbearbeitet	
2.319	Migration eines Servers	C Zertifikat			05 AS Aussonderung	unbearbeitet	

Sum

Abbildung 5.5: Opus-i Maßnahmen

ID	Anforderung	opus-i	Bewertung
IT-Grundschutz und ISO27001 Funktionalitäten			
F1	Dokumentation des Anwendungsbereichs/Scope des Unternehmens (ISO/IEC 27001 4.3)	ja	2
F2	Dokumentation der Informationssicherheitspolitik (ISO/IEC 27001 5.2)	ja	2
F4	Berichterstellung über die Leistung des ISMS (ISO/IEC 27001 5.3, 9.1)	ja	2
F5	Dokumentation von Risiken und Chancen sowie Maßnahmen (ISO/IEC 27001 6.1.1)	ja	2
F6	Klassifizierung von Werten bzgl. Kritikalität und Empfindlichkeit (ISO/IEC 27002 8.2)	ja	2
F7	Speicherung von IT-Assets (Unterteilung in primary und supporting assets) (ISO/IEC 27002 8.1.2, ISO/IEC 27005)	ja	2
F8	Dokumentation von Risiko-Assessments zur Festlegung von Bedrohungen und Schwachstellen (ISO/IEC 27005 Annex E.1)	ja	2
F9	Dokumentation von Risiko-Wahrscheinlichkeiten und Risiko-Auswirkungen (ISO/IEC 27005 Annex E.1)	ja	2
F10	Dokumentation der Kriterien zur Beurteilung von Risiken sowie der Risikoidentifikation, -analyse und -bewertung (ISO/IEC 27001 6.1.2)	ja	2
F11	Dokumentation eines SoA (ISO/IEC 27001 6.1.3)	ja	2
F12	Dokumentation des Informationssicherheitsziels (ISO/IEC 27001 6.2)	ja	2
F14	Dokumentation von Audits und Managementbewertungen (ISO/IEC 27001 9.2, 9.3)	teilweise	1
QV6	Import/Export GSTOOL	ja	2
QV9	Importfunktion für IT-Grundschutzkatalog und Referenzierung	ja	2
QV11	Vorgefertigte Self-Assessments	ja	2
QV29	Importfunktion für ISO-Normentexte	ja	2
Risikomanagement-Funktionalitäten			
QV28	Schutzbedarfsmatrix	ja	2
QV26	Vererbungsmechanismen für Schutzbedarf	ja	2
QV24	Ergänzende Maßnahmen	ja	2
QV25	Unterstützung klassischer Bedrohungs- und Risikoanalysen	ja	2
Reporting			
QV31	Microsoft Office Kompatibilität	ja	2
QV32	Visuelle Darstellung von Status- und Umsetzungsständen	ja	2
QV33	Konfiguration/Filtermöglichkeiten der Reportingausgabe	ja	2
User Experience und Benutzerfreundlichkeit			
F3	Zuweisung von Zuständigkeiten und Bekanntmachung von Rollenzuweisungen/Benutzerverwaltung (ISO/IEC 27001 5.3)	ja	2
F13	Dokumentenlenkung (ISO/IEC 27001 7.5)	ja	2
F15	Unterstützung eines kontinuierlichen Verbesserungsprozesses (ISO/IEC 27001 4.4)	ja	2
F17	Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen	ja	2
NF1	Performanz	teilweise	1
F18	Modellierung und Verwaltung komplexer IT-Verbünde	ja	2
F19	Konzeption der Struktur anhand vorhandener Inhalte	nein	0
NF2	Verlässlichkeit	teilweise	1
QV23	Unterstützung mehrerer Anwendungsbereiche/Scopes	nein	0
QV21	Netzwerkfähigkeit	ja	2
QV18	Unterstützung mehrerer Sprachen	nein	0

Tabelle 5.2: Funktionsumfang des Dokumentationstools opus-i

User Experience und Benutzerfreundlichkeit

opus-i existiert nur als Windows-Applikation. Die Installation erfordert, dass sich das Anwendungsverzeichnis direkt unterhalb des Pfades <C:\> befindet, da das Programm andernfalls nicht ordnungsgemäß ausgeführt werden kann. Hier wurde offenbar mit relativen Pfaden gearbeitet, wodurch es auf Systemen ohne entsprechende Berechtigung bereits hier zu Problemen kommen kann.

Die Benutzeroberfläche ist übersichtlich gestaltet. Die verwendeten Symbole und die Optik von modalen Fenstern lassen darauf schließen, dass auch hier nicht auf das native grafische User-Interface von Windows eingesetzt wurde. Der Umgang mit der farblichen Gestaltung ist gut gelungen. So werden zusammengehörige Teile eines Formulars voneinander abgegrenzt und so die Übersicht erhöht. Auch in Bereichen der Maßnahmenumsetzung und der Risikoanalyse wird mit visuellen Elementen gearbeitet, wodurch ein Gesamteindruck schnell erfasst werden kann.

Die Parameter der Risikoanalyse, der Eintrittswahrscheinlichkeit und des Schadenspotentials werden in einer Matrix dargestellt, die eine Aufteilung der Akzeptanzkriterien in die drei Bereiche „akzeptabel“, „so niedrig wie vernünftigerweise praktikabel“ und „inakzeptabel“ mit den zugehörigen Farben „Grün“, „Gelb“ und „Grün“ im sog. Traffic Light Protocol (TLP) darstellt.

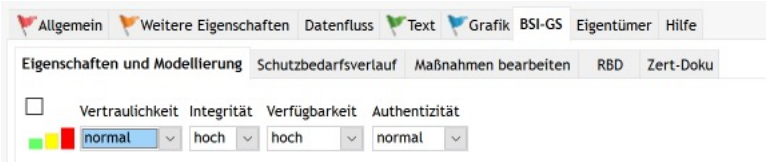


Abbildung 5.6: Opus-i Schutzbedarf

Zusammenfassung

opus-i bietet neben den wichtigsten Funktionalitäten, die bei der Dokumentation eines ISMS benötigt werden, auch nützliche Features wie Self-Assessments oder VDA Security Assessments. Dabei bleibt die Flexibilität aufgrund des modularen Aufbaus erhalten, wodurch die Software auch im Zuge der Entwicklung neuer Module im Unternehmenseinsatz auch über einen längerfristigen Zeitraum weitere Managementbereiche unterstützen kann. Weiterhin erlaubt die breite Unterstützung bekannter Datenbanksysteme wie MySQL und Microsoft SQL eine Integration im Unternehmensumfeld, wodurch sich zusätzliche finanzielle Neuaufwendungen durch Anschaffung teurer Soft- und Hardwarelösungen reduzieren lassen. Insbesondere PostgreSQL-Datenbanken sind auch im Unternehmensumfeld nicht an eine Nutzungslizenz gebunden.

Der Anspruch, einem Nutzer, der über kein spezielles Fachwissen besitzt, die Themen der ISO/IEC 27001 und der Risikobehandlung näher zu bringen, erreicht der Entwickler durch gezielte Farbwahl von Schaltflächen aber auch durch den Einsatz visueller Hilfsmittel wie der Risikobehandlungsmatrix. Darüber hinaus sind die Inhalte gut strukturiert und voneinander

getrennt. Zwar ergeben sich durch den komplexen Aufbau eines ISMS teilweise Ansichten mit mehreren kaskadierenden Reiteransichten, die jedoch stets mit einer Beschreibung ausgestattet sind.

5.2.3 ISIS12

Allgemeine Informationen

ISIS12 stellt ein Dokumentationstool dar, das auf der BSI-Grundschutzmethodik aufbaut und insbesondere mittelständischen Unternehmen durch Implementierung eines 12-Schritte-Plans, eine Zertifizierung im Bereich der ISO/IEC 27001 ermöglichen sollte. In den Mittelpunkt stellt der für die Entwicklung verantwortliche Bayerische IT-Sicherheitscluster e.V., dessen Mitglieder sowohl Unternehmen als auch Hochschulen sind, eine einfach zu handhabende Schnittstelle zur Dokumentation der IT-Informationssicherheit.

Die nachfolgende Übersicht stellt die Version 1.3 vom 17.03.2017 dar, die speziell für das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften zum Lehrzweck lizenziert wurde.

Systemkompatibilität

Bei der Anwendung handelt es sich um eine Webanwendung auf Basis der Programmiersprache PHP. PHP-Skripte setzen eine serverseitige Nutzung voraus und werden Clientseitig innerhalb eines Browsers aufgerufen. Dadurch besteht die Möglichkeit, die Anwendung auch auf mobilen Endgeräten wie Smartphones und Tablets auszuführen.

ID	Anforderung	ISIS12	Bewertung
Systemkompatibilität			
QV4	Client/Server Infrastruktur	ja	2
QV5	Desktop-Client (nativ)	Linux (nein) MacOS (nein) Windows (nein)	0
QV16	Mobile Apps	nativ (nein) webapp (nein)	0
QV3	Datenbanksysteme Unterstützung	nein	0

Lizenzierungsmodelle

Die Software wird nur als Komplettpaket angeboten. Bei einer Jahreslizenz belaufen sich im ersten Jahr die Kosten auf ca. 600 EUR. Für die Folgejahre müssten ca. 300 EUR kalkuliert werden. Neben der Anwendung selbst bietet das IT-Sicherheitscluster e.V. noch ein Handbuch an, in dem der sog. 12-Schritte-Plan anhand von Beispielen näher erläutert wird.

Funktionsumfang

ISIS12 gibt der Herstellung und Dokumentation eines ISMS innerhalb einer Organisation einen Rahmen. Der Fokus liegt ganz klar auf den eigens entwickelten 12-Schritte-Plan, welche in Abbildung 5.7 dargestellt ist.

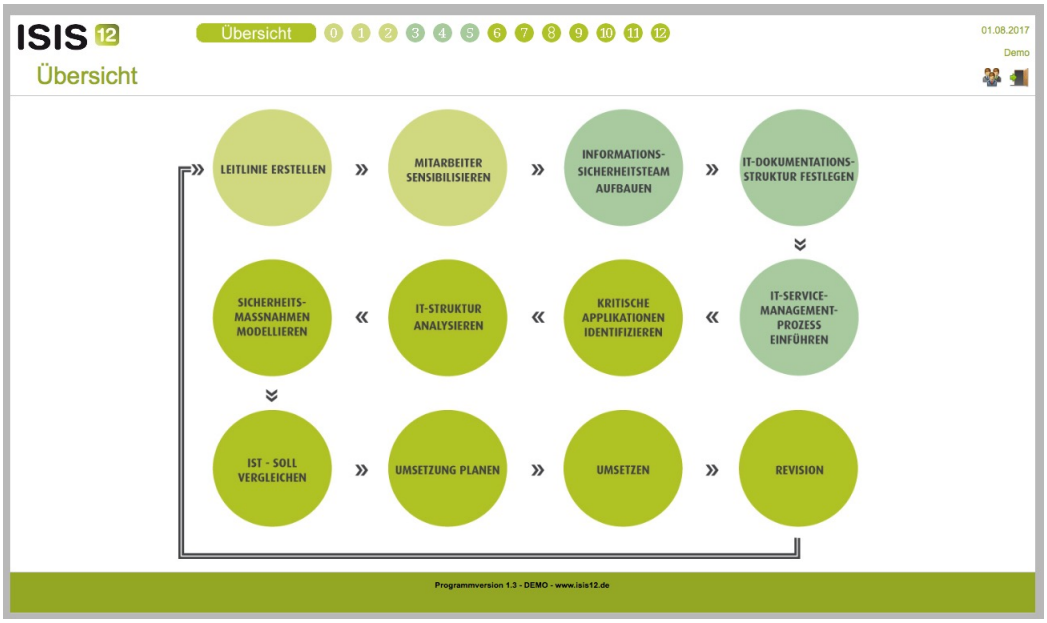


Abbildung 5.7: ISIS12 - 12-Schritte-Plan

Wie der Abbildung 5.7 zu entnehmen ist, beschäftigen sich die ersten fünf Phasen hauptsächlich mit der Vorbereitung zur Herstellung eines ISMS. So wird zu Beginn der Nutzer mit einem Fragebogen konfrontiert, der dazu dient, den Ist-Stand der Organisation bzgl. der IT-Informationssicherheit zu ermitteln, aber auch Anforderungen, die es noch zu erledigen gilt, zu identifizieren. Die Anwendung an sich gibt innerhalb der ersten Schritte nur wenig Informationen preis, wie die Anforderungen im konkreten zu erfüllen sind, weshalb das separate Handbuch an dieser Stelle mit weiterführenden Informationen und Best Practices ergänzende Informationen liefern kann.

Ab der sechsten Phase beginnt der operative Teil des Tools. Hier werden zunächst unternehmenskritische Bausteine und Maßnahmen definiert. Vorgefertigte Maßnahmen und Bausteine orientieren sich anhand des IT-Grundschutzkatalogs und können durch individuelle Einträge ergänzt werden. Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit eines jeden Bausteins anhand vorher festgelegter Schutzbedarfskategorien zu definieren.

Da die zu betrachtenden Bausteine abhängig von konkreten IT-Systemen und Infrastrukturen sind, werden diese im nächsten Schritt definiert. Zu Menge der secondary Assets (vgl. 2.2.3) zählen insbesondere Client- und Serversysteme, Softwareanwendungen aber auch Standorte, deren Schutzbedarf nochmals individuell in den vorher benannten Kategorien festgestellt und definiert werden.

Die letzten vier Phasen umfassen unterschiedliche Perspektiven auf die Gesamtübersicht der umzusetzenden Sicherheitsmaßnahmen. So werden zunächst alle umzusetzenden Maßnahmen aufgelistet und entsprechend ihres Umsetzungsstatus farblich gekennzeichnet. Anschließend wird eine Kostenabschätzung aufgestellt, die sowohl einmalige aber auch laufende Kosten in Bezug mit einer Priorität berücksichtigt.

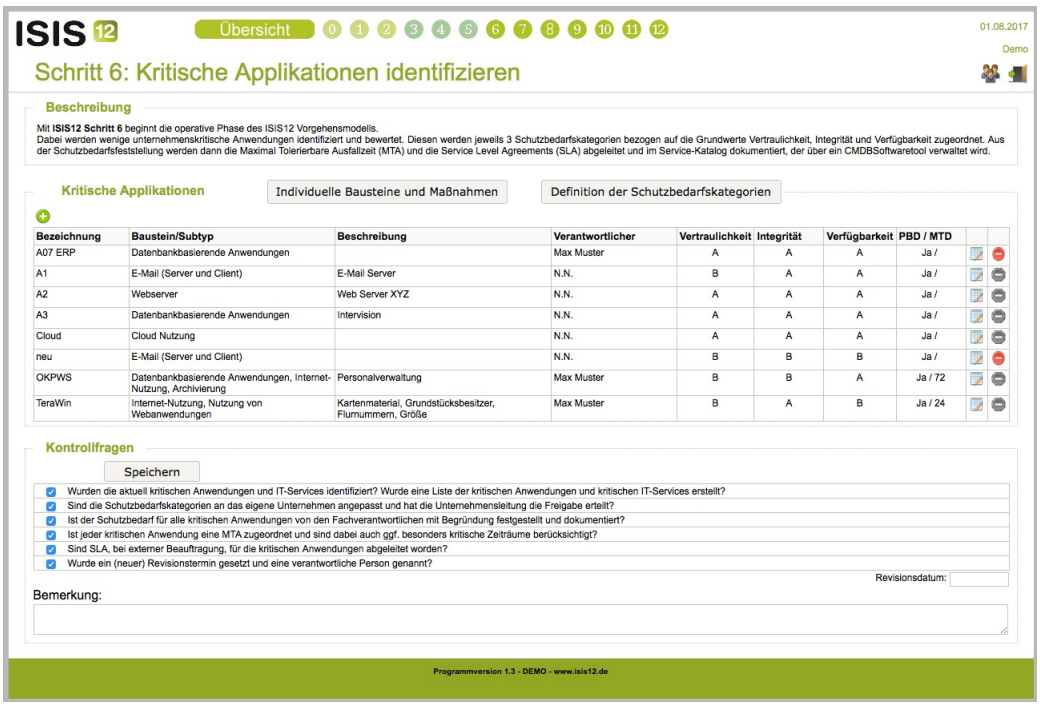


Abbildung 5.8: ISIS12 - Kritische Applikationen identifizieren

Die letzten beiden Phasen beziehen sich explizit auf die Umsetzung und zukünftige Kontrolle der festgelegten Maßnahmen. So werden individuelle Verantwortliche festgelegt und Zeiträume für Umsetzung und dem Schulungsbedarf festgehalten.

Dateneingabe und -persistenz

Anders als bei den bisherigen Tools, findet die Datensicherung in Form von Klartext-Dateien statt, die innerhalb eines Unterverzeichnisses der Webanwendung abgelegt werden. So erübrigt sich die Einrichtung eines Datenbanksystems. Des weiteren besteht die Möglichkeit ohne die Anwendung Zugriff auf die hinterlegten Daten zu erhalten und diese durch *parsing* individuell weiterzuverwenden und Funktionen zu ergänzen.

User Experience und Benutzerfreundlichkeit

Durch die Implementierung von ISIS12 als PHP-Anwendung wird eine Client-Server Infrastruktur zwingend vorausgesetzt. Eine Einrichtung bestimmter PHP-Module wird nicht benötigt, jedoch sind Schreibrechte des Webserver-Benutzers *www-data* notwendig, um die eingegebenen Daten sichern zu können. Anschließend ist die Webanwendung innerhalb jedes beliebigen Webbrowsers aufrufbar. Der Aufbau ist sehr übersichtlich gestaltet. Zu Beginn wird nochmals eine Gesamtübersicht über die ISIS12-Phasen zur Verfügung gestellt und anschließend linear Punkt für Punkt bearbeitet. Die minimalistische Oberfläche und die gekürzten Bemerkungen innerhalb der unterschiedlichen Phasen deuten allerdings darauf hin, dass die Entwickler des Tools davon ausgehen, dass der Katalog bei der Nutzung der Anwendung zumindest zu Beginn parallel mitbenutzt wird.

ID	Anforderung	ISIS12	Bewertung
IT-Grundschutz und ISO27001 Funktionalitäten			
F1	Dokumentation des Anwendungsbereichs/Scope des Unternehmens (ISO/IEC 27001 4.3)	ja	2
F2	Dokumentation der Informationssicherheitspolitik (ISO/IEC 27001 5.2)	teilweise	1
F4	Berichterstellung über die Leistung des ISMS (ISO/IEC 27001 5.3, 9.1)	ja	2
F5	Dokumentation von Risiken und Chancen sowie Maßnahmen (ISO/IEC 27001 6.1.1)	ja	2
F6	Klassifizierung von Werten bzgl. Kritikalität und Empfindlichkeit (ISO/IEC 27002 8.2)	ja	2
F7	Speicherung von IT-Assets (Unterteilung in primary und supporting assets) (ISO/IEC 27002 8.1.2, ISO/IEC 27005)	teilweise	1
F8	Dokumentation von Risiko-Assessments zur Festlegung von Bedrohungen und Schwachstellen (ISO/IEC 27005 Annex E.1)	teilweise	1
F9	Dokumentation von Risiko-Wahrscheinlichkeiten und Risiko-Auswirkungen (ISO/IEC 27005 Annex E.1)	teilweise	1
F10	Dokumentation der Kriterien zur Beurteilung von Risiken sowie der Risikoidentifikation, -analyse und -bewertung (ISO/IEC 27001 6.1.2)	ja	2
F11	Dokumentation eines SoA (ISO/IEC 27001 6.1.3)	ja	2
F12	Dokumentation des Informationssicherheitsziels (ISO/IEC 27001 6.2)	teilweise	1
F14	Dokumentation von Audits und Managementbewertungen (ISO/IEC 27001 9.2, 9.3)	teilweise	1
QV6	Import/Export GSTOOL	nein	0
QV9	Importfunktion für IT-Grundschutzkatalog und Referenzierung	teilweise	1
QV11	Vorgefertigte Self-Assessments	teilweise	1
QV29	Importfunktion für ISO-Normentexte	nein	0
Risikomanagement-Funktionalitäten			
QV28	Schutzbedarfsmatrix	nein	0
QV26	Vererbungsmechanismen für Schutzbedarf	nein	0
QV24	Ergänzende Maßnahmen	ja	2
QV25	Unterstützung klassischer Bedrohungs- und Risikoanalysen	ja	2
Reporting			
QV31	Microsoft Office Kompatibilität	nein	0
QV32	Visuelle Darstellung von Status- und Umsetzungsständen	ja	2
QV33	Konfiguration/Filtermöglichkeiten der Reportingausgabe	nein	0
User Experience und Benutzerfreundlichkeit			
F3	Zuweisung von Zuständigkeiten und Bekanntmachung von Rollenzuweisungen/Benutzerverwaltung (ISO/IEC 27001 5.3)	teilweise	1
F13	Dokumentenlenkung (ISO/IEC 27001 7.5)	teilweise	1
F15	Unterstützung eines kontinuierlichen Verbesserungsprozesses (ISO/IEC 27001 4.4)	ja	2
F17	Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen	teilweise	1
NF1	Performanz	ja	2
F18	Modellierung und Verwaltung komplexer IT-Verbünde	teilweise	1
F19	Konzeption der Struktur anhand vorhandener Inhalte	nein	0
NF2	Verlässlichkeit	ja	2
QV23	Unterstützung mehrerer Anwendungsbereiche/Scopes	nein	0
QV21	Netzwerkfähigkeit	ja	2
QV18	Unterstützung mehrerer Sprachen	nein	0

Tabelle 5.3: Funktionsumfang des Dokumentationstools ISIS12

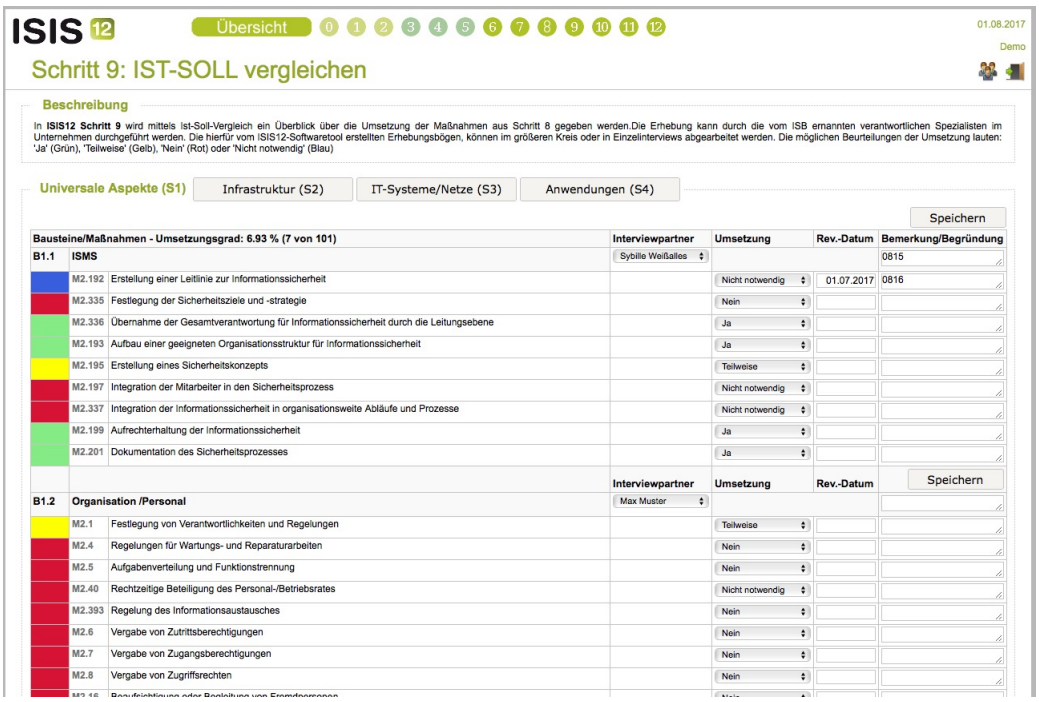


Abbildung 5.9: ISIS12 - Soll/Ist-Vergleich

Die User Experience des Tools leidet durch fehlende JavaScript-Elemente, die den Zusammenhang zwischen Objekten verdeutlichen könnten. Es fehlen clientseitig ausgeführte Animationen oder Möglichkeiten ohne einen Neuaufbau der Seite Änderungen vorzunehmen. Bei den umgesetzten Maßnahmen unterstützen zwar farbliche Akzente die Übersicht über den jeweiligen Umsetzungsstatus, jedoch wurden diese bei der allgemeinen Benutzerführung nicht berücksichtigt. So hätte man beispielsweise bereits durchgeführte Phasen als fertiggestellt kennzeichnen oder eine Darstellung über den aktuellen Stand der derzeitigen Iteration geben können, nachdem das 12-Punkte-System iterativ zum Zwecke einer kontinuierlichen Optimierung durchlaufen werden sollte. Weiterhin fehlen dem Tool Responsive Design Elemente, die eine Nutzung auf mobilen Endgeräten wie Tablets oder Smartphones unterstützen würde.

Zusammenfassung

ISIS12 bietet eine verkürzte Form des IT-Grundschutzkatalogs, der sich auf die wesentlichen Elemente beschränkt. Dabei wird der Prozess zur Herstellung eines ISMS innerhalb von 12 vordefinierter Phasen unterstützt. Durch die leichtgewichtige Implementierung innerhalb einer Webanwendung ist die Kompatibilität auf vielen Systemen gewährleistet. Darüber hinaus schafft es ISIS12 auch inhaltlich auf die Kernthemen des BSI-Grundschutzes innerhalb seines 12-Phases-Programms einzugehen und deckt mit dem zyklischen Vorgehen zudem den PDCA-Zyklus zur kontinuierlichen Verbesserung ab.

Die tatsächliche Dokumentation von konkreten Werten wird jedoch eingeschränkt, indem die Flexibilität durch die strikt vorgegebenen Eingabemasken bei individuellen Organisati-

onsstrukturen und den zugehörigen individuellen Geltungsbereichen des ISMS minimal ist. Auch die Schnittstelle zu anderen Managementsystemen ist aufgrund des leichtgewichtigen Ansatzes nicht gegeben. Die Datenhaltung innerhalb von Klartextdateien zeigt weiterhin, dass die Zielgruppe für ISIS12 eher auf kleinere Unternehmen mit einem überschaubaren Asset-Inventar und einer geringen Nutzerzahl ausgelegt ist.

5.3 Vergleich

Nachstehende tabellarische Zusammenfassung (siehe Tabellen 5.4 und 5.5) zeigt den Funktionsumfang aller getesteten Dokumentationstools. Die Kriterien, die bei der Betrachtung der einzelnen Tools berücksichtigt wurden, basieren auf der grundsätzlichen Zielvorgabe, die sich aus der Anforderungsanalyse ergeben hat. Die Ergebnisse des Vergleichs umfassen die ursprünglich festgelegte Bewertung aus Abschnitt 4.3. Dabei wurde die Signifikanz des Kriteriums x mit dem Wert multipliziert, der angibt, in welcher Art das Kriterium umgesetzt wurde.

ID	Anforderung	verinice	opus-i	ISIS12
Systemkompatibilität				
QV4	Client/Server Infrastruktur	18	18	18
QV5	Desktop-Client (nativ)	12	6	0
QV16	Mobile Apps	6	0	0
QV3	Datenbanksysteme Unterstützung	6	12	0
$\sum$		42	36	18
IT-Grundschutz und ISO27001 Funktionalitäten				
F1	Dokumentation des Anwendungsbereichs/Scope des Unternehmens (ISO/IEC 27001 4.3)	24	24	24
F2	Dokumentation der Informationssicherheitspolitik (ISO/IEC 27001 5.2)	24	24	12
F4	Berichterstellung über die Leistung des ISMS (ISO/IEC 27001 5.3, 9.1)	24	24	24
F5	Dokumentation von Risiken und Chancen sowie Maßnahmen (ISO/IEC 27001 6.1.1)	24	24	24
F6	Klassifizierung von Werten bzgl. Kritikalität und Empfindlichkeit (ISO/IEC 27002 8.2)	24	24	24
F7	Speicherung von IT-Assets (Unterteilung in primary und supporting assets) (ISO/IEC 27002 8.1.2, ISO/IEC 27005)	18	18	18
F8	Dokumentation von Risiko-Assessments zur Festlegung von Bedrohungen und Schwachstellen (ISO/IEC 27005 Annex E.1)	18	18	18
F9	Dokumentation von Risiko-Wahrscheinlichkeiten und Risiko-Auswirkungen (ISO/IEC 27005 Annex E.1)	18	18	18
F10	Dokumentation der Kriterien zur Beurteilung von Risiken sowie der Risikoidentifikation, -analyse und -bewertung (ISO/IEC 27001 6.1.2)	18	18	18
F11	Dokumentation eines SoA (ISO/IEC 27001 6.1.3)	18	18	18
F12	Dokumentation des Informationssicherheitsziels (ISO/IEC 27001 6.2)	24	24	12
F14	Dokumentation von Audits und Managementbewertungen (ISO/IEC 27001 9.2, 9.3)	18	9	9
QV6	Import/Export GSTOOL	6	6	0
QV9	Importfunktion für IT-Grundschutzkatalog und Referenzierung	6	6	3
QV11	Vorgefertigte Self-Assessments	6	6	3
QV29	Importfunktion für ISO-Normentexte	12	12	0
$\sum$		282	273	225

Tabelle 5.4: Analysierte Kriterien potentieller Dokumentationstools Teil 1

ID	Anforderung	verinice	opus-i	ISIS12
User Experience und Benutzerfreundlichkeit				
F3	Zuweisung von Zuständigkeiten und Bekanntmachung von Rollenzuweisungen/Benutzerverwaltung (ISO/IEC 27001 5.3)	18	18	18
F13	Dokumentenlenkung (ISO/IEC 27001 7.5)	18	18	9
F15	Unterstützung eines kontinuierlichen Verbesserungsprozesses (ISO/IEC 27001 4.4)	24	24	24
F17	Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen	0	18	9
NF1	Performanz	9	9	18
F18	Modellierung und Verwaltung komplexer IT-Verbünde	18	18	9
F19	Konzeption der Struktur anhand vorhandener Inhalte	0	0	0
NF2	Verlässlichkeit	18	9	18
QV23	Unterstützung mehrerer Anwendungsbereiche/Scopes	6	0	0
QV21	Netzwerkfähigkeit	18	18	18
QV18	Unterstützung mehrerer Sprachen	12	0	0
$\sum$		141	132	123
Risikomanagement-Funktionalitäten				
QV28	Schutzbedarfsmatrix	18	18	0
QV26	Vererbungsmechanismen für Schutzbedarf	12	12	0
QV24	Ergänzende Maßnahmen	18	18	18
QV25	Unterstützung klassischer Bedrohungs- und Risikoanalysen	18	18	18
$\sum$		66	66	36
Reporting				
QV31	Microsoft Office Kompatibilität	18	18	0
QV32	Visuelle Darstellung von Status- und Umsetzungsständen	6	12	12
QV33	Konfiguration/Filtermöglichkeiten der Reportingausgabe	12	12	0
$\sum$		36	42	12
$\sum$		567	549	414

Tabelle 5.5: Analysierte Kriterien potentieller Dokumentationstools Teil 2

6 Konzeption eines ISMS-Informationsmodells

In diesem Kapitel wird die Konzeption eines geeigneten ISMS-Informations- und Datenmodells dargestellt. Dabei werden die Erkenntnisse aus dem vorangegangenen Vergleich unterschiedlicher Dokumentationstools (vgl. Abschnitt 5.2) zu einer universellen Grundstruktur zusammengeführt. Grundvoraussetzung stellt die Festlegung einer sinnvollen und zweckmäßigen Basis dar, die in der Lage ist, die Mindestanforderungen aus ISO/IEC 27001 zu erfüllen ohne dabei unnötigen Dokumentationsaufwand zu verursachen. Ein solches grundständiges Informations- und Datenmodell stellt den Aufbau eines ISMS ohne die Abhängigkeit an ein konkretes Dokumentationstool dar, wodurch es implementierungsunabhängig als Orientierungshilfe einer Dokumentation des Anhangs A der ISO/IEC 27001 genutzt werden kann.

6.1 Abgeleitete Informationsmodelle bereits existenter Dokumentationstools

Nach der Analyse von am Markt erhältlichen Dokumentationstools im Bereich des Informationssicherheitsmanagements in Kapitel 5.2 war es möglich, durch die Nutzung der Tools und Implementierung eines fiktiven Szenarios eine Art Informationsmodell mit Hilfe des optischen Feedbacks abzuleiten.

Eine solche Skizze sollte Aufschluss darüber geben, welche Beziehungen und Klassen bei der Dokumentation eines ISMS sinnvoll und zu berücksichtigen wären. Darüber hinaus ist es ebenfalls interessant zu analysieren, welche unterschiedlichen Ansätze durch die Softwareentwickler im Zusammenhang mit der Nutzerführung gewählt wurden. Da alle Tools den Anspruch besitzen, eine möglichst hohe Normkonformität zu ermöglichen, obwohl ISO/IEC-27001 offiziell keine konkreten Attribute oder Leitfäden zur Dokumentation eines ISMS vorgibt, besteht die Möglichkeit des Einsatzes unterschiedlicher Implementierungsansätze.

6.1.1 Informationsmodell von verinice.

Abbildung 6.1 stellt ein durch die Nutzung abgeleitetes Informationsmodell der Software verinice. dar. Bereits auf den ersten Blick ist ersichtlich, dass in verinice. die Maßnahme (Control) zu einem Schlüsselelement der zugrunde liegenden Dokumentation erhoben wurde. So haben Controls durch sog. Control-Level eine direkte Auswirkung auf die Schutzziele und stehen dabei nur sekundär mit dem Information-Asset und dem zugehörigen Risikomanagementprozess in Beziehung. Eine distinktive Eigenschaft von verinice. ist es zudem, konkrete Szenarien festzulegen, die durch Schwachstellen und Bedrohungen definiert und durch eine Eintrittswahrscheinlichkeit entsprechende Relevanz erhalten (Abschnitt 2.2.4). Ein solches Szenario übt somit einen Einfluss auf das Informationasset aus.

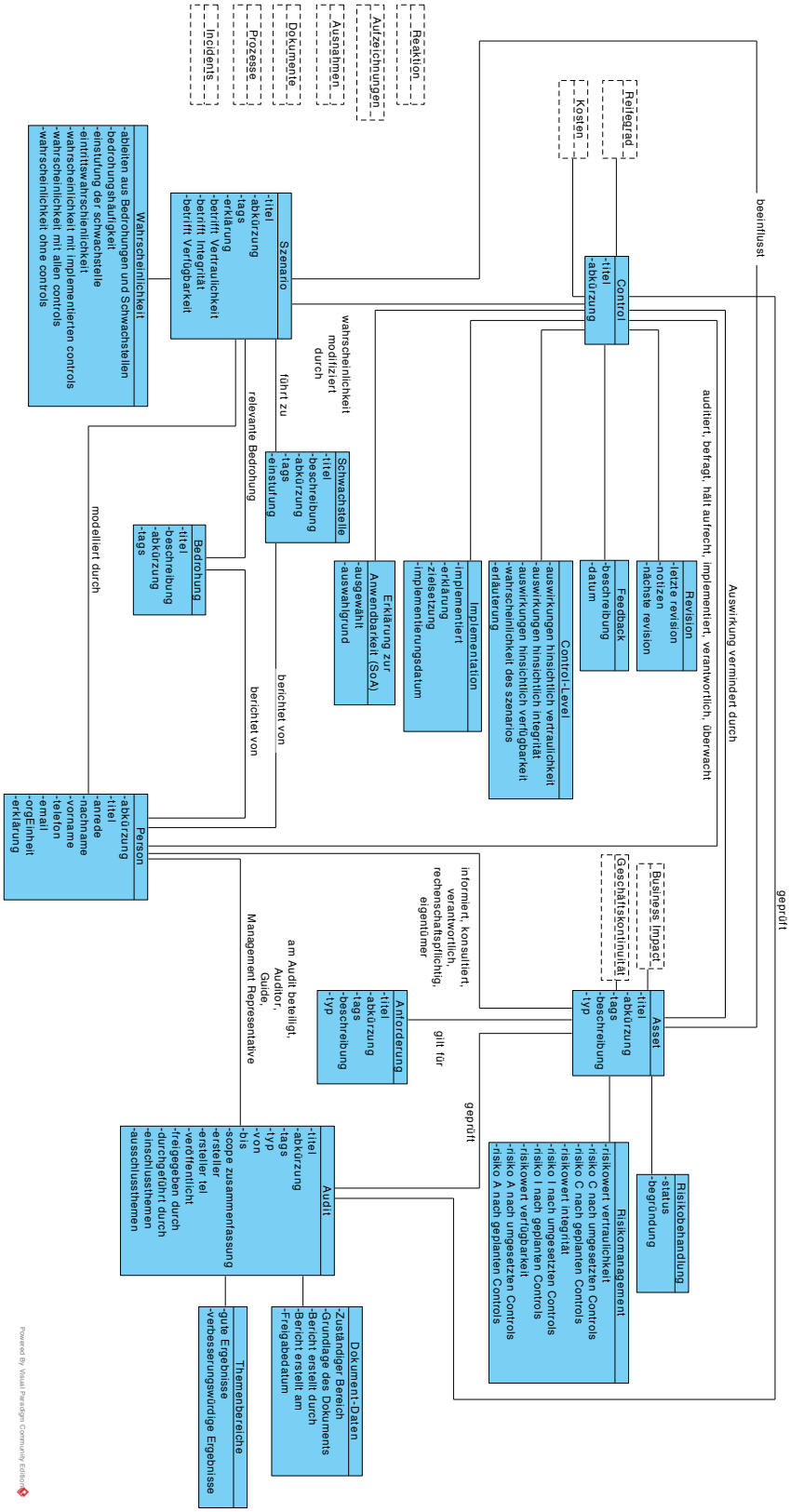


Abbildung 6.1: Informationsmodell der Objektklassen in *Vernice*.

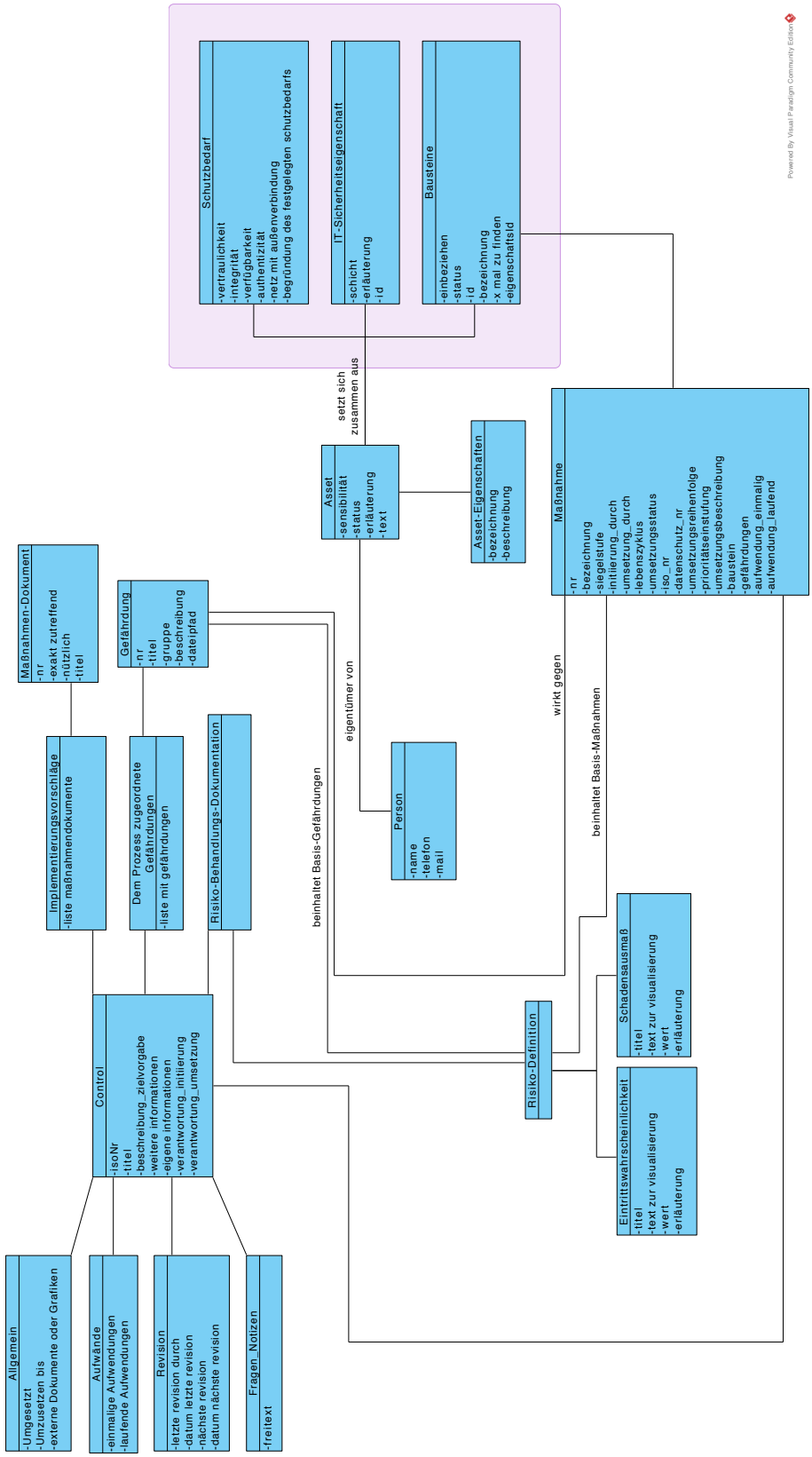


Abbildung 6.2: Informationsmodell der Objektklassen in opus-i

6.1.2 Informationsmodell von opus-i

Das Informationsmodell von opus-i unterscheidet sich von dem Informationsmodell von verinice. Die Kernkomponenten Control, Maßnahme und Information-Asset sind abgebildet, doch deren Beziehungen untereinander sind etwas geschachtelter. Die Gefährdung, die eine Art Äquivalent zur vorhergehenden Klasse „Szenario“ darstellt, ist in diesem Fall über einer Klasse „Risiko-Definition“ mit der Eintrittswahrscheinlichkeit und dem Schadensausmaß verbunden. Auch die Zusammensetzung des Information-Assets aus Schutzbedarf und Bausteinen sind Indikatoren dafür, dass sich opus-i näher am BSI-Grundschutz als an der ISO/IEC 27001 orientiert [KRS13].

6.2 Mindestanforderungen der ISO/IEC 27001

Die ISO/IEC 27001 [Int15a] beschreibt, wie in Kapitel 2.2.1 aufgezeigt, normative Mindestanforderungen an ein ISMS. Die Inhalte der Mindestanforderungen sind organisatorischer Natur und dienen dazu, die Gestaltung, Lenkung und Entwicklung eines zweckorientierten Systems zu unterstützen. Nachstehend werden typische ISMS-Richtlinien beschrieben, die beispielhaft die Mindestanforderungen der Norm abzudecken vermögen.

6.2.1 Informationssicherheits-Leitlinie

Die Informationssicherheits-Leitlinie ist eine übergeordnete Richtlinie, die den Geltungsbereich des ISMS und alle dazugehörigen Eckdaten festlegt.

Im ersten Schritt zur Herstellung eines ISMS verlangt die Norm nach der Festlegung des Geltungsbereichs, also die Definition welche konkreten Geschäftprozesse von dem ISMS eingeschlossen werden und welche nicht. Hierbei unterscheidet die Norm [Int15a] zwischen *externen Themen* und *internen Themen*. Externe Themen umfassen beispielsweise politische oder branchenspezifische Themen, die Einfluss auf das organisationseigene ISMS nehmen können. Interne Themen hingegen spiegeln sich im Bezug auf Mitarbeiter (Kultur, Sprache, ...) bzw. Abhängigkeiten aufgrund von Organisationsstandorte (Konzernteil/Eigenständigkeit, National/International, ...) wieder. Weiter müssen Schnittstellen und Abhängigkeiten zwischen Tätigkeiten mit Bezug zum ISMS, die von der Organisation selbst durchgeführt werden, und Tätigkeiten, die von anderen Organisationen durchgeführt werden, berücksichtigt werden [Int15a].

Die oberste Leitung (Vorstand/Geschäftsführung) muss Verpflichtung für die Planung, Umsetzung, Prüfung und Verbesserung des ISMS übernehmen [Int15a]. Dazu zählt die Definition und Sicherstellung einer festgelegten Informationssicherheitspolitik mit zugehörigen Informationssicherheitszielen. Brenner et. al. [BOH+17] beschreiben die Informationssicherheitspolitik als Dokument, dass einen für alle am ISMS beteiligte Personen verbindlichen Charakter besitzt und daher allgemein verständlich formuliert und direkt oder indirekt an alle Betroffenen aktiv kommuniziert werden muss.

6.2.2 Richtlinie zu Rollen, Verantwortlichkeiten und Befugnissen

Die Richtlinie zu Rollen, Verantwortlichkeiten und Befugnissen behandelt die Aufteilung von Verantwortlichkeiten im Zusammenhang mit dem ISMS. Die oberste Leitung muss sicherstel-

len, dass Verantwortlichkeiten und Rollen in Bezug auf die Informationssicherheit festgelegt und bekannt gemacht werden [Int15a].

6.2.3 Richtlinie zum Asset- und Risikomanagement

Die Richtlinie zum Asset- und Risikomanagement legt fest, in welchem Klassifizierungsschema Assets, Risiken und Maßnahmen eingeordnet werden und wie die Maßnahmen innerhalb der Unternehmensprozesse integriert sind. Der Risikomanagementprozess muss darüber hinaus beschrieben werden und eine Informationssicherheitsrisikobeurteilung und Informationssicherheitsrisikobehandlung umfassen. Die Informationssicherheitsrisikobeurteilung umfasst neben der Festlegung von Kriterien zur Risikoakzeptanz [Int15a] auch die Risikomanagementprozesse zur Identifikation, Abschätzung und Bewertung der Risiken (vgl. 2.2.4).

Die Informationssicherheitsrisikobehandlung muss ebenfalls in Form eines dokumentierten Prozesses angemessene Optionen aus den Ergebnissen der Risikobeurteilung bilden [Int15a]. Als Orientierung dient hier ISO/IEC 27001 Anhang A. Die Erstellung der Erklärung zur Anwendbarkeit (vgl. 2.2.5), sollte bestenfalls als separates Dokument ausgelagert werden.

6.2.4 Richtlinie zur Dokumentation von Informationen

Die Richtlinie zur Dokumentation von Informationen legt fest, in welcher Art und Weise Dokumente und Aufzeichnungen hinterlegt und aufbewahrt werden müssen. Der Anwendungsbereich umfasst alle zu dokumentierenden Informationen, die für die Wirksamkeit des ISMS notwendig sind und von der Norm gefordert werden [Int15a]. Ein wichtiger Aspekt ist die Dokumentenlenkung, die bereits in Abschnitt 2.3.4 beschrieben wurde und die Festlegung von Format, Kennzeichnungen und die Implementierung eines regelmäßigen Überprüfungs- und Genehmigungsprozesses (Review) umfasst.

6.2.5 Richtlinie zur Bewertung und Verbesserung der Wirksamkeit des ISMS

Die Richtlinie zur Bewertung und Verbesserung der Wirksamkeit des ISMS definiert die Methode zur Überwachung, Messung, Analyse und Bewertung des ISMS [Int15a]. Es muss eine klare Festlegung über die Art und Weise der Überprüfung vorherrschen, nämlich des Zeitpunkts der Prüfung und Auswertung sowie der Verantwortlichkeiten für Prüfung und Auswertung. Als Prüfungswerkzeug schreibt die Norm ein regelmäßiges internes Audit vor (vgl. 3.2.3), dass durch die Organisation selbst zu organisieren und zu verantworten ist. Neben den internen Audits müssen Managementbewertungen geplant werden, die die Wirksamkeit und Angemessenheit des ISMS gewährleisten. Sämtliche Ergebnisse von Überprüfungsmaßnahmen müssen als dokumentierte Information/als Nachweis aufbewahrt werden.

Sollten bei den Überprüfungsmaßnahmen Nichtkonformitäten festgestellt werden, ist die Organisation verpflichtet, diesen mit entsprechenden Gegenmaßnahmen entgegen zu treten. Bezüglich jeder Nichtkonformität müssen alle Informationen und die jeweils eingeleiteten Korrekturmaßnahmen als Nachweis dokumentiert werden.

6.3 Informationsmodell der Mindestanforderungen aus ISO/IEC 27001

Aus den Mindestanforderungen der ISO/IEC 27001 lässt sich ein Informationsmodell, wie in Abbildung 6.3 aufgezeigt ableiten, das aufzeigt, wie die Zusammenhänge der aus Abschnitt 6.2 benannten Compliance-Richtlinien in Verbindung stehen. Die Richtlinien besitzen einen definierten Anwendungsbereich, der organisationsübergreifend sein kann. Die übergeordnete Informationssicherheits-Leitlinie ist innerhalb des festgelegten Geltungsbereichs des ISMS gültig. Die Informationssicherheitsleitlinie legt wiederum die Grenzen und den Geltungsbereich des ISMS fest wodurch sich je nach organisationsaufbau (Konzern, Standorte, Geschäftsbereiche, ...) unterschiedliche Scopes ergeben. Innerhalb der einzelnen Scopes kommt die individuelle Betrachtung der Informationswerte, Risiken und Schutzmaßnahmen zum tragen, welche im nachstehenden Abschnitt erläutert werden.

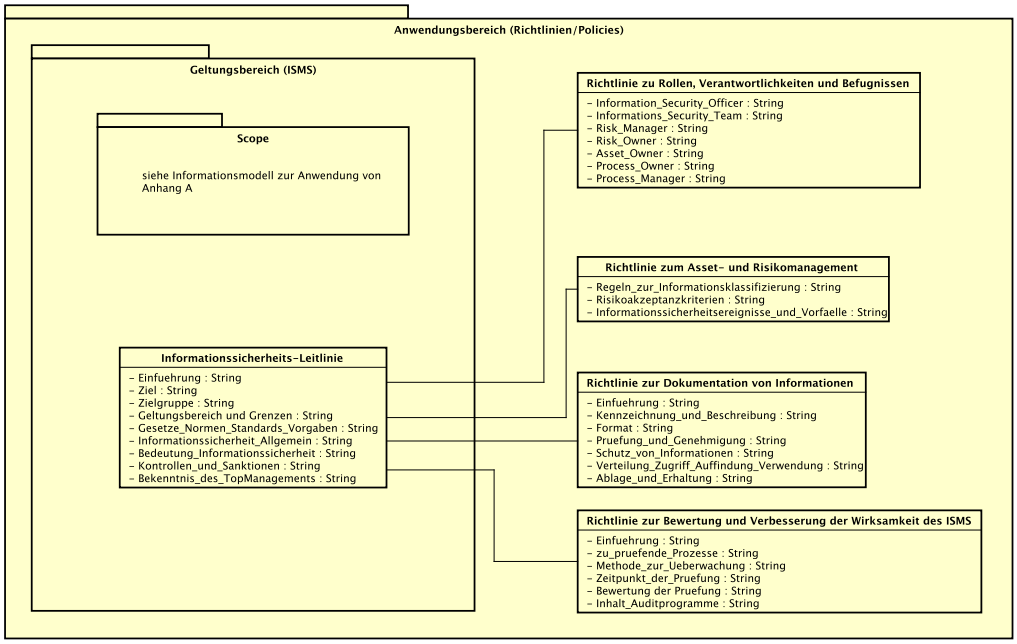


Abbildung 6.3: Informationsmodell - Mindestanforderungen

6.4 Informationsmodell zur Anwendung der Maßnahmen aus ISO/IEC 27001 - Anhang A

In diesem Kapitel wird das ergänzende Informationsmodell in Bezug auf Abschnitt *6 Maßnahmen zum Umgang mit Risiken und Chancen* der ISO/IEC 27001 modelliert. Als Input dienen hierbei die Kriterien der ISO/IEC 27001 (Abschnitt 4.2.1), die aus der Anforderungsanalyse identifizierten Kriterien (Abschnitt 4.3) und die abgeleiteten Dokumentationsmodelle der getesteten Dokumentationstools (Abschnitt 6.1).

6.4.1 Definition von Klassen und Relationen

Neben der konkreten Anforderungen zur Dokumentation bzgl. Dokumentenlenkung (vgl. ISO/IEC 27001 Kapitel 7.5) gilt es nach Kapitel 6.1.1 [Int15a] vor allem Informationswerte, zugehörige Risiken und Maßnahmen zu dokumentieren. Diese sind daher die Basis (vgl. Abbildung 6.4) des Informationsmodells.

Abbildung 6.4: Basis des Informationsmodells

Wird der Informationswert gemäß der Definition aus 2.2.3 innerhalb des abstrakten Informationsmodells 6.4 betrachten, kann festgestellt werden, dass oftmals eine Beziehung zwischen den tatsächlich schützenswerten Informationen und abhängigen Komponenten existiert. So können sich zum Beispiel sensible Informationen auf einem Computersystem befinden, welche physisch von den tatsächlichen Komponenten her austauschbar oder sogar vernachlässigbar wären, aber gegenüber der beinhaltenden Informationen, Schwachstellen und Bedrohungen aufweisen, die es im Zweifel zu behandeln gilt.

Die Schlussfolgerung, dass nicht die Informationswerte selbst, einem bestimmten Risiko ausgesetzt sind, sondern die den Informationswerten zugrunde liegenden *unterstützenden Assets* oder auch *supporting Assets* erscheint logisch. Diese Unterscheidung wird auch im Rahmen der Anforderungsanalyse (vgl. F7) und der DIN ISO/IEC 27005:2014-02 (ISO/IEC 27005) ersichtlich und wurde bereits in Abschnitt 2.2.3 erörtert.

Um jedoch dem Managementcharakter der Norm, also dem aktiven Beitrag zur Steuerung und Gestaltung von Unternehmensprozessen gerecht zu werden, wird das Modell so konzipiert, dass zwar Abhängigkeiten zwischen Informationswerten und IT-Assets (Hardware, Software, ...) bestehen aber lediglich das Risiko im Zusammenhang mit tatsächlichen Informationen als Informationswert betrachtet wird, wie in Abbildung 6.5 dargestellt wurde.

Die Ermittlung von Risiken findet innerhalb der Risikoanalyse statt (vgl. 2.2.6). Die Risikoanalyse resultiert aus Kriterien zur Risikobewertung (Abschnitt 2.2.4) wonach in der Regel bei entsprechender Risikosignifikanz eine oder mehrere Risikobehandlungsmaßnahmen eingeführt werden. Wie in Abschnitt 2.2.2 beschrieben, kommt es bei Übersetzungen von Begrifflichkeiten der internationalen Norm zu Überschneidungen, wodurch bestimmte Begriffe zwar gleich benannt sind aber nicht das Gleiche bedeuten. So beispielsweise auch bei dem Begriff der Maßnahme, der von dem englischen Begriff der *Control* stammt. Aus diesem Grund ist es wichtig, zwischen konkreten Risikobehandlungsmaßnahmen und den Maßnahmen bzw. Controls aus ISO/IEC 27001 zu differenzieren. Das Informationsmodell in Abbildung 6.5 stellt eine dahingehende Ergänzung dar.

Zur besseren Unterteilung der Klassen wurden diese zusätzlich noch in übergeordnete Pakete (AssetInventory, Risikomanagement, SoA) eingeordnet, welche die Klassen thematisch voneinander abgrenzen.

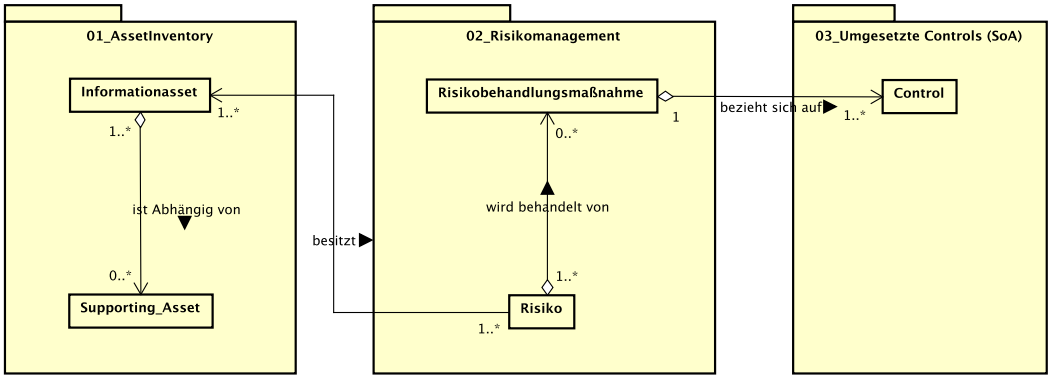


Abbildung 6.5: Ergänzung zur Basis des Informationsmodells

6.4.2 Definition von Attributen und Attributwerten

Nachdem die Basis für ein Informationsmodell geschaffen ist (vgl. Abbildung 6.5), werden die einzelnen Klassen mit Attributen ausgestattet. Die Attributauswahl sollte zu Beginn minimalisiert werden, da das Informationsmodell durch weitere Hilfsklassen und Ergänzung von beispielsweise Vererbungsbeziehungen besonders schnell anwachsen kann. Weiter muss der Anwendungsbereich der ISMS-Dokumentation berücksichtigt werden, damit möglichst wenig bis keinerlei redundante Informationen mit Dokumentationen anderer Managementsysteme existieren und die gewünschte Zweckmäßigkeit gewährleistet werden kann.

Asset-Inventory

Wichtige Inputs für das Risikomanagement im Zusammenhang mit Information-Assets stellen die Attribute *Wertigkeit* und *Schutzbedarf* dar. Bezüglich der Wertigkeit können Informationswerte unterschiedliche Kritikalitäten aufweisen und im Zusammenhang mit Informationssicherheitsvorfällen unterschiedliche Einflüsse auf die Organisation nach sich ziehen.

Um die Wertigkeit einschätzen zu können, sollten folgende Parameter bestimmt werden:

- Qualitativer Arbeitsaufwand bei Ausfall des Assets
- Finanzieller Aufwand für Wiederherstellung des Assets
- Zeitliche Beeinträchtigung der Servicefähigkeit bei Ausfall des Assets

Optional kann der Reputationsschaden bei Verlust eines speziellen Assets noch als zusätzlicher Faktor bei der Wertigkeit betrachtet werden.

Neben der Wertigkeit gilt es, den Schutzbedarf anhand der aus Abschnitt 2.1.3 beschriebenen Informationssicherheitsziele zu bestimmen und eine sinnvolle Abstufung zu finden.

Für das Asset-Inventory ergibt sich somit der Aufbau aus Abbildung 6.6.

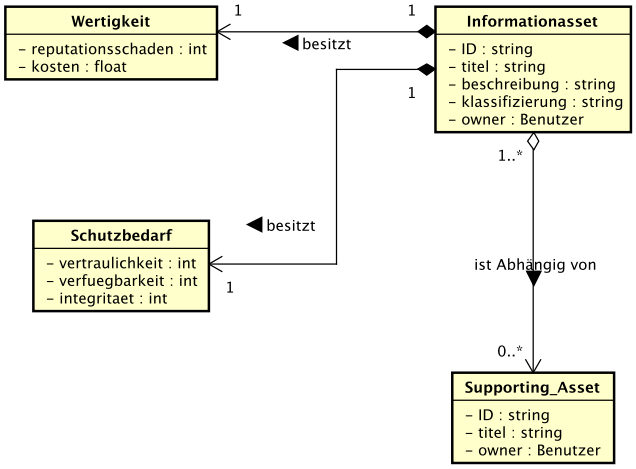


Abbildung 6.6: Asset-Inventory Attribute

Risikomanagement

Das Objekt des Risikos wird wie in Abschnitt 2.2.4 beschrieben, durch Bedrohungen und Schwachstellen definiert. Daher muss die Kombination dieser Eigenschaften zwingend zur Klasse des Risikos gehören. Im zweiten Schritt der Risikoeinschätzung muss das Risiko bewertet werden. Dies geschieht über die Einschätzung der Eintrittswahrscheinlichkeit und des Schadenspotentials, sodass diese ebenfalls wichtige Attribute der Risiko-Klasse darstellen.

Risikobehandlungsmaßnahmen stellen konkrete Schutzmaßnahmen dar, die eine explizite Auswirkung auf die Eintrittswahrscheinlichkeit und dem Schadenspotential von Risiken haben können. Allerdings können Schutzmaßnahmen auch weitere Risiken oder andere nachteilige Effekte nach sich ziehen. Abbildung 6.7 zeigt die konkreten Attribute der behandelten Klassen.

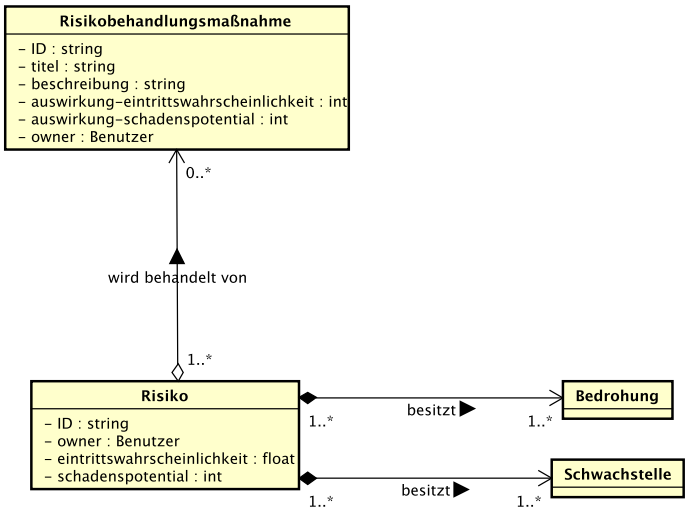


Abbildung 6.7: Risikomanagement - Attribute

Umgesetzte Controls

Bei Controls handelt es sich um individuelle Maßnahmen und Maßnahmenziele aus dem ISO/IEC 27001 Anhang A. Um die Anforderungen eines Zertifizierungsaudits erfüllen zu können, muss die Organisation nachweisen, dass sie sämtliche Maßnahmen des Anhangs A innerhalb einer Erklärung zur Anwendbarkeit aufführt und die Umsetzung oder Nicht-Umsetzung entsprechend begründet.

Eine einfache Klassifizierung sollte die meist verwendeten Begründungen umfassen:

- Gesetzliche Vorgaben
- Vertragliche Vorgaben
- Risikobehandlung
- Best Practise

Um die Umsetzung des Controls auch nachweisbar belegen zu können, bietet sich die Referenzierung auf zugehörige Dokumente und Aufzeichnungen an:

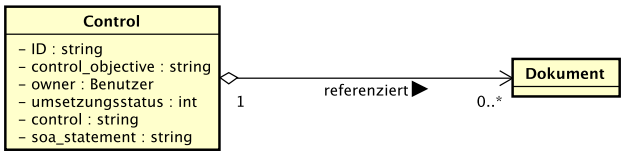


Abbildung 6.8: Umgesetzte Controls (SoA) - Attribute

6.4.3 Finales Dokumentationsmodell

Abbildung 6.9 stellt zusammenfassend das finale Informationsmodell mit allen zugehörigen Klassen und Attributen dar.

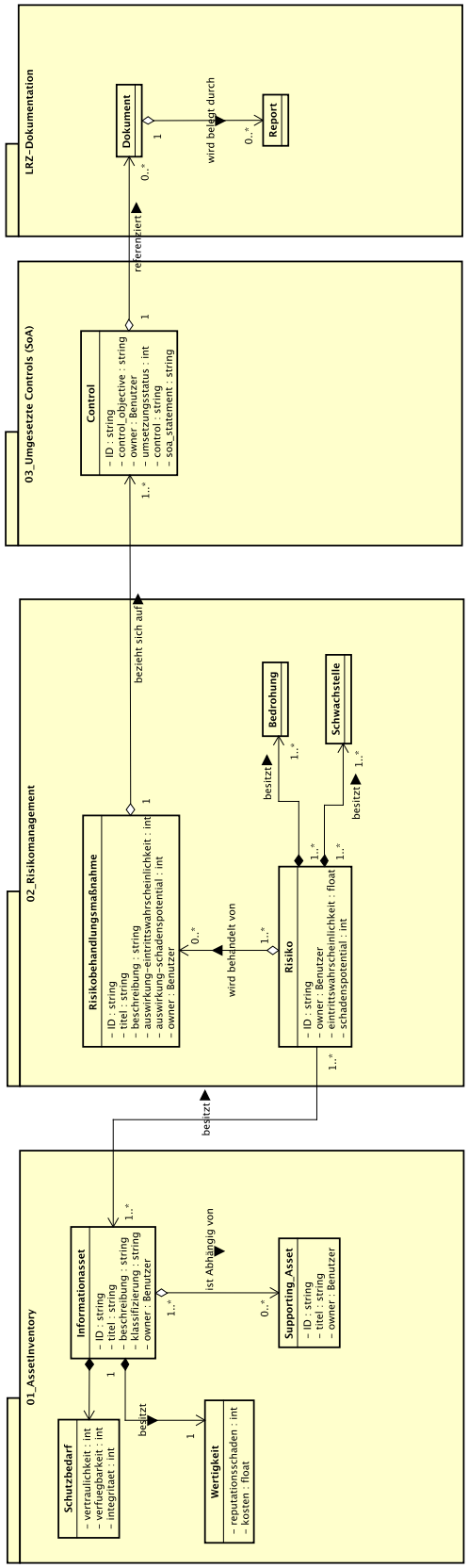


Abbildung 6.9: Finales Informationsmodell

6.5 Zusammenfassung

Zunächst wurden anhand der Mindestanforderungen aus der ISO/IEC 27001 mögliche Vorgaben von Richtlinien bereitgestellt, die die Rahmenbedingungen des einzuführenden ISMS vorgeben. In Kapitel *6 Maßnahmen zum Umgang mit Risiken und Chancen* wird die Dokumentation von Risiken im Zusammenhang mit Informationswerten und den Controls aus dem ebenfalls normativen Anhang A der ISO/IEC 27001 gefordert.

Danach wurden die Erkenntnisse aus dem Vergleich der Dokumentationstools verwendet, um ein exemplarisches Informationsmodell abzuleiten, welches im Zusammenhang mit den Mindestanforderungen der Norm ein allgemeingültiges Informationsmodell bildet. Im Zuge der Entwicklung des Informationsmodells wurden den betrachteten Klassen zur besseren Übersicht eine minimale notwendige Anzahl an Attributen zugewiesen.

Die Implementierung des aufgezeigten Informationsmodells findet im nächsten Kapitel statt.

7 Prototypische Implementierung des entwickelten Informationsmodells

Die prototypische Implementierung des Informationsmodells innerhalb des Kollaborationstools Confluence des Unternehmens Atlassian mit Sitz in London und Sidney wird nachstehend beschrieben. Atlassian Confluence wird seit Mitte 2015 überwiegend im Bereich der Dokumentation des IT-Service Managements am LRZ eingesetzt und kontinuierlich mit Inhalten ergänzt. Aus diesem Grund bieten sich die Schnittstellen zu bereits vorhandenen Inhalten an, um diese innerhalb der zu etablierenden ISMS-Dokumentation entsprechend zu referenzieren.

Im ersten Abschnitt dieses Kapitels werden die Funktionen von Confluence vorgestellt. Die Analyse findet in Form der bereits vorangegangenen Untersuchung von ISMS-Dokumentationstools statt. Es ist zu erwarten, dass ein allgemeines Dokumentationstool gegenüber spezialisierter Anwendungen im Bereich der ISO/IEC 27001 funktional unterlegen ist. Bei der Implementierung wird sich herausstellen, ob das konzeptionierte Informationsmodell dem Anspruch eines implementierungsunabhängigen Ansatzes gerecht wird und sich dennoch die Mindestanforderungen der ISO/IEC 27001 vollständig abbilden lassen.

Der zweite Abschnitt behandelt die Implementierung innerhalb des IT-Dienstes *Sync+Share* am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften. Dabei werden die Dokumentationsstruktur und die Vergabe von Attributwerten anhand konkreter Beispiele dargestellt.

7.1 Funktionsumfang von Confluence

7.1.1 Allgemeine Informationen

Confluence ist eines der Kollaborationstools des in Australien gegründeten Unternehmens Atlassian und wurde 2003 mit dem Ziel, eine einfache Enterprise-Wissensmanagementlösung zu liefern, entwickelt. Dabei setzt Atlassian den Fokus auf Zusammenarbeit und Teamwork und stellt mit Confluence ein flexibles Tool zur Sicherung von Informationen auf Webseiten zur Verfügung. Durch die Ähnlichkeit der Seitenstruktur mit marktüblichen Webblogs ist es Nutzern möglich, sich ohne besondere Vorkenntnisse in dem Tool zurechtzufinden. Ähnlich wie das im Vorfeld getestete ISIS12, wird Confluence hauptsächlich als Web-Applikation angeboten.

Die nachfolgende Analyse bezieht sich auf die am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften eingesetzte Version 6.1.3 vom 27.05.2017.

7.1.2 Systemkompatibilität

Confluence ist in der Programmiersprache Java entwickelt worden und bleibt damit erneut plattformunabhängig. Die Serverinstallationsdateien existieren für die Desktop-Betriebsysteme Linux und Microsoft Windows. Vorausgesetzt wird das Java Runtime Environment (JRE) in der Version 1.8 oder das korrespondierende Java Development Kit (JDK). Darüber hinaus wird die Ausführung in Docker-Containern unterstützt. Bei der Installation wird deutlich, dass sich die Entwickler bei den Java Enterprise Bibliotheken und Tools bedient haben. Eine Nutzung der Java Enterprise Platform (J2EE) ist naheliegend, da Confluence lediglich als Webanwendung innerhalb eines Apache Tomcat Webservers ausgeführt wird und somit prädestiniert für die Nutzung von Java Servlets und Java ServerPages ist. Aufgrund der Java-Implementierung entsteht eine ähnliche Speicherproblematik wie bei verinice. So empfiehlt Atlassian auf seiner Homepage minimal sechs Gigabyte an Arbeitsspeicher.

Die Webseite an sich ist responsive und wird daher auch im Browser als Webapp dargestellt. Hier sind jedoch nicht alle Funktionen wie auf der Desktop-Version enthalten, wodurch die Bedienbarkeit eingeschränkt ist. Ein ähnliches Bild zeichnet sich auch bei der Nutzung der App ab. Die App ist derzeit nicht mit der selbstgehosteten Serverversion kompatibel, die am LRZ eingesetzt wird.

7.1.3 Lizenzierungsmodelle

Das Lizenzierungsmodell von Atlassian sieht zwei unterschiedliche Hosting-Möglichkeiten vor: Cloud und Self-Hosted. Bei der Cloudlösung zahlen Kunden im Rahmen eines monatlichen Endgelds für die Nutzungslizenz der Software. Die Kosten steigen je nach Anzahl der Nutzer an. Die sog. *Starterlizenz* umfasst zehn Nutzer für zehn USD pro Monat, wodurch der Einstieg vergleichsweise preiswert gestaltet ist. Bei steigender Nutzerzahl steigt dieser jedoch schnell in den drei- bis vierstelligen Bereich, wodurch ab 100 Nutzer bereits 300 USD und bei maximal 2000 Nutzern, 1000 USD pro Monat zu entrichten sind.

Das Self-Hosted-Paket ermöglicht auf der anderen Seite aufgrund des self-deployments höhere Kontrolle über die Daten. Allerdings steigt somit auch das Ausfallrisiko, da man sich mit der zugrunde liegenden Server-Infrastruktur und der Bereitstellung und Absicherung des Webzugriffs ebenfalls auseinandersetzen und beispielsweise für regelmäßige Datensicherungen die Verantwortung übernehmen muss. Da gerade für Unternehmen mit mehr als 2000 Nutzern lediglich für die Self-Hosted-Option entsprechende Lizenzen zur Verfügung stehen, versucht Atlassian durch Wartungsangebote für einen Zeitraum von bis zu 12 Monaten und einer Unterstützung bei der Wiederherstellung korrupter Daten die Attraktivität dieser Angebote zu steigern.

Für Kunden, die sich noch nicht endgültig entschieden haben, ob das Tool für sie eine sinnvolle Option darstellt, stellt Atlassian eine 30 Tage Testversion zur Verfügung.

7.1.4 Funktionsumfang

Confluence zeichnet sich durch eine hohe Flexibilität und Erweiterbarkeit aus, die durch Module (sog. *Makros*) ermöglicht wird. Nach dem Installationvorgang stehen bereits mehrere Makros, die zum Beispiel die Darstellung von Diagrammen oder Code-Blöcken ermöglichen

bereit. Um die Übersicht über verfügbare Makros zu gewährleisten, stellt Atlassian einen gesonderten Marketplace für sämtliche seiner Softwareprodukte zur Verfügung. Alleine die Confluence-Makros umfassen mit 800 Einträgen bereits einen Großteil des Marketplace.

Der grundsätzliche Workflow gestaltet sich so, dass registrierten Nutzern ein persönlicher Arbeitsbereich (sog. *Space*) zugeordnet wird, indem bereits Seiten und Unterseiten erstellt werden können. Um dem kollaborativen Nutzen Rechnung zu tragen, können solche Arbeitsbereiche auch zwischen mehreren Nutzern geteilt und veröffentlicht werden. Die Bearbeitung solcher Seiten findet in Form eines WYSIWYG-Editors (*„What You See Is What You Get“*) statt und unterscheidet sich nur minimal von gängigen Texteditoren. Der Editor umfasst, wie in Abbildung 7.1 dargestellt, die Standard Formatierungstools sowie Tabellen, Listen und Zentrierungsmöglichkeiten. Für einfache Seiten, lassen sich über Makros auch Microsoft Office Dokumente (Word- oder Excel-Dokumente) importieren. Für komplexere Inhalte wie Grafiken, Videos oder Diagramme, lassen sich entweder ein Makro zu Umschaltung zwischen Text und HTML oder Makros mit entsprechendem Frontend nutzen.

Mit ihrem Seitentitel erhalten Seiten selbst eine eindeutige ID, die nur einmal innerhalb gewählten Space existieren definiert werden darf. Diese Eigenschaft muss bei dem Aufbau einer Dokumentationshierarchie beachtet werden, um Kollisionen zu vermeiden. Eine weitere Differenzierung lässt das Tool durch einen hierarchischen Aufbau zwischen Seiten und Unterseiten und dem Hinzufügen von sog. *Tags* zu. Diese Tags werden im Zusammenhang mit bestimmten Makros wie den Seiteneigenschaftsberichten notwendig, da diese ermöglichen gezielt auf Informationen einer Seite von einer anderen Seite aus zuzugreifen.

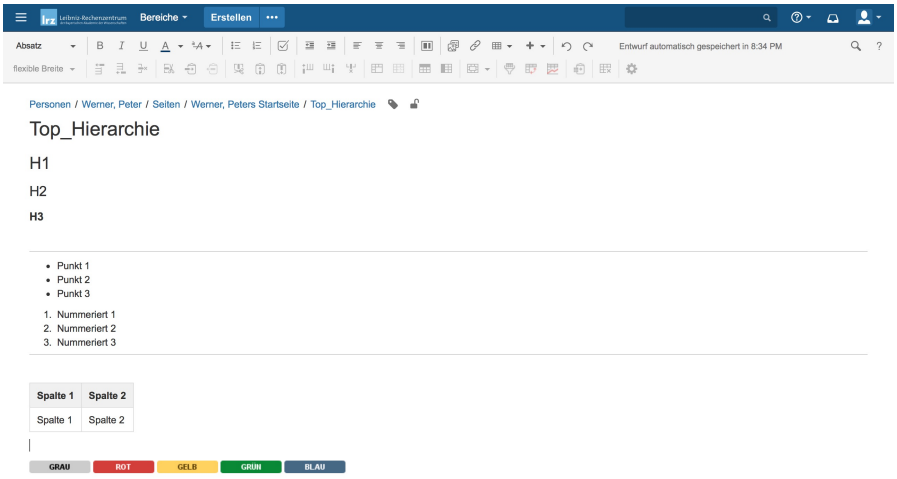


Abbildung 7.1: Confluence - Editor

Zu den Kernfunktionalitäten zählen ebenfalls eine granulare Benutzerverwaltung, mit der der Zugriff auf einzelne Spaces konfiguriert werden kann, sowie eine Kommentar- und Suchfunktion.

7.1.5 Dateneingabe und -persistenz

Die Datenhaltung findet in einem relationalen Datenbanksystem statt. Ähnlich wie bei opusi, werden mehrere Datenbanksysteme wie PostgreSQL, MySQL, Oracle DB und Microsoft SQL Server unterstützt. Die Testversion von Confluence nutzt anders als die Produktivsysteme das Open Source JavaSQL-Datenbanksystem *H2*.

Mit jedem Speichervorgang pro Seite wird intern eine neue Version angelegt und sämtliche vorangegangenen Änderungen gesichert. Dadurch ist es möglich, über einen gewissen Zeitraum hinweg, sämtliche Versionen einer Seite nachzuvollziehen und Änderungen im Zweifel schnell wieder zurücksetzen zu können.

7.1.6 Benutzererfahrung und Benutzerfreundlichkeit

Die Kompatibilität ist auf allen Betriebssystemen gegeben. Als Webanwendung wird lediglich ein aktueller Browser vorausgesetzt, der in der Lage sein muss, JavaScript auszuführen. Die Webanwendung reagiert, abhängig vom zugrunde liegenden Serversystem und der Performance auf Clientseite, entsprechend schnell. Für mobile Endgeräte liefert Confluence ein Responsive-Design, dass sich an unterschiedlichen Displaygrößen oder der Bildschirmorientierung des Endgeräts anpasst.

7.1.7 Zusammenfassung

Atlassian stellt mit Confluence eine Plattform zur Verfügung, die durch anderen angebotenen Softwarepakete wie zum Beispiel ServiceDesk und der Projektplanungssoftware JIRA sinnvoll ergänzt wird. Darüber hinaus stellt sich die webbasierte Nutzeroberfläche aufgrund der Plattformunabhängigkeit als besonders zukunftsorientiert dar, da eine einheitliche Schnittstelle auf sämtlichen Endgeräten bereitgestellt werden kann und zusätzlicher Arbeitsaufwand durch Installation von Softwarepaketen entfällt. Weiterhin fördert Atlassian durch Zurverfügungstellung eines offenen Marktplatzes für Makros die stetige Weiterentwicklung der Software, nicht nur durch Eigenentwicklung sondern auch durch Drittentwickler.

7.2 Implementierung der Inhalte anhand von Sync+Share

Die Implementierung der ISMS-Dokumentation basiert auf der zuvor entwickelten Modellierung eines Informationsmodells. Durch den Einsatz innerhalb einer individuellen Organisationsstruktur kann es im Verlauf der Entwicklung zu kleineren Änderungen in der Implementierung kommen, die entsprechend begründet werden müssen. Die Aufteilung der drei Kernbereich Asset-Inventory, Risikomanagement und Controls bleibt bestehen.

Die Grundlage für die Einschätzung von Werten (Schutzziele, Schadenspotential, ...) findet anhand des dienstspezifischen Sicherheitskonzeptes des Dienstes Sync+Share in der Version 1.1 vom 09.09.2015 statt.

7.2.1 Asset-Inventory

Das Asset-Inventory hält sämtliche Informationassets und Supporting Assets bereit. Im Kontext des LRZ existiert bereits eine gut dokumentierte CMDB, die sämtliche Supporting As-

sets in detailierter Form aufführt. So kann im ersten Schritt auf eine zusätzliche Aufführung innerhalb der ISMS-Dokumentation verzichtet und der Fokus auf die zu betrachtenden Informationswerte gelegt werden.

Die Einordnung der Schutzziele findet anhand einer Matrix (vgl. Abbildung 7.2) in vier unterschiedliche Stufen statt.

Klassifikation		Vertraulichkeit	Integrität	Verfügbarkeit
0	UNBEDEUTEND	ÖFFENTLICH	INFORMATIONEN OHNE GESCHÄFTSRELEVANZ	NUR UNTERSTÜTZENDE FUNKTION (JEDERZEIT ERSETZBAR)
1	NORMAL	INTERN	SICHTPRÜFUNG BEI EINGABE AUSREICHEND; BEARBEITUNG JEDERZEIT MÖGLICH	MEHRERE TAGE AUSFALL UNKRITISCH
2	HOCH	VERTRAULICH	PLAUSIBILITÄTSPRÜFUNG BEI INBETRIEBNAHME	MEHRERE STUNDEN AUSFALL UNKRITISCH
3	SEHR HOCH	STRENG VERTRAULICH	ELEKTRONISCHE SIGNATUR/VERSCHLÜSSELTE ÜBERTRAGUNG	KRITISCHE AUSWIRKUNG BEI WENIGEN MINUTEN AUSFALL

Abbildung 7.2: Informationasset - Klassifizierung von Schutzzielen

Im Zusammenhang mit den individuellen Schutzzielen, muss insbesondere das Schadenspotential betrachtet werden. Das Schadenspotential dient ergänzend zu den Schutzzielen dazu, die Auswirkungen bezüglich der Schutzziele im Falle eines Risikoeintritts abschätzen zu können. Das Schadenspotential wird ebenfalls in vier Klassen eingeteilt und steht im Zusammenhang mit der Risikoabschätzung, der sich in Abschnitt 7.2.2 gewidmet wird.

Das Schadenspotential dient in Kombination mit der Wertigkeit eines Assets dazu, die individuellen Informationassets voneinander differenzieren zu können. So stellen im Falle eines Ausfalls des Informationassets potentielle Reputationsschäden aber auch die Kosten zur Wiederherstellung des Informationassets wichtige Parameter dar, die die Wertigkeit eines individuellen Informationassets definieren. Die Unterteilung in vier Stufen ist in Abbildung 7.3 dargestellt.

Klassifikation		Reputationsschäden	Wert der Infrastruktur
0	UNBEDEUTEND	kaum wahrnehmbarer Schaden	< 10.000 Euro
1	SPÜRBAR	kurzzeitig in der lokalen Region wahrnehmbar	< 100.000 Euro
2	KRITISCH	überregionale Berichterstattung	< 1.000.000 Euro
3	KATASTROPHAL	permanenter Reputationsschaden	> 1.000.000 Euro

Abbildung 7.3: Informationasset - Klassifizierung der Wertigkeit

Im Rahmen des Sync+Share Dienstes ergeben sich folgende relevante Informationassets:

- Personendaten
- Authentifizierungsdaten
- Nutzerdaten

Personendaten

Die Personendaten umfassen allgemeine Informationen bezüglich der Nutzer von Sync+Share. Bei diesen Informationen handelt es sich überwiegend um demographische Informationen wie Name, Kontaktdaten und Lichtbild, die nicht zwingend als streng vertraulich einzustufen sind aber aufgrund der datenschutzrechtlichen Gesetzgebung zumindest vertraulich behandelt werden müssen. Die Integrität der Daten werden durch den Nutzer bestimmt, der innerhalb seiner Profileinstellungen jederzeit Anpassungen vornehmen kann. Da die Informationen hauptsächlich dem informativen Zweck dienen und für die Diensterbringung nicht von Relevanz sind, wird das Verfügbarkeitsziel von mehreren Tagen Ausfall als angemessen erachtet.

Authentifizierungsdaten

Authentifizierungsdaten umfassen Passworthashes, Login-Tokens und den Benutzernamen/E-Mail Adresse der Nutzer von Sync+Share aber auch anderer Dienste, sofern sie innerhalb des selben Datenbanksystems aufbewahrt werden. Das Vertraulichkeitsziel der Daten ist ebenfalls als *Vertraulich* einzustufen. Die Integrität muss durch verschlüsselte Kommunikationsverfahren und Signaturen gewährleistet werden. Das Verfügbarkeitsziel beträgt maximal einige Stunden Ausfall, da ohne Zugriff auf die Authentifizierungsdaten die Diensterbringung nicht mehr möglich ist.

Nutzerdaten

Die Nutzerdaten umfassen individuelle Dateien und Verzeichnisse aktiver Nutzer von Sync+Share. Dem Verfügbarkeitsziel der Nutzerdaten wird ein geringer Wert zugeschrieben, da laut dienstspezifischem Sicherheitskonzept durch lokale Synchronisation eine Beeinträchtigung des Dienstes nicht zwangsläufig den Zugriff auf die Daten beschränkt. Für die Vertraulichkeit ist der Nutzer selbst aufgrund der Sharing-Funktionalität verantwortlich, da er den Zugriff auf die Daten selber bestimmen kann. Die Integrität der Daten besitzt keinerlei ergänzende Geschäftsrelevanz.

7.2.2 Risikomanagement

Das Risikomanagement beinhaltet die Risikoobjekte sowie die zugehörigen Risikobehandlungsmaßnahmen. Das Risiko selbst definiert sich aus Bedrohungen und Schwachstellen, die sich als Listenelemente innerhalb der einzelnen Risikoobjekte gut darstellen lassen und somit keine eigenständigen Unterseiten benötigen. Ergänzend dazu dient eine Beschreibung, in der ein Risikoszenario beschrieben wird, das exemplarisch für den Fall eines Risikoeintritts skizziert wird. Zu beachten sind ebenfalls die definierten Seiteneigenschaften, die den Risikoowner, das Risikoniveau, den Bearbeitungsstatus und die Einstufung aus der Risikobewertung festlegen.

Im Fall des Sync+Share Dienstes und der aus Abschnitt 7.2.1 definierten Informationswerte wurden im Zusammenhang mit dem dienstspezifischen Sicherheitskonzept folgende Risiken identifiziert:

- Datenträgerausfall im Speichersystem

- Missbrauch
- Physische Beeinträchtigung
- Technischer Systemangriff
- Umwelteinfluss (Höhere Gewalt)
- Unbeabsichtigter Systemausfall
- Verlust von Versorgungsdiensten

Um die Relevanz der Auswirkungen eines Risikos in Bezug auf das Schadenspotential innerhalb des Informationsassets miteinander vergleichen zu können, werden für die Bewertung der Auswirkungen neben der qualitativen Klassifizierung boolesche Werte wie *ja* und *nein* gewählt, die Auskunft darüber geben, ob ein gewisses Schutzziel durch das Risiko verletzt oder beeinflusst wird.

Das übergeordnete Risikoniveau, welches sich aus der Eintrittswahrscheinlichkeit und dem Schadenspotential ergibt, wird anhand der sog. Risikomatrix (vgl. Abbildung 7.4) identifiziert.

Eintrittswahrscheinlichkeit/ Schadenspotential	UNWAHRSCHEINLICH 1x in 100 Jahren	NICHT AUSGESCHLOSSEN 1x in 20 Jahren	MÖGLICH 1x in 5 Jahren	HÄUFIG 1x im Jahr
< 10.000 Euro (UNBEDEUTEND)	GERING	GERING	GERING	MITTEL
< 100.000 Euro (SPÜRBAR)	GERING	GERING	MITTEL	HOCH
< 1.000.000 Euro (KRITISCH)	GERING	MITTEL	HOCH	HOCH
> 1.000.000 Euro (KATASTROPHAL)	MITTEL	HOCH	HOCH	HOCH

Abbildung 7.4: Risikomanagement - Risikomatrix/Risikoniveau

Nachstehend werden die Risiken „Datenträgerausfall im Speichersystem“ und „Technischer Systemangriff“ exemplarisch näher betrachtet.

Datenträgerausfall im Speichersystem

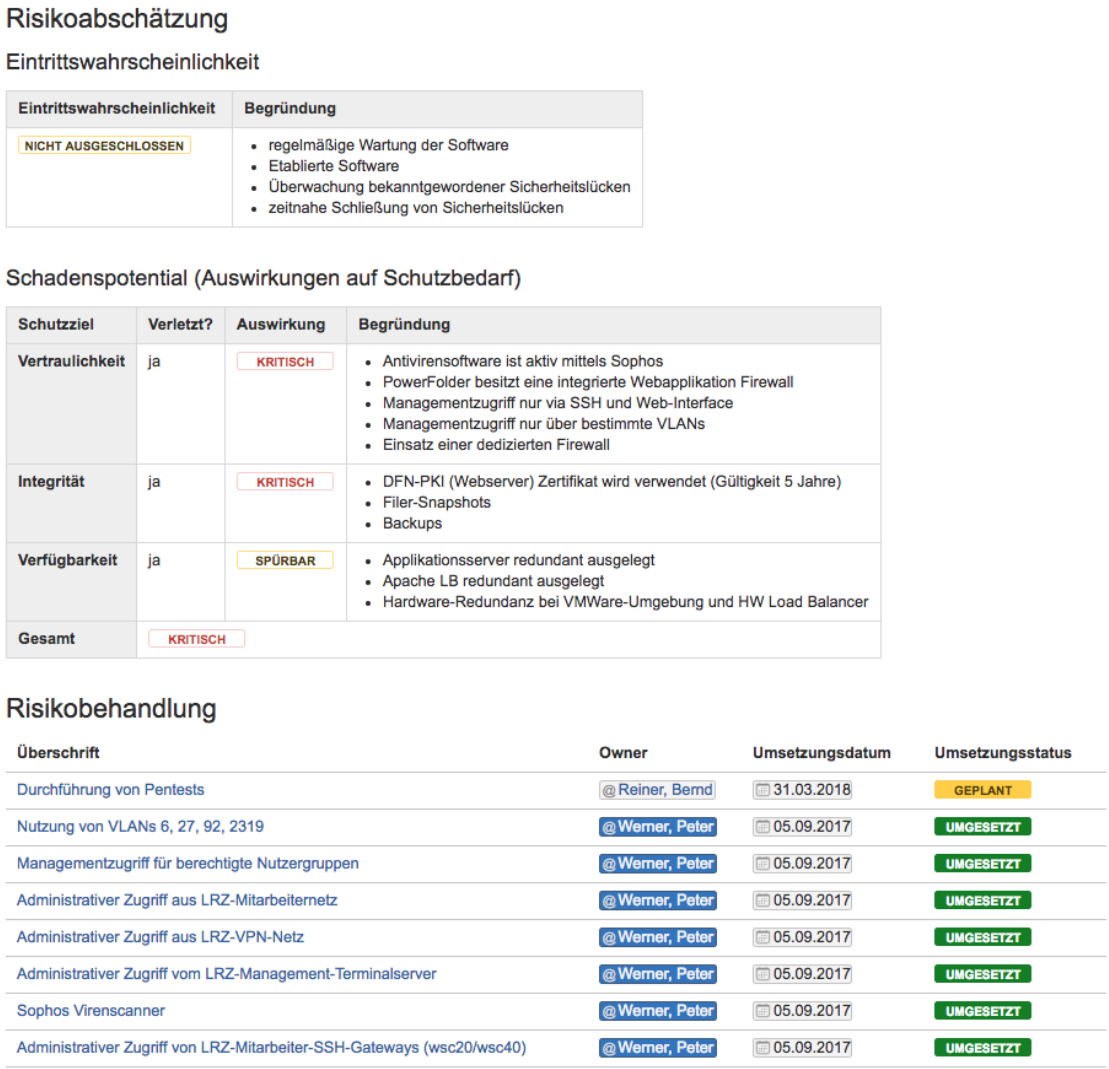
Das Risiko des Datenträgerausfalls im Speichersystem hat auf sämtliche Informationswerte Einfluss, da die relevanten Informationen auf Festplatten bzw. Solid-State-Disk (SSD) gesichert werden, deren Lebensdauer durch übermäßigen Gebrauch (Anzahl Schreibzugriffe, Defekte Sektoren, ...) vermindert wird. Bezüglich der Eintrittswahrscheinlichkeit besteht immer die Gefahr, dass Datenträger ausfallen können. Diese Auswirkungen zeigen sich jedoch nur in einem Integritäts- und/oder Verfügbarkeitsschaden.

Relevante Risikobehandlungsmaßnahmen umfassen beispielsweise Hardwareredundanzmechanismen in Form von Redundant Array of Independent Disks (RAID) - Konfigurationen oder auch Backups.

Technischer Systemangriff

Das Risiko des technischen Systemangriffs umfasst sämtliche softwarebezogenen Attacken, die auf ein System gefahren werden. Dabei ist es nicht von Bedeutung, um welche Art von Angriff es sich handelt (Trojaner, Viren, ...). Als Schwachstellen können sowohl Bugs oder ungepatchte Systeme aber auch unzureichend geschützte Systeme identifiziert werden. Im Kontext des Sync+Share Dienstes ist die Eintrittswahrscheinlichkeit als *häufig* einzustufen. Die Auswirkungen über alle Schutzziele hingegen bleibt unbedeutend, da durch bereits etablierte Best-Practice Maßnahmen ein angemessener Schutz erzielt wird.

Antivirensoftware, die Einschränkung von Benutzerrechten, Firewallregeln oder auch Systemupdates stellen wirksame Risikobehandlungsmaßnahmen dar, um dem Risiko eines Systemangriffs entgegenzutreten.



Risikoabschätzung

Eintrittswahrscheinlichkeit

Eintrittswahrscheinlichkeit	Begründung
NICHT AUSGESCHLOSSEN	• regelmäßige Wartung der Software • Etablierte Software • Überwachung bekanntgewordener Sicherheitslücken • zeitnahe Schließung von Sicherheitslücken

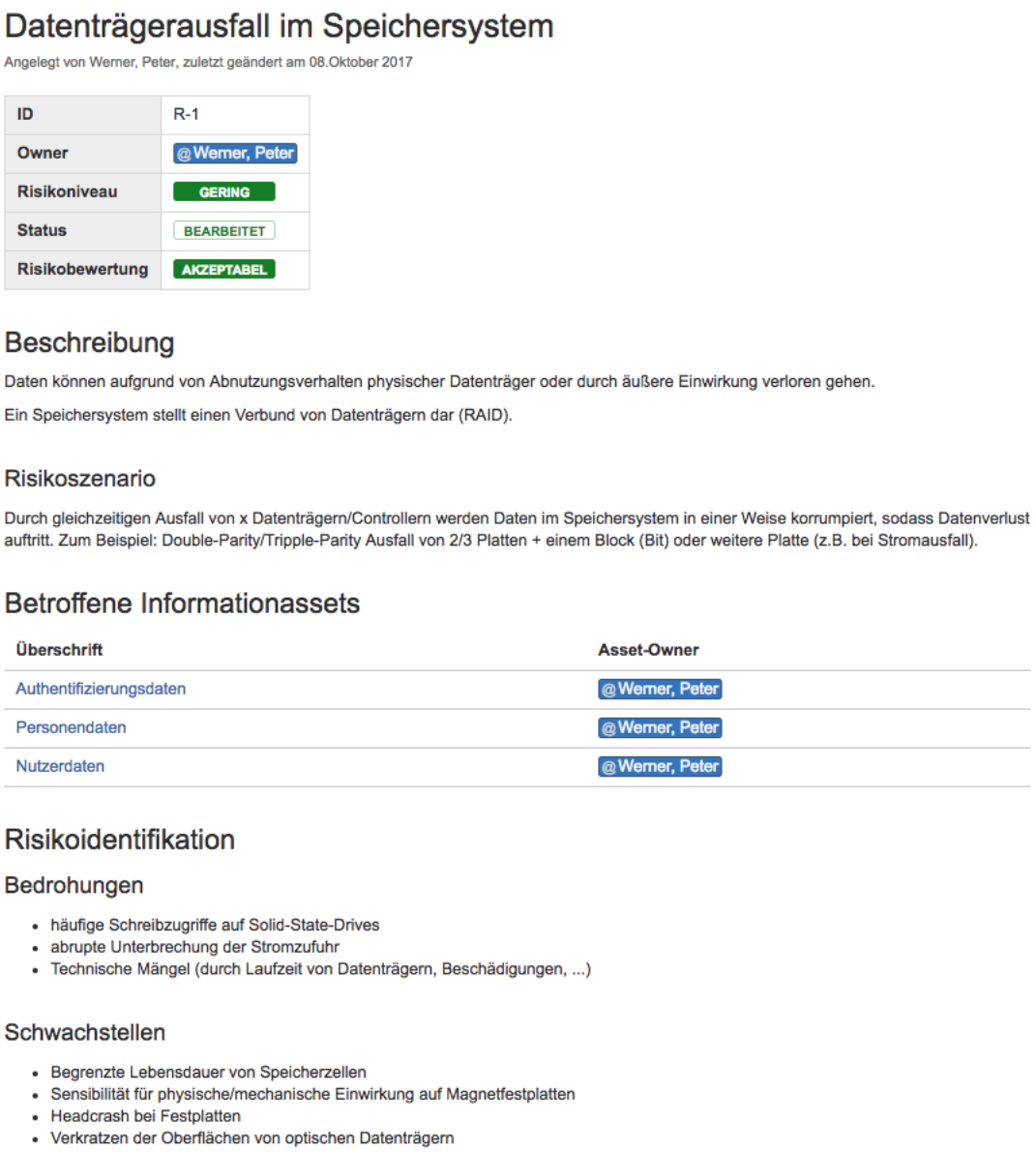
Schadenspotential (Auswirkungen auf Schutzbedarf)

Schutzziel	Verletzt?	Auswirkung	Begründung
Vertraulichkeit	ja	KRITISCH	• Antivirensoftware ist aktiv mittels Sophos • PowerFolder besitzt eine integrierte Webapplikation Firewall • Managementzugriff nur via SSH und Web-Interface • Managementzugriff nur über bestimmte VLANs • Einsatz einer dedizierten Firewall
Integrität	ja	KRITISCH	• DFN-PKI (Webserver) Zertifikat wird verwendet (Gültigkeit 5 Jahre) • Filer-Snapshots • Backups
Verfügbarkeit	ja	SPÜRBAR	• Applikationsserver redundant ausgelegt • Apache LB redundant ausgelegt • Hardware-Redundanz bei VMWare-Umgebung und HW Load Balancer
Gesamt	KRITISCH		

Risikobehandlung

Überschrift	Owner	Umsetzungsdatum	Umsetzungsstatus
Durchführung von Pentests	@Reiner, Bernd	31.03.2018	GEPLANT
Nutzung von VLANs 6, 27, 92, 2319	@Werner, Peter	05.09.2017	UMGESETZT
Managementzugriff für berechtigte Nutzergruppen	@Werner, Peter	05.09.2017	UMGESETZT
Administrativer Zugriff aus LRZ-Mitarbeiternetz	@Werner, Peter	05.09.2017	UMGESETZT
Administrativer Zugriff aus LRZ-VPN-Netz	@Werner, Peter	05.09.2017	UMGESETZT
Administrativer Zugriff vom LRZ-Management-Terminalserver	@Werner, Peter	05.09.2017	UMGESETZT
Sophos Virenscanner	@Werner, Peter	05.09.2017	UMGESETZT
Administrativer Zugriff von LRZ-Mitarbeiter-SSH-Gateways (wsc20/wsc40)	@Werner, Peter	05.09.2017	UMGESETZT

Abbildung 7.5: Technischer Systemangriff: Risikoabschätzung und Risikobehandlung



Datenträgerausfall im Speichersystem

Angelegt von Werner, Peter, zuletzt geändert am 08.Oktober 2017

ID	R-1
Owner	@Werner, Peter
Risikoniveau	GERING
Status	BEARBEITET
Risikobewertung	AKZEPTABEL

Beschreibung

Daten können aufgrund von Abnutzungsverhalten physischer Datenträger oder durch äußere Einwirkung verloren gehen.

Ein Speichersystem stellt einen Verbund von Datenträgern dar (RAID).

Risikoszenario

Durch gleichzeitigen Ausfall von x Datenträgern/Controllern werden Daten im Speichersystem in einer Weise korrumpiert, sodass Datenverlust auftritt. Zum Beispiel: Double-Parity/Tripple-Parity Ausfall von 2/3 Platten + einem Block (Bit) oder weitere Platte (z.B. bei Stromausfall).

Betroffene Informationassets

Überschrift	Asset-Owner
Authentifizierungsdaten	@Werner, Peter
Personendaten	@Werner, Peter
Nutzerdaten	@Werner, Peter

Risikoidentifikation

Bedrohungen

- häufige Schreibzugriffe auf Solid-State-Drives
- abrupte Unterbrechung der Stromzufuhr
- Technische Mängel (durch Laufzeit von Datenträgern, Beschädigungen, ...)

Schwachstellen

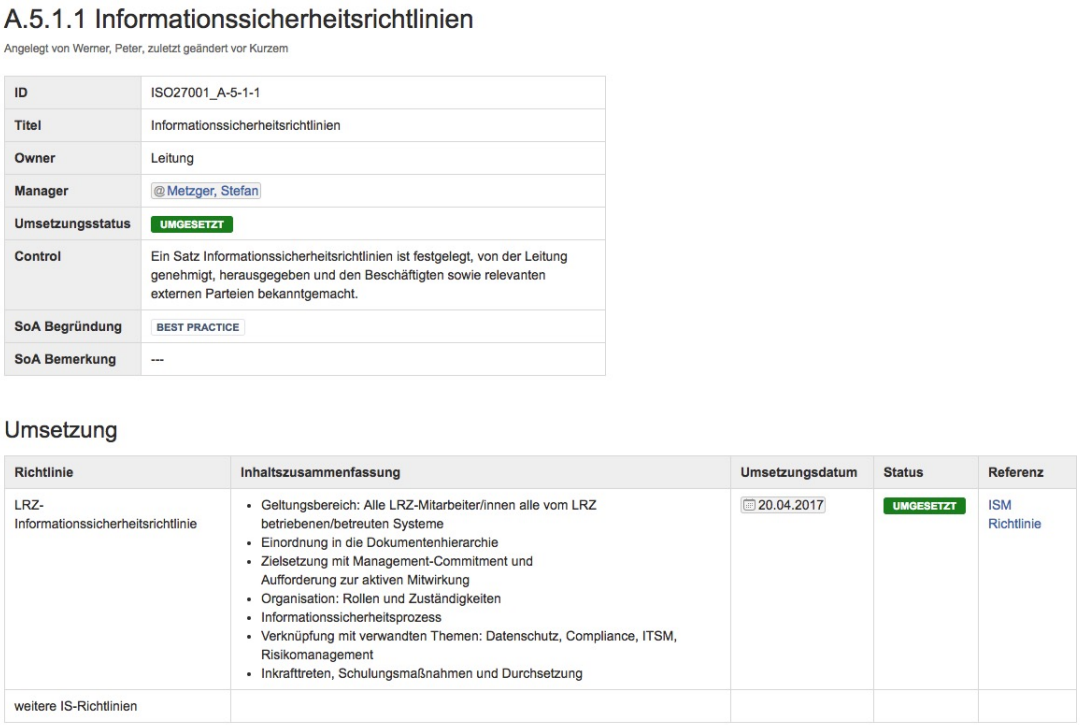
- Begrenzte Lebensdauer von Speicherzellen
- Sensibilität für physische/mechanische Einwirkung auf Magnetfestplatten
- Headcrash bei Festplatten
- Verkratzen der Oberflächen von optischen Datenträgern

Abbildung 7.6: Datenträgerausfall im Speichersystem: Bedrohungen und Schwachstellen

7.2.3 Controls

Die Controls stehen im direkten Zusammenhang mit den Risikobehandlungsmaßnahmen und werden innerhalb des Objekts der Risikobehandlungsmaßnahme referenziert. Das Objekt der Control (vgl. Abbildung 7.7) dient anschließend als übergeordnete Maßnahme, in der Querverweise auf konkrete Dokumente wie Richtlinien, die die Umsetzung vorgeben, referenziert werden.

Ergänzt wird diese Ansicht durch eine Unterseite, die die Erklärung zur Anwendbarkeit beinhaltet. Hier werden innerhalb einer Auflistung die individuellen SoA-Begründungen und



A.5.1.1 Informationssicherheitsrichtlinien

Angelegt von Werner, Peter, zuletzt geändert vor Kurzem

ID	ISO27001_A-5-1-1
Titel	Informationssicherheitsrichtlinien
Owner	Leitung
Manager	@Metzger, Stefan
Umsetzungsstatus	UMGESETZT
Control	Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.
SoA Begründung	BEST PRACTICE
SoA Bemerkung	---

Umsetzung

Richtlinie	Inhaltszusammenfassung	Umsetzungsdatum	Status	Referenz
LRZ-Informationssicherheitsrichtlinie	• Geltungsbereich: Alle LRZ-Mitarbeiter/innen alle vom LRZ betriebenen/betreuten Systeme • Einordnung in die Dokumentenhierarchie • Zielsetzung mit Management-Commitment und Aufforderung zur aktiven Mitwirkung • Organisation: Rollen und Zuständigkeiten • Informationssicherheitsprozess • Verknüpfung mit verwandten Themen: Datenschutz, Compliance, ITSM, Risikomanagement • Inkrafttreten, Schulungsmaßnahmen und Durchsetzung	20.04.2017	UMGESETZT	ISM Richtlinie
weitere IS-Richtlinien				

Abbildung 7.7: Darstellung von Controls als Objekte

SoA-Bemerkungen aus den Controls referenziert und in Kombination mit dem Umsetzungsstatus aufgelistet. Ergänzend dazu bietet Confluence die Möglichkeit, Tabelleninhalte in Pivottabellen umzuwandeln und diese über Diagrammfunktionen grafisch darzustellen. Damit wird eine schnelle Übersicht über die Menge der bereits umgesetzten Controls ermittelt.

7.3 Dokumentenmanagement in Confluence

Kemmler et. al. [BK17] haben das Thema Dokumentenmanagement im Rahmen der Dokumentation der Servicemanagementprozesse am Beispiel des LRZ behandelt und dabei fünf unterschiedliche Plugins für Confluence anhand der Anforderungen der ISO/IEC 20000 sowie zusätzlich definierte Mindestanforderungen an ein Dokumentensteuerungsverfahren evaluiert. Unter Berücksichtigung des Ziels einer leichtgewichtigen Implementierung wurden die *Adaptavist Page Information Tools*, das *ServiceRocket Reporting Plugin*, das *Comala Workflow Plugin* sowie die *Comala Publishing Plugins* miteinander verglichen.

In Anbetracht des Wartungsaufwands, Anschaffungskosten und Erfüllung der Anforderungen, wurden die Comala Plugins ausgewählt, um die Steuerung der Dokumentation des Service Management Systems zu gewährleisten. Das Plugin ermöglicht eine Abbildung der Workflow- und Genehmigungsprozesse innerhalb des Dokumentenmanagementsystems (vgl. Abbildung 7.8).

Kemmler et. al. [BK17] beschreiben Erfahrungen sowie Vorteile und Nachteile, die sich

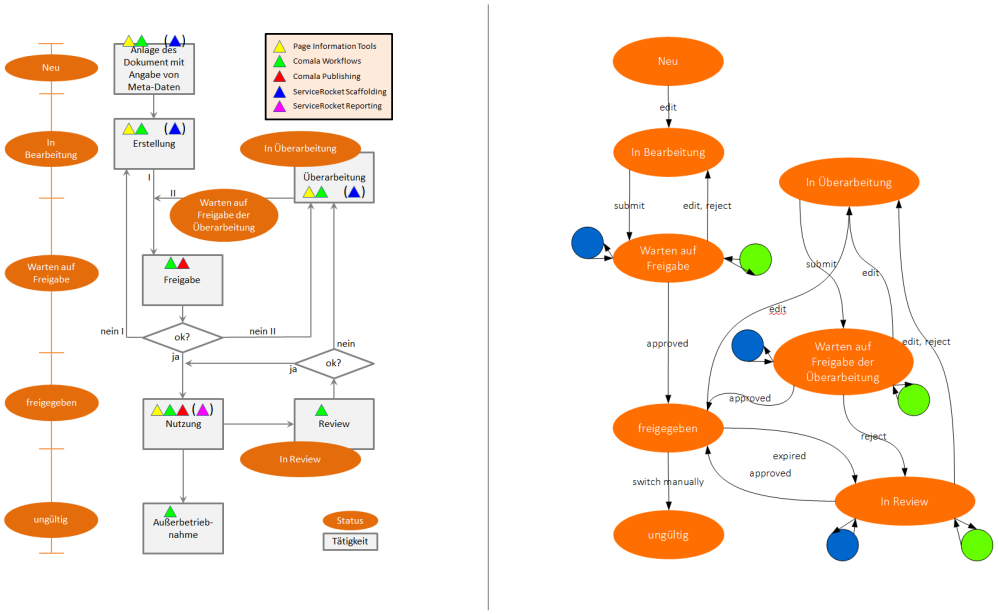


Abbildung 7.8: Dokumentensteuerungsverfahren und Abbildung als Comala Workflow

durch eine Implementierung ergeben haben. Als großer Vorteil wird die weitestgehende Anforderungserfüllung im Zusammenhang mit den relativ geringen Kosten genannt. Auch die Bedienbarkeit wird positiv erwähnt und gestaltet sich für IT-ferne Mitarbeiter als leicht erlernbar. Negativ werden lediglich einige spezielle Eigenarten wie die automatisierte Benachrichtigungsfunktion oder fehlende Validierung von Workflow-Parametern genannt.

Zusammenfassend lässt eine Einführung der Comala Plugins auch die Ergänzung zusätzlicher Plugins zur Steuerung von Dokumenten zu. Durch die Erfahrungen im Bereich der Service Management Dokumentation ist die Übertragung der Funktionen auf die ISMS-Dokumentation möglich.

7.4 Workflow

Die Definition der Seiten und Attribute innerhalb der Kategorien sollte durch ein Aktivitätsdiagramm ergänzt werden, um den Workflow bei der Dokumentation von Assets, Risiken und Maßnahmen nachvollziehen zu können. Abbildung 7.9 zeigt den Workflow anhand definierter Kategorien.

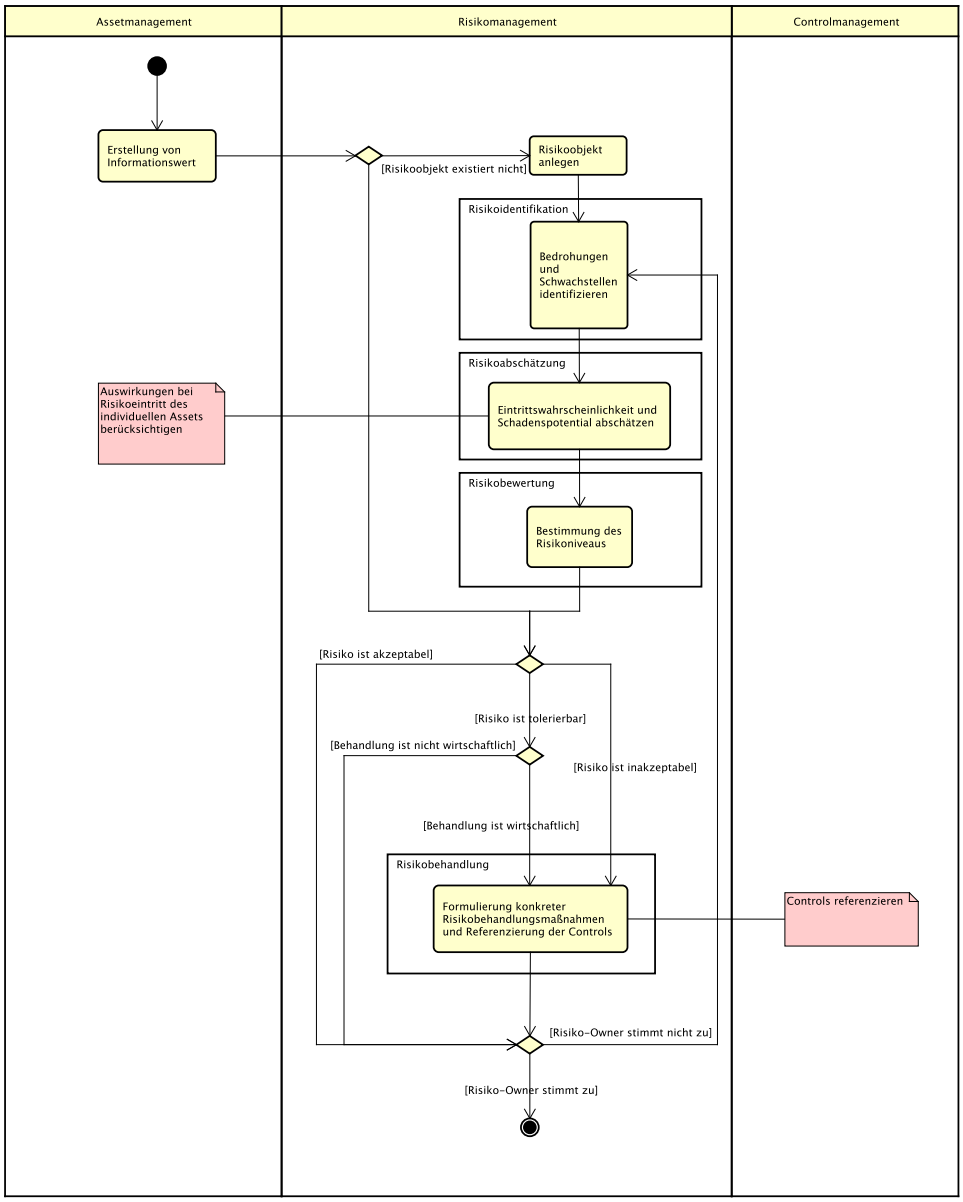


Abbildung 7.9: Workflow ISMS-Dokumentation

7.5 Vergleich zwischen prototypischer Implementierung und vorhandenen Dokumentationstools

Nachdem die Implementierung des Informationsmodells in Confluence erfolgt ist, kann ein Vergleich mit den Ergebnissen aus Abschnitt 5.3 Aufschluss darüber geben, ob die Implementierung den Anforderungen gerecht wird oder nicht.

ID	Anforderung	verinice	opus-i	ISIS12	Confluence
Systemkompatibilität					
QV4	Client/Server Infrastruktur	18	18	18	18
QV5	Desktop-Client (nativ)	12	6	0	0
QV16	Mobile Apps	0	0	0	6
QV3	Datenbanksysteme Unterstützung	6	12	0	12
$\sum$		36	36	18	36
Risikomanagement-Funktionalitäten					
QV28	Schutzbedarfsmatrix	18	18	0	18
QV26	Vererbungsmechanismen für Schutzbedarf	12	12	0	0
QV24	Ergänzende Maßnahmen	18	18	18	18
QV25	Unterstützung klassischer Bedrohungs- und Risikoanalysen	18	18	18	9
$\sum$		66	66	36	45
Reporting					
QV31	Microsoft Office Kompatibilität	18	18	0	18
QV32	Visuelle Darstellung von Status- und Umsetzungsständen	6	12	12	12
QV33	Konfiguration/Filtermöglichkeiten der Reportingausgabe	12	12	0	12
$\sum$		36	42	12	42
User Experience und Benutzerfreundlichkeit					
F3	Zuweisung von Zuständigkeiten und Bekanntmachung von Rollenzuweisungen/Benutzerverwaltung (ISO/IEC 27001 5.3)	18	18	18	18
F13	Dokumentenlenkung (ISO/IEC 27001 7.5)	18	18	9	9
F15	Unterstützung eines kontinuierlichen Verbesserungsprozesses (ISO/IEC 27001 4.4)	24	24	24	24
F17	Nutzung visueller Gestaltungsmöglichkeiten von Schaltflächen und Schnittstellen	0	18	9	18
NF1	Performanz	9	9	18	18
F18	Modellierung und Verwaltung komplexer IT-Verbünde	18	18	9	9
F19	Konzeption der Struktur anhand vorhandener Inhalte	0	0	0	18
NF2	Verlässlichkeit	18	9	18	18
QV23	Unterstützung mehrerer Anwendungsbereiche/Scopes	6	0	0	0
QV21	Netzwerkfähigkeit	18	18	18	18
QV18	Unterstützung mehrerer Sprachen	12	0	0	6
$\sum$		141	132	123	156

Tabelle 7.1: Vergleich zwischen Confluence und den bereits getesteten Dokumentationstools

ID	Anforderung	verinice	opus-i	ISIS12	Confluence
IT-Grundschutz und ISO27001 Funktionalitäten					
F1	Dokumentation des Anwendungsbereichs/Scope des Unternehmens (ISO/IEC 27001 4.3)	24	24	24	24
F2	Dokumentation der Informationssicherheitspolitik (ISO/IEC 27001 5.2)	24	24	12	24
F4	Berichterstellung über die Leistung des ISMS (ISO/IEC 27001 5.3, 9.1)	24	24	24	24
F5	Dokumentation von Risiken und Chancen sowie Maßnahmen (ISO/IEC 27001 6.1.1)	24	24	24	24
F6	Klassifizierung von Werten bzgl. Kritikalität und Empfindlichkeit (ISO/IEC 27002 8.2)	24	24	24	24
F7	Speicherung von IT-Assets (Unterteilung in primary und supporting assets) (ISO/IEC 27002 8.1.2, ISO/IEC 27005)	18	18	18	18
F8	Dokumentation von Risiko-Assessments zur Festlegung von Bedrohungen und Schwachstellen (ISO/IEC 27005 Annex E.1)	18	18	18	18
F9	Dokumentation von Risiko-Wahrscheinlichkeiten und Risiko-Auswirkungen (ISO/IEC 27005 Annex E.1)	18	18	18	18
F11	Dokumentation eines SoA (ISO/IEC 27001 6.1.3)	18	18	18	18
F10	Dokumentation der Kriterien zur Beurteilung von Risiken sowie der Risikoidentifikation, -analyse und -bewertung (ISO/IEC 27001 6.1.2)	18	18	18	18
F12	Dokumentation des Informationssicherheitsziels (ISO/IEC 27001 6.2)	24	24	12	24
F14	Dokumentation von Audits und Managementbewertungen (ISO/IEC 27001 9.2, 9.3)	18	9	9	18
QV6	Import/Export GSTOOL	6	6	0	0
QV9	Importfunktion für IT-Grundschutzkatalog und Referenzierung	6	6	3	0
QV11	Vorgefertigte Self-Assessments	6	6	3	0
QV29	Importfunktion für ISO-Normentexte	12	12	0	0
$\sum$		282	273	225	252
$\sum$		561	549	414	531

Tabelle 7.2: Vergleich zwischen Confluence und den bereits getesteten Dokumentationstools

7.6 Zusammenfassung

Die Implementierung des Informationsmodells zeigt, dass ein allgemeines Dokumentationstool wie Confluence in der Lage ist, die Anforderungen die an die Dokumentation eines ISMS gestellt sind, zu erfüllen. In Hinblick auf Performanz und Erweiterbarkeit übertrifft Confluence aufgrund des Atlassian Marketplaces seine Konkurrenz. Durch den webbasierten Aufbau ist es möglich, beliebige Erweiterungen mittels Javascript auch selbst zu erstellen und das Werkzeug noch näher an die eigenen Bedürfnisse anzupassen. Im direkten Vergleich mit den spezialisierten Dokumentationstools (vgl. Abschnitt 5.3) gibt es einige Kriterien, die man bei Confluence durch manuelle Arbeit selbst ergänzen muss. So ist beispielsweise der Import für den IT-Grundschutzkatalog oder der ISO/IEC 27001 Anforderungen eine nützliche Funktion, die durch integrierte Schwachstellenscanner oder auch Automatismen zu regelmäßigen Self-Assessments ergänzt wird.

8 Zusammenfassung der Ergebnisse und Ausblick

8.1 Ergebnisse

Diese Arbeit hat zum Ziel, die Bestandteile eines wirksamen ISMS in den Kontext der praxisnahen Implementierung innerhalb einer Organisation zu setzen. Weiter stellt sie ein allgemeines Informationsmodell zur Verfügung, dass ermöglicht, ein ISMS anhand der notwendigen Anforderungen für eine Zertifizierung im Bereich der ISO/IEC 27001 in ein unabhängiges und allgemeines Dokumentationstool zu implementieren.

Beginnend mit den Grundlagenkapiteln, die sich mit der allgemeinen Thematik der ISO/IEC 27001 befassen und wichtige Einblicke zum Verständnis einer zweckorientierten Dokumentation liefern, wurde ein Kriterienkatalog entwickelt, der die Anforderungen an eine Dokumentation eines ISMS im Zusammenhang mit der Gewichtung aller Beteiligten Interessengruppen und der Gewichtung jedes individuellen Kriteriums berücksichtigt.

Anschließend wurden drei der am Markt angebotenen Dokumentationstools getestet und evaluiert. Das Ergebnis dieser Evaluation stellte dar, dass die am Markt angebotenen Dokumentationstools teilweise große Unterschiede bezüglich ihres Funktionsumfangs aufweisen.

Diese Ergebnisse bildeten die Grundlage für ein Informationsmodell, dass in der Lage sein soll, die Thematik der ISO/IEC 27001 normenkonform abzubilden. Das finale Informationsmodell wurde letztlich in das am LRZ bereits eingeführte Dokumentationstool Confluence innerhalb einer prototypischen Implementierung in die Praxis überführt, da die Dokumentation des Service Management Systems (SMS) bereits im ersten Schritt der Migration zu Confluence erfolgreich integriert wurde und nun die ISMS-Dokumentation folgen soll. Mit Confluence ist das LRZ in der Lage ohne zusätzliche Anschaffungs- und Schulungskosten neben der vorhandenen Schnittstellen zur Dokumentation des ISMS eine organisationsweite Einheitlichkeit herzustellen.

Die Implementierung zeigte, dass die Thematik des Informationssicherheitsmanagements zwar grundsätzlich durch die Dokumente des Standards einen Rahmen besitzen, dieser jedoch einen Interpretationsspielraum beinhaltet. Da die Interpretation der Normeninhalte immer im Kontext der Organisation verstanden werden sollten, zeigt auch diese Arbeit lediglich eine Möglichkeit auf, wie die Dokumentation eines ISMS erfolgen kann.

Die konkrete Definition von Werten oder die Art und Weise, wie diese definiert sind (quantitativ/qualitativ) sollte daher stets durch den zuständigen Informationssicherheitsbeauftragten (ISB) oder beteiligten Managementverantwortlichen und im Kontext der Organisation/des Unternehmens erfolgen.

8.2 Ausblick

Das Ziel einer strukturierten Dokumentation ist die Herstellung einer Nachweisbarkeit und Wiederholbarkeit innerhalb eines prozessorientierten Systems. Aufgrund der Anzahl zu verwaltender IT-Dienste verfolgt das LRZ durch Orientierung und Herstellung einer Konformität zu internationalen Normen eine Optimierung von Prozessen. Somit können sowohl die Leistungsfähigkeit und Sicherheit erhöht und die Reaktionszeiten und Kosten vermindert werden.

Diese Arbeit legt mit der Implementierung einer ISMS-Dokumentation innerhalb eines konkreten Dienstes den Grundstein für die organisationsweite, einheitliche Einführung einer ISMS-Dokumentation. Dabei ist vor allem darauf zu achten, bereits im Vorfeld eine Struktur zur Abbildung relevanter Informationswerte unabhängig von der dienstspezifischen Perspektive festzulegen. Weiterhin steigt mit der Anzahl an dokumentierter Risiken die Anzahl an Kollisionen, da unter Umständen die Notwendigkeit besteht, zwischen Risiken noch weiter zu differenziert oder zu abstrahieren.

Der zweite Schritt einer organisationsübergreifenden Implementierung sollte die Kontrolle der individuellen Risikoniveaus in Bezug zur Risikobewertung und den festgelegten Risikoakzeptanzkriterien umfassen, da durch die Dokumentation und Einordnung in ein allgemeingültiges Schema (vgl. Risikomatrix, Auswirkung, Eintrittswahrscheinlichkeit in Abschnitt 7.2.2) inakzeptable Risiken aufgedeckt werden können, die es noch zu behandeln gilt.

Während der Implementierung ist zudem aufgefallen, dass der Atlassian Marketplace viele Makros bietet, die den Workflow zur Bearbeitung von Risiken, Assets und Maßnahmen unterstützen können. So existieren beispielsweise Makros, die ermöglichen, mehreren Seiten ein bestimmtes *Tag* zuzuweisen (Label Manager for Confluence by Köstebek Teknoloji), um so eine Referenzierung zwischen Risiken und mehreren Informationassets herzustellen.

Die integrierten Hierarchie- und Tagfunktionen schränken jedoch die Navigation innerhalb der ISMS-Dokumentation ein. Es ist beispielsweise möglich von konkreten Risikoobjekten auf betroffene Informationswerte zu schließen, jedoch ist die umgekehrte Referenzierung ohne weitere Makros nicht möglich. Auch in diesem Fall würde sich ein Makro zur Ergänzung der *Tag*-Managementfunktionalität anbieten um eine Rückreferenzierung zu erreichen und diese dann auf den entsprechenden Seiten mithilfe der Seiteneigenschaftsberichte abzubilden.

Abkürzungsverzeichnis

AKDB	Akademie der Bildenden Künste . . . 23
BDSG	Bundesdatenschutzgesetz . . . 7
BSI	Bundesamt für Sicherheit in der Informationstechnik . . . 6
BVB	Bibliotheksverbund Bayern . . . 23
CCSC	Commercial Computer Security Centre . . . 5
CHM	Change Management . . . 9
CISO	Chief Information Security Officer . . . 32
CMDB	Configuration Management Database . . . 52
CONFM	Configuration Management . . . 9
COSO ERM	Committee of the Sponsoring Organizations of the Treadway Comission Enterprise Riskmanagement . . . 7
CSC	Computer Sciences Corporation . . . 35
DISC	Delivering Information Solutions to Customers . . . 5
DMS	Dokumentationsmanagementsystem . . . 20
DSGVO	Datenschutz-Grundverordnung
engl.	Abkürzung für englisch
F	Funktionale Anforderung . . . 38
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen . 6
GOBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff . . . 6
IKS	Internes Kontrollsystem . . . 7
ISACA	Information Systems Audit and Control Association . . . 12
ISAE	International Standard on Assurance Engagements . . . 7
ISB	Informationssicherheitsbeauftragter . . . 32
ISMS	Informationssicherheits-Managementsystems . . . 1
ISO/IEC 27001	DIN ISO/IEC 27001:2014-02 . . . 1
ISO/IEC 27002	DIN ISO/IEC 27002:2014-02 . . . 8
ISO/IEC 27005	DIN ISO/IEC 27005:2014-02 . . . 71
ITIL	Information Technology Infrastructure Library . . . 9
ITSEC	IT Security Evaluation and Certification . . . 5

ITSM	IT-Servicemanagement ... 9
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich ... 6
KPI	Key Performance Indicator
KRITIS	Kritische Infrastrukturen ... 7
KVP	Kontinuierlicher Verbesserungsprozess
LRZ	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften ... 4
LRZ-IDM	LRZ-Identity-Managementsystem ... 24
MWN	Münchner Wissenschaftsnetz
NF	Nicht-funktionale Anforderung ... 38
RAID	Redundant Array of Independent Disks ... 83
SCCM	Microsoft System Center Configuration Manager ... 24
SMS	Service Management Systems ... 9
SNSB	Staatliche Naturwissenschaftliche Sammlungen Bayerns ... 23
SoA	statement of applicability ... 14
SoA	Statement of Applicability ... 14
S-Ox	Sarbanes-Oxley Gesetz ... 7
SSD	Solid-State-Disk ... 83
TLP	Traffic Light Protocol ... 55
USD	United States Dollar
V2C	Zentrum für Virtuelle Realität und Visualisierung ... 24
vgl.	Abkürzung für: vergleiche [...] (als Verweis auf eine nicht wortwörtlich, sondern umschrieben zitierte Stelle aus einer Informationsquelle
WLAN	Wireless Local Area Network ... 27

Abbildungsverzeichnis

Literaturverzeichnis

[And08] Andenmatten, Martin: *ISO 20000: Praxishandbuch für Servicemanagement und IT-Governance*. Symposion, Düsseldorf, 1. Aufl. Auflage, 2008.

[BF11] Breiter, Andreas und Arne Fischer: *Implementierung von IT Service-Management: Erfolgsfaktoren aus nationalen und internationalen Fallstudien*. Xpert.press. Springer-Verlag Berlin Heidelberg, Berlin, Heidelberg, 2011.

[BK17] Bastian Kemmler, Jule Anna Ziegler, Andreas Lohrer: *Leichtgewichtiges Dokumentenmanagement zur Unterstützung eines Service Management Systems am Beispiel des LRZ*. DFN-Forum Kommunikationstechnologien, 2017.

[BOH+17] Brenner, Michael, Nils Otto vor dem gentschen Felde, Wolfgang Hommel, Stefan Metzger, Helmut Reiser und Thomas Schaaf: *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung*. Hanser, München, 2., neu bearbeitete und erweiterte Auflage Auflage, 2017.

[Buc07] Buchsein, Ralf: *IT-Management mit ITIL V3: Strategien, Kennzahlen, Umsetzung*. Edition CIO. Vieweg, Wiesbaden, 1. Aufl. Auflage, 2007.

[Bun90] Bundesministerium der Justiz und für Verbraucherschutz: *Bundesdatenschutzgesetz (BDSG)*, 20.12.1990.

[Bun95] Bundesminiterium der Finanzen: *Grundsätze ordnungsmäßiger Buchführung: GoBS*, 07.11.1995.

[Bun15] Bundesregierung: *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme: IT-Sicherheitsgesetz*, 17. Juli 2015.

[csc15] *GSTOOL QUO VADIS? - Evaltuation von Information Security Management System Tools als Grundschutz Tool Alternativen*. Computer Sciences Corporation (CSC), 2015.

[eur08] *Qualitätsmanagementsysteme - Anforderungen (ISO 9001:2008); Dreisprachige Fassung EN ISO 9001:2008*. Technischer Bericht, Europäisches Komitee für Normung, 2008.

[EWSW13] Ertl-Wagner, Birgit, Sabine Steinbrucker und Bernd C. Wagner: *Qualitätsmanagement und Zertifizierung: Praktische Umsetzung in Krankenhäusern, Reha-Kliniken, stationären Pflegeeinrichtungen*. Erfolgskonzepte - Praxis- & Krankenhaus-Management. Springer, Berlin and Heidelberg, 2. Aufl. Auflage, 2013.

[fSidI96] Informationstechnik, Bundesamt für Sicherheit in der: *BSI-Grundschutz Katalog*, 1996.

[Gmb13] GmbH, TUEV SUED Akademie: *Foundation-Training: Information Security Management System gemäß ISO/IEC 27001.* Technischer Bericht, 08.11.2013.

[Gmb16] GmbH, TUEV SUED Akademie: *Information Security Officer gemäß ISO/IEC 27000 ff.* 11.08.2016.

[Gra14] Grande, Marcus: *100 Minuten für Anforderungsmanagement: Kompaktes Wissen nicht nur für Projektleiter und Entwickler.* Springer Vieweg, Wiesbaden, 2., aktual. Aufl. Auflage, 2014.

[Inf16] Information Systems Audit and Control Association (ISACA): *Implementierungsleitfaden ISO/IEC 27001:2013: Ein Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013*, Mai 2016.

[Int15a] Internation Organisation for Standardization: *ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary.* 2014-01-15.

[Int15b] Internation Organisation for Standardization: *ISO/IEC 27002: Information technology — Security techniques — code of practice for information security management.* Technischer Bericht, 2014-01-15.

[Int15c] Internation Organisation for Standardization: *ISO/IEC 27003: Information technology — Security techniques — information security management system implementation guidance.* Technischer Bericht, 2014-01-15.

[Int15d] Internation Organisation for Standardization: *ISO/IEC 27005: Information security risk management.* Technischer Bericht, 2014-01-15.

[Int15] Internation Organisation for Standardization: *ISO/IEC 21500:2012 Guidance on project management.* Technischer Bericht, 2013-07-15.

[iso16] *History of the ISO 27000 Standards*, 2016.

[Kai] Kai Jendrian: *Der Standard ISO/IEC 27001:2013.* DuD: Datenschutz und Datensicherheit, (08/2014):552–557.

[Kli15] Klipper, Sebastian: *Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010.* Edition <Kes>. Springer -Vieweg, Wiesbaden, 2., überarb. Aufl. Auflage, 2015.

[KRS13] Kersten, Heinrich, Jürgen Reuter und Klaus-Werner Schröder: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung.* Edition <Kes>. Springer Vieweg, Wiesbaden, 4., aktualisierte und erw. Aufl. Auflage, 2013.

[KSK11] Klett, Gerhard, Klaus-Werner Schröder und Heinrich Kersten: *IT-Notfallmanagement mit System: Notfälle bei der Informationsverarbeitung sicher beherrschen.* Praxis. Vieweg+Teubner Verlag / Springer Fachmedien Wiesbaden GmbH Wiesbaden, Wiesbaden, 1. Aufl. Auflage, 2011.

[lrz16] *Jahresbericht 2015*. Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften, 2016.

[Rat] Rat der Europäischen Union: *Schutz kritischer Infrastrukturen: 2008/114/EG*.

[Rei16] Reiss, Manuela: *Dokumentationsmanagement als Erfolgsfaktor eines effektiven Informationssicherheitsmanagements*. FHWS Science Journal, 3 (2015)(2):34–42, 2016.

[RR09] Reiss, M. und G. Reiss: *Praxisbuch IT-Dokumentation*. Pearson Deutschland, 2009.

[Sow17] Sowa, Aleksandra: *Management der Informationssicherheit: Kontrolle und Optimierung*. Lehrbuch. Springer Vieweg, Wiesbaden, 2017.