Information Security

Wechselwirkungen von Service und Security Management

Wie beeinflussen Prozesse / Aktivitäten der Service Management Domain ein Information Security Management System?

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Mario-Valentin Trompeter BSc
is161532

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Mag. Dr. Tjoa

St. Pölten,01.06.2018

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

St. Pölten, 01.06.2018

(Unterschrift Autor/Autorin)

Zusammenfassung

Es ist ein deutlicher Trend zu verzeichnen, dass auch in Zukunft der Ruf nach Zertifizierung ein unbedingtes Erfordernis für IT Organisationen darstellen wird, weshalb sich die vorliegende Diplomarbeit im Besonderen mit den Wechselwirkungen zwischen IT Service und Security Management beschäftigt.
Regelwerke fördern nicht nur die Transparenz und Vergleichbarkeit, vielmehr stationieren diese auch ein Zeichen für Qualität. Dritten wird es ermöglicht, anhand etwaiger Anforderungen diverse Bereiche wie Planung, Kontrolle und Monitoring besser abzudecken. Zahlreiche Standards am Markt machen die Entscheidungsfindung für das Management jedoch keinesfalls leichter.

Dennoch richten die Organisationen vermehrt ihre IT Landschaft nach Regelwerken der IT Service und Security Management Domain aus, um den Marktanforderungen gerecht zu werden. Demzufolge sind anschließend zur Übersicht der vorliegenden Standards die bekanntesten Vertreter der vorliegenden Themenbereiche, die ISO/IEC 20000, die ISO/IEC 27001 respektive die ISO/IEC 27002 selektiert, um auf deren Basis fortführende Aussagen in einem Tool abzubilden.

Das Herzstück bildet dabei eine Kreuztabelle, welche die Abhängigkeiten darstellt. Mithilfe von Expertinnen und Experten aus Forschung und Wirtschaft wurde eine Matrix entwickelt, um Aussagen über die gegenseitigen Abhängigkeiten wissenschaftlich ausdrücken.
Durch das im Zuge dieser Arbeit konzipierte Assessment Tool, können auf Basis der entwickelten Kreuztabelle und Auditbewertungen weitere Berechnungen durchgeführt werden.
Organisationen wird dadurch ermöglicht vorausschauend zu eruieren, welche Prozesse und Kontrollen mit welchen Standards am besten abgedeckt werden, wie sie sich in Kombination auswirken und wo die einzelnen Schnittstellen zwischen diesen zu finden sind.

Das Tool agiert dabei zum einen als unterstützendes Werkzeug im Zuge von Audits zur Dokumentation und zum anderen können mit den entstehenden Ergebnissen Entscheidungen zu Standards getroffen, beziehungsweise entsprechende Handlungen durchgeführt werden.

Abstract

There's a distinct trend that the call for certification will continue to be an implicit requirement for IT organizations in the future. This is why this diploma thesis deals in particular with the interaction between IT service and security management.
Standards do not only promote the transparency and comparability, but rather also set a sign of quality too. Third parties will be better able to cover various areas such as planning, control and monitoring based on any requirements. However, many market standards do not make decision making easier for management.

Nonetheless, organizations are increasingly aligning their IT landscape with IT service and security management frameworks to meet market demands. As a result, the best known representatives of the present subject areas are listed as an overview of the existing standards and afterwards probably the most important ones, the ISO / IEC 20000, ISO / IEC 27001 respectively ISO / IEC 27002 are selected, in order to use them to formulate further statements in a tool.

The heart of this thesis is a cross table, which depicts the dependencies. With the help of experts from research and industry, a matrix was developed to scientifically express statements about mutual dependencies. Through a developed assessment tool, further calculations can be carried out on the basis of the cross influence table and audit evaluations.
This enables organizations to anticipate, which processes and controls are best covered by which standards, how they work in combination and where to find the different interfaces between them.

On the one hand, the tool acts as a supporting tool in the course of audits for documentation and on the other hand, on basis of the created results decisions about standards can be made respectively corresponding actions carried out.

Inhaltsverzeichnis

1. EINLEITUNG 1

1.1. PROBLEMHINTERGRUND 1
1.2. PROBLEMSTELLUNG 1
1.3. MOTIVATION UND BEDEUTUNG 1
1.4. METHODEN 2
1.5. AUFBAU DER ARBEIT 2
1.6. ABGRENZUNG DER ARBEIT 2

2. GRUNDLAGEN 3

2.1. RELEVANTE NORMEN, FRAMEWORKS & STANDARDS 4
2.1.1. IT-Compliance 4
2.1.2. Normen, Standards und Rahmenwerke 5
2.1.2.1. Organisationen 6
2.1.2.2. ISO/IEC-Standards 7
2.1.2.3. DIN EN-Standards 7
2.1.2.4. Alternative Normen und Standards 7
2.1.3. Nutzen und Verantwortlichkeiten von Standards 7
2.1.4. Standards versus Best Practices 8
2.1.4.1. PDCA Zyklus 10
2.1.4.2. Weitere Standards zu Management Systemen 11
2.2. IT SERVICE MANAGEMENT 13
2.2.1. ITIL 14
2.2.1.1. ITIL Security Management 18
2.2.2. ISO/IEC 20000 Serie 19
2.2.3. COBIT 24
2.3. IT SECURITY MANAGEMENT 25
2.3.1. ISO/IEC 27000 Familie 27
2.3.1.1. ISO/IEC 27000 29
2.3.1.2. ISO/IEC 27001 29
2.3.1.3. ISO/IEC 27002 31
2.3.1.4. ISO/IEC 27003 32
2.3.1.5. ISO/IEC 27004 32
2.3.1.6. ISO/IEC 27005 33
2.3.1.7. Weitere ISO 27000 Subnormen 33
2.3.1.8. ISO/IEC 27013 34
2.3.2. IT-Grundschutz des BSI 36
2.3.2.1. Die BSI-Standards 36
2.3.2.2. Die IT Grundschutzkataloge 37
2.4. SCHWERPUNKTE DER STANDARDS 38
2.5. VERSIONSÜBERSICHT DER VORGESTELLTEN REGELWERKE 39
2.6. ZERTIFIZIERUNGSMÖGLICHKEITEN DER REGELWERKE 40
2.7. ALTERNATIVEN / WEITERE STANDARDS 42
2.8. IMS – INTEGRIERTES MANAGEMENTSYSTEM 43

3. KOMBINATIONEN 45

3.1. GEGENÜBERSTELLUNG / VERGLEICH / MATRIX 45
3.2. ZUSAMMENSETZUNGEN / SCHNITTPUNKTE DER LITERATUR 46
3.3. KENNZAHLEN UND REIFEGRADMODELLE 48
3.3.1. Capability Maturity Model Integration (CMMI) 49

3.3.2. Process Maturity Framework nach ITIL (PMF) 51
3.3.3. ISO/IEC 33000 | ISO/IEC 15504 (SPICE) 51

4. ASSESSMENT TOOL 53

4.1. VORGEHEN DER MODELL-ERSTELLUNG 53
4.2. TOOL „SERVICEM2SECM.XLSX“ 53
4.2.1.1. Verwendete Kapitel und Kontrollen 54
4.2.1.2. Kurzbeschreibung der Kapitel & Kontrollen 55
4.2.1.3. Funktionen des Tools 60
4.2.2. Überblick zum Assessment Tool 60
4.2.2.1. Beurteilung zur Einflussmatrix 64
4.2.3. Evaluation der Daten zum Modell / Experteninterview 66
4.2.3.1. Experteninterviews 75
4.2.3.2. Zusammenfassung der Einflussmatrix 78
4.2.3.3. Auswirkungen durch den Reifegrad 82
4.2.4. Konfiguration im Tool 84
4.2.5. Auswertungen im Tool 85
4.2.6. Zusammenfassender Bericht des Tools 85

5. ABSCHLUSS 87

5.1. ZUSAMMENFASSUNG 87
5.2. ERGEBNISREFLEXION 88
5.3. AUSBLICK 89

ANHANG A 91

ANHANG B 95

ANHANG C 96

LITERATURVERZEICHNIS 97

Abbildungsverzeichnis

Abbildung 1 Primärer Zusammenhang vom Themen in der IT-Security [4, p. 67] 4
Abbildung 2 Einordnung der Organisationen und Standards [5, p. 4] 6
Abbildung 3 Kategorisierung von IT-Standards [10, p. 8] 8
Abbildung 4 PDCA-Modell von Deming [16, p. 17] 10
Abbildung 5 Service Lifecycle von ITIL [17, p. 62] 16
Abbildung 6 Bücherstruktur ITIL [7, p. 22] 17
Abbildung 7 ISO/IEC 20000 Struktur und Aufbau [20, p. 228] 21
Abbildung 8 Geltungsbereich der ISO/IEC 20000 [20, p. 227] 23
Abbildung 9 CIA Triade 26
Abbildung 10 Beziehungen der ISMS Familie [30, p. 21] 29
Abbildung 11 Matrix mit den Ausprägungen der Regelwerke [3, p. 195] 38
Abbildung 12 Roadmap der vorgestellten Regelwerke 40
Abbildung 13 CMMI Maturity Levels 50
Abbildung 14 Übersicht zum Assessment Tool 54
Abbildung 15 Bereich Navigation 61
Abbildung 16 Bereich Security Management 61
Abbildung 17 Bereich Service Management 62
Abbildung 18 Bereich Konfiguration 62
Abbildung 19 Registerblatt zur Kontrolle 63
Abbildung 20 Lese- und Bewertungsrichtung der Matrix 65
Abbildung 21 Erweiterte Ansicht der Unterkapitel 66
Abbildung 22 Matrix mit Subkapitel 67
Abbildung 23 Wechselwirkung Bewertung is161532 74
Abbildung 24 Einflussmatrix Markus Schiemer, BSc BSc MSc MSc MBA 76
Abbildung 25 Einflussmatrix Mag. Manfred Spanner, MSc 76
Abbildung 26 Einflussmatrix FH-Prof. Mag. Dr. Simon Tjoa 77
Abbildung 27 Einflussmatrix Dipl.-Ing. Herfried Geyer 77
Abbildung 28 Vollständige Einflussmatrix 78
Abbildung 29 Optische Übereinstimmung der Evaluierungen 79
Abbildung 30 Varianzanalyse der Evaluierung 80
Abbildung 31 Eindeutige Übereinstimmungen der Experten 81
Abbildung 32 Detailwerte der eindeutigen Übereinstimmungen 81
Abbildung 33 Matrix zum Reifegrad der Kapitel 83
Abbildung 34 Auswirkung des Reifegrades 83
Abbildung 35 Konfiguration der Basismatrix 84

Tabellenverzeichnis

Tabelle 1 Übersicht der ISO/IEC 27k Familie [29, p. 1ff] 28
Tabelle 2 Zusammenfassung von vorgestellten Service Management Regelwerken 39
Tabelle 3 Zusammenfassung von vorgestellten Security Management Regelwerken 39
Tabelle 4 Übersicht der Zertifizierungen [19, p. 16ff] 41
Tabelle 5 Alternative Sicherheitsstandards [19, p. 19ff] 43
Tabelle 6 Vergleich von IT und Sicherheitsstandards [7, p. 37] 46
Tabelle 7 Interdependenz der Standards ausgehend von der ISO 27001 und d 20000 47
Tabelle 8 Verwendet Kapitel im Assessment Tool 55
Tabelle 9 Farbcode der Bewertung 66
Tabelle 10 Mapping ISO20k Kapitel 4 vs. ISO27k1, ISO27k2 69
Tabelle 11 Mapping ISO20k Kapitel 5 vs. ISO27k1, ISO27k2 70
Tabelle 12 Mapping ISO20k Kapitel 6 vs. ISO27k1, ISO27k2 71
Tabelle 13 Mapping ISO20k Kapitel 7 vs. ISO27k1, ISO27k2 72
Tabelle 14 Mapping ISO20k Kapitel 8 vs. ISO27k1, ISO27k2 73
Tabelle 15 Mapping ISO20k Kapitel 9 vs. ISO27k1, ISO27k2 74

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
CCO	Chief Compliance Officer
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technology
CSO	Chief Security Officer
DIN	Deutsche Industrie-Norm
IEC	International Electrotechnical Commission
IMS	Integrierte Managementsystem
IS	Informationssicherheit
ISM	
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
ITSM	IT Service Management
OECD	Organisation for Economic Co-operation and Development
RCB	Registered Certification Body
ROI	Return on Investment
SM	Service Management
SMS	Service Management System
SPICE	Software Process Improvement and Capability Determination
TR	Technical Report

1. Einleitung

Das erste Kapitel der Arbeit, Einleitung, vermittelt zuerst einen Überblick über den Problemhintergrund, die Problemstellung und die Motivation. Außerdem werden die Methoden zur Problemlösung geklärt und ein Ausblick auf die folgenden Abschnitte hergestellt.

1.1. Problemhintergrund

Im Rahmen der Diplomarbeit wird die Wechselbeziehung zwischen IT Service und Security Management behandelt. Dabei soll geklärt werden, wie die einzelnen Prozesse, respektive Aktivitäten der Service Management Domain ein Informationssicherheits-Managementsystem beeinflussen. Bei der Implementation eines weiterführenden Standards in eine Organisation finden oftmals Aussagen und Prognosen auf Basis von Vermutungen, zweifelhaften Schätzungen oder reinen Erfahrungen statt. Demzufolge steigt die Notwendigkeit zugunsten eines Werkzeuges, mit welchem qualifizierte Aussagen ermöglicht werden.
Diese Arbeit verfolgt die Entwicklung eines Basis-Tools, um aussagekräftige Effekte, bezüglich der Korrelation eines entsprechenden Standards der Service oder Security Management Domain treffen zu können.

1.2. Problemstellung

Durch die im Problemhintergrund genannten Standpunkte, ergeben sich für diese Diplomarbeit folgende Fragestellungen.

Hauptfragen:

- Welche Wechselwirkungen gibt es zwischen den Domänen des IT Service und Security Managements?
- Wie können etwaige Abhängigkeiten dargestellt, ausgewertet und daraufhin fortführende Aussagen deren Basis getroffen und prognostiziert werden?

Abgeleitete Fragen:

- Welche Kombinationen von Standards des IT Service und Security Management können als sinnvoll betrachtet werden?
- Gibt es vordefinierte Kombinationen von Standards des IT Service und Security Management?
- Ist eine maßgebliche Abhängigkeit von IT Service und Security Management festzustellen?

1.3. Motivation und Bedeutung

Das Tool, dass im Zuge dieser Diplomarbeit entsteht, soll Entscheidungsträgern in Organisationen helfen, einen Überblick zu erlangen, welche Bereiche eines Standards durch einen anderen abgedeckt werden, welche Auswirkungen gegebenenfalls entstehen, welcher Detaillierungsgrad vorhanden ist und welche Veränderungen einhergehen.
Es existieren bereits Standards, wie beispielsweise die ISO 27013 (siehe Abschnitt 2.3.1.8) worin die integrierte Umsetzung der ISO/IEC 27001 und der ISO/IEC 20000-1 beschrieben wird. Allerdings bieten die derzeitigen Modelle noch kein derartiges Werkzeug, um weiterführende Aussagen über die Wechselwirkungen beider genannten Standards zu treffen. Ziel ist daher, mithilfe von Expertinnen und Experten die Erstellung einer Einflussmatrix zu erarbeiten. Mithilfe dieser kann die Korrelation zwischen den einzelnen Bereichen beschrieben und abgebildet werden.

Durch bestmögliche Verwendung der Standards, im Hinblick auf die zugrundeliegenden Gegebenheiten, kann das Management die Auswirkungen, von IT Service und Security Management, den Interessensgruppen optimal darlegen.
Somit kann die Effektivität der IT Standardwerke durch qualifizierte Aussagen bei der Einführung dieser, bestmöglich genutzt und gemessen werden.

1.4. Methoden

Die Arbeit verwendet die Methode der Literaturrecherche aus wissenschaftlicher Fachliteratur, Internet-Recherche, Dissertationen sowie Fachzeitschriften, um dabei die entsprechenden Basis zum Praxisteil herzustellen.
Im Zuge der Ausarbeitung wird ein Assessment Tool entwickelt, mit welchem die Kapitel und Kontrollen der definierten Standards, im Zuge von Audits abgearbeitet werden können, um anschließend die Abhängigkeiten und Wechselwirkungen festzustellen. Durch einen Fragebogen und einer Bewertung von Domain-Experten werden die Aussagen über die Wechselwirkungen validiert.

1.5. Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in fünf wesentliche, aufeinander aufbauende Kapitel.

Um die grundlegenden Begriffe als auch die dazugehörigen Standards und Normen zu verstehen, verlangt es als Einführung, Kapitel Eins, in welchem über die Grundlagen hinaus, Service und Security Management beschrieben wird. Dazu werden die Organisation und der Nutzen der Standards und Normen vorgestellt. Außerdem werden allgemeine, immer wiederkehrende Konzepte zu den beiden Themengebieten grundlegend konkretisiert.

Aufbauend darauf, werden die bedeutendsten und die am meist verwendeten Standards und Normen vorgestellt. Angesichts der Vielzahl an detailreichen Differenzierungen, werden in diesem Kapitel die Schwerpunkte, eine Versionsübersicht und weiterführende Alternativen hervorgehoben.

Darauf aufbauend, werden im Abschnitt Drei, mögliche Kombinationen vorgestellt, ehe die Notwendigkeit von Kennzahlen mithilfe von Reifegradmodellen erklärt wird. Diese werden später im Hauptteil, rund um das Assessment Tool, zugunsten weiterer Metriken einfließen.

Den Kern der Arbeit bildet das sogenannte Assessment Tool, welches im Zuge dieser Arbeit entsteht. Dabei wird im betreffenden Kapitel Vier, das Vorgehen der Erstellung, dessen Funktionen und eine Benutzung schrittweise, mithilfe von Grafiken, ausführlich beschrieben.

Abschließend werden die Erkenntnisse, die im Zuge der Ausarbeitung entstanden sind, zusammengefasst. Eine Ergebnisreflexion und eine Ausblick auf weiterführende Arbeiten zum Forschungsthema runden diese Arbeit ab.

1.6. Abgrenzung der Arbeit

Es ist nicht das Ziel dieser Arbeit, sämtliche veröffentlichte Standards und Normen lediglich einzuordnen und gegenüberzustellen. Vielmehr soll ein neues Tool erstellt werden, womit weiterführende Aussagen anhand des Mappings von ausgewählten Standards getroffen werden können.

Außerdem findet bei dem Thema Qualitätsmanagement eine Abgrenzung statt, selbst wenn dieses Thema in vielen Bereichen sehr stark korreliert. Das Zusammenspiel und die Einbindung der verschiedenen angebotenen Standardwerke in diesen Bereichen, würde über den Rahmen dieser Diplomarbeit hinausgehen.

2. Grundlagen

In der modernen IT spielt die Verwendung von Normen und Standards eine wesentliche Rolle. Durch Normen kann ein einheitliches Verständnis von IT-Systemen ermöglicht werden. Außerdem wird durch die Vereinheitlichung die Verflechtung von Produkten und deren Dienstleistungen mitunter unter verschiedenen Anbietern gewährleistet und zusätzlich sichergestellt, dass dabei ein gewisses Maß an Qualität und Sicherheit erreicht werden kann. [1, p. 3] Demzufolge kann die Verwendung eines jeweiligen Standards oder Rahmenwerkes entsprechende Auswirkungen mit sich ziehen. Unternehmensintern kann dadurch eine Art Leitfaden hergestellt werden und damit entsteht eine wesentliche Erleichterung für Unternehmen bei der Erarbeitung von verschiedensten Themenbereichen. Ebenso bringen Standards und Rahmenwerke eine unternehmensweite einheitliche Umsetzung von Anforderungen im jeweiligen Gebiet mit sich. [2, p. 7]

Unternehmen können anhand von Standards nach außen einen Nachweis erbringen, dass ein einheitliches und überdies vergleichbares Vorgehen erbracht wurde. Besonders von Bedeutung gewinnt dieser Aspekt sofern es sich bei dem jeweiligen Standard oder dem Rahmenwerk um einen/s mit der Möglichkeit zur Zertifizierung handelt. Insbesondere im Qualitätsmanagement kann eine fehlende Möglichkeit der Zertifizierung beispielsweise das Ausschlusskriterium im Zuge einer Ausschreibung bedeuten. [2, p. 7]
Regelwerke und Standards bieten auch darüber hinaus eine Gebrauchsanweisung oder Anhaltspunkte, womit die Verwirklichung der Maßnahmen in der Praxis verifiziert werden kann. Die Standards agieren demnach als Werkzeug zur Überwachung, Überprüfung und Reportage in Betracht auf folgende Reviews und Audits. [3, p. 188]

In der Informationssicherheit werden für die Umsetzung daher vermehrt Standards und Rahmenwerke entwickelt. Beispielweise sind hierbei die ISO/IEC 2700x oder auch der IT-Grundschutz zu erwähnen, welche in späterer Folge noch genauer vorgestellt werden zu erwähnen. Durch Anwendung von sogenannten Standards und Rahmenwerken kann gewährleistet werden, dass allgemein anerkannte Methoden und Vorgehen zur Einhaltung der Informationssicherheit Anwendung gefunden haben und eingeflossen sind. Je nach Standard kann eine regelkonforme Umsetzung mittels eines Audits geprüft und gegebenenfalls mittels eines Zertifikats bescheinigt werden. Die Zertifizierung bringt dadurch den Nachweis über die Konformität des Standards für sämtliche Kunden, Lieferanten oder anderweitige Partner. [2, p. 7]

Ebenso existieren vielerlei Standards, in welchen die Informationssicherheit nur einen untergeordneten, kleinen Teil darstellen oder nur aus einer gewissen Fachperspektive in Betracht gezogen werden. Demzufolge entstehen Überschneidungen im Hinblick der Rahmenwerke und Standards. [2, p. 7]

Aufgrund unterschiedlicher Themenbereiche, kommt es oftmals zu Überschneidungen und mehrfacher Relevanz von Standards für Unternehmen. Durch diese Überschneidungen entsteht ein maßgeblicher Bedarf an Koordination. Im Hinblick auf Anforderungen eines bereits implementierten Standards oder Rahmenwerkes können Anforderungen widerrufen oder korrigiert werden. Ebenso kann demgegenüber unbeabsichtigt ein Mehraufwand entstehen, sofern Standards in vergleichbarer Weise bereits umgesetzt wurden. [2, p. 7]

Eine Auswahl zugunsten von Standards oder eines Regelwerkes basieren nicht zuletzt auch oft bezüglich externer Anforderungen an Organisationen. Ein Beispiel solcher Anforderungen sind zum einen die Kunden selbst, aber auch gesetzliche und regulative Ansprüche wie „Sarbanes-Oxley Act“ in den USA oder „Payment Card Industries“, kurz PCI für Organisationen rund um Zahlkartenysteme. [3, p. 188]

Aus den beschriebenen Erläuterungen widmet sich dieses Kapitel den Grundlagen zum Thema Service und Security Management sowie dessen Standards beziehungsweise Rahmenwerken. Diese zwei grundlegenden Begriffe stellen die Basis für die folgenden Abschnitte der Arbeit dar.

An dieser Stelle muss auch vermerkt werden, dass die folgend angeführten Normen und Standards keine vollständige Auflistung darstellen. Vielmehr werden spezielle, bestimmte Normen gewählt und diese näher erläutert, um deren Zusammenhänge anschließend gegenüberstellen zu können.

2.1. Relevante Normen, Frameworks & Standards

Weltweit wird zwischen einer Vielzahl von Vorgehen und Standards unterschieden. Zumeist sind diese durch eine standardisierte Benennung und einer entsprechenden Kennzahl erkennbar. Es folgt daher eine kurze einleitende Vorstellung bezüglich der wichtigsten Normen.

2.1.1. IT-Compliance

Die IT-Compliance nennt die Tätigkeiten, welche ein IT-Security Manager ausführen sollte. Man spricht dabei von Handlungsvorgaben, welche aufgrund von Vorschriften, sowohl intern als auch extern, normativ oder durch gesetzliche Regeln vorgegeben werden. [4, p. 67]

Nachfolgende Grafik stellt einen Überblick zur IT-Compliance dar und zeigt dessen Abhängigkeiten.

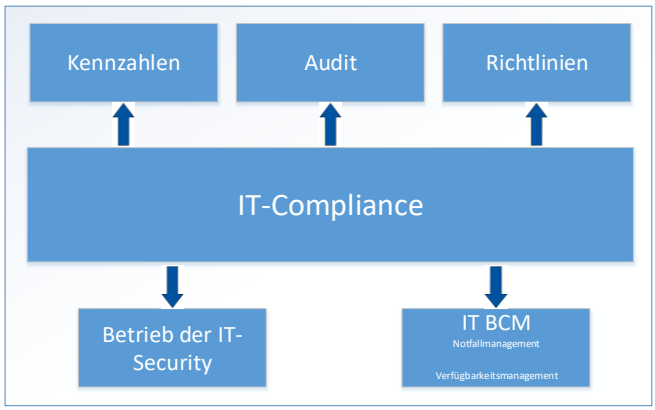

Abbildung 1 Primärer Zusammenhang vom Themen in der IT-Security [4, p. 67]

Formal betrachtet wird unter dem Term „IT-Compliance“ die regelkonforme Handlung einer Organisation im Sinne der regulativen, externen und eigenen Regelwerke als auch die Einhaltung von gesetzlichen Vorschriften verstanden. Um ein Missverständnis bezüglich der Rangordnung der Compliance Aspekte zu vermeiden, gibt es daher eine Reihenfolge, welche es zu beachten gilt. Gesetze haben sowohl gegenüber Betriebsvereinbarungen als auch internen Organisationsrichtlinien Vorrang. Ebenso sind Vereinbarungen insgesamt, also auch mit Kunden an gesetzlichen Richtlinien auszurichten. [4, p. 68]

Bei der Deklaration von gesetzlichen Anforderungen im Bereich IT-Security sind folgende Gesetze wie das GmbH-Gesetz, Aktiengesetz beziehungsweise das Bundesdatenschutzgesetz ausschlaggebend.
Damit wird zwar zum einen der Umgang mit personenbezogenen Daten abgehandelt, andererseits liegt jedoch die Verantwortung von unsachgemäßen Tätigkeiten bei der Unternehmensleitung. Ein Datenschutzbeauftragter versucht demnach personenbezogene Daten mittels IT-Security Maßnahmen zu schützen. Der IT-Security Manager hingegen ist mit der Aufgabe betraut, diese Umsetzung aktiv zu lenken. Daher ist die IT-Compliance als Teil der Corporate Governance und als Teil des Unternehmensleitbildes zu betrachten. [4, p. 68]

Standards und Normen profitieren aus den genannten Aspekten und gewinnen daher stark an Einfluss und Bedeutsamkeit. In Gebieten wo der Rahmen unzureichend definiert ist, welcher durch Gesetze allerdings vorgeschrieben wird, sind jene Mittel zweckmäßig, um adäquate Vorgehensweise zeitgerecht, transparent und vergleichbar umzusetzen. [4, p. 68]

2.1.2. Normen, Standards und Rahmenwerke

In der IT-Security wurden inmitten der 1990er Jahre zahlreiche Standards, Normen sowie Best Practices geschaffen. Eine ganze Reihe davon findet noch heute Anwendung im großen Stil. Als Beispiel sind dazu ITIL, CoBit oder auch die ISO 27000-Reihe zu nennen. Darüber hinaus sind gesetzliche Vorschriften ein Grund warum Standards wie beispielsweise das Bundesdatenschutzgesetz „BDSG“ immer noch Verwendung findet. [4, p. 70]

Der Markt bietet eine unübersichtlich große Anzahl von Dienstleistern welche die beschriebenen Teilbereiche, größtenteils aus technischer Sicht unterstützen. [4, p. 70] Beispielsweise zeigt ein Blick in den Katalog[1] der Standards der ISO „International Organization for Standardization“ ein eindrucksvolles Angebot an Regelwerken.

All diese Produkte stehen in enger Verbindung mit dem Begriff der IT-Compliance. Die genannten Punkte decken eine Vielzahl der Vorgaben ab, können dennoch nicht umfassenden, ganzheitlichen Schutz gewährleisten. Erschwerend kommt die Tatsache hinzu, dass sich viele dieser Produkte immer mehr von der Grundaufgabe rund um den Informationsschutz entfernen. Zum Exempel wird Lizenzmanagement zwar als Aufgabe der IT-Compliance betrachtet, jedoch ist damit nur mehr wenig Verbindung zur eigentlichen IT-Security gegeben. [4, p. 70]

Diverse gesetzliches Bestimmungen und Vorgaben fungieren als Rahmenbedingungen in Organisationen zur Notwendigkeit von Informationsschutzmaßnahmen. Diese Gesetze sind nicht ausschließlich an die Entscheider der IT, sondern vielmehr an die Unternehmensleitung gerichtet. [4, p. 71]

Abseits der Sorgfaltspflicht, an die jede beteiligte Person verpflichtet ist, müssen Vorkehrungen getroffen werden, um potentielle Schäden am Unternehmen abzuwenden. Diese Vorkehrungen und Maßnahmen sind vor allem in und rund um die Bereiche der IT angeordnet. [4, p. 71]

Grundsätzlich sind kaum verbindliche Vorgaben für die Informationssicherheit und deren Aufgaben gegenwärtig. Solange sowohl der Schutz von Daten als auch die Schutzziele, wie in Punkt 2.3 IT Security Management beschrieben, der Verfügbarkeit und Integrität dienen, steht es der Organisation frei, ihr Security Management nach Belieben umzusetzen. [4, p. 72]
Entgegen einer datenschutzbeauftragten Person kann das Security Management, abseits von gesetzlichen Grundlagen, individuell auf die Sicherheitsanforderungen der Organisation sämtliche Handlungen abwickeln. Somit eröffnen sich dem Unternehmen sämtliche Möglichkeiten für ein angemessenes Sicherheitssystem. Bereits implementiere Vorgehensmodelle lassen sich dabei ideal in die vorhandene Umgebung adaptieren und weiter ausbauen. [4, p. 72]

Außerdem ist es wenig zielführend etwas Bestehendes neu zu erfinden in Anbetracht dessen, dass Kollegen der Branche selbst auch bereits ähnlichen Herausforderungen gegenüber gestanden sind. Demzufolge sind aus der Reihe von Erfahrungen bereits wertvolle Standards aufgekommen, welche zum heutigen Zeitpunkt als erprobt und ausgereift betrachtet werden können. Internationale Standards haben sich über Jahre hinweg bewährt und gelten damit auch für nationale als Richtungsweiser. Ein Beispiel ist das BSI, das Bundesamt für Sicherheit in der Informationstechnologie, wie in Punkt 2.3.2 IT-Grundschutz des BSI noch detaillierter erläutert wird. Gerade international tätige Organisation sehen sich gezwungen auf international anerkannte Standards zurückzugreifen, um damit sämtliche Voraussetzungen für entstehende Geschäfte zu erfüllen. [4, p. 72]

[1] https://www.iso.org/committee/45306/x/catalogue/ [Zugriff am 22 März 2018].

2.1.2.1. Organisationen

Durch die folgende Grafik soll eine Darstellung der involvierten Organisationen hinter den Standards geboten werden. Diese ist nicht vollständig, sie soll vielmehr eine Zusammenfassung der wichtigsten Organisationen rund um die Themen von Standards und Normen im Bereich von Sicherheits- und Service Management der Informationstechnologien sein.

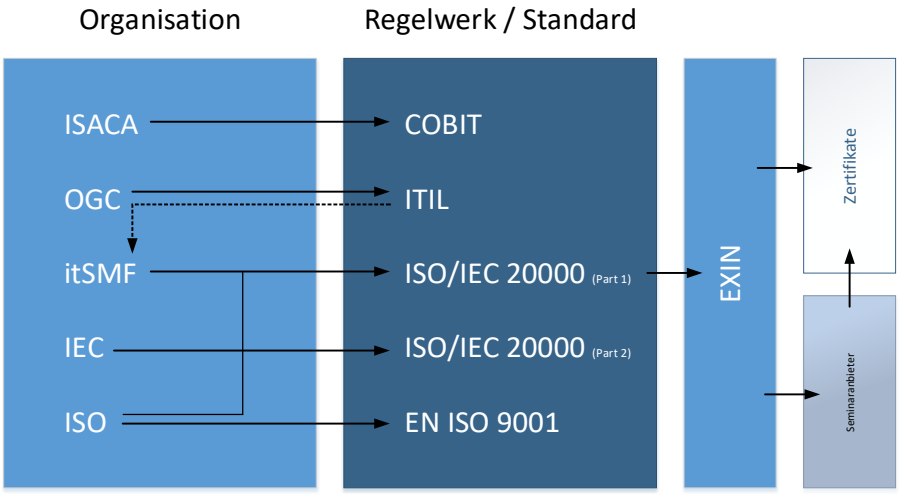

Abbildung 2 Einordnung der Organisationen und Standards [5, p. 4]

Die ISACA, bekannt als Information Systems Audit and Control Association, versteht sich als unabhängige, gemeinnützige, globale Vereinigung. Die Organisation bemüht sich um die Entwicklung, Einführung und Anwendung von weltweit akzeptierten, branchenführenden Kenntnissen und Praktiken für Informationssysteme. [6] Die Organisation der ISACA steht unter anderem hinter dem Framework COBIT welches im Abschnitt 2.2.3 vorgestellt wird.

Das OGC, Office of Government Commerce, ist der ursprüngliche Eigentümer rund um ITIL, welcher in Punkt 2.2.1 ITIL näher vorgestellt wird. Die OGC ist eine Organisation der Regierung von Großbritannien. Im Jahr 2001 ist die CCTA in die OGC transformiert und hat sich somit zum neuen Eigentümer von ITIL entwickelt. Durch die OGC wird die Verwendung von „Best-Practice“ Ansätzen gefördert, womit auch diese als der aktuelle Herausgeber der IT Infrastructe Library, „ITIL“ agiert. [7, p. 20]

Das itSMF, Information Technology Service Management Forum tritt als Netzwerk zugunsten von ITIIL Spezialisten in Erscheinung. Das itSMF wurde 1991 in England gegründet und gilt als das erste Forum für IT-Servicemanagement. Mittlerweile findet sich das itSMF in unzähligen Ländern wieder wie beispielsweise GB, USA, AUS, DE, CAN, usw. Das itSMF erweist seine Dienste als Non-Profit Organisation, welche durch deren Mitglieder ausgeführt und geprüft wird. [7, p. 20f]

Die IEC, International Electrotechnical Commission, wurde 1906 gegründet und ist die weltweit führende Organisation für die Erstellung und Veröffentlichung internationaler Normen für alle elektronischen beziehungsweise verwandten Technologien.
Die IEC bietet Unternehmen, Branchen und Regierungen eine Plattform, um die von ihnen benötigten internationalen Standards einzuhalten, zu diskutieren und weiterzuentwickeln. [8]

Die International Standards Organisation, kurz ISO genannt, wurde 1946 gegründet und hat ihren Sitz in Genf. Die ISO ist eine unabhängige, nichtstaatliche internationale Organisation mit 162 nationalen Normungsgremien.

Über deren Mitglieder werden Experten zusammengeführt, um Wissen zu teilen sowie freiwillige, konsensorientierte, marktrelevante internationale Standards zu entwickeln, die Innovationen unterstützen und Lösungen für globale Herausforderungen bieten. [9]

Durch Exin, Exameninstitut voor Informatica, gibt es eine international anerkannte Möglichkeit der Zertifizierung von ITIL-Qualifikationen. Mittels EXIN und der ISEB, dem Information Systems Exmination Board, existieren international aktive, unabhängige Anbieter welche von der OCG beauftragt sind um IT-Prüfungen abzunehmen. Diese beschäftigen sich obendrein mit der Entwicklung der Qualifikationsstandards und arbeiten in Kooperation mit der OGC und dem itSMF an fortlaufenden Erneuerungen zur Zertifizierung von ITIL. [7, p. 21]

2.1.2.2. ISO/IEC-Standards

Bei den ISO/IEC Standards handelt es sich um internationale Normen die unter der Aufsicht von einem Subkomitee nach einem Konsensverfahren produziert werden. Daraufhin werden diese durch öffentliche Umfragen entwickelt. Der jeweilige Standard folgt der Namensgebung ISO/IEC gefolgt von einer entsprechenden Nummerierung. Beispielsweise ist der Standard ISO/IEC 20000 zu nennen, welcher in weiterer Folge noch beschrieben wird. [10, p. 7] Wie bereits erwähnt, steht die Abkürzung ISO für „International Organisation for Standardisation“, wobei „International Electrotechnical Commission“ mit IEC abgekürzt wird. [11, p. 1]

2.1.2.3. DIN EN-Standards

DIN Standard welche in der Namensgebung ein EN beinhalten entsprechen der europäischen Normen. Diese Standards werden ebenso wie zuvor die ISO-Standards durch ein Konsensverfahren mit anschließender Umfrage in der Öffentlichkeit bestätigt. Eine Norm beginnend mit DIN entspricht einer deutschen Norm. Durch den Zusatz DIN EN weiß die Leserschaft, dass es sich um eine europäische Norm handelt welche im deutschen Normenwerk integriert wurde. [10, p. 7]

2.1.2.4. Alternative Normen und Standards

Als Alternative zu den bereits erwähnten Normen und Standards ist beispielsweise der, in Punkt 2.3.2 beschriebene, IT-Grundschutz des BSI zu nennen. Standards und Normen wie diese wurden von Konsortien, Behörden oder Interessensgruppen erstellt. Im Gegensatz zu den zuvor erwähnten Standards sind diese Normen bei den Regeln nicht eingeschränkt und ermöglichen somit die Befugnis einer Mitwirkung.

Nationale wie auch internationale Standards müssen dem Regelwerk zufolge in Intervallen von maximal fünf Jahren einer Revision unterzogen werden. [10, p. 7]

2.1.3. Nutzen und Verantwortlichkeiten von Standards

Da die Verwendung von Informationstechnologien keinem Selbstzweck zugrunde liegt, ist deren Verwendung mit bestem Nutzen zu präferieren. Jedenfalls bringt die Verwendung von Managementsystemen unbestrittene Vorteile mit sich. [10, p. 7]
Unternehmensintern vermitteln Standards Hilfestellung und Unterstützung bei der Etablierung von IT-Prozessen sowie generischen Maßnahmen bis hin zu detailreichen technischen Anleitungen um nur einige wenige Punkte zu nennen. [10, p. 7]
Als Außenwirkung bringt die Anwendung beziehungsweise der Nachweis der Verwendung von Standards immer größere Vorteile mit sich. Besondere Auswirkungen zeigen sich im Bereich von Ausschreibungen, wo eine Zertifizierung oftmals verpflichtend gefordert wird. Für die Bereitstellung von Kapital, kann diese ein entscheidender Faktor für das Unternehmen sein. Zuletzt ist noch festzuhalten, dass Organisationen im Bereich von kritischen Infrastrukturen den Nachweis über die Einhaltung von Standards erbringen müssen. [10, p. 7]

Über eine Organisation betrachtet, sind unzählige Personen besonders mit dem Thema IT-Sicherheit beauftragt oder zu mindestens darin involviert. Gerade im Bereich der Sicherheit ist es nicht nur das Aufgabengebiet der IT, sich rund um dieses Thema vertraut zu machen. Vielmehr sind praktisch sämtliche Unternehmensbereiche- und funktionen inmitten von sensiblen Daten mit dieser Thematik verstrickt. Demnach unterscheidet die folgende Grafik 3 Blöcke, welche sich in Management, Prozesse und Technik unterteilen. [10, p. 8]

In folgender Abbildung ist eine mögliche Kategorisierung der Sicherheitsstandards durch die BITKOM [10, p. 8] zu sehen.

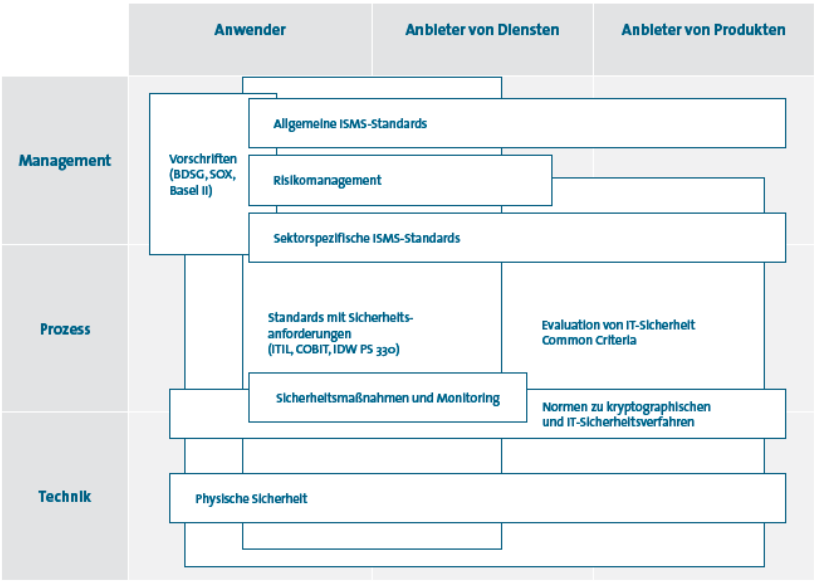

Abbildung 3 Kategorisierung von IT-Standards [10, p. 8]

Wie in Abbildung 1 zu erkennen, werden die Standards und Normen horizontal aus der Perspektive nach Anwender, Anbieter von Diensten und Anbieter von Produkten unterschieden. Vertikal ist nach den Gesichtspunkten von Management, Prozess und Technik zu unterscheiden.

2.1.4. Standards versus Best Practices

Die Anwendung von Standards beziehungsweise Best Practices findet zunehmend vermehrte Anwendung, weil gerade die Wichtigkeit einer gesteigerten Leistung, Transparenz der Werte und ein Anstieg der Kontrolle über die Aktivitäten in der IT wesentliche Beweggründe darstellen. [12, p. 112]

Standards werden im ITIL V3 Glossary folgend beschrieben:

"A mandatory requirement. Examples include ISO/IEC 20000 [...], an internal security standard for Unix configuration, or a government standard for how financial records should be maintained. The term is also used to refer to a code of practice or specification published by a standards organization such as ISO or BSI." [13, p. 59]

Standards eignen sich für Organisationen um weitreichende Anleitungen und Verweise im Hinblick auf die Durchführung von Maßnahmen in Angelegenheiten der Praxis zu vollziehen. Standards dienen somit bei der Umsetzung vorwiegend zum Zwecke ihrer Überwachung, Verifikation aber auch Berichterstattung, im Sinne von Audits und Reviews.

Damit bringen Standards eine verbesserte Übersichtlichkeit, Vergleichbarkeit, Überprüfbarkeit, Argumentationsbasis und viele weitere Gründe mit sich. [3, p. 188]

Best Practice Ansätze werden hingegen als Muster oder Verfahrensweise definiert, womit sie bestmögliche Ergebnisse bieten und obendrein als Modellansatz in Betracht gezogen werden können. Best Practice stellt dabei einen anwendungsbezogenen Ablauf zur Verfügung. Vorliegende Erfahrungen erfolgreicher Unternehmungen werden systematisiert, diverse Praxislösungen verglichen und anhand betrieblicher Ziele beurteilt. Auf deren Basis wird anschließend eine Grundlage erstellt mit welcher das Verfahren und die Darstellung bestmöglich zum Erreichen der Ziele beitragen können. [12, p. 112]

Das ITIL V3 Glossary beschreibt einen Best Practice Ansatz wie folgt:

"Proven activities or processes that have been successfully used by multiple organizations. ITIL is an example of best practice." [13, p. 7]

Eine Vielzahl an Gründen sind entscheidend, weshalb eine Anwendung von IT Best Practices ausschlaggebenden Einklang gefunden hat. Im Folgenden werden diese aufgezählt: [12, p. 112]

- Die Geschäftsleitung und Vorstände ersuchen um bessere Erträge aus der Investition in die IT. Die IT soll demnach Stakeholder Value bestmöglich erweitern.
- Bedenken bezüglich der Steigerung von allgemeinem Ausgaben der IT.
- Anforderung aufgrund von Regulierungen in Gebieten wie beispielsweise dem Datenschutz oder dem Finanzreporting.
- Stetig steigende Komplexität der IT-Risiken wie beispielsweise Netzwerksicherheit.
- Anforderungen bezüglich standardisierter Ansätze, anstelle von speziell Entwickelten um dadurch kostenoptimierend zu verfahren.
- Beurteilungen von Beratern und Analysten, die Empfehlungen zugunsten von Best Practice Ansätzen aussprechen.
- Selektion von Service Providern im Sinne des Service Outsourcing. [12, p. 112]

Best Practice Ansätze sind an keine spezielle Branche gebunden. Besonderen Anreiz finden Best Practice Ansätze dadurch, dass sie auch nur für jene bestimmte Abläufe verwendet werden können, in welchen Verbesserungen erzielt werden sollen. Die Anpassungsmöglichkeiten auf individuellen Situationen ist somit auch für kleine Unternehmen durchaus eine passende Option. [12, p. 112]

Best Practice bedeutet demzufolge, dass anhand von allgemein vorherrschenden Standards gearbeitet und sich daran orientiert wird. Hauptaugenmerk liegt dabei auf der bestmöglichen Steigerung der in sich vereinten Vorteile.

Best Practice Ansätze versprechen sich dadurch: [14, p. 34]

- Steigerung der Zufriedenheit der Kunden
- Steigerung der Zufriedenheit des Personals und der daraus folgende Senkung von Fluktuation
- Klarheit durch funktionserprobte Vorgehensweisen
- Steigerung des RIO [14, p. 35]

Letztlich wird ebenso, beispielsweise bei COBIT, siehe Abschnitt 2.2.3, auch von sogenannten Frameworks gesprochen. Ein Framework kennzeichnet eine allgemeine Richtlinie, die ein Unternehmen adaptieren kann. Ein Framework kann zahlreiche Komponenten enthalten, schreibt jedoch nicht die zu treffenden Schritte vor. Es stellt die möglichen Maßnahmen zur Strukturierung und Realisierung der neuen Umgebung vor. [15, p. 7]

2.1.4.1. PDCA Zyklus

Die ISO Standards, besonders die ISO 9001, ISO 14001, ISO 27001 sowie auch andere sind auf dem gleichen prozessorientierten Ansatz aufgebaut. [2, p. 27] Ebenso bedient sich ITIL dem im Folgenden beschriebenen Management Vorgehen, weshalb dieses hier vorweg allgemein erläutert werden soll. [16, p. 17]

Genau gesagt ist von einem kontinuierlichen Verbesserungsprozess die Rede, besser bekannt als PDCA Zyklus nach Deming, welcher wie bereits angedeutet aus dem Qualitätsmanagement kommt. [2, p. 27] Durch die allgemeine Verwendung des PDCA Zyklus, entsteht auch ein weiterer vorteilhafter Aspekt, so dass mit hoher Wahrscheinlichkeit bereits Kenntnisse in diesem Bereich im jeweiligen Unternehmen vorzufinden sind. Auf Ebene der Unternehmensleitung bringt dies den Vorteil, dass diese Vorgehensweise bereits bekannt sein sollte und somit Argumentationen erleichtert werden. [4, p. 409]
Der PDCA Zyklus ist den Buchstaben nach in vier wesentliche Phasen gegliedert. [2, p. 27] Sicherheit ist ein kontinuierlicher, sich ständig ändernder Prozess, weshalb ein kontinuierlicher Verbesserungsprozess wie folgt dargestellt von Bedeutung ist. [17, p. 481]

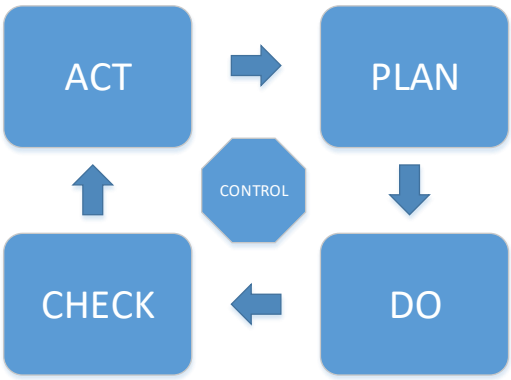

Abbildung 4 PDCA-Modell von Deming [16, p. 17]

Der Ablauf im PDCA Zyklus verfolgt einen Prozess in welchem die diversen Einzelschritte jeweils mit dem Output des vorangegangen Schrittes als Input für den kommenden Schritt versorgt werden. [4, p. 408]

Genauer genommen ist dem PDCA laut Brunnstein [16, p. 17] noch ein weiterer Punkt hinzuzufügen, da bereits abseits des Security Managements Anforderungen im Hinblick auf das PDCA Modell einfließen. Diese sollten vorweg abgelegt und bewertet werden.
Außerdem ergänzt Brunnstein [16, p. 17] den PDCA Zyclus um ein weiteres Merkmal, der Control Phase wodurch der Prozess mit ITIL konform wird.

Die Gliederung eines IKT- bzw. eines detaillierten Sicherheitsmanagementsystems kurz SMS oder ISMS beginnt im ersten Schritt mit der Planung (Plan). Darauf folgt die Umsetzung (Do) inklusive Pilotierung, Betrieb und dazugehöriges Monitoring sowie Test, Reporting beziehungsweise Controlling. In der Phase der Überwachung (Check) wir das System analysiert, bewertet und geprüft. Als letzte Phase agiert die Verbesserung (Act) wobei die Ergebnisse verarbeitet werden. Die Resultate sind zugleich die Einleitung für die folgende Durchführung eines PDCA-Zyklus und fließen in die kommende Phase der Planung ein. [17, p. 482]

Zu Beginn werden in der Phase der Planung (Plan) des Risikomanagementsystems von der Geschäftsleitung die relevanten Rollen ausgewählt. Je nach Größe der Organisation werden entsprechend der oder die Chief Compliance Officer (CCO), der oder die Chief Security Officer (CSO) beziehungsweise der oder die Chief Information Security Officer (CISO) sowie weitere Rollen und Verantwortlichkeiten festgelegt. Im Zuge dessen sollte auch das Organigramm des Unternehmens dahingehend adaptiert werden. [17, p. 482]
Der oder die CCO, CSO, CISO und weitere Rollen gehen sowohl externen Erwartungen wie beispielsweise den Gesetzen, Bestimmungen von Aufsichtsbehörden, Standards, Normen als auch den verpflichtenden Verträgen nach. Zu ihren Aufgaben zählt auch der Entwurf von Tätigkeiten zum Aufbau der Managementprozesse. Der Risiko-Managementprozess wird beschlossen, ein Mindestmaß sowie Grenzszenarien werden vereinbart. Der oder die CCO, CSO und CISO besiegeln damit die Risiko Politik eines Unternehmens und stimmen diese mit der Geschäftsleitung ab. [17, p. 482]
Die genannten Personen definieren konsistente Klassen in Bezug auf Sicherheit, Risiko und Kontinuität. Zusammen mit den Prozessverantwortlichen werden die Anforderungen mittels Business Analysen erhoben. Dem folgen entsprechende Berichte samt detaillierten Informationen.
Die beauftragten Personen für Sicherheit, Kontinuitäts- und Risikomanagement legen die Kontrollelemente (Controls) und dessen Kennzahlen fest. Diese bilden die Basis für das folgende Monitoring, Controlling beziehungsweise das Reporting sowie Prüfungen im weiteren Verlauf. [17, p. 483]

Die nächste Phase im PDCA Zyklus behandelt die Umsetzung (Do). Beispielsweise werden Mitarbeiter und Mitarbeiterinnen sensibilisiert indem sie an Schulungen teilnehmen. Die jeweils operativ beauftragten Personen für die Prozesse und Ressourcen realisieren den Betrieb anhand der beschlossenen Konzepte und Maßnahmen. Der Betrieb wird dabei gemessen und durch „monitoring“ dahingehend überwacht, dass den Anforderungen kontinuierlich nachgekommen werden kann. Meldungen werden bestenfalls sofort erkannt und daraufhin ausgewertet wodurch umgehend reagiert werden kann. [17, p. 484]
Bezüglich der Anforderungen an das Controlling werden von der Geschäftsleitung sämtliche Daten ermittelt. Damit werden Soll-Ist-Vergleiche ermittelt, Prognosen konzipiert und analysiert und etwaige Differenzen festgehalten, um darauf folgend Maßnahmen zur Korrektur zu erwägen. Die Ergebnisse im Controlling werden dokumentiert und in zyklischen Berichten an die jeweiligen Empfänger adressiert. Statuts, Maßnahmen sowie die ausstehenden Risiken werden in geeigneter Form festgehalten und entsprechend den internen sowie externen Stakeholdern kommuniziert. Durch diese bewusste Einbeziehung der Interessensgruppen, wird ein adäquates Vertrauen und Bewusstsein zum Risikomanagement hergestellt. [17, p. 484]

In wiederkehrenden Abständen werden Prüfungen (Check) abgehalten. Dabei ist der Fokus auf Sicherheitsprüfungen, allgemeine Tests sowie Übungen gelegt. Diese werden im Anschluss analysiert, dokumentiert und dessen Ergebnisse verarbeitet. [17, p. 484]

In der abschließenden Phase der Verbesserung (Act) werden die gewonnen Ergebnisse des Betriebs und der Aufbau zu einer Rückkopplung in die jeweiligen Phasen des Lebenszyklus genutzt. Fortschritt und Entwicklung werden damit in Folge von Verbesserungen und Erneuerungen ausgelöst.
Neue Produkte, Dienstleistungen, Ressourcen oder Prozesse benötigen möglicherweise neue oder abgeänderte Lebenszyklusmodelle. [17, p. 484]

2.1.4.2. Weitere Standards zu Management Systemen

Die Standards rund um die Informationssicherheit, das Service aber auch Qualitäts- und Umweltmanagement haben ähnliche Strukturen und stellen in vieler Hinsicht gleichermaßen dieselben Anforderungen:

- Verantwortung des “Top-to-Middle-Managements”
- systematische Struktur der Dokumentation
- Ziel der kontinuierlichen Verbesserung
- Einhaltung der Anforderungen

- Wartung und Betrieb der Systeme [18]

Da die ISO/IEC 9000, rund um das Qualitätsmanagement sämtliche noch folgende Standards dieser Arbeit oftmals streift oder sich starke Querverbindungen zeigen, wird dieser zum besseren Verständnis, kurz vorgestellt.

Die ISO 9000-Serie lässt sich als eine der bislang bedeutensten ISO Normen charakterisieren. [19, p. 9] Nicht umsonst findet dieser Standard in sämtlichen weiterführenden Bedeutung und Berührung.

Grundlegende Prinzipien von Qualitätsmanagement sind vor allem:

- Kundenorientierte Organisation
- Deutliche Führung
- Einbezug von Menschen
- Prozessorientierung
- Systematischer Ansatz von Management
- Stetige Verbesserung
- Entscheidungsfindung anhand von Fakten [20, p. 227]

Entscheidend ist als Basis für das Management von Qualität, diesen Begriff klar zu definieren. In der Praxis findet diese Definition oftmals wenig Anklang und findet demnach wenig zufriedenstellende Bedeutung. Tatsächlich ist die Definition von Qualität schwer nachvollziehbar beziehungsweise messbar. [20, p. 227] Als Definition von Qualität im Sinne von Servicemanagement, wie dies im Kapitel 2.2 noch näher beschrieben wird, versucht es Beims [20, p. 227], wie folgt zu konkretisieren:

„Qualität ist die Lieferung eines Services mit den vereinbarten Eigenschaften und in der vereinbarten Qualität."
[20, p. 227]

Der Standard rund um die DIN EN ISO 9000:2000 definiert Qualitätsmanagement als…
„aufeinander abgestimmte Tätigkeiten zur Leitung und Lenkung einer Organisation" [21, p. 4]

Durch die ISO 9000 Norm wird von den Organisationen verlangt, ihre Produkte, Prozesse und Dienstleistungen angesichts der Anforderungen der Kunden auszurichten.
Historisch entstammt die Norm der 70er Jahre vom Militär. In den 80er Jahren entwickelte sich daraus eine britische Norm, die heutigen ISO 9000er Reihe. [19, p. 9]
Eine Revision um die ISO 9000 wurde 2008 ins Leben gerufen, hatte aber keine strukturellen Änderungen widerfahren sondern eher eine Schärfung von Formulierungen um sich Fehldeutungen zu entziehen. [21, p. 136] Letztendlich hat die ISO 9001 mit einer Großrevision eine wesentliche Überarbeitung im Jahr 2015 erhalten. [21, p. 146]

Die Norm rund um die ISO 9000 Reihe gliedert sich nun in die folgenden Teilbereiche:

- DIN EN ISO 9000: Grundlagen und Begriffe
- DIN EN ISO 9001: Qualitätsmanagementsysteme und Forderungen
- DIN EN ISO 9004: Leitfaden zur Leistungsverbesserung
- DIN EN ISO 9011: Leitfaden für Audits von Qualitätsmanagementsystem und/oder Umweltmanagementsystem. [21, p. 121]

Die zuvor dargestellten vier Normen der sogenannten ISO 9000er Serie reflektieren die Basis um ein Qualitätsmanagementsystem. Sowohl dessen Begriffe, Anforderungen zur Zertifizierung als auch Anforderungen für die Schaffung von Qualitätselementen. Außerdem findet sich darin der wirksame Aufbau von branchenübergreifenden Qualitätsmanagementsystemen. [21, p. 121]

Ein Qualitätsmanagementsystem mithilfe der ISO 9001 ist ein angesehenes, weit verbreitetes Mittel der Wahl um Optimierung im Unternehmen zu erlangen. Eine Zertifizierung anhand des Qualitätsmanagementsystem nach der ISO 9001 kann demnach nicht unbedeutende Vorteile mit sich bringen und zudem als Instrument des Vertrauens fungieren. [21, p. 158]

In den meisten Fällen dient ISO 9001 für das Qualitätsmanagement als Grundlage für integrierte Managementsysteme wie dies im Kapitel 2.8 noch genauer erläutert wird. Österreich umfasst bereits rund 5.000 Unternehmen laut CIS [18], die nach ISO 9001 zertifiziert sind.
Die häufigste Variante besteht daher darin, ISO/IEC 27001 oder ISO/IEC 20000 nach dem bestehenden Qualitätsmanagement aufzubauen. Die beiden genannten Standards werden demzufolge noch genauer betrachtet. Allerdings ist in der Theorie jede andere Ordnung ebenso denkbar. [18]

Da die für ein besseres Verständnis notwendigen Grundlagen nun abgedeckt sein sollten, werden die nächsten beiden Kapitel, das IT Service Management und das IT Security Management von elementarer Bedeutung sein, um das daraus entstehende Assessment Tool zu entwickeln.

2.2. IT Service Management

Service Management ist mitunter gerade zu einem Modewort in der IT Branche empor gestiegen. Sämtliche anspruchsvolle Unternehmen haben in irgendeiner Form einen Plan, um optimal IT-Service Management zu dokumentieren. Zumeist geht es dabei in erster Instanz um Kosten einzusparen. Doch ist dies tatsächlich der Grundgedanke der sich hinter diesem Term versteckt? [20, p. 1]

Mit dem Terminus Service versteht sich eine festgelegte Aufgabe, beispielsweise eine Dienstleistung, welche nötig ist, um eine definierten Prozess auszuführen. [14, p. 30]
Darüber hinaus findet der Begriff IT Service Management mittlerweile vielerlei Anwendung, wobei es nicht einfach ist die eigentliche Verwendung beantworten zu können. In der ITIL Literatur selbst, findet sich folgende Verwendung des Begriffes: [20, p. 3]

„Service Management is a set of specialized organisational capabilities for providing value to customers in the form of services“ [22, p. 15]

Sinngemäß ist damit die Steuerung sämtlicher organisatorischer, fachlicher Fähigkeiten gemeint, welche zur Bereitstellung und zur Bildung von Mehrwert in Form von Services erzeugt wird.
Die genannten Fähigkeiten rund um die Nutzung von vorhandenen Ressourcen umzuwandeln in wertsteigernde Serviceleistungen kann als Kernaktivität von Servicemanagement betrachtet werden. [20, p. 3]

Unter dem Begriff IT-Service Management versteht sich also die Einbeziehung von Prozessen, Methoden und Technologien, welche relevant sind, um ideale Unterstützung der Geschäftsprozesse einer Organisation mit IT zu gewährleisten. ITSM stellt dazu den Grundstein, um eine bestmögliche IT-Umgebung mit all den notwendigen IT Services abzubilden. [12, p. 113]

Ziel ist es damit einem Kunden zu ermöglichen, dass dieser sich nicht um die IT-Service-Erbringung sorgen muss, sondern vielmehr voll und ganz den Fokus auf die Ausführung der eigentlichen Geschäftstätigkeit legen kann. Ein Kunde möchte sich deshalb gänzlich auf dessen Service Provider verlassen können und ist demnach auch bereit, dies mit einem entsprechenden Preis zu honorieren. Durch das Business sind Partner erwünscht,

die sich um diese Produkte und Resultate kümmern und eine einwandfrei funktionierende IT mithilfe von Dienstleistungen zur Verfügung stellen. [12, p. 113]
Vom reinen Technologie Lieferant, zum erfolgreichen strategischen Serviceanbieter mit messbaren Mehrwert überzugehen stellt IT-Organisationen oftmals vor Herausforderungen. IT Service Management verspricht Abhilfe zu diesen Themenstellungen zu schaffen. [7, p. 17]

Ein IT Service definiert sich dabei wie folgt: Er erstellt die Gelegenheit, für einen Kunden einen erheblichen Mehrwert zu generieren, indem das Ergebnis oder die Zielerreichung entsprechend verbessert oder begünstigt wird. Auf ihn selbst, entfallen dabei möglicherweise sämtliche Kosten und Risiken, er muss aber dabei keiner Verantwortung nachkommen.
Ein IT-Service ist basierend auf der Verwendung von Informationstechnologie und forciert dabei die Businessprozesse eines Kunden. Zum Zwecke des IT Service werden demnach Personen, Prozesse sowie Technologien in Verbindung gebracht. Dies alles sollte in einem entsprechenden Service Level Agreement bestimmt und festgehalten sein. [12, p. 113]

Ursprünglich war die IT Erbringer im Sinne von Lieferant von Produkten wie beispielsweise Hard- oder Software. Mit steigender Abhängigkeit von Organisationen und der Informationstechnologie sind diese nun allerdings als Dienstleistungsbereich zu betrachten. Demnach stellt sich die Frage wodurch ein Produkt von einem Service diversifiziert werden können:
Entgegen Produkten sind Services nicht greifbar, das heißt ein Service kann physisch nicht gegenwärtig sein und kann demnach nicht wie ein Produkt ausgehändigt werden. Services werden zur gleichen Zeit erbracht und konsumiert. Bei Produkten ist dies nicht der Fall. Services werden sowohl von Maschinen als auch von Menschen erbracht wodurch eine weitere Unterscheidung zu Produkten entsteht. [12, p. 113]

Im Fokus steht bei der Leistung eines Services die Wahrnehmung durch den Kunden. Der Wert des jeweiligen Service wird dabei durch den Kunden selbst bei entsprechender Unterstützung im Zuge der Geschäftstätigkeit wahrgenommen. Die darauf bezogene Erwartung der Kunden, sowie dessen Qualität spielt eine bedeutende Rolle, da speziell der Kunde und dessen Anwender bedeutende Einwirkung auf die Bereitstellung des Service ausüben. [12, p. 114]

Mittlerweile ist eine sehr starke Korrelation bezüglich des Erfolgs eines Unternehmens und der Abhängigkeit zur IT festzuhalten. Ziele von Organisationen können ausschließlich dann erreicht werden, wenn die richtigen IT-Services in entsprechender Qualität unterstützend vorhanden sind. Demzufolge ist eine Ableitung der Ziele der IT-Organisation zu jenen des Unternehmens unumgänglich. Nur so kann es gelingen, die hohen Ansprüche und Erwartungen der Organisation abzudecken. [7, p. 18f]

Werden die anfallenden Kosten von IT-Services über den gesamten Lebenszyklus hin betrachtet, so lässt sich feststellen, dass gerade durch dringende Anpassungen horrende Kosten verursacht werden. Umso mehr steht demnach die Aufgabe im Mittelpunkt, IT-Service Leistungen in vereinbarter Qualität und zu vereinbarten Kosten auszuliefern. [7, p. 19]
Dem IT-Service Management ist es daher zum Ziel gesetzt, Lieferung und Unterstützung von IT-Service Leistungen, maßgeschneidert auf die Anforderungen von Organisationen zu erbringen. [7, p. 19]

Da sich der Fokus dieser Arbeit schwerpunktmäßig auf ITIL sowie der ISO 20000 beschränkt werden unter anderem diese beiden detailreicher vorgestellt. Anschließend möchte zur Thematik auch noch Cobit kurz erwähnt werden, bezugnehmend auf dessen nicht unwichtiger Relevanz.

2.2.1. ITIL

Zahlreiche Organisationen sehen sich der Herausforderung konfrontiert, Kunden mit hohen Ansprüchen in Bezug auf IT-Services und diesbezüglicher Transparenz und Vergleichbarkeit zu bedienen. Nicht einfacher wird dies

durch die Tatsache, dass Organisationsstrukturen nicht mehr den Anforderungen der heutigen Zeit entsprechen. Eine Lösung verspricht das Servicemanagement, mitunter ITIL zu schaffen. [7, p. 17]
Unter der Information Technology Infrastructure Library, kurz ITIL genannt ist eine Sammlung von Vorschlägen und Referenzen gemeint, die bestmögliche IT Services anbieten können. [23, p. 50]
Herausgegeben, weiterentwickelt sowie gewartet wird ITIL vom Office of Government Commerce, kurz OGC. [2, p. 26] Ursprünglich war ITIL ein Produkt der CCTA „Central Computer and Telecommunications Agency", welche eine britische Organisation der Regierung darstellt. Im Jahr 2001 wurde die CCTA in die OGC übergeleitet. [7, p. 20]
Momentan befindet sich der ITIL Standard in der Version V3, kurz als ITIL 3.0 bezeichnet. Erschienen ist diese Versionierung im Jahr 2007. [2, p. 26]

Am Anfang war ITIL als eine Serie für das Service Management geplant und sollte mehr als 40 Bücher und 26 Module über IT Service beinhalten. Bezeichnet wurde damit die Erstversion als ITIL 1.0.
Mittels Anpassungen und Weiterentwicklung entstand zwischen den Jahren 2000 und 2004 ITIL 2.0, worin Adaptionen an die IT-Umwelt berücksichtigt und aufgenommen wurden. Diese Anpassung wurde in dieser Version in acht wesentliche Bücher zusammengefasst. [24, p. 38]

Nach Jahren hat sich die Informationstechnologie zu einem vermehrt kritisch wachsenden Faktor entwickelt wenn es um Geschäftsprozesse in Organisationen geht. Mangelhafte IT-Systeme haben dabei nicht selten erhebliche Verluste mit sich gebracht und damit immense Folgeschäden verursacht.
ITIL hat mit der Version 3 im Jahr 2007, diese Tatsache berücksichtigt und versucht, mit dem Abschnitt „Service Strategy" Wissen zugunsten der Ausrichtung der IT-Services festzuhalten und zu vermitteln. Diverse Providertypen als auch Sourcing Strategien finden nun Anklang in Bezug auf die Gestaltung von IT-Services.
Durch eine umfassende Erneuerung der im Jahr 2007 entstandenen ITIL Version 3 wurden weitere Erfahrungen rund um eine im Jahr 2011 erschienene weitere Überarbeitung, der ITIL Edition 2011 gesammelt.
Mit der Überarbeitung, ITIL Edition 2011 ist eine, laut Autoren, überarbeitete Version entstanden, welche ausdrücklich nicht als neue Version anzusehen ist. Bestehende Projekte bedürfen demzufolge keiner grundsätzlichen Anpassung. Ebenso gilt diese Tatsache für bestehende Prozesse, welche auf Grundlage von der ursprünglichen Version 3 implementiert wurden. Zusammenfassend lassen sich folgende wesentliche Erneuerungen der Edition 2011 festhalten: [20, p. 12f]

- Überarbeitung im Sinn der Einheitlichkeit der Struktur der fünf Bücher
- Überarbeitung und Austausch diverser Grafiken
- Überarbeitung von Prozessen und dessen Struktur in diversen Kapiteln
- Treffendere Beschreibung der Schnittstellen innerhalb des ITIL Lifecycles
- Einarbeitung von Feedback durch die ITIL Community [20, p. 12f]

Die aktuelle Version von ITIL gliedert sich demnach in drei wesentliche Teilbereiche:

- ITIL Core welche den Kernpublikationen entspricht
- ITIL Complementary Guidance worin die Ergänzungen beschrieben sind
- ITIL Web Support Services [24, p. 38]

Die Kernpublikationen von ITIL umfassen in der „Core" ein Bündnis von fünf Büchern in welchen ein Vorgehen durch einen Lebenszyklus von Service-Strategie, Service Design bis hin zu kontinuierlichen Service-Verbesserung dargestellt wird. In den genannten Büchern werden wiederum die folgenden Themen dargeboten:

- Service Strategy
- Service Design

- Service Transition
- Service Operation
- Continual Service Improvement [24, p. 38f]

Frei von einer erkennbaren Struktur ist das Service Management nicht mehr als eine Anhäufung von Verfahren auf Beobachtungen mit womöglich widersprechenden Zielen. Deshalb beschreiben die Bücher des „Core Guidance“ die Phasen im Service Lifecycle durch einen organisierten Rahmen über die Aktivitäten. [20, p. 15] Der Lifecycle von ITIL wird in folgender Grafik wie folgt dargestellt:

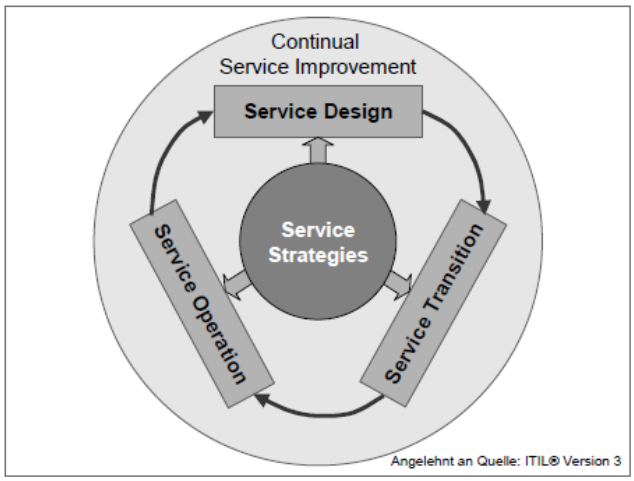

Abbildung 5 Service Lifecycle von ITIL [17, p. 62]

Im „Complementary Guidance“ werden über die Core hinaus weitere Ergänzungen mithilfe von Literatur bereitgestellt. Dies wird mittels Pocket Guides oder auch in einer online Subskription verwirklicht.
Im letzten Abschnitt der Teilbereiche, die Web Support Services, finden sich auf einer sperat dargestellten Plattform weiterführende Inhalte wie Templates oder Fallstudien. [20, p. 14]

In jedem Band der ITIL Bibliothek wird ein gewisser Themenbereich abgearbeitet. Dabei werden die diversen Grundlagen, Eckpfeiler und Ziele zu den relevanten Prozessgruppen erläutert. Auf Basis der Beschreibung passiert dabei eine ständige Überarbeitung rund um neue Erkenntnisse zum Gebrauch der IT-Infrastruktur. [7, p. 21]

Die ITIL Bücher werden daher kontinuierlich überarbeitet und komprimiert, um fortlaufend neue Erkenntnisse und Erfahrungen einzugliedern. Die nachstehende Grafik stellt die Bücherstruktur von ITIL dar. [7, p. 22]

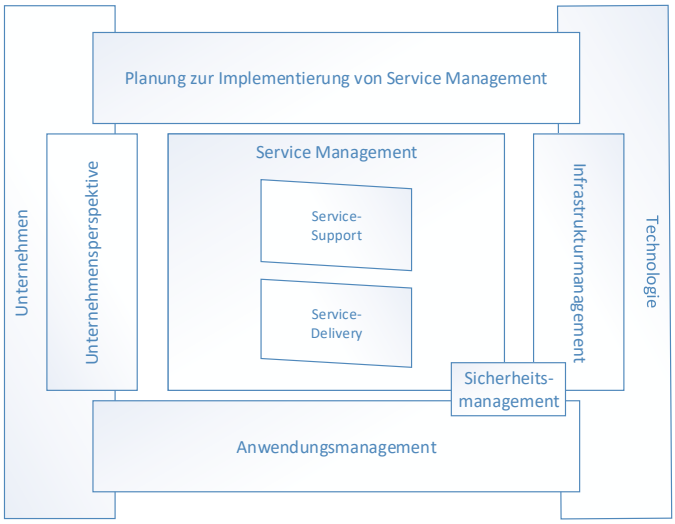

Abbildung 6 Bücherstruktur ITIL [7, p. 22]

Die dargestellte Grafik beschreibt die fünf Hauptbereiche von ITIL und dessen Büchern.

- Geschäftliche Perspektive mittels “The Business Perspective”
- Planung und Lieferung von IT-Services mittels „Service Delivery“
- Unterstützung und Betrieb der IT-Services mittels „Service Support“
- Management der Infrastruktur mittels „ICT Intrastructure-Management“
- Management der Anwendungen mittels „Applications-Management“

Ziel ist es mittels ITIL ein möglichst hohes Maß an Qualität bezüglich IT-Services zu liefern. Die Ausrichtung von Kunden steht demnach im Fokus. Wie auch andere Standards wird in ITIL versucht keine exakten Prozesse oder Abläufe zu definieren, vielmehr werden der Zweck und eine Richtung vorgegeben. Dies unterscheidet ITIL beispielsweise auch mit Standards wie die ISO 9000 und Total-Quality-Richtlinien in welchen definierte Prozesse und Beschreibungen exakt bestimmt sind. Aufgrund der sehr unterschiedlichen Prozessstrukturen der IT-Organisationen hat sich dies allerdings als wenig vorteilhaft herausgestellt. Demzufolge wurde ein „Best Practice“ Standard als erstrebenswert betrachtet, um eine praxistaugliche Norm für vielfältige Anwendungsfälle griffbereit zu haben. [7, p. 21]

Mittlerweile lässt sich der ITIL Standard als weltweit akzeptiertes Vorgehen für maßgebliche Steuerungsprozesse in der IT betrachten. ITIL stellt dafür eine Bibliothek mit „best practices“ zur Verfügung welche die Methoden zur Planung und Steuerung von IT-Servicemanagement unterstützen. [2, p. 26]
Im ITIL Rahmenwerk wird daher versucht, Services für Kunden effizient in Bezug auf die Kosten zu betreiben und darüber hinaus bestmögliche Kundenorientierung zu bieten. Bei dem empfohlenen Vorgehen handelt es sich um erprobte Vorgehensweisen aus der Praxis. Demzufolge wurde die Anwendung von ITIL in mehrfachen wissenschaftlichen Studien analysiert und dessen Tauglichkeit bestätigt. [23, p. 50]

ITIL wird darüber hinaus als Herstellerunabhängig betitelt und bezeichnet sich wie bereits erwähnt, als eine Sammlung von Best Practices. Um für Kunden einen skalierbaren Ansatz zu gewährleisten, welcher überdies Effizienzsteigerung verspricht und dabei gleichbleibende Service sicherstellt, wird ein prozessorientierter Ansatz erstellt. [23, p. 50]
Wesentlicher Erfolgstreiber von ITIL ist dessen unverkennbare Tauglichkeit für die Praxis, womit sämtliche Organisationen ihre Prozesse individuell und optimal umzusetzen vermögen. [16, p. 35]

Durch bessere Bewertung, Steuerung und Kontrolle kann in Unternehmen ein hohes Maß an Professionalität in Hinsicht der IT-Organisation garantiert werden. Kriterien zur Messung können ein wesentlicher Treiber, zur Steuerung und Beurteilung sein. [23, p. 50]
ITIL ist zu gewissen Branchen unabhängig und bietet dadurch nicht zuletzt, eine außerordentliche Allgemeingültigkeit. Durch die ITIL Gemeinde, welche durch das itSMF, IT Service Management Forum vorangetrieben wird, wird ein fortlaufender Austausch an Informationen zur Verfügung gestellt. [16, p. 35]

Die ITIL Bibliothek stellt ihr Wissen in etwa 40 Veröffentlichungen in englischer Sprache zur Verfügung. Wesentliche Bestandteile wie beispielsweise der Service Support oder der Service Delivery sind zudem bereits in deutscher Sprache erschienen. [2, p. 26]
Sowohl die ITIL Bücher als auch weiterführende Publikationen rund um die Thematik, werden kostenlos angeboten. [4, p. 86]
Aufbauend zu ITIL hat das British Standard Institute außerdem den BS 15000 Standard erstellt. Mit diesem ist es möglich, ITIL mit dem BSI Code of Practice für IT Service Management (PD0005) zu integrieren. Dadurch ergibt sich die Grundlage, den Standard entgegen den Formalitäten zu prüfen. Aus diesem Anlass ist es Organisationen möglich, sich nach dem Standard zu zertifizieren. [2, p. 26]

Hauptaugenmerk von ITIL ist natürlich nicht die IT-Security. Auch hier ist es im Sinne von ganzheitlichen Managementsysteme nützlich, die sichere Handhabung von Daten in IT-Systemen mittels Dokumentation von IT-Prozessen und Organisation zu forcieren. Gerade bei Umgestaltungen beziehungsweise Neustrukturierungen von Prozessen nach ITIL, kann für die IT-Security und dessen Vorhaben das Einfließen dieser Aufzeichnungen einen erheblichen Mehrwert verzeichnen. [4, p. 86]
Sowohl in der Grunddefinition der Informationssicherheit, wie auch auf die damit einhergehenden Ziele in diesem Bereich, wird wiederholt in den Büchern hingewiesen. Als Fundament für eine unternehmensübergreifendes IT-Security Management ist dies allerdings bei Weitem nicht abgeschlossen. [4, p. 87]

Da der Fokus dieser Arbeit eng verknüpft mit der Domain der IT-Security einhergeht, soll folgender Unterpunkt die ITIL Security außerordentlich hervorheben und somit kurz erläutern.

2.2.1.1. ITIL Security Management

Ab ITIL V3 ist der ISM-Prozess, Informationssicherheitsmanagementprozess als Teilbereich der Service Design Phase untergebracht. In dieser Phase wird sichergestellt, dass die Informationssicherheit mit jener der Sicherheit im Unternehmen verbunden ist. Zudem wird gewährleistet, dass sämtliche Service Tätigkeiten im Zuge der Informationssicherheit ausgeführt werden. Das ISM trägt dabei Verantwortung, dass die Politik der Informationssicherheit im Unternehmen den Anforderungen der ganzheitlichen Organisation entspricht. Dabei werden korrespondierende Kontrollelemente der Sicherheit zum Schutze der IT bereitgestellt. [17, p. 63]

Ein ISMS, welches in diesem Zusammenhang von ITIL auf die ISO 27001 referenziert, inkludiert zur zentralen Lenkung sowohl die sogenannten „Control's" als auch die Phasen Plan, Implement, Evaluate und Maintain die an den PDCA-Zyklus erinnern. Hauptaugenmerke in der Phase der Planung sind Empfehlungen zugunsten entsprechenden Maßnahmen der Sicherheit, aufbauend auf den Grundanforderungen seitens der Organisation. Diese enthalten die IS-Politik, Anforderungen von Service und Operational Level Agreements, kurz SLA und OLA, Underpinning Contracts, kurz UC sowie auch die Vorgaben im Sinne der Gesetzgebung. In der Phase der Implementierung werden anschließend Werkzeuge und Kontrollelemente zur Ausführung der IS-Politik verwendet, wobei dabei angemessene Verfahren führend sind. Die Platzierung von Verantwortlichkeiten bezüglich der Assets sowie auch die Einteilung von Informationen spielt dabei eine nicht weniger wichtige Bedeutung. Die Phase der Evaluierung umfasst externe als auch interne Audits. Zweck der Pflegephase ist die Überwachung und Kontrolle von Sicherheitsmaßnahmen sowie der Ausbau von Vereinbarungen zum Zwecke der Sicherheit. [17, p. 63]

Nachdrücklich verweist ITIL darauf, dass die Sicherstellung von Security weder als einzelner Vorgang im Lebenszyklus betrachtet werden kann, noch im Zuge der Technologie im System aufgehoben werden kann.
Als ausschlaggebende Prozesse, welche Schnittstellen zum ISM darstellen, erwähnt ITIL folgende stichwortartige Punkte:

- Incident- und Problem Management im Zuge von Ereignissen der Sicherheit
- IT Service Continuity Management im Hinblick der Analyse auf die Geschäftseinflüsse, sowie Tests von Kontinuitätsplänen
- Service Level Management im Sinne der Erfassung von Anforderung der Sicherheit
- Change Management in Bezug der Änderungsbewertung
- Configuration Management bezüglich der Sicherheitsklassifizierung
- Availability Management hinsichtlich der integrierten Risikoanalysen
- Capacity Management im Hinblick der Auswahl zu neuen Technologien
- Financial Management im Zuge der Bereitstellung von Finanzmitteln
- Supplier Management bezüglich vertraglicher sicherheitsrelevanter Inhalte [17, p. 63f]

Dem ITIL Framework zufolge, ist der nächste logische Schritt, das „ISO Pendant“ an dieser Stelle vorzustellen.

2.2.2. ISO/IEC 20000 Serie

Der Standard ISO 20000 „Information technology – Service management“ ist eine Norm, mit der Möglichkeit zur Zertifizierung für IT-Servicemanagement. [2, p. 26] Mittelfristig wird sich laut Beims [20, p. 225] , die ISO 20000 zu einer unentbehrlichen Möglichkeit der Zertifizierung wandeln sofern es um IT-Service Anbieter geht. Im Unterschied zu Service Management Frameworks wie es ITIL darstellt, ermöglicht die ISO/IEC 20000 Aussicht auf eine Zertifizierung und bringt damit den Nachweis mit sich, angemessene Qualität darzulegen. Ausschreibungen ohne die Anforderung nach Konformität von ITIL sind bereits kaum mehr zu finden, wobei eben solche Formulierungen zu hinterfragen sind. Zu einer „Konformität“ zugunsten einer Sammlung von „best practice“ Ansätzen wie es ITIL darstellt, ist es schwierig einen Nachweis zu erbringen. Durch die ISO/IEC 20000 kann hier angesetzt werden womit eine entsprechend konforme Bewertung einhergeht. [20, p. 225]

Der Ursprung der Norm ist zurückzuführen auf den British Standard BS 15000 der British Standard Institution. [2, p. 26]
Dieser British Standard wurde im Jahr 2000 ins Leben gerufen und daraufhin in den Jahren 2003 und 2004 überarbeitet. Demzufolge bestand ursprünglich der Standard aus den folgenden Elementen:

- BS 15000-1: 2002 Specification for Service Management
- BS 15000-2: 2003 Code of Practice for Service Management
- PD 0015:2002 IT-Service Management Self-Assessment Workbook [20, p. 226]

Die ISO/IEC 20000 Norm kann als messbarer Standard im Bereich der Qualitätssicherung für IT-Servicemanagement bezeichnet werden. Die ISO 20000 spezifiziert demnach die Mindestanforderungen durch Prozesse einer Organisation um IT-Services in bestimmter Qualität abbilden und managen zu können. [7, p. 28f]
Die ISO/IEC 20000, auch als „Information Technology Service Management“ bezeichnet, ist ein internationaler Standard und fördert sowohl ein prozessorientiertes als auch integriertes Vorgehen bei der Planung und Bereitstellung von IT-Services. [20, p. 226]

Durch diesen ISO Standard können Kundenanforderungen effektiv durch einen integrierten Ansatz von Prozessen, mithilfe von IT Services verwirklicht werden. Dazu werden sowohl Anforderungen als auch ein Prozessmodell zur fortlaufenden Verbesserung der Prozesse beschrieben. [2, p. 26]
Die ISO/IEC 20000 illustriert für Service Management einen integrierten prozessorientierten Ansatz. Im ersten Teil wird dabei den Anforderungen nachgekommen, Services in jener Qualität auszuliefern, damit Kunden ihren bestmöglichen Nutzen dabei erlangen: [17, p. 59]
Für diese Zwecke kennt die ISO 200000 folgende Prozessgruppen:

- Service Delivery Prozesse
- Release Prozesse
- Resolution Prozesse
- Beziehungsmanagement-Prozesse
- Steuerungsprozesse [17, p. 59]

Im Jahr 2005 wurde daraufhin eine grundlegende Überarbeitung auf Basis dieser Standards unternommen, wodurch dieser nun wie folgt in drei wesentliche Elemente gegliedert wurde:

- Part 1, die ISO/IEC 20000-1:2011, beschreibt die Spezifikationen der Norm im Sinne der sogenannten “shall” Anforderungen welche unumgänglich durchgeführt werden müssen. Zum Erlangen der erwünschten Zertifizierung müssen demzufolge sämtliche in der Norm enthaltenen Anforderungen entsprechend erfüllt sein.
- Part 2, die ISO/IEC 20000-2:2011, hingegen beschreibt die Empfehlungen welche notwendig sind um eine adäquate Umsetzung zu ermöglichen. Die Beschreibung erfolgt dabei mithilfe von “should” Anforderungen. Damit stellt dieser Teil der Norm “Guidance on the application of service management systems” zusätzliche Leitlinien zur Verfügung um Auditoren und Service Providern eine möglichst wertvolle Umsetzung von Part 1 zu ermöglichen.
- Part 3, die ISO/IEC 20000-3: 2009 erweitert Part 2 mit Anleitungen um den Scope festzulegen sowie auch die Konformität zu bestätigen.
- Part 4, die ISO/IEC 20000-4: 2010 skizziert ein Prozessreferenzmodell zugunsten der Prozesse zum Service Management und fungiert überdies als Anhaltspunkt zur Errichtung eines Prozessbewertungsmodells in Anbetracht der ISO/IEC 15504.
- Part 5, die ISO/IEC 20000-5: 2010 stellt einen exemplarischen Ratgeber dar, um das Service Management zu implementieren. Dabei wird vor allem darauf geachtet, den Mindestanforderungen der ISO/IEC 20000-1 zu entsprechen. Besonders spricht dieser Teil Service Provider an, welche an einer Konformität zugunsten der ISO/IEC 20000 arbeiten beziehungsweise in diesem Umfeld als beratende Dienstleister in Erscheinung treten. [20, p. 226]

Derzeit widerfährt die ISO/IEC 20000-1 einer Überarbeitung hinsichtlich einer neuen Struktur und ist für die Wiederveröffentlichung im Jahr 2018 vorgesehen. [25]

Die Struktur rund um die ISO/IEC 20000 gliedert sich in neun Abschnitte. Den ersten fünf, werden Vorgaben und Rahmenbedienungen zugeschrieben, wobei Abschnitt 6 bis 9 den jeweiligen IT-Service Management Prozessen gewidmet ist. Die Folgende Grafik zeigt einen Überblick der ISO/IEC 20000 Struktur:

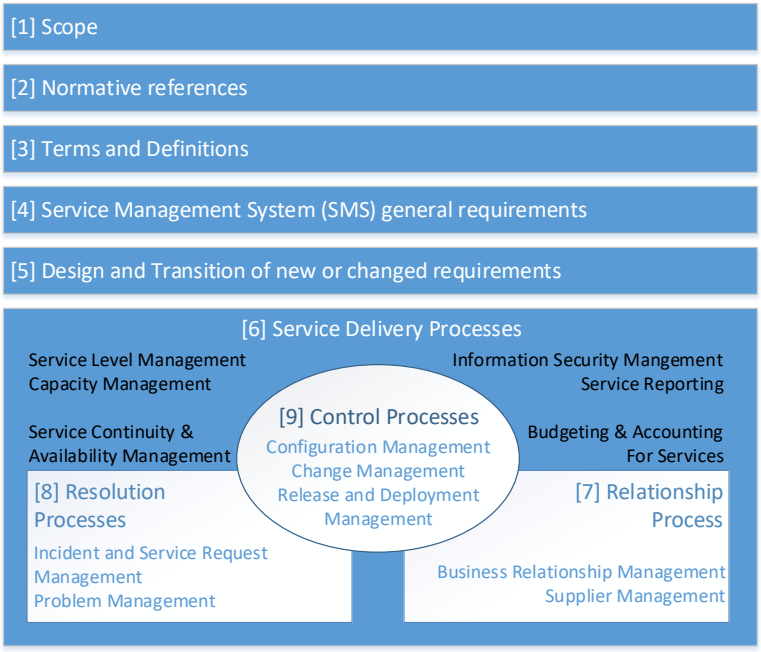

Abbildung 7 ISO/IEC 20000 Struktur und Aufbau [20, p. 228]

Die einzelnen 9 Abschnitte der dargestellten Abbildung 7, werden nun im Folgenden kurz zusammengefasst.

Abschnitt 1, der Scope rund um die ISO/IEC 20000 reglementiert sowohl die Planung, den Aufbau, die Einführung, den Betrieb, die Überwachung, die Prüfung, die Aufrechterhaltung als auch die Verbesserung zugunsten des Service Managements. Zudem sind die Anforderungen hinsichtlich Design, Übertragung, Lieferung und Verbesserung von Services darin vorgeschrieben. Damit hilft die ISO/IEC 20000 wesentlich im Bezug einer objektiven Vergleichbarkeit zwischen diversen Service Anbietern. Es entsteht ein solides Grundelement, um bei Ausschreibungen eine konsistente Bewertung zu ermöglichen.

Als Grundlage zur einheitlichen Nomenklatur des Service Managements erzeugt die ISO/IEC 20000 beispielsweise eine Erfordernis für eine ausnahmslose und konsistente Supply Chain. [20, p. 228]

Abschnitt 2, welcher sich mit den Normativen Verweisungen befasst wurde eingebaut, um eine konsistente Nummerierung, am Beispiel der ISO 20000-2, zu erlangen. [20, p. 229]

Abschnitt 3, enthält die Definitionen und Begriffe, welche im weiteren Verlauf der Norm Referenz finden. Im Detail sind dabei die folgenden Begriffe wie Availability, Configuration Baseline, Continual Improvement und viele mehr umfasst, um nur einige hier anzuführen. [20, p. 229]

Abschnitt 4, beschreibt die allgemeinen Anforderungen im Hinblick auf das Service Management System. Dabei werden die Vollständigkeit sämtlicher Prozesse, Tools und Ressourcen, welche Koordination zur Zielerreichung verlangen koordiniert. Sich anbahnende Aufgaben des Management sollen in Bezug auf Qualität geplant, durchgeführt, dokumentiert und stetig verbessert werden. Mittels eines gut arbeitenden Managementsystems werden die effektive und ideale Bereitstellung von IT-Services ermöglicht. [20, p. 231]

Mithilfe des PDCA Zyklus nach Deming, wie er in Punkt 2.1.4.1 bereits vorgestellt wurde, umfasst dieser Bestandteil, ergänzend zur Management Ebene, auch noch unter anderem die Planung und Durchführung

sämtlicher erforderlichen Maßnahmen zur Konstruktion eines stetigen Verbesserungsprozesses im Service Management System. [20, p. 231]

Abschnitt 5, kennzeichnet das Design und die Transition von neuen beziehungsweise geänderten Services. Dabei wird beschrieben, inwiefern neue oder geänderte Services in beschlossener Qualität zu fixierten Kosten bereitgestellt werden können. Um dies zu schaffen, beschreibt die Norm entsprechende Mindestanforderungen. [20, p. 234]

Die Übrigen Abschnitte 6 bis 9 bearbeiten die relevanten ISO/IEC 20000 ITSM Prozesse und sind nochmals in fünf Prozessbereiche gegliedert. [20, p. 235]

Abschnitt 6, rund um die Service Delivery Prozesse entspricht weiten Teilen derselben Prozesse von ITIL 2 und schildert die Planung von Services auf längere Sicht. Dabei werden Elemente wie Service Level Management, Service Reporting oder Capacity Management beispielsweise erläutert. [20, p. 236]

Abschnitt 7, umfasst Relationsship Prozesse und beinhaltet demnach die Prozesse Business Relationship Management und Supplier Management. Sämtliche Beziehungen eines Service Anbieters und dessen Kunden werden darin angeführt. Der Abschnitt gewährleistet, dass beiden Parteien sowohl Bedürfnissen und Fähigkeiten als auch die Grenzen bewusst sind und überdies die Pflichten und Verantwortungen kennen. [20, p. 239f]

Abschnitt 8, als Resolution Prozesse betitelt, nennt die Handhabung mit Serviceaussetzungen und versucht Störungen und Ausfälle zu vermeiden. Die darin erwähnten Prozesse umfassen Incident and Service Request Management sowie Problem Management. [20, p. 241]

Abschnitt 9, mit dem Titel Control Prozesse versehen, ist im Gebrauch zur Beschaffung von Informationen. IST Zustände der IT-Infrastruktur aber auch die Effektivität des Änderungsmanagement stehen dabei im Fokus der Informationsbetrachtung. Die im Abschnitt geschilderte Prozessgruppe umschreibt Configuration Management, Change Management sowie auch Release and Deployment Management. [20, p. 242]

Darüber hinaus ist die ISO/IEC 20000 auf Basis der Grundlagen des Qualitätsmanagements orientiert, wie dies genauer in ISO/IEC 9000 erläutert ist. [2, p. 27] Der Geltungsbereich welchem die ISO/IEC 2000 zugrunde liegt, veranschaulicht folgende Grafik.

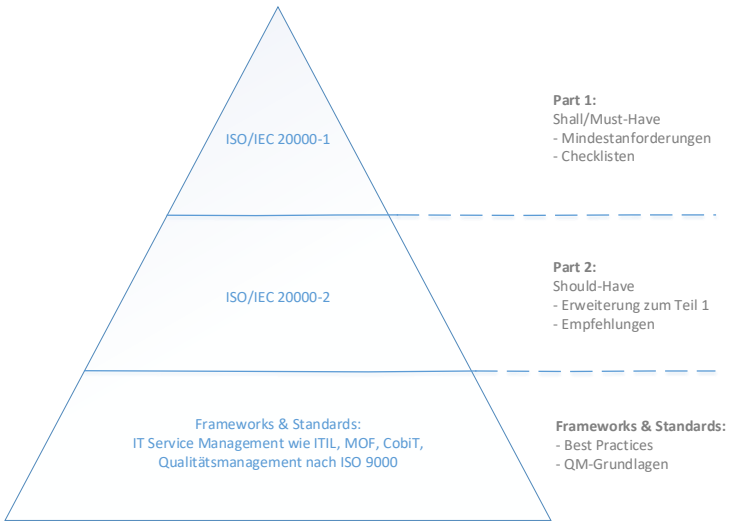

Abbildung 8 Geltungsbereich der ISO/IEC 20000 [20, p. 227]

Die ISO Norm 20000 kann als konform zu ITIL betrachtet werden. ITIL ist im Gegensatz zur ISO Norm als „best practise“ Ansatz allerdings nicht zertifizierbar und stellt demnach keine Anforderungen im Hinblick auf die Umsetzung. In der ISO Norm 20000 werden Inhalte mit der ISO Norm 9000 „Quality management systems – Fundamentals and vocabulary“ in Verbindung gebracht. Die ISO Norm bedient sich dabei auch an den „best practises“ von ITIL und ermöglicht allerdings dabei eine Norm zur Zertifizierung. [2, p. 27]
Demnach kann einer entsprechenden Umsetzung der ISO 20000 gegebenenfalls eine Zertifizierung folgen. Damit wird es möglich eine Organisation und dessen Management von IT-Services mittels international anerkannten Standards objektiv zu beurteilen und zu vergleichen. Die Zertifizierung selbst, muss daher von einer autorisierten Organisation, einem sogenannten Registered Certification Body, kurz RCB erfolgen. [7, p. 29]

Als Basis bedient sich die ISO/IEC 20000 Norm für die Service-Management-Prozesse am PDCA-Zyklus, wie er bereits im Abschnitt 2.1.2.1 erläutert ist. Die ISO Norm referenziert für alle Prozesse zum Einsatz des Plan-Do-Check-Act Zyklus. [17, p. 60]
Im Sinne der Informations-Security verweist die Norm zum ISO/IEC 27002, welche hierzu genauere Anweisungen verspricht. Die ISO 20000-1 verlangt, dass die Informationssicherheit vom Management freigestellt wird und diese offen an sämtliche Stakeholder kommuniziert wird. Ebenso werden sämtliche zweckmäßigen Kotrollelemente verlangt. Ergänzend sollen sicherheitsrelevante Vorfälle entsprechend dem Incident Management berichtet und dokumentiert werden. [17, p. 60]
Die ISO/IEC 20000-2 erwähnt überdies ergänzend, dass beispielsweise Assets der IT wie eine Rechnung, Dokumente und Informationen festgehalten und klassifiziert werden müssen um die jeweilige Verantwortlichkeiten im Sinne der Asset-Eigner zu ermitteln. Eine stetige Bewertung des Sicherheitsrisikos ist ebenso dokumentiert festzuhalten. Die jeweiligen Risiken dabei, werden sowohl nach der Art der Bedrohung, der Wahrscheinlichkeit des Eintritts als auch dessen möglichen Folgen und Erfahrungswerten in die Dokumentation eingespeist. Die ISO/IEC 20000-2 verlangt außerdem die genaue Definition von Rollen und dessen Verantwortlichkeiten sowie auch Schulungen im Sinne der Sensibilisierung. Sämtliche Änderungen dürfen keine Auswirkung auf die Kontrollelemente ausüben. [17, p. 60]

Zuletzt möchte erwähnt werden, dass ein großer Anteil an Übereinstimmungen von Prozessen bezüglich der ISO/IEC 20000 und ITIL vorliegt. Dies ist nicht zuletzt durch die Tatsache gegeben, dass sich einige Autoren sowohl an dem einen als auch anderen Projekt beteiligt haben. Die Erfüllung der ITSM-Prozesse rund um ITIL bewirkt eine ausgezeichnete Ausgangssituation für eine Zertifizierung der Organisation in Betracht auf die ISO/IEC 20000. [20, p. 245]

Als abschließender Unterpunkt zum IT Service Management folgt noch eine zusammengefasste Vorstellung von Cobit da sämtliche Querverweise und Referenzen zu diesem Standard abgedeckt werden sollen.

2.2.3. COBIT

Experten zufolge wird COBIT als Regelwerk, ergänzend zu ITIL im Service Management, bezeichnet. [26] Cobit, besser gesagt Control Objectives for Information and related Technology ist ein Produkt des Governance Institute, kurz ITGI sowie der Information Systems Audit and Control Association, auch als ISACA bekannt. Mittels der sogenannten Control Objectives wird im Zuge des COBIT Frameworks das IT-Governance eines Unternehmens unterstützt. Mittels dem COBIT-Framework soll erreicht werde, dass eine Organisation dessen Gewinn, durch die Fokussierung der IT auf die Geschäftstätigkeit, maximieren kann. Zudem ist sichergestellt dass sämtliche IT-Risiken effektiv gesteuert werden können sowie dass die IT-Ressourcen bestmöglich angewandt werden. COBIT nennt sich selbst ein allgemein renommiertes Rahmenwerk zur Kontrolle für die IT. [17, p. 65] Der Einbezug von COBIT im Service Management, als komplementären Schritt zu weiteren Service Management Standards wie beispielsweise ITIL wird als zwangsläufiger Evolutionsschritt betitelt. [26]

Zur Unterstützung von COBIT wurde demnach bei der Erstellung des Referenzmaterials durch die folgenden „Best Practices“ und Normen folgendes angewendet:

- ISO 17799:2005
- ITIL
- Reifegradmodell CMM und CMMI
- Project Management Body of Knowledge (PMBOK) [17, p. 65]

Im COBIT Rahmenwerk bildet sich die Form eines dreidimensionalen Quaders, welcher mithilfe der Achsen Anforderungen im Hinblick auf Geschäftliches in horizontaler Richtung darstellt. Hingegen werden in vertikaler Richtung die IT-Ressourcen aufgelistet. Geschäftliche Anforderungen deuten auf Kriterien wie Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Gesetzeskonformität sowie Zuverlässigkeit im Sinne der Informationen. Als IT-Ressource versteht COBIT Anwendungen, sämtliche Infrastruktur, das Personal sowie auch die Informationen selbst. Die IT-Prozesse sind wiederum unterteilt in die Ebenen Domänen, Prozesse sowie Aktivitäten. [17, p. 66]

Das COBIT Prozessmodell ist unterteilt in vier Domänen welche sich wie folgt gliedern:

- Planen und Organisieren
- Beschaffen und Implementieren
- Liefern und Unterstützen
- Überwachen und Prüfen [17, p. 66]

Diese vier Domänen sind wiederum in 34 generische Prozesse, sowie 214 Aktivitäten heruntergebrochen. Für die jeweiligen Prozesse sind zudem nochmals spezifische Kontrollziele sowie Merkmale im Sinne des Reifegrades festgehalten. [17, p. 66]
Zur Darstellung der Inhalte in COBIT enthält die Domäne „planen und organisieren“ zehn Prozesse und kümmert sich abseits von strategischen und architektonischen Themengebieten, ebenso dem Projekt-, Qualitäts- und Personalmanagement. Der Domaine „beschaffen und implementieren“ ist beispielsweise die Versorgung von IT-Ressourcen und das Releasemanagement zuzuschreiben.
In der Domäne „liefern und unterstützen“ sind dreizehn Prozesse zu verzeichnen. Darunter sammeln sich Aufgaben hinsichtlich Management, welche ebenso aus ITIL bekannt sind. In ITIL ist dies im Service Support, Problem- und Konfigurationsmanagement, dem Service Delivery Management, dem Service Level Management,

dem Kapazitäts- und Performancemanagement als auch weiteren Themenbereichen bekannt welche sich im Finanz-, Sicherheits- oder Kontinuitätsmanagement auseinander setzen. Im Gegensatz zu ITIL verfolgt COBIT eine ausgeprägte Sicht im Sinne der Prozessorientierung für Kontrolle und Reifegrad. [17, p. 66]

Um zu verstehen was Kontrolle in COBIT bedeuted, muss die Domäne „liefern und unterstützen“ und deren Prozess zur Sicherstellung der Systemsicherheit ergründet werden. COBIT beansprucht als oberstes Kontrollziel in einem Sicherheitsmanagementprozess, um Schutz jeglicher IT-Ressourcen zu gewährleisten, dass Integrität der Informationen herrscht. Darunter verstehen sich definierte Rollen und Verantwortlichkeiten, Verfahren als auch Richtlinien sowie Testen und Monitoring. [17, p. 66]
Die anschließende Ebene welche mithilfe von detaillierten Kontrollzielen arbeitet, fokussiert sodann auf Aktivitäten, deren Prozessen beziehungsweise Inhalt. Beispielsweise wird versucht zu gewährleisten, dass Viren, Würmer, Spyware als auch sämtliche weitere betrügerische interne Software vor den IT-Systemen ferngehalten werden. Ein Maß der Erfüllung der IT-Kontrollziele dieses Prozesses kann erreicht werden, indem die Menge der Systeme ermittelt wird, auf welche die Anforderungen zugunsten der Sicherheit nicht erfüllt werden. [17, p. 66f]

Als wesentliche Stärke von COBIT sind die Menge an Kontrollen zu erwähnen, womit eine ideale Messbarkeit, Überwachung und Steuerung zum Zwecke der IT-Prozesse gewährleistet wird. Die jeweiligen Prozesse hingegen sind dabei limitiert festgehalten. An dieser Stelle stellen sowohl ITIL als auch die ISO 200000 Dokumentationen, Ansätze für die Prozesse zur Verfügung, wobei in diesen wiederum weniger Kontrollen durchgeführt werden. [17, p. 67]

Dem IT Service Management zufolge widmen wir uns im nächsten Abschnitt dem IT Security Management um den zweiten wesentliche Bereich rund um das entstehende Assessment Tool zu definieren.

2.3. IT Security Management

Bevor einzelne Security Management Standards vorgestellt werden, dienen die kommenden Absätze um einen ganzheitlichen Einblick zum Thema Security Management zu erarbeiten.

Die Informationssicherheit stellt keinen Selbstzweck dar, vielmehr eine Anhäufung von Qualitätsmetriken, welche im Hinblick auf eine Organisation unbedingt verfolgt werden müssen. [16, p. 7]

Organisationen benötigen für deren Geschäftstätigkeiten Informationen sämtlicher Art, um bestmöglich eine Produktion zu gewährleisten oder Dienstleistungen in einer Art von Service zu unterstützen. Diese Informationen werden seit jeher verwendet, wie beispielsweise jene bezüglich Kunden und Lieferanten oder auch über interne Abläufe. Allerdings hat sich im Laufe der Zeit durch die Digitalisierung die Informationsmenge vervielfacht. Unverändert ist jedenfalls die Tatsache dass die Informationen gerade dann schützenswert sind, sobald diese von Geschäftsprozessen benötigt werden. [16, p. 7]

Die gegenwärtigen Geschäftsprozesse hingegen sind demnach eine Folge aus übergeordneten Unternehmenszielen. Geschäftsprozesse stellen Forderungen hinsichtlich der Qualitätsmerkmale an die jeweiligen Informationen. Dabei kommt es oftmals zu den größten Problemen, da Informationen aufgrund unzureichender Qualität nicht die gewünschten Ergebnisse liefern. Eine Möglichkeit dabei ist die Fachbereiche mittels Modellierungsverfahren, wie beispielsweise UML in die IT-Diktion zu integrieren. [16, p. 7]
Durchaus gleichbedeutend ist es, in diesem Zusammenhang auch die nicht funktionalen Qualitätsanforderungen in Betracht zu ziehen. Wartbarkeit, Benutzbarkeit oder Performance sind nur wenige Beispiele die man hier anführen kann. [16, p. 8]

An diesem Punkt kommt das Security Management ins Spiel, indem damit die Qualitätsmerkmale entsprechend der Information Security geplant, unterstützt, überwacht und entwickelt werden. Die Merkmale der Qualität

werden dabei wie folgt, in die drei wesentlichen Punkte der CIA Triade, Confidentiality, Integrity und Availability unterteilt. Grafisch dargestellt ist dies in der folgenden Abbildung. [16, p. 8]

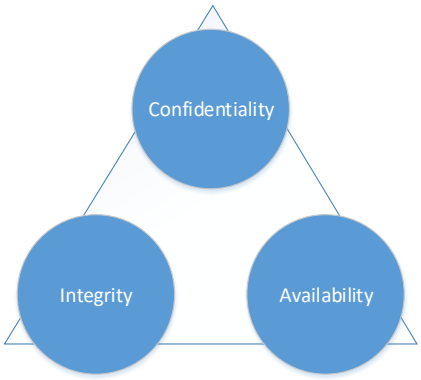

Abbildung 9 CIA Triade

Confidentiality, zu Deutsch die Vertraulichkeit, repräsentiert, dass auf Information nur berechtigte Personen und Systeme Zugriff erlangen.
Integrity, zu Deutsch Integrität, beschreibt die Dimension in welcher Informationen gespeichert, verarbeitet oder übertragen werden. Ausschlaggebend ist dabei die Tatsache, dass Informationen nicht durch Unbefugte manipuliert wurden und somit unverändert ihr Ziel erreichen.
Availability, zu Deutsch Verfügbarkeit, vermittelt die Stufe in welcher das IT Service zu festgelegten Zeiträumen zur Nutzung erreichbar ist. [16, p. 8]

Zu den zuvor genannten, drei wesentlichen Information Security Qualitätsmerkmalen der CIA Triade sind weiters noch folgende Qualitätsmerkmale zu hinzuzufügen.

- Authentizität (englisch Authenticity)
- Zurechenbarkeit (englisch Accountability)
- Vertrauenswürdigkeit (englisch Trustworthiness)
- Unleugbarkeit (englisch Non-Repudiation) [16, p. 8]

In der Information Security wird eine Information demnach dann als sicher eingestuft, wenn Vertraulichkeit, Integrität sowie Verfügbarkeit entsprechend vorhanden und garantiert sind.
Im Anschluss der Definition der Qualitätsmerkmale, müssen die Informationen entsprechend der Anforderungen klassifiziert werden. Mittels der Klassifizierung soll sichergestellt werden, dass der Aufwand entsprechend dem Schutz bestmöglich funktioniert. Aufbauend auf der Klassifizierung folgt demnach die Planung von Maßnahmen und deren Implementierung. [16, p. 9]

Im Security Management werden die Maßnahmen überwacht und der Unternehmensleitung entsprechend berichtet. Diese kann anschließend aus der Erreichung der Sicherheitsziele die Unterstützung zu den Unternehmenszielen ableiten. Zweck des Prozesses ist eine angepasste Information Security zum Unternehmen. [16, p. 9]

Die nachfolgenden Unterkapitel beschreiben die wichtigsten Security Management Standards. Dabei werden diese kurz vorgestellt, um anschließend mit denen des Service Management in Verbindung gebracht zu werden. Der Einfachheit halber wird die ISO/IEC 27000 Reihe in Folge oftmals kurz als ISO 27k, ISO 27000 beziehungsweise ISO 27k-Reihe oder Familie bezeichnet.

2.3.1. ISO/IEC 27000 Familie

Das Regelwerk der ISO/IEC 2700x, oder auch ISO-27k-Reihe genannt, ist hinsichtlich der Aufgabe zum Informations-Sicherheits-Management entstanden. Ziel ist es Sicherheitsmanagement mit Fokus auf Informationstechnologien restlos abzudecken. [27, p. 164] Kurz erwähnt, ist das zentrale Thema der ISO 27k Familie das Informationssicherheitsmanagement, kurz ISM. [17, p. 49]

Rund zehn Jahre zuvor konnte die ISO/IEC 27000 noch als schlichte Norm wahrgenommen und der IT-Grundschutz im Gegenzug als umfangreich betitelt werden. Diese Auffassung hat sich in den vergangen Jahren allerdings komplett neu gestaltet. Mittlerweile umfasst die Familie über 29 Veröffentlichungen, sowie weitere bevorstehende Entwürfe für neue Substandards. Bei dieser Auswahl, ist es selbst für Fachkräfte schwierig, den Überblick zu bewahren. Demzufolge kann zum jetzigen Zeitpunkt in Anbetracht der ISO/IEC 27000 Familie nicht mehr von einer schlichten Norm gesprochen werden. [28, p. 37]

Um die ISO/IEC 2700x bildet sich ein Rahmenwerk zur Verwirklichung eines Informations-Sicherheits-Management-System, kurz ISMS. Anhand des ISMS werden die Anforderungen des Grundschutzes, sowie die vom Management der IT-Security und dessen Risiken, berücksichtigt. [27, p. 164] Die ISO/IEC 27000 Serie beschreibt demnach die Definition, Grundbegriffe, Konzepte sowie Prinzipien für ein ISMS. [11, p. 1]

Im Zentrum des Standards, der ISO/IEC 27k Serie liegt daher der ISMS Standard, die ISO/IEC 27001, durch welchen die Prozesse vorgegeben werden. Durch diesen wird eine stetige Verbesserung und laufende Kontrolle der Informationssicherheit gewährleistet. Analog zu diesem existiert zudem der ISO 900x Standard, welcher sich vorwiegend dem Qualitätsmanagement widmet. [27, p. 164]

Wie in anderen Norm-Familien würde es sich rentieren, eine eigene Arbeit oder ein Buch dazu zu verfassen. Gerade auch in der ISO/IEC 27000 Familie gibt es Subnormen, welche weniger Bekanntheit erreicht haben. Vielerlei Pläne können der Website zu den veröffentlichten Standards entnommen werden, welche diese noch ergänzen. Die Familie befindet sich jedenfalls in ständiger Weiterentwicklung, weshalb sich eine regelmäßige Überprüfung der Standards als nützlich erweist. [28, p. 43] Langfristig soll die ISO 2700x-Reihe, die Standards 27000 bis 27019 sowie auch 27033 bis 27044 umfassen. [4, p. 73]

Bevor die Standardreihe ISO/IEC 27k näher betrachtet wird, dient die folgende Tabelle dem Überblick über die weiteren ISO Familie und dessen derzeitigen Subnormen.

Bezeichnung	Erscheinung	Titel	Kurznotizen
ISO/IEC 27000	2016	Information security management systems - Overview and vocabulary	Übersicht / Einführung in die ISO27k Standards als ganzheitliche Übersicht
ISO/IEC 27001	2013	Information security management systems — Requirements	Formelle Spezifikation eines ISMS
ISO/IEC 27002	2013	Code of practice for information security controls	Eine relativ umfangreiche Informationsquelle für Sicherheitskontrollziele und grundsätzlich akzeptierten praxisrelevanten security controls
ISO/IEC 27003	2017	Information security management system implementation guidance	Beratung für die Umsetzung von ISO27k, erweitert um Step-by-Step Empfehlungen zur ISO/IEC 27001
ISO/IEC 27004	2016	Information security management - Measurement	Maßnahmen und Messungen zur Beurteilung der Wirksamkeit

			eines implementierten ISMS, Sehr empfehlenswerte Zweitversion
ISO/IEC 27005	2011	Information security risk management	Beschreibt die generellen Information Risk Management Prinzipien, ohne dabei nähere Methoden darzustellen. Diese Version ist veraltet und verlangt einer Überarbeitung
ISO/IEC 27006	2015	Requirements for bodies providing audit and certification of information security management systems	Formale Anleitung für die Zertifizierungsstellen
ISO/IEC 27007	2011	Guidelines for information security management systems auditing	Auditing der Management System Elemente vom jeweiligen ISMS
ISO/IEC 27008	2011	Guidelines for auditors on information security controls	Prüfung der Informationssicherheit Elemente des ISMS
ISO/IEC 27009	2016	Sector-specific application of ISO/IEC 27001 – requirements	Anleitung für die Entwicklung neuer ISO27k-Standards
ISO/IEC 27010	2015	Information security management for inter-sector and inter-organisational communications	Information über die Informationssicherheit zwischen Industriezweigen und / oder Nationen, insbesondere solche, die "kritische Infrastruktur" betreffen
ISO/IEC 27011	2016	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Informationssicherheitskontrollen für die Telekommunikation Industrie; auch "ITU-T Empfehlung x.1051 genannt
ISO/IEC 27013	2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Kombinieren von ISO27k / ISMS mit IT Service Management / ITIL

Tabelle 1 Übersicht der ISO/IEC 27k Familie [29, p. 1ff]

Die dargestellte Tabelle ist keine vollständige Aufzählung der ISO 27k Familie. Diese beinhaltet lediglich die für die Arbeit in Betracht kommenden Subnormen, weshalb bei der ISO/IEC 27013 ein Stopp der Aufzählungen gemacht wird. Diese Subnorm tritt in den engeren Fokus, da sie sich einer annähernden Thematik wie jener dieser Arbeit stellt.

Beinhalten wird die Normenreihe ISO/IEC 27k der Voraussicht nach sowohl den ISO Standard 27000-27019 als auch den ISO Standard 27030-27044. Jede einzelne Subnorm dieser Reihe behandelt spezifische Themenbereiche und Aspekte in Anbetracht der IT-Sicherheit und bezieht sich dabei jeweils auf die ISO/IEC 27001. Jeder dieser weiteren Substandards behandelt praktische Anwendbarkeit und dient dem besseren Verständnis der ISO/IEC 27001 [11, p. 2].

Wie in der vorangegangenen Abbildung 2 ersichtlich wird in der ISO/IEC 27k Reihe demnach zwischen diversen Subnormen unterschieden welche folgend der Reihe nach näher erläutert werden.

Die ersten vorgestellten fünf Standards, bilden die Kernfamilie und betrachten speziell das ISMS. Das ISMS stellt das Hauptaugenmerk der Publikationen dar, womit diese sehr wichtig sind. [28, p. 38]

Die ISO/IEC 27k Standards lassen sich dritteln und kategorisieren. Den Anfang machen die ersten fünf Standards welche den Kern der Publikationen darstellen. Im zweiten Drittel der Subnormen wird Auditing und Zertifizierung thematisiert. Im letzten Drittel werden sämtliche restliche Standards der Reihe mit eigens abgegrenzten Themengebieten behandelt. [28, p. 38f] Im Folgenden zeigt Abbildung 10 dies grafisch dargestellt.

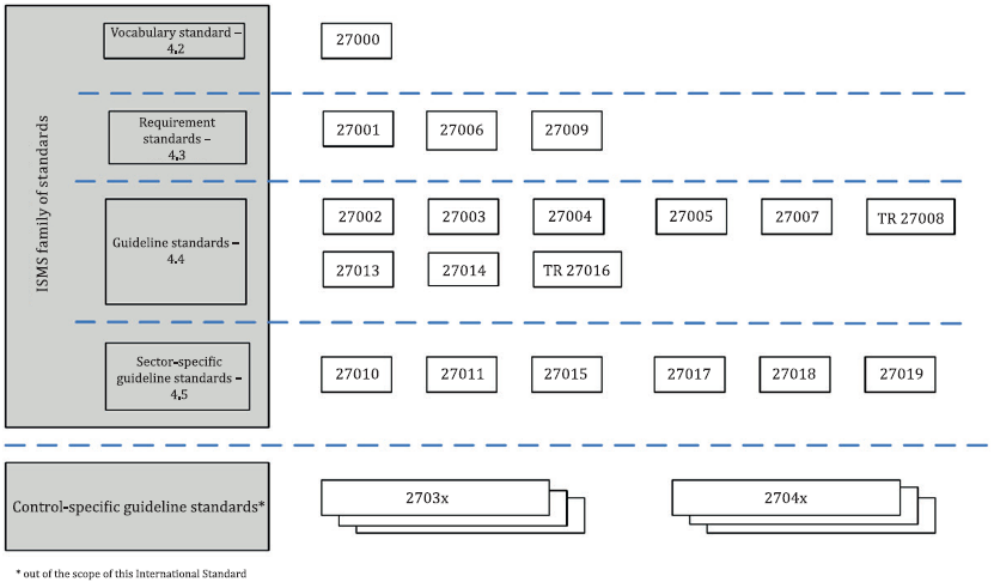

Abbildung 10 Beziehungen der ISMS Familie [30, p. 21]

2.3.1.1. ISO/IEC 27000

In der ISO/IEC 27000 werden die „Fundamentals and Vocabulary“ näher erläutert, um einen Überblick und einer thematische Einführung in die ISO/IEC 27k Serie zu verschaffen. Außerdem rückt das Vokabular zum Verständnis der Zertifizierungsnorm in den Fokus. [31, p. 1] Die ISO/IEC 27000 beschreibt die Zusammenhänge der verschiedenen folgenden Standards der ISO/IEC 27k Familie. [11, p. 1]

2.3.1.2. ISO/IEC 27001

Die ISO/IEC 27001 „Information Security Management System - Requirements“ ist ein Erzeugnis aufgrund von steigender Komplexität in der Informationstechnologie. Dadurch hat sich eine vermehrte Nachfrage nach Zertifizierungen in den vergangen Jahren entwickelt. Die ISO/IEC 27001 definiert die Anforderungen im Hinblick auf den Aufbau, der Einführung, den Betrieb sowie die Kontrolle, laufende Entwicklung, Wartung und Dokumentation eines ISMS unter Betrachtung von Risiken. [11, p. 1] Die ISO/IEC 27001 kann als Herzstück der ISO/IEC 27k Reihe betrachtet werden. Das als Prozess dargestellte Managementsystem basiert auf dem PDCA Zyklus nach Deming, wie er bereits im Punkt 2.1.2.2 vorgestellt wurde. [27, p. 165] In der Planungsphase, sowie auch im „Plan“ des Deming Cycle, wird der Aufbau des ISMS behandelt. Im Abschnitt „Do“, der Durchführungsphase, wird die Ausübung im Sinne der Implementierung in den Betrieb thematisiert. Anschließend beschreibt die Prüfungsphase „Check“, wie sowohl durch Monitoring als auch durch Reviews zeitgerecht Sicherheitsdefizite bemerkt werden und überdies Potenzial auf Verbesserung nachgewiesen wird. Die abschließende Phase „Act“, die Verbesserungsphase, legt deren Hauptaugenmerk auf die Korrektur, Wartung sowie Verbesserung. [17, p. 51]

Die Organisation definiert in der Planungsphase sämtliche Regelungen und Rahmenbedingungen rund um das Unternehmen oder die Organisation im Sinne des Geltungsbereiches für das ISMS. Ausschlaggebend für den Geltungsbereich sind festgelegte Anforderungen an die Sicherheit von sämtlichen Parteien der Interessenvertreter und Stakeholder. Gesetzliche, vertraglich definierte wie auch Unternehmens- und regulatorische Anforderungen rücken in den Fokus der Planung für das ISMS. Mithilfe einer Risikoinventur werden anschließend sämtliche Risiken erhoben, analysiert und daraufhin bewertet. Über eine Optimierung am Schluss, werden diverse Handlungsoptionen zum Portfolio der Risiken festgehalten. [17, p. 51f]
In der Durchführungsphase zielt der Fokus auf die Ausführung des Risikomanagements sowie auf passende Kontrollen zum Betrieb des ISMS. Training und Schulungen spielen dabei in dieser Phase eine beträchtliche Rolle. [17, p. 52]
In der Prüfungsphase passiert die Beobachtung, Prüfung und Kontrolle des ISMS. Mittels Monitoring entdeckt man rechtzeitig Mängel im Hinblick auf sicherheitsrelevante Vorkommnisse. Mittels wiederkehrenden Audits und Reviews wird entsprechendes Potenzial zur Verbesserung des ISMS gefunden. [17, p. 52]
In der abschließenden Etappe, der Verbesserungsphase werden sämtliche ermittelte Optimierungsmöglichkeiten für das ISMS aufgespürt und vorgenommen. In dieser Phase werden die ausgewählten Änderungen demnach entsprechend kommuniziert um das gewünschte Ergebnis zu erzielen. [17, p. 52]

Die Norm bietet einen Anhang, welcher zu diversen Controls aus der ISO/IEC 27002 verlinkt. Praktische Hilfestellung für die Umsetzung findet in der Norm allerdings keinen Anklang. [11, p. 1]
Überblicksartig werden daher in den ISO/IEC 27001 folgende Themen zusammengefasst bearbeitet:

- Definitionen und Begriffe
- Informationssicherheitsmanagementsystem, kurz ISMS
- Verantwortung im Bezug auf Management
- Internes Audit des ISMS
- Management-Review des ISMS
- Verbesserung und Entwicklung des ISMS
- Kontrollen und Kontrollziele im Anhang A
- OECD-Prinzipien im Anhang B [17, p. 51]

Um die Kontrollziele zu erreichen und weitere Kontrollen zu gewährleisten bietet Anhang A in der ISO/IEC 27001 zur Steuerung des ISMS folgende Punkte an:

- Sicherheitspolitik
- Interne Informationssicherheit und deren Organisation gegenüber dritten Parteien
- Management bezüglich Unternehmenswerte
- Sicherheit für Personen
- Physische Sicherheit
- Management von Betrieb und Kommunikation
- Überwachung von Zugriff sowie Zugangskontrolle
- Erwerb, Ausbau und Erhaltung von Informationssystemen
- Management im Sinne informationssicherheitsbetreffender Vorkommnisse
- Management der Geschäftskontinuität
- Compliance, zu Deutsch Konformität [17, p. 52]

2.3.1.3. ISO/IEC 27002

In der ISO/IEC 27002 welche unter dem Titel „Code of practice for Information Security Management" fungiert, ist die Zielsetzung als das Rahmenwerk für das ISM zu definieren. In älterer Literatur ist die ISO/IEC 27002 bislang als ISO 17799:2005 in Erscheinung getreten. Dabei ist festzuhalten, dass der ISO 17799 Standard ohne nennenswerte Modifikationen in den ISO/IEC 27002 übergeleitet wurde.
Grundsätzlich ist die Kernaufgabe der ISO/IEC 27002 der Aufbau eines funktionstüchtigen Sicherheitsmanagements und dieses in weiterer Folge in der Organisation zu verflechten. Die notwendigen Maßnahmen im Sinne der Sicherheit werden dabei nur knapp erläutert. Da die Hinweise und Empfehlungen auf Ebene des Managements angedacht sind, bringen diese wenig technische Details mit sich. Mithilfe der ISO/IEC 27002 entsteht eine Möglichkeit, den Anforderungen der ISO/IEC 27001 gerecht zu werden. [11, p. 1]
Behandelt werden in dieser Subnorm die folgenden Themengebiete:

- Risk Assessment und Treatment – Bewertung sowie Behandlung von jeglichen Risiken.
- Security Policy – Ermittlung, Konzipierung, Prüfung und Herausgabe einer schriftlich festgehaltenen Sicherheitspolitik
- Organization of Information Security – Organisation von interner Informationssicherheit als auch jener bezüglich Dritte
- Asset Management – Management zum Zwecke der Vermögenswerte wie beispielsweise Festlegung von Verantwortung und Klassifizierung für Inventar
- Human Resources Security – Management von Personalsicherheit. Zum Beispiel Verantwortung und Perspektive bezüglich Sicherheit vor, während und nach einer Beschäftigung. Mitunter fallen hier auch Themen wie die Rückgabe von Unternehmensobjekten oder auch die Entfernung sämtlicher Zugangs- und Zugriffsmöglichkeiten nach Beendigung eines Verhältnisses.
- Physical and Environmental Security – Beschreibt sämtliche Anweisungen zum Zwecke der Festigung von Räumlichkeiten, Sicherung von externen Gefährdungen, Sicherheitszonen oder auch Zugriff- und Zutrittskontrollen.
- Communications and Operations Mangement – Sämtliche Trennungen der Funktionen innerhalb der Organisation. Beispielsweise werden Entwicklung, Test und Produktion, Management von externen Dienstleistungen, Systemplanung- und abnahme oder auch Informationstransfer beziehungsweise Monitoring aufgeteilt.
- Access Control – Behandlung von Themen rund um Passworteinsatz, Policy bezüglich „clear desk and screen", Netzwerkzugang- und Segmentierung, Mobile Computing und Telearbeit sowie Zugangs- und Zugriffssicherheit.
- Information Systems Acquisition, Development and Maintenance – Analyse im Sinne der Anfoderungen und Spezifikationen, Prüfung von Input als auch Aufarbeitung von Output, Sicherheit mittels Verschlüsselung und Schutz sämtlicher Organisationsdateien und Quellcodes.
- Information Security Incident Management – Dokumentation zu sicherheitsbedeutenden Vorkommnissen sowie Entdeckung von Sicherheitsmängel, Verantwortlichkeiten sowie das Vorgehen bei Ereignissen bezüglich Sicherheitsaspekten. Sicherung von Beweisen, Notfallplanung, Bewertung und Monitoring mit Bezug auf anfallende Kosten sind hier ebenso maßgebende Themengebiete.
- Business Continuity Management – Organisationsweit- beziehungsweise übergreifende Einhaltung und Entwicklung des Business Continuity Managements, in Deutsch Management der Geschäftskontinuität. Nicht außer Acht zu lassen ist hierbei sowohl der Ausbau des Rahmenwerks zur fortlaufenden konsistenten Geschäftskontinuität, Inventur der Risiken beziehungsweise Bedrohungen, Entwicklung, Einführung und Test, als auch die Aufrechterhaltung sämtlicher weiterer Business Continuity Maßnahmen.
- Compliance – Zu Deutsch Konformität, beschreibt die Bestimmung aller gesetzlichen, vertraglichen oder von Aufsichtsbehörden festgelegten Verpflichtungen. Die Beachtung von Urheberrecht,

gesetzeskonformen Schutz von Verlust bezüglich Informationen, sowie deren Zerstörung oder Verfälschung sind Themenbereiche an dieser Stelle. [17, p. 53f]

2.3.1.4. ISO/IEC 27003

Die ISO/IEC 27003 „Information Security Management System Implementation Guidance“ bezeichnet, fungiert als Handbuch zur Implementierung für ein ISMS Projekt. In dieser Subnorm werden Darstellung, Spezifizierung sowie vorbereitende Aktivitäten der Planung eines Information Security Management System beschrieben. [31, p. 1]
Die darin enthaltene Vorgangsweise kann wie folgt, in fünf wesentliche Projektphasen aufgeteilt werden:

- Befugnis durch die Geschäftsleitung zum Beginn des ISMS Projektstarts.
- Definition eines Geltungsbereiches, begrenzten Rahmens und von einer Politik zum ISMS.
- Ausübung von Analysen zur Informationssicherheits-Anforderungen.
- Erfassung und Beurteilung von Risiken sowie das Planen ihrer Behandlung.
- Entwurf des ISMS [17, p. 54f]

Die Abschnitte zu den jeweiligen Projektphasen sind in einer identischen Gliederung aufgebaut und enthalten damit die Aktivitäten, eine Anleitung, den In- und Output beziehungsweise anderweitige Informationen. [17, p. 55]
Im Anhang A ist eine Checkliste zu Aktivitäten vorzufinden, welche den Aufbau und die Implementierung des ISMS erarbeitet. Ferner beinhaltet der Anhang eine Liste von Rollen und Verantwortlichkeiten im Sinne der IT-Sicherheit. Anhang C stellt außerdem weitere Informationen zu internen Audits bereit. [17, p. 55]
Anhang D erläutert hierarchische Strukturen von Policies, welche sich in drei Ebenen gliedert. Die Herausgeber der Norm merken dabei an, dass weiterführende Policy-Ebenen notwendig sein können. An oberster Stelle des dreistufigen Konzepts steht eine allgemeine Policy zum Zwecke des Überblicks. Beispielsweise Sicherheits-, Datenschutz-, und Marketingpolitik sind hierbei aufzulisten. Die darauf folgende Ebene befasst sich ebenso mit themenspezifischen Policies. Beispielsweise wird hier überblicksartig die Informationssicherheitspolitik vorgestellt. Die letzte der drei Ebenen, die unterste, verweist zu detaillierten Policies. Beispielsweise werden Richtlinien bezüglich Zugangskontrollen, gesperrten Bildschirmen beziehungsweise der Arbeitsplatzordnung, Verwendung von Netzwerkdiensten und Datenaustausch- oder Sicherung dargestellt. [17, p. 55]
Anhang E formuliert Themenbereiche rund um Monitoring und Messungen. Unterstützend sollen durch Messungen und deren Ergebnisse Reviews für das Management wirken. Nach erfolgreicher Identifikation der zu überwachenden Assets, werden Messziele, erforderliche Tätigkeiten, und Ergebnisse für das Berichtswesen ermittelt und mittels dem Messprogramm für IT-Sicherheit in die Tat umgesetzt. [17, p. 55]

2.3.1.5. ISO/IEC 27004

Die ISO/IEC 27003 „Information Security Management System Measurement“ behandelt die Fragestellungen welche sich ergeben, sobald man bereits weit fortgeschritten ist. Dabei sollen Fragen geklärt werden, wie weit man beispielsweise bei der Implementierung mit einem ISMS gekommen ist. Außerdem soll aufgeklärt werden, in welchem Ausmaß die Sicherheit der Informationen gemessen und bewertet werden kann. [28, p. 38]
Mittels Messung erfolgt im Anschluss daran die Bewertung des ISMS. Abhängig von Größe und Umfang der Organisation richtet sich auch die Komplexität, sodass Klein- und Mittelständische Unternehmen, KMU’s beispielsweise die Messung kompakter vollziehen können. [17, p. 56]
In der ISO/IEC 27004 werden daher in Kapitel 5 die Ziele im Hinblick auf ein Messsystem für das ISMS beschrieben. Die Erfüllung der Anforderungen wie auch die Wirtschaftlichkeit und Deckung mit externen Anforderungen, spielen dabei eine nicht weniger wichtige Rolle. Messmodelle als auch deren maßgeblichen Elemente sind die Hauptpfeiler in diesem Kapitel. Messgrößen, Messfunktion, Messmethoden, Entscheidungskriterien, analytische Modelle, Indikatoren und zuletzt Messergebnisse werden dabei näher

erläutert. Mithilfe einer Abbildung wird die Beziehung zum PDCA-Zyklus und zur ISO/IEC 27001 hergestellt. [17, p. 56]
Ein Verantwortungsbereich des Managements ist auch hier, Rollen und Verantwortlichkeiten zum Zwecke der Orientierung und zur Gestaltung eines Rahmens herzustellen. Das Erbringen von erforderlicher finanzieller Hilfe und Personal gebührt ebenso dieser Managementaufgabe. Als weitere Themenbereiche sind hier noch Schulungen, Sensibilisierungen und Kompetenzentwicklung einzubringen. [17, p. 56]
Kapitel 7 beschreibt die Entwicklung und den Ausbau des Messsystems, wobei hier besonders die Festlegung des Informationsbedarfs, die Entwicklung von einem Messkonstrukt, die Sammlung der Daten mit der anschließenden Analyse und nicht zuletzt das Berichtswesen von Bedeutung ist. Es folgt das Kapitel zur Analyse der Daten, wobei ein Reporting der Messergebnisse angehängt wird. Schließlich beschreibt Kapitel 10 die Bewertung und Überarbeitung des Messsystems der Informationssicherheit. [17, p. 56]
Anhang A fungiert als Vorlage, welche als generisches Konstrukt der Messung etikettiert wird, womit IS-Messverfahren deklariert werden können. Anhang B hingegen, stellt Beispiele von Messgebilden vor, welche als Vorlage dienen. Die Beispiele beschreiben Themenbereiche wie Passwortpolicies, kontinuierliche Verbesserungsmaßnahme, Zutrittskontrollen sowie Schulungen. [17, p. 56f]

2.3.1.6. ISO/IEC 27005

Die ISO/IEC 27005 „Information Security Risk Management" behandelt Empfehlungen bezüglich dem Risiko Management in Hinsicht der Informationssicherheit. Dabei wird unter anderem bei der Umsetzung im Sinne der Anforderungen zur ISO/IEC 27001 Hilfe geleistet. Spezielle Methoden für das Risiko Management werden dabei allerdings nicht vorgegeben.
Die ISO/IEC 27005 löst mitunter den bis dato Standard 13335-2 ab, welcher eine Anleitung zum Management für IT-Sicherheit gegeben hat. [11, p. 1]
Der Risikomanagementprozess der ISO/IEC 27005 startet mit der Definition der Rahmenbedingungen und Grenzen wie beispielsweise dem Wirkungsgebiet, der Risikofähigkeit- und bereitschaft sowie der Integration von verfügbaren Ressourcen. Dem folgt die Risikobewertung „Risk Assesment" sowie die Risikobehandlung „Risk Treatment". In der Risikobewertung werden Aspekte von der Risikoanalyse „Risk Analysis" mit jenen Elementen der Risikoidentifikation „Risk Identification", der Risikoeinschätzung „Risk Estimation" als auch der Risikoevaluierung „Risk Evaluation" entgegen der individuellen Risikokriterien der Organisation verglichen.
Möglichkeiten der Risikobehandlung sind diese zu vermeiden, übertragen, reduzieren oder sie einfach zu akzeptieren. Die „Risk Acceptance", zu Deutsch Risikoannahme bringt den Abschluss hervor. Elemente aus Risikokommunikation, Monitoring sowie deren Review umfassen den Ablauf. [17, p. 57]

Im Hinblick auf das Assessment Tool im Abschnitt 4 wird insbesondere die ISO/IEC 27001 und 27002 eine wichtige Rolle spielen. Die ISO/IEC 27003 bis ISO/IEC 27005, als auch die im Folgenden noch relevanten weiteren Subnormen, möchten der Vollständigkeit halber kurz erläutert werden.

2.3.1.7. Weitere ISO 27000 Subnormen

Die weiteren fünf Substandards der ISO 27k beschreiben die Themen der Auditierung und Zertifizierung im Detail. Besondere Beachtung wird diesbezüglich dem Gedanken der Qualitätssicherung durch Auditoren für das ISMS geschenkt. [28, p. 38]

In der ISO/IEC 27006 welche als „Requirements for bodies providing audit and certification" betitelt ist, werden Aspekte für Organisationen zum Zwecke der Zertifizierungen und Audits abgehandelt. Außerdem werden darin spezifische Anforderungen zum ISMS ergänzt. [28, p. 39]
Ähnliches gilt für die ISO/IEC 27007, welche den Titel „Guidelines for auditing" trägt. Dieser Substandard ist ein Leitfaden für Auditoren und Auditorinnen. Darüber hinaus gilt dieser Standard auch für jene Personen als lesenswert, welche eine Zertifizierung in Erwägung ziehen. [28, p. 39]

Die ISO/IEC 27008, auch „Guidance for auditors on ISMS controls“ genannt, beschreibt den Tätigkeitsbereich eines Auditors mit dem Fokus auf die entsprechende Prüfung von Controls.
In der ISO/IEC 27009 welche als „Sector/Service-Specific Third-Pary Accredited Certifications” beschrieben wird, sind Gestaltungen rund um die Zertifizierungen dargeboten. [28, p. 39]

Das letzte Drittel der zuvor genannten Einteilung beschreibt die Standards ab ISO/IEC 27010 bis zur ISO/IEC 27050. Bei diesen Standards ist die Rede von sehr stark begrenzbaren Themenbereichen, aber ebenso spezifischen Ergänzungen zu diversen Abschnitten aus ISO/IEC 27002. [28, p. 39]

In der ISO/IEC 27010, genauer „Information security management for inter-sector and inter organizational communications” wird dargestellt, wie diverse ISMS inmitten einer Organisation miteinander in Einklang gebracht und durch Synchronisaton miteinander kombiniert werden können. [28, p. 39]

Die ISO/IEC 27011, definiert als „Guidelines for telecommunications organizations based on ISO/IEC 27002”, behandelt grundlegende Anforderungen im Sinne der CIA Triade wie im Abschnitt 2.3 bereits vorgestellt, also Vertraulichkeit, Integrität sowie Verfügbarkeit. Dieser Standard gewinnt besondere Bedeutung für Telekommunikationsunternehmen.

Der ISO/IEC 27013 Standard „Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1” thematisiert Hilfestellung sofern ISO/IEC 27001 implementiert werden soll. Dabei ist die ISO/IEC 20000-1 bereits ein fixer Bestandteil. Die umgekehrte Reihenfolge, das heißt ISO/IEC 27001 ist vorgegeben und ISO/IEC 20000-1 soll implementiert werden, ist ebenso ein plausibles Szenario im Standard. Letztendlich kann aber auch eine gleichzeitige Einführung der beiden Standards in Betracht gezogen werden.

Da dieser Substandard zum Teil verstärkt die Thematik dieser Arbeit stützt, möchte hier dieser Standard ausführlicher in Punkt 2.3.1.8 besprochen werden.
Weitere Standards ab dem ISO/IEC 27014 werden an dieser Stelle nicht mehr dargestellt, da diese nicht explizit Teil dieser Arbeit sind und für den weiteren Verlauf keinen Mehrwert bringen würde.

2.3.1.8. ISO/IEC 27013

Mit der ISO/IEC 27013 tritt eine Norm in Erscheinung, mit der eine integrierte Implementierung für das Service Management rund um die ISO 20000-1 erfolgt. Damit werden die Prozesse der ISO 27001 ebenso berücksichtigt. [17, p. 50]

Im Jahr 2015 wurde die ISO/IEC 27013 überarbeitet und publiziert, um den aktualisierten ISO/IEC 27001: 2013 Standard und die Information Security Management System Anforderungen wie auch die ebenso erneuerte ISO/IEC 27000: 2014, zu berücksichtigen. [25]

ISO/IEC 27001 wurde in Übereinstimmung mit vielen weiteren Standards wie der ISO 9001, ISO 14001 und ISO/IEC 22301 konzipiert und kann somit in die Struktur für Management Standards integriert werden. [25]

Die ISO/IEC 27013 trägt die Bezeichnung „Information technology — Security Techniques – Guidance on the integrated implementation of ISO/IEC 27001and ISO/IEC 20000-1“.
Der darin beschriebene Inhalt soll für jene Organisationen nützlich sein, die planen beide Standards zu vereinen. Aber auch für Organisationen welche es sich zum Ziel gesetzt haben, eine bereits implementierte Norm in einem integrierten Managementsystem (Siehe Kapitel 2.8) zu verknüpfen. Der Standard enthält keinen Text anderer Normen und muss in Verbindung mit der ISO/IEC 27001 und der ISO/IEC 20000-1 betrachtet werden. [25]

Der Kern des Dokuments umfasst 15 Seiten plus 23 Seiten Anhang und Referenztabellen. Infolge der üblichen Einführungs- und Pflichtklauseln enthält der Standard folgende Punkte: [25]

- Überblick der ISO/IEC 27001 und der ISO / IEC 20000-1
- Ansätze zur integrierten Umsetzung
  - Überlegungen zum Umfang
  - Vor-Implementierungs-Szenarien
- Überlegungen zur integrierten Implementierung
  - Potenzielle Herausforderungen
  - Mögliche Gewinne
- Anhang A (informativ) Korrespondenz zwischen ISO/IEC 27001: 2005 und ISO/IEC 20000-1: 2011
- Anhang B (informativ) Vergleich der ISO/IEC 27000: 2009 und ISO/IEC 20000-1: 2011 Bedingungen [25]

Die Beziehung zwischen der Informationssicherheit und dem Service-Management ist so eng, dass die Vorteile der Übernahme beider Standards unübersehbar sind. Demzufolge widmet sich der ISO/IEC 27013 Standard der Integration der ISO/IEC 27001 zur Informationssicherheit und ISO/IEC 20000-1 für das Service-Management beziehungsweise auch umgekehrt.
Der Guide basiert demnach auch auf den veröffentlichten Versionen der beiden internationalen Standards ISO/IEC 27001: 2005 und ISO/IEC 20000-1: 2011. [32, p. 7]

Der ISO / IEC 27013 zufolge, werden Service Management und Information Security Management oft so behandelt, als wären sie weder miteinander verbunden noch voneinander abhängig. Der Kontext für eine solche Trennung besteht darin, dass das Service-Management effizient und rentabel bezogen werden kann, während das Informationssicherheits-Management oft nicht als grundlegend für die effektive Bereitstellung von Diensten verstanden wird. Als Ergebnis wird das Service Management häufig zuerst implementiert. [25]

Besonders Management- und Organisationsprozesse können aus den Ähnlichkeiten zwischen den internationalen Normen und ihren gemeinsamen Zielen profitieren. [32, p. 7]

Zu den wichtigsten Vorteilen einer integrierten Implementierung gehören:

- die Glaubwürdigkeit eines wirksamen und sicheren Dienstes für interne oder externe Kunden der Organisation
- die Verringerung der Kosten für ein integriertes Programm aus zwei Projekten, bei denen sowohl das Service-Management als auch die Informationssicherheit Teil der Strategie einer Organisation sind
- eine Verkürzung der Umsetzungszeit aufgrund der integrierten Entwicklung von Prozessen, die beiden Standards entsprechen
- Beseitigung nicht benötigter Redundanzen
- ein besseres Verständnis von Service und Security Management für die Sichtweisen der jeweils anderen
- eine für ISO/IEC 27001 zertifizierte Organisation kann die Anforderungen an die Informationssicherheit leichter in Betracht der ISO/IEC 20000-1: 2011 erfüllen, beziehungsweise vice versa [32, p. 7]

Die verwendeten Begriffe und Definitionen der ISO/IEC 27000: 2013 und der ISO/IEC 20000-1: 2011 erfahren einen sehr hilfreichen Vergleich in Bezug auf die Implementierung eines integrierten Managementsystems. [25]

Die ISO/IEC 27013 stellt zusammenfassend ein wesentliches Dokument für diejenigen dar, die ein integriertes Managementsystem mithilfe der ISO/IEC 27001 und der ISO/IEC 20000-1 erwägen. [25]

Als zusätzlicher Standard wird im Folgenden noch der IT-Grundschutz des BSI vorgestellt, da sich dieser nicht zuletzt großer Beliebtheit erfreut und somit neben der ISO 27000er Reihe beim Thema Security Management nicht fehlen sollte.

2.3.2. IT-Grundschutz des BSI

Wie bereits erwähnt besteht die Aufgabe der Informationssicherheit nicht lediglich aus der Absicherung von IT-Systemen und dem Schutz von Informationen, sondern vielmehr dem Aufbau eines Managementsystems um der Nachhaltigkeit zukünftiger Gefahren entsprechend entgegenzuwirken. Zu diesem Zweck stellt das BSI eine ausführliche Hilfestellung für sämtliche Unternehmen zur Verfügung um einen schnellen und erfolgreichen Einstieg in die Thematik zu gewährleisten. [33, p. 13]
Durch den IT Grundschutz wird eine Vorgangsweise angeboten, die ein Sicherheitsmanagement infolge von eindeutigen Empfehlungen im Sinne von Maßnahmen gewährleistet. Dabei werden nicht nur technische Blickpunkte beleuchtet, sondern es wird ebenso auch auf organisatorische, infrastrukturelle sowie personelle Betrachtungen geachtet. Dadurch wird ermöglicht, ein effizientes, schnelles und wirtschaftliches Sicherheitsniveau für den Normalbedarf zu schaffen. [33, p. 13]
Ursprünglich wurde der IT Grundschutz für Behörden erfasst, wobei sich dieser in weiterer Folge seit 1994 als Instrument für Informationssicherheit als äußerst erfolgreich und wertvoll erwiesen hat. Zur kostenlosen Verfügung steht der IT-Grundschutz für Unternehmen diverser Größen sowie sämtlicher Branchen und Bereiche. [33, p. 13]
Als besondere Stärke des IT-Grundschutz ist dessen Vergleichbarkeit mittels Soll-Ist Analysen zu erwähnen also auch dessen praxistaugliche Anweisungen welche durch eine maßgebliche Akzeptanz seitens staatlicher Referenzquellen unterstrichen wird. Nicht ohne Grund ist deshalb der IT-Grundschutzkatalog im deutschsprachigen Raum als weit verbreiteter Standard für Informationssicherheit etabliert. Oftmals wird der IT-Grundschutzkatalog beispielsweise bei deutschen Behörden referenziert oder gar dessen Umsetzung vorgeschrieben. [33, p. 14]

Der IT-Grundschutz gliedert sich in zwei wesentliche Teile, den BSI-Standards und die IT-Grundschutzkataloge.

2.3.2.1. Die BSI-Standards

Momentan besteht der BSI-Standard aus vier Substandards welche im Folgenden kurz erläutert werden:

BSI-Standard 100-1 „Managementsysteme für Informationssicherheit“
Dieser Standard handelt von den generellen Anforderungen an ein ISMS, Managementsystem für Informationssicherheit. Die darin enthaltenen Vorgaben hinsichtlich des ISMS sind soweit spezifisch ausreichend definiert, um die Implementierung und den Betrieb des ISMS zu gewährleisten. Sie sind aber ebenso generisch gehalten, um an besondere Umstände von Unternehmen abgestimmt zu werden. Ausschlaggebend ist dabei, dass der Standard inhaltlich kompatibel im Bezug zu anderen Standards, wie beispielsweise der ISO/IEC 27001 bleibt. Damit sind eine internationale Bewertung und ein Vergleich garantiert. [33, p. 14]

BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“
Dieser Standard beschreibt eine Step-by-Step Anweisung in Hinsicht auf ein Managementsystem für Informationssicherheit. Darin enthalten sind Beschreibungen wie er in der Praxis gegliedert, aufgebaut und geführt werden kann. Wichtige Elemente in diesem Zusammenhang sind dabei der Aufbau des Sicherheitsmanagementsystems, also auch jener der jeweiligen Struktur im Sinne der Organisation. Eingehend wird in diesem Standard erläutert, inwiefern sachgemäße Maßnahmen zur Sicherheit eruiert werden können. Dabei wird zudem auch detailliert erklärt, welche Gesichtspunkte bei der Umsetzung in Betracht zu ziehen sind. Eine Beantwortung findet der Bezieher oder die Bezieherin obendrein auf Fragen bezüglich der Aufrechterhaltung und ebenso den Ausbau der Informationssicherheit in einer laufenden Ausführung. [33, p. 14]

BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“
Der dritte Standard dieser Reihe widmet sich der Methodik für Risikoanalyse, welche sich für den Fall anbietet, dass eine Organisation mithilfe des IT-Grundschutzes zu agieren versucht. Ist im jeweiligen Unternehmen bereits eine andere Risikomanagement-Methode im Einsatz, kann diese ebenso verwendet werden. [33, p. 14]

BSI-Standard 100-4 „Notfallmanagement“
Dieser Standard beschreibt die wesentlichen Punkte für ein Notfallmanagementsystem. Diese Managementdisziplin besticht durch ihre zahlreichen Schnittstellen zum Sicherheitsmanagement, welche im Notfallmanagement unumgänglich sind. [33, p. 14]

2.3.2.2. Die IT Grundschutzkataloge

Die IT-Grundschutzkataloge des BSI sind in verschieden Bausteine strukturiert. Jeder dieser Bausteine behandelt dabei einen entsprechenden Bereich wie organisatorische, technische oder infrastrukturelle Aspekte. Beispielsweise sind hier Schutzmaßnahmen für eine spezifische technische Plattform, Erwartungen an Maßnahmen zur Schulung oder auch Thematiken im Sinne der Sicherheit bezüglich eines Serverraums vorgesehen. Jeder Baustein beschreibt vorerst die Materie inhaltlich skizziert, dann werden die Bedrohungen aufgezeigt, welche das Asset beeinträchtigen können, ehe im Anschluss auf konkrete Anordnungen verknüpft wird, um die Bedrohungen unter Kontrolle zu haben. [33, p. 15]

Die angesprochenen Bausteine gliedern sich in fünf Schichten welche wie folgt eingeteilt sind:

- Übergreifende Aspekte: Dem hinzuzurechnen sind Bausteine wie Sicherheitsmanagement. Wobei im BSI-Standard 100-1 beschrieben wird, WAS auszuführen ist, bringt dieser Baustein mit dem WIE mehr Klarheit in den Kontext. Auch Aspekte wie Patch- und Änderungsmanagement oder Outsourcing sind Themen, welche im Punkt der übergreifenden Aspekte zu finden sind. Zuletzt genannte Beispiele zeigen die enge Abbildung, wie dies auch bei klassischen IT Management Frameworks, wie beispielsweise ITIL der Fall ist.
- Infrastruktur: Diese Ebene beschäftigt sich, wie aus dem Namen zu erkennen ist, mit Hilfestellungen zum Schutz von physischen Assets im Sinne von Gebäuden, Rechenzentren, Büroräumlichkeiten, klassischen und mobilen Arbeitsplätzen aber auch mit der Verkabelung der IT Landschaft eines Unternehmens.
- IT-Systeme: Dieser Baustein beschreibt Anweisungen, wie diverse Betriebssysteme sowie andere IT-Geräte wie Mobiltelefone, Multifunktionsgeräte oder Netzwerkgeräte abgesichert werden sollen.
- Netze: In dieser Ebene werden die Vorgaben auf die Sicherheit für heterogene Netzwerke wie beispielsweise das Netzmanagement, WLAN oder VoIP, Bluetooth beziehungsweise andere Netzwerktechnologien- und Komponenten erfasst.
- Anwendungen: Die letzte der fünf Ebenen beschäftigt sich mit Anordnungen für die Nutzung diverser Software wie beispielsweise SAP, Microsoft Exchange Server, Active Directory oder der allgemeinen Verwendung des Internet. [33, p. 15]

Zusammenfassend kann man beim IT-Grundschutz-Katalog derzeit von 88 Bausteinen sprechen, welche wiederum in etwa 1600 Empfehlungen für IT-Sicherheit zusammengefasst werden können. Derzeit umfasst der IT-Grundschutz-Katalog rund 5.000 Seiten und inkludiert in diesem Umfang fachliches Know-How mit entsprechenden Anordnungen für Informationssicherheit. [33, p. 15]
Nichtsdestotrotz ist es aber auch mit dem IT-Grundschutz nicht möglich, für sämtliche IT-Systeme in jeglicher Art und Umfang Bausteine zur Verfügung zu stellen. Aus diesem Grund gibt es für individuelle Produkte neben den erwähnten, noch weitere generische Bausteine für den Fall, dass die vorhandenen nicht verwendet werden können. [33, p. 15]

Da die wesentlichen Standards rund um Service und Security Management nun vorgestellt wurden, dient das nachstehende Kapitel nochmals der Übersicht und dem Vergleich der Standards.

2.4. Schwerpunkte der Standards

Das Hauptaugenmerk der Regelwerke liegt zumeist auf einem differenzierten Schwerpunkt, daher sind sie sowohl in ihrer Ausprägung im Hinblick auf „Planung und Organisation“, „Beschaffung und Einführung“, „Auslieferung und Unterstützung“ als auch als „Überwachung“ verschieden ausgerichtet.
Aber auch hinsichtlich Anleitungen bezüglich Kontrolle, Risikomanagement und Maßnahmen finden sich grundlegende Unterschiede. Die Regelwerke rund um ITIL oder die ISO/IEC 27002 enthalten Vergleichs-Tabellen mit deren Hilfe es möglich ist, Aussagen wie in Abbildung 11 zu treffen. Darin werden die Unterstützungstiefe und die Breite der Anwendung gegenübergestellt. [3, p. 195]

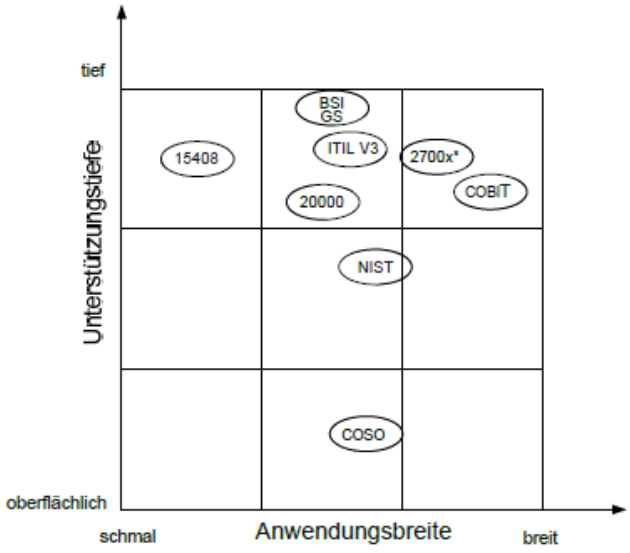

Abbildung 11 Matrix mit den Ausprägungen der Regelwerke [3, p. 195]

Die Unterstützungstiefe beschreibt den Detailierungsgrad technischer und betrieblicher Natur. Mit der Anwendungsbreite soll das Sicherheitsniveau in Bezug auf Vollständigkeit verstanden werden. [3, p. 195]
Hinsichtlich der Konzentration auf Teilbereiche der IT-Security, grenzt dies oftmals dementsprechend die Anwendungsbreite ein.
Manche Regelwerke verpflichten sich nur der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit und unterlassen dabei die Betrachtung weiterer Ziele der Informationstechnologien wie Compliance oder auch Effektivität. [3, p. 195]

Zu Beginn soll die darauf folgende Tabelle wesentliche Unterschiede der vorgestellten Service Management Regelwerke hervorheben, um anschließend das gleiche für Security Management in Tabelle 3 darzustellen.

ISO20000	ITIL v3	COBIT
Standard und “Code of Practice”	Best Practice	Rahmenwerk
Zertifizierung für einen Dienstleister	Qualifikationen für Einzelpersonen	Qualifikationen für Einzelpersonen
eindeutige High-Level-Anforderungen für Prozesse und das Management System	Detaillierte Best Practice Anleitung, Beschreibung und Implementierung	COBIT erzeugt eine optimale Ausrichtung zwischen Business und IT
organisatorische Struktur ist unabhängig	definiert viele Funktionen und Prozesse, Rollen und Verantwortlichkeiten	integrativer, offenerer Ansatz als Good Practices
13 Prozesse wobei der Lebenszyklus nicht explizit spezifiziert ist; keine Funktionen	26 Prozesse und vier Funktionen in fünf Lebenszyklen dokumentiert	38 Prozesse sind einheitlich und vollständig dargestellt
Bestimmtes Set von erforderlichen Unterlagen	Beschreibungen der wichtigsten Dokumentation	COBIT ist stärker strukturiert als beispielsweise ITIL

Tabelle 2 Zusammenfassung von vorgestellten Service Management Regelwerken

Wie bereits angekündigt, zeigt die nachstehende Tabelle zusammengefasst die Grundlagen der beiden vorgestellten Security Management Regelwerke

ISO 27k Reihe	IT-Grundschutz des BSI
Internationales Regelwerk	Nationales Regelwerk
Generisches Prozedere	Vordefiniertes Prozedere
Grundlegende Dokumentation	Detailreiche Dokumentation
Prozessorientierter Ansatz	Hierarchischer Ansatz
Komplette Risikoanalyse	Keine grundlegende Risikoanalyse; nur bei einem verstärktem Bedarf an Schutz
Kostenpflichtig	Kostenlos
Umsetzung Wirtschaftlich rentabel	Umsetzung mit hohen Kosten verbunden

Tabelle 3 Zusammenfassung von vorgestellten Security Management Regelwerken

Nachfolgendes Kapitel ermöglicht einen Überblick zu den Versionierungen, beziehungsweise zu den zeitlichen Publizierungen der Regelwerke.

2.5. Versionsübersicht der vorgestellten Regelwerke

Die vorgestellten Standards, Normen und Best Practices widerfahren einer ständiger Überarbeitung und Weiterentwicklung, um den aktuellen Trends und Anforderungen stets gerecht zu werden. Dies bringt aber unweigerlich eine Vielzahl an Versionierungen und Unterscheidungen mit sich, wodurch selbst für Experten gewisse Herausforderungen entstehen.
Um den Überblick der vielen Regelwerke und deren ständigen Revision zu bewahren, soll die folgende Abbildung 12 helfen. Diese Grafik veranschaulicht eine Roadmap über die vergangen zwei Jahrzehnte, wobei oberhalb des Zeitstrahls die Service- und unterhalb der Achse die Security Management Standards mit den Jahreszahlen der wesentlichen Versionen gekennzeichnet sind.

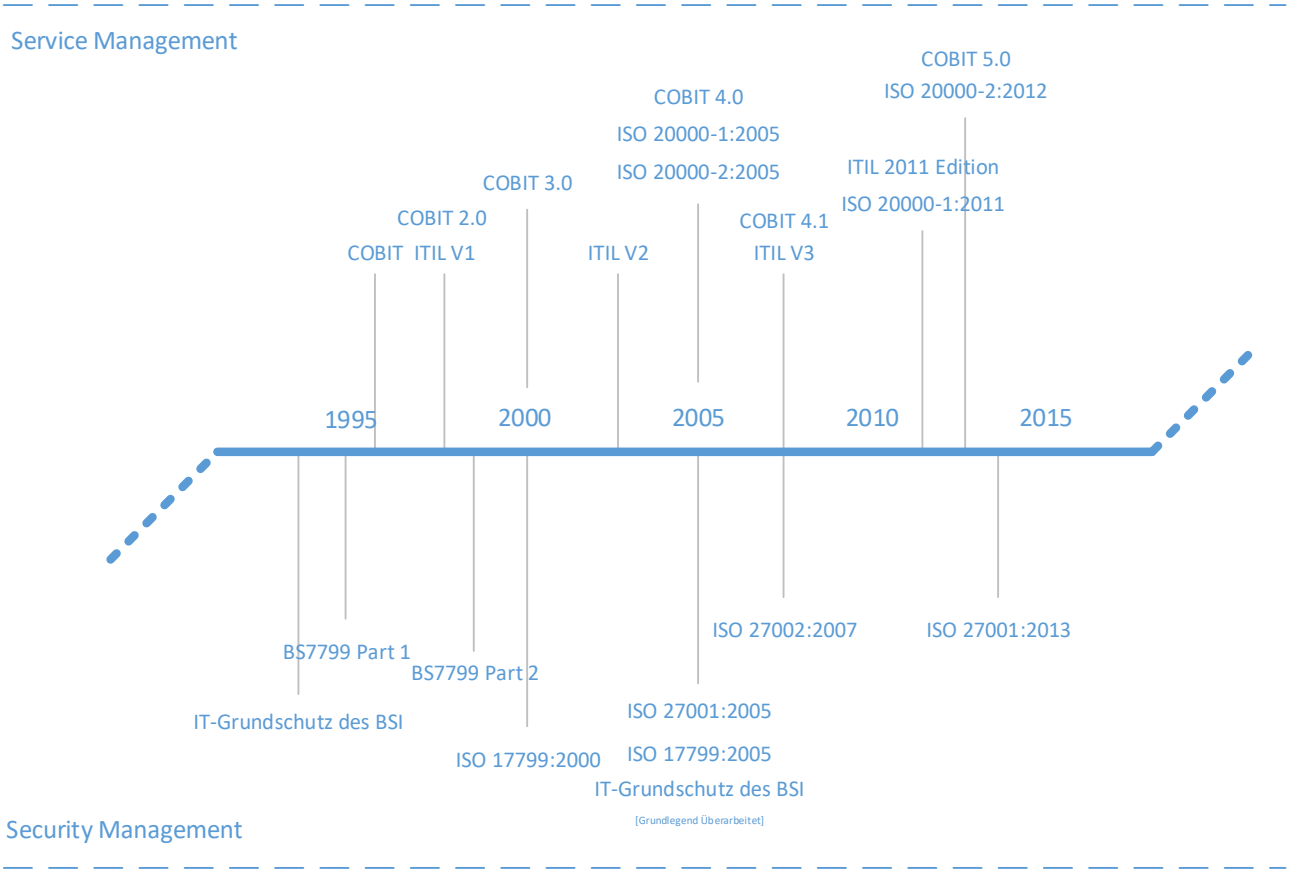

Abbildung 12 Roadmap der vorgestellten Regelwerke

Der IT-Grundschutz des BSI kann entgegen der anderen Regelwerke keine federführenden Meilensteine aufweisen. Er stellt in dieser Grafik demnach eine Sonderstellung dar, da dieser einer laufenden Überarbeitung seit der Einführung im Jahr 1994 widerfährt. Bei der grundlegenden Überarbeitung im Jahr 2005 handelt es sich um die Aufteilung des Grundschutzbuchs in die IT-Grundschutz-Kataloge, wie sie in Kapitel 2.3.2.2 näher beschrieben sind. [34]

Nachfolgendes Kapitel klärt über die Möglichkeit zur Zertifizierung anhand der vorgestellten Regelwerke auf.

2.6. Zertifizierungsmöglichkeiten der Regelwerke

Das große Ausmaß an Modellen, nach denen in der IT-Sicherheit zertifiziert werden kann ist erheblich. Unterschiede ergeben sich in der Bekanntheit, Anerkennung, Anwendungsfläche sowie an den Kosten. Zertifikate, übersetzt Bescheinigungen können elementar von jeder Partei erteilt werden. Allerdings können nur akkreditierte Stellen auch die unerlässliche Basis für Vertrauen und international anerkannte Akzeptanz garantieren. [19, p. 16]
Bezugnehmend auf den nicht unwesentlichen Aufwand einer Zertifizierung sollte daher vorweg genauestens eruiert werden, warum diese angestrebt wird und welches Ziel damit verbunden ist. Dabei ist ein wesentlicher Faktor, ob die Kosten im Vergleich zum Aufwand im richtigen Verhältnis stehen. Nachfolgend werden daher die Standards stichwortartig im Sinne der Zertifizierbarkeit erläutert. [19, p. 16]

ISO 27001	
Einsatz	Unabhängig von der Branche und Organisation ist die Anwendung für das vollständige Unternehmen möglich. Möglich sind außerdem Einschränkungen auf gewisse Teile wie beispielsweise etwaige Geschäftsprozesse.
Aufwand	Abhängig von den jeweiligen Sicherheitsmaßnahmen ist die Einführung eines ISMS abzuleiten.
Anerkennung	starke internationale Reputation
Zertifizierer	Wichtig ist das Augenmerk darauf zu legen, dass die Zertifizierungsprogramme einer entsprechenden Akkreditierung zugesprochen werden.
Nutzen	Beispielsweise das Erfüllen der Forderungen von Basel II, S-Ox oder Solvency II. Möglichkeit der Teilnahme an Beschaffungsmärkten. Entwicklung von Vertrauen bei Kunden und Kundinnen. Hohes Maß an Nutzen im Sinne der IT-Security.
Kosten	In Abhängigkeit des jeweiligen Zertifizierungsprogramms ist mit zehn- bis fünfzigtausend Euro je nach Größe der Organisation zu rechnen.
ISO 27001 auf Grundlage des IT-Grundschutzes	
Einsatz	Theoretisch komplette Organisation mit sämtlichen Informationstechnologie-Anwendungen denkbar – in der Praxis hingegen sind Einschränkungen auf diverse IT-Anwendungen sowie bedeutungslosere IT-Verbünde der Fall.
Aufwand	Beträchtlicher Aufwand im Hinblick auf die Modellierung für die Analyse des Schutzes. Empfohlen wird daher aufgrund der Komplexität den Umfang und dessen Struktur auf die Expertise von externen Beratern anzuknüpfen.
Anerkennung	Besondere Anerkennung in Deutschland, hingegen sonst zumeist als Referenzmodell in europäischen Richtlinien.
Zertifizierer	Bundesamt für Sicherheit in der Informationstechnik
Nutzen	Siehe ISO 27001, jedoch mit Einschränkung in Hinsicht auf die internationale Beliebtheit.
Kosten	Die Preisspanne ist zwischen zwanzig- und hunderttausend Euro zu beziffern.
ISO 20000 (ITIL)	
Einsatz	Service Bereich in der IT einer Organisation
Aufwand	Entwicklung eines entsprechenden IT Service Managements inklusive ISO 27001 für konkrete Gebiete der IT-Services.
Anerkennung	starke internationale Reputation
Zertifizierer	Wichtig ist das Augenmerk darauf zu legen, dass die Zertifizierungsprogramme einer entsprechenden Akkreditierung zugesprochen werden.
Nutzen	Möglichkeit der Teilnahme an Beschaffungsmärkten. Entwicklung von Vertrauen bei Kunden und Kundinnen. Ausbau der internen IT-Services.
Kosten	Für die Zertifizierung ist mit etwa zehntausend Euro zu rechnen.
COBIT	
Einsatz	Personenzertifizierung
Aufwand	IT-Management-Probleme verstehen, mit denen Unternehmen konfrontiert sind. Demzufolge die Fähigkeit COBIT einsetzen zu können, um auf Herausforderungen entsprechend zu reagieren.
Anerkennung	internationale Reputation
Zertifizierer	ISACA
Nutzen	Foundation Exam ermöglicht das Wissen zu demonstrieren, indem eine Prüfung mit Abschlusszertifikat erworben wird
Kosten	Abhängig von Stufe und Testanbieter

Tabelle 4 Übersicht der Zertifizierungen [19, p. 16ff]

Da nun die die wichtigsten Standards beider Themengebiete vorgestellt und verglichen wurden, soll das darauf folgende Kapitel noch auf mögliche weitere Regelwerke rund um dieses Thema hinweisen.

2.7. Alternativen / weitere Standards

Aufgrund der Fülle an Standards und Normen würde eine vollkommene Aufzählung über den Rahmen dieser Arbeit hinausgehen und wäre vermutlich kaum durchführbar. Demzufolge wird in diesem Abschnitt nochmals kurz auf die Alternativen hingewiesen.

Man unterscheidet mittlerweile derart viel Standards, Richtlinien und Empfehlungen im IT-Security Bereich, dass an dieser Stelle nicht alle erläutert werden können. Im jeweiligen Einzelfall empfiehlt es sich jedoch, genauestens zu prüfen ob ein spezifischer „Best Practice“ oder ein gewisser Standard verbindliche Vorgaben bestmöglich abdeckt. [16, p. 98]
Die Menge der verfügbaren Standards beschäftigt sich dabei allerdings auch mit einem sehr eingeschränkten Kreis an Adressaten.
Dies unterscheidet die Standards von anderen, wenn diese eine tatsächliche Hilfestellungen bei der Ausführung von konkreten Anwendungsfällen in der Informationssicherheit bieten. Um einen Überblick zu gewinnen worin die Hauptaugenmerke- beziehungsweise Unterschiede liegen, dient die folgende, stichworthaltige Tabelle. [19, p. 19]

Themenbereich	Standard/Norm	Anhang A ISO 27001 Beziehung
Kryptografie, Digitale Signaturen, Key Management, Verschlüsselung, Hash-Funktionen, Authentisierung von Kommunikationspartnern, Datenauthentisierung	ISO 9979, 10116, 18033, 9796, 14888, 10118, 15946, 9797, 9798, 11770, 15946, 18031, 18032	Kein nennenswerter Bezug vorhanden, in seltenen Umständen kann ein Vorteil für IT-Experten durch den A.12.3 entstehen, beim Schutz durch kryptografische Verfahren
Guidelines für das Management von IT Security	ISO 13335	Stark ausgeprägte Verbindung, allerdings sind die älteren technischen Reports entbehrlich, weil diese bereits in der ISO 27000-Reihe integriert sind.
Netzwerksicherheit	ISO 18028	Kann als äußerst förderlich bei der Feststellung von Handlungsnotwendigkeit bezüglich Netzwerkvorgaben im Rahmen der A.10, A.11 und A.12 Norm sein.
Evaluation und IT Security Assurance	ISO 15408, 15292, 15446, 15443, 18045	Weniger von Bedeutung da dies sehr bestrebte Standards sind, die stark formalisierte Vorgehen der Sicherheitseinstufung ermöglichen. Mehrfache funktionelle Ansätze sind enthalten. Praxisrelevante Bedeutung im Sinne der Sicherheitsbeurteilung meist sehr getrennt vorhanden, wie beispielsweise durch Systeme wie Firewalls, Kartenanwendungen oder Mailguards.
Public Key Infrastructure (PKI), Dienste für Zeitstempel, Non-repudiation	ISO 13888 15945, 18014 14516	Kein nennenswerter Bezug vorhanden, Spezialisten können sich die Standards zu Nutzen machen bei der Verwirklichung von A.12.2.3 Nachrichtenintegrität und A.10.9.x Schutz von E-Commerce-Diensten und deren Nutzung

PKI-Dienste und Trust Center	ETSI 101456, 102042, 101861	Mehrfache inhaltliche Beziehungen der technischen Spezifikation der ETSI zur ISO 27001
Verwendung von Intrusion Detection Systemen	ISO 18043	Nur von Bedeutung, sofern der Gebrauch solcher Systeme im Rahmen der Anwendung mit dem Standard betrachtet wird.
Security Incident Management	ISO 18044	Konkrete Verbindung zu A.13, welcher im technischen Report mehrfache Anweisungen zur Handhabung des Management von Vorfällen der Sicherheit preis gibt

Tabelle 5 Alternative Sicherheitsstandards [19, p. 19ff]

Zu den bereits erwähnten Normen und Standards bezüglich IT-Security sind viele weitere ähnlicher Art bekannt, welche einerseits die IT-Security Aspekte in anderer Betrachtung auffassen oder aber für gewisse Teilbereiche Abhilfe schaffen wollen. [4, p. 87]
Wie zuvor beschrieben sind die Standards rund um die ISO/IEC 27k Reihe festzuhalten. Einem IT-Security Spezialisten oder einer IT-Security Spezialistin ist es nahezulegen, sich diesbezüglich immer auf dem aktuellen Stand zu halten und Neuerscheinungen gewissenhaft zu verfolgen. [4, p. 87]
Neben diesen Normen haben sich weitere Standards per se als nützlich erwiesen. Standards rund um die ISO 15504 beschreiben beispielsweise ein Fortschrittsystem, womit der Rahmen durch Kennzahlen festgehalten werden kann. Aber auch die ISO 15408 „Common Criteria“ bringt erheblichen Mehrwert indem ein System zur Bewertung im Sinne der IT-Security geschaffen wird. [4, p. 87]
Darüber hinaus existieren unzählige Normen zum Schutze der physischen Sicherheit. Dies umfasst Bauvorschriften und Anordnungen, wie feuerfeste Türen oder auch einbruchssichere Fenster verwirklicht werden sollen. Häufig sind diese Normen als DIN-Norm vorhanden und versprechen dadurch einen entsprechenden Mehrwert für ein Unternehmen. [4, p. 87]

Zusammenfassend lässt sich festhalten, dass sämtliche Interessensvertretungen ihre Empfehlungen beim Aufbau eines ISMS aussprechen. Industrie- und Handelskammern können sich dabei als ideale Ansprechperson erweisen. [16, p. 98]

2.8. IMS – Integriertes Managementsystem

Da die einzelnen Standards, Normen und Best Practices bereits vorgestellt wurden, soll an dieser Stelle noch auf integrierte Managementsysteme hingewiesen werden. Diese ermöglichen davon einen ganzheitlichen Ansatz und stellen damit ein sehr hilfreiches Konzept zur Verfügung, in welchem ebenso auch das konzipierte Assessment Tool in späterer Folge Anwendung finden könnte. Dementsprechend soll der Ansatz in diesem Kapitel vorgestellt und in Erinnerung gerufen werden.

Vorweg sollen an dieser Stelle, die beiden Begriffe und deren Eigenschaften von einem integrierten Managementsystem definiert werden. [21, p. 443]
Entsprechend der ISO 9000:2013 ist ein Managementsystem dadurch gekennzeichnet, dass darin Handlungen zur Steuerung und Leitung eines Unternehmens abgebildet werden. In Summe dienen die darin enthaltenen Funktionen der Platzierung von Politik und operativen Zielen ebenso wie der betreffenden Realisation. Besonders die Planung, Entscheidung, Organisation, Kontrolle sowie die Lenkung erhalten besondere Aufmerksamkeit im Sinne der Funktionen eines Managementsystems. [21, p. 443]
Teilaufgaben eines Managementsystems sind sowohl die Entdeckung von Chancen und eine proaktive Ausrichtung, als auch das Entdecken von Gefahren. Managementsysteme fördern das ständige Weiterentwickeln im Hinblick auf die Kultur der fortlaufenden Verbesserung.
Demnach kennzeichnet ein optimales Managementsystem, eine von Menschen gezeichnete Organisationskultur wie folgt:

- klare, transparente sowie solide Prozesse
- eindeutige Verantwortlichkeiten und Organisationsstrukturen
- Zufriedenheit von Kunden und Mitarbeitern
- Risiko- und Kostenminimierung [21, p. 443f]

Integration kann bezugnehmend auf die Herstellung einer Einheit betrachtet werden. Integration versucht die Einbeziehung sowie Verschmelzung in ein großes Ganzes einzuleiten.
Integration versucht daher für eine ganzheitliche Organisationsführung eine funktionelle wie auch fachliche Strukturierung zu bilden, ohne dabei den Gesamtüberblick außer Acht zu lassen. Integration beschreibt außerdem die Symbiose von gesonderten Elementen und Teilaspekten im Hinblick auf das große Ganze und wie dieses gewinnbringend kollektiv organisiert werden kann. [21, p. 444f]

Ein integriertes Managementsystem, kurz IMS kann demzufolge im Allgemeinen wie folgt konkretisiert werden:
Es handelt sich dabei um ein Instrument der Steuerung zum Zwecke der Unternehmensführung. Dabei werden in dem jeweiligen Managementsystem diverse Teilmanagementsysteme wie beispielsweise Qualitätsmanagement, Arbeits- und Gesundheitsschutz oder eben Sicherheitsmanagement vollständig in einer einheitlichen Struktur miteinander in Einklang gebracht.
Ein integriertes Managementsystem ist zudem auf die Einhaltung diverser internationaler und nationaler Normen, Gesetzes- und Behördenvorgaben konzentriert, um diesbezüglich effektiv die Umsetzung der Ziele zu ermöglichen. [21, p. 445]

Wie eingangs, im Kapitel 2.1.4.2 Weitere Standards zu Management Systemen, können mittels Kombination der Standards, Synergien durch Systemintegration erreicht werden:

- Vereinfachte Handhabung, Klarheit und Transparenz
- Gemeinsame Audits für mehrere Systeme entlasten die obersten Führungsebenen
- Gemeinsame Dokumentation umfasst sämtliche Management- und Geschäftsprozesse
- Möglichkeit zur Geld und Zeiteinsparung [18]

Typische integrierte Managementsysteme können demnach beispielsweise ISO 9001 Qualitätsmanagement, ISO/IEC 27001 Informationssicherheitsmanagement, ISO/IEC 20000 IT Service Management als auch viele weitere mögliche Standards umfassen. Eine Beschränkung auf lediglich diese Standards besteht dabei nicht. [18]

Da sich der Fokus dieser Arbeit jedoch nicht auf Ausprägungen dieser oder konkreter Produkte beschränkt, wird dies hier als ausreichend betrachtet. Vielmehr werden im folgenden Kapitel die möglichen Kombinationen der Standards in der Theorie betrachtet, ehe im Kapitel 4 der „Kern“ der Arbeit, das Assessment Tool vorgestellt wird.

3. Kombinationen

Aufbauend auf den zuvor vorgestellten Standards widmet sich dieses Kapitel ihrer möglichen Kombinationen, sowie auch deren Gegenüberstellung und dem anschließenden Vergleich mit den Übereinstimmungen. Es bringt eine zusammenfassende Darstellung der theoretischen Überschneidungen aufgrund von Literatur. Dieser Abschnitt zeigt die vorherrschenden Überschneidungen gemäß verschiedener Fachliteratur und versucht diese durch Gegenüberstellungen darzustellen, ehe im darauffolgenden Kapitel mit dem Assessment Tool gezielt ausgewählte Standards des Service und Security Management Verwendung finden.

3.1. Gegenüberstellung / Vergleich / Matrix

Zusammenfassend versucht das folgende Kapitel die vorgestellten Standards miteinander in Kontext zu bringen und diese gegenüberzustellen.

Durch die Anwendung von Sicherheitsstandards soll ein entsprechendes Niveau an Sicherheit unter Berücksichtigung von angemessenen Kosten erreicht werden. [7, p. 37] Die nachstehende Tabelle zeigt eine auszugsweise Übersicht, der Standards, Normen und Best Practices.

	Bekannte IT-Sicherheitsstandards			IT-Standards Service Management	
	ISO 27002 (ISO 17799)	ISO 27001 (BS 7799-2)	IT-GSHB	Cobit	ITIL
Art der Organisation					
Banken / Versicherungen	H	H	H	H	H
Behörden / Verwaltungen	H	H	H	H	H
Beratung	N	N	H	H	H
HW / SW Hersteller	P	P	H	P	H
IT-Dienstleister	H	H	H	H	H
Gesundheitswesen	H	H	H	P	H
Kanzleien	H	H	H	P	N
Handwerk & Industrie	P	P	H	H	H
Dienstleister	P	P	H	H	H
Internationale Ausrichtung	H	H	P	H	H
IT-Relevanz der Organisation					
Niedrig	N	N	H	N	N
Mittel	P	P	H	P	P
Hoch	H	H	H	H	H
Rolle innerhalb der Organisation					
Management	H	H	H	H	H
Revisor	P	P	P	H	P
IT-Sicherheitsbeauftragter	H	H	H	P	H

IT-Leitung	H	H	H	H	H
Administratoren	P	P	H		P
Projektmanagement	H	H	P	P	P
Entwicklung	P	P	P		
Merkmale des Standards					
Produktorientiert			P		
Systemorientiert	H	H	H	H	
Technisch			H		N
Organisatorisch	H	H	H	P	H
Strategisch	H	H	H	H	H
Konzeptionell	H	H	H	H	H
Operationell			H	H	H
Kosten	Kostenpflichtig	Kostenpflichtig	Kostenlos	Kostenpflichtig	Kostenpflichtig

Tabelle 6 Vergleich von IT und Sicherheitsstandards [7, p. 37]

Legende:

Relevanz: H = hoch P = Partiell N = Niedrig

In Tabelle 1 wurden die unterschiedlichen Standards hinsichtlich ihrer Merkmale und Eigenschaften in Beziehung gesetzt. Im nachfolgenden Abschnitt werden die Standards bezüglich der Überschneidungen ihrer Kapitel in Zusammenhang gesetzt.

3.2. Zusammensetzungen / Schnittpunkte der Literatur

Im entstehenden Modell, dem Assessment Tool in Abschnitt 4, wird das Service- mit dem Security Management durch ein Mapping zu den Wechselwirkungen dargestellt werden. Als Basis des Mapping werden die Kapitel der Standards herangezogen.
In diesem Unterkapitel soll dazu vorweg eine Übersicht der vorgestellten Standards und deren Überschneidung laut Literatur festgehalten werden. Dazu werden die jeweiligen Kapitel der Standards in einer großen Matrix korreliert und dessen Gemeinsamkeiten laut Literaturanalyse dargestellt. Ausgangspunkt der Tabelle ist eine Matrix der ISO 27001 und der ISO 20000 der Advisera Expert Solutions Ltd. [35] Ausgehend von der Matrix mit den Standards der ISO 27001 und der ISO 20000 wurden diese um ITIL und IT Grundschutz, sofern Beziehungen vorhanden, in Relation in die Tabelle gesetzt. Somit umfasst die nachstehende Abbildung der Tabelle zwei Vertreter der Service-, sowie zwei der Security Management Domain. [36] [37]

Da die Tabelle eine Vielzahl von Überschneidungen hervorbringt, würde dies den Rahmen der folgenden A4 Seite überschreiten, beziehungsweise deren Lesbarkeit stark beeinträchtigen. Daher zeigt die folgende Tabelle eine vereinfachte Abbildung mit vereinfachter Bezeichnung zum Überblick. Die komplette Tabelle inklusive der Bezeichnung der Kapitel findet sich im Anhang B.

Mit der nachstehenden Abbildung der Tabelle soll ein Überblick der Kapitel der Standards und deren Beziehung vermittelt werden.

Service Management			Security Management		
ITIL		ISO/IEC 20000-1:2011	ISO/IEC 27001:2013	IT-Grundschutz	
Kapitel	*Bezeichnung*	*Kapitel*	*Kapitel*	*Kapitel*	*Bezeichnung*
		0			
		0.1	0.1		
		-	0.2		
		1	1		BSI-Standard 100-2, Kapitel 1 Einleitung
		1.1	-		
		1.2	-		
		2	2		BSI-Standard 100-1, Kapitel 1.5 Literaturverzeichnis
		-	-		
		-	-		
		3	3		IT-Grundschutz-Kataloge, Glossar
		-	-		
		-	-		
	Verschiedene ITIL-Prozesse aus Service Strategie, Service Design und Kontinuierliche Service-Verbesserung (CSI)	4.5 7	4		
		4.5.1	4.1	100-2, 3.2.1	Ermittlung von Rahmenbedingungen
	Business Relationship Management	7.1			
		4.5.1	4.2	100-2, 3.2	Konzeption und Planung des Sicherheitsprozesses
	Business Relationship Management	7.1			
		4.5.1	4.3	100-2, 3.3.2, 4	
		-	4.4	100-1, 3	ISMS-Definition und Prozessbeschreibung
				100-2, 2	Informationssicherheitsmanagement mit IT-Grundschutz
			5		
		4.1.1	5.1	100-2, 3.1	Übernahme von Verantwortung durch die Leitungsebene
		6.6.1 a)			
		4.1.2	5.2	100-2, 2, 3	
		6.6.1			
		4.1.3	5.3	100-2, 3.4	Organisation des Sicherheitsprozesses
		4.1.4			
	Supplier Management und Service Level Management	4.2			
	Strategie-Management für IT Services und verschiedene Prozesse aus Kontinuierliche Service-Verbesserung (CSI)	4.1 4.5.2 4.5.5 6.6.1 c) and d)	6		
		-	6.1		
		4.5.5.1	6.1.1	100-2, 3, 4, 5	
		4.5.2 j) 4.5.3 d)	6.1.2	100-2, 3, 4	
		6.6.1 c) 6.6.2	6.1.3	100-2, 4, 5	
		4.1.1 6.6.1 b)	6.2	100-2, 3	
		4 5.2 6	7		
		4.4.1	7.1	100-2, 3.5	Bereitstellung von Ressourcen für die Informationssicherheit
		4.4.2	7.2	100-2, 3.4.3	Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation
			7.3	100-2, 3.6	Einbindung aller Mitarbeiter in den Sicherheitsprozess
	Verschiedene Service-Strategie-, Service-Design- und Service-Transition-Prozesse	5.2 c)	7.4	100-2, 3.6	Einbindung aller Mitarbeiter in den Sicherheitsprozess
	Service Level Management	6.2			
	Verschiedene Service-Strategie-, Service-Design- und Service-Transition-Prozesse	4.3	7.5		
		-	7.5.1	100-2, 6.2	Informationsfluss im Informationssicherheitsprozess
		-	7.5.2	100-1, 4.3	Kommunikation und Wissen
		-	7.5.3	100-2, 6.2	Informationsfluss im Informationssicherheitsprozess
	IT Service Continuity Management und Availability Management Information Security Management	4.5.3 6.3 6.6	8		
		4.5.3 e)	8.1	100-2, 5	Umsetzung der Sicherheitskonzeption
		4.5.3 d)	8.2	100-2, 3, 4	
		6.3.1			
		4.5.3 d)	8.3	100-2, 4, 5	
		6.3.2			
		6.6.2			
		6.6.3			
	IT Service Continuity Management und Availability Management Information Security Management	4.5.4 6.3 6.6	9		
		4.5.4.1	9.1	100-2, 6	Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
		6.3.3			
		4.5.4.2	9.2	100-2, 6.1.1	Methoden zur Überprüfung des Informationssicherheitsprozesses
		6.6.1 e)			
		4.5.4.3	9.3	100-2, 6.1	Überprüfung des Informationssicherheitsprozesses in allen Ebenen
		6.6.1 f)			
		4.5.5	10		
		4.5.5.1	10.1	100-2, 6.1	Überprüfung des Informationssicherheitsprozesses in allen Ebenen
		4.5.5.2	10.2		

Tabelle 7 Interdependenz der Standards ausgehend von der ISO 27001 und d 20000

Mit der Tabelle 7 wurde versucht einen Überblick zu den Beziehungen der Standards laut Literatur zu dokumentieren.
Ehe zum angekündigten Modell in Abschnitt 4 und dem eigentlichen Mapping übergegangen wird, sollen abschließend im Kapitel 3.3 noch Kennzahlen und Reifegradmodelle vorgestellt werden, um anhand dieser das Assessment Tool zu erweitern.

3.3. Kennzahlen und Reifegradmodelle

Zur weiteren Abstützung der Werte und Kennzahlen im entwickelten Assessment Tool, sollen durch bereits etablierte Reifegradmodelle weiterführende Aussagen getroffen werden. Demzufolge werden hier vorweg die bekanntesten Reifegradmodelle vorgestellt und im Anschluss daraus ein Geeignetes gewählt und im Tool integriert, um mit den Kennzahlen in der Forschungsarbeit weitere Aussagen treffen zu können.

Zur Erfüllung von IT-Leistungen mithilfe von Services, sind entsprechende Prozesse unabdingbar. Oftmals erscheinen Organisationen eher technisch orientiert, beziehungsweise arbeiten diese vielmehr mittels Funktionen. Dadurch ist eine grundlegende Änderung erforderlich, womit eine entschlossene Vorbereitung sowie Planung einhergeht. Mittels einer prozessorientierten Denk- und Arbeitsweise, werden Aufgaben nicht mehr in isolierten Fachbereichen betrachtet. Vielmehr findet ein organisationsübergreifender Arbeitsprozess statt, mit welchem Aktivitäten bearbeitet werden können und Definitionen über Rollen zu Ressourcen eingeordnet werden. [20, p. 3]
In den zuvor beschrieben Kapiteln wurde darauf hingewiesen, messbare Ziele zu definieren. Um die vereinbarten Ziele auch wirklich erreichen zu können, sind zählbare Kennzahlen notwendig. Wie zugleich in anderen Bereichen der Informationstechnologie, spielt die Standardisierung eine wesentliche Rolle bei der Darbietung von Services. Umso besser die Erbringung der IT-Services standardisiert ist, desto wichtiger und entscheidender wird eine Messung ihres Erfolges. „Nur etwas Gemessenes, kann auch gesteuert werden“, behauptete der Amerikaner Peter Drucker in einem Zitat: [20, p. 193]

„If you can’t measure it, you can’t manage it“ [20, p. 193]

Grundsätzlich sollten Ziele SMART formuliert werden. Dieses Prinzip ist ein Akronym und beschreibt die Wörter spezifisch, messbar, akzeptiert, realistisch sowie terminiert. [20, p. 194] Ihren Bedeutungen wird hier nicht weiter Aufmerksamkeit geschenkt, beziehungsweise werden diese als verstanden betrachtet.

Durch Kennzahlen soll sichergestellt werden dass die Quantifizierung bei der Formung eines IT-Unternehmens verwendet werden kann. [20, p. 195]
Kennzahlen haben aber auch eine strenge Abhängigkeit untereinander und den basierenden Kennzahlensystemen. Kennzahlen vertreten sich nicht nur alleine, sondern bringen oftmals Wechselwirkungen mit sich. [20, p. 208]
Sie alleine sind allerdings auch wenig zufriedenstellend im Hinblick auf eine erfolgreiche IT-Strategie. Dazu bedarf es komplexeren und aufwendigeren Systemen. [20, p. 209]

Demzufolge gibt es einen sogenannten Reifegrad der Organisationen. Dieser kann anhand der Ausbreitung hinsichtlich der Planung, Umsetzung beziehungsweise der Erfüllung von IT-Services ermittelt werden. [20, p. 3]
Der Reifegrad ist ein Element der IT-Strategiemethode und kann sowohl als eigenstehende sowie auch als geschlossene Methode Anwendung finden. [38, p. 6]
Durch ein sogenanntes Reifegradmodell soll sichergestellt werden, dass eine Einheit wie beispielsweise ein Prozess, respektive dessen Gruppe, sowie auch eine Organisation selbst, in mehreren Stufen bewertet werden kann. [38, p. 13f]

Durch den Begriff „Reife“ soll erläutert werden, dass es im Kontext des Ergebnisses ein gewisses Maß an Qualität und Leistung zu erreichen gilt. Für den Terminus Reifegrad hingegen findet sich in der Literatur kaum eine allgemeingültige Definition, höchstens Beschreibungen, die sich dem annähern. [39, p. 175]
Die Reifegradmodelle basieren zumeist auf definierten Rangstufen bis hin zur Verbesserung des jeweiligen Prozesses oder Objektes. Sachgemäß erfolgt die Bewertung beziehungsweise individuelle Reife anhand von Methoden wie beispielsweise Fragebögen. Mittels Ermittlung der IST Situation lassen sich anschließend Empfehlungen für Verbesserungen ableiten. [38, p. 13f] Die Ermittlung des Reifegrades basiert demnach auf konzipierten Konzepten und Modellen, welche sich mit der Zeit etabliert haben. Mithilfe des Ergebnisses des Reifegradmodells, soll in weiterer Folge eine Ausgangsbasis geschaffen werden, um weitere Aktivitäten einer IT-Organisation festzulegen. [20, p. 3]

Die bekanntesten Modelle davon, werden im Folgenden näher vorgestellt, um im Anschluss eines, für das spätere Assessment Tool im Abschnitt 4, zu den Kennzahlen heranzuziehen.

3.3.1. Capability Maturity Model Integration (CMMI)

Das Modell CMMI, “Capability Maturity Model Integration” genannt, ist ein Prozess Referenzmodell, siehe auch ISO/IEC 21827. [17, p. 77] CMMI ist die Weiterentwicklung des 1987 entstanden CMM, kurz „Capability Maturity Model“. CMMI in der Version 1.2 wurde 2006 publiziert und bedient neben dem ursprünglichen Schaffungsgedanken der Softwareentwicklung ebenso Bereiche wie die Dienstleistung oder Beschaffung. [20, p. 215] Der Grundgedanke war die Kompatibilität zu SPICE zu gewährleisten. Zudem wollte man den Aufwand soweit wie möglich gering halten. [39, p. 176]
Das Modell CMMI hat sich über die Jahre hinweg nicht nur zur Bestimmung der Prozessreife im Softwareentwicklungsbereich bewährt, sondern ebenso über viele Jahre seine Stärke als Modell im IT-Servicemanagement bewiesen. Ebenso verwendet ITIL ein CMMI angelehntes Modell um die Prozessreife zu bekräftigen. [20, p. 215] CMMI besticht demnach als das wohl weit verbreitetste Reifegradmodell im IT-Bereich. [39, p. 158]

Sämtliche Ziele und Aktivitäten werden in Prozessgebieten dargestellt und sollen Verbesserung mit sich bringen. Eine Erreichung solcher Prozessgebiete geht mit jener des übergeordneten Ziels einher. Die genannten Prozessgebiete teilen sich in die folgenden vier Bereiche:

- Project Management
- Engineering
- Support
- Process Management [20, p. 215]

CMMI unterscheidet demnach zwei Arten, die kontinuierliche und die stufenförmige Darstellung von Modellen, welche im Folgenden beschrieben werden. [20, p. 215] Diese stellt auch den gravierendsten Unterschied zwischen CMM und CMMI dar. [39, p. 176]
Die kontinuierliche Darstellung umfasst sechs Fähigkeitsgrade sowie Capability Levels einer Skala von null bis fünf, respektive dessen Potenzial zur Verbesserung. Mittels der Darstellung entsteht sowohl eine Möglichkeit des organisationsinternen, als auch unternehmensübergreifenden Vergleichs, welcher durch die ISO/IEC 15504, siehe Abschnitt 3.3.3, entsprechend genutzt werden kann. [20, p. 215]
Die genannten Capability Levels nennen sich wie folgt:

- 0 – Incomplete (Unvollständiger Prozess): Ein Prozess wird nicht beziehungsweise unvollendet erbracht und die Ziele werden dahingehend nicht erreicht.
- 1 – Performed (Durchgeführter Prozess): Das Ziel von signifikanten Prozessen wird erreicht und die angestrebten Ergebnisse erstellt.

- 2 – Managed (Gesteuerter Prozess): Die Prozessaktivitäten finden entsprechende Planung und Überwachung mittels angemessener Ressourcen.
- 3 – Defined (Definierter Prozess): Der Prozess entspricht dem Fähigkeitsgrad des Levels Zwei und zudem den Prozessstandards der Organisation. Die Ergebnisse beinhalten außerdem den kontinuierlichen Verbesserungsprozess, kurz „KVP“.
- 4 – Quantitatively Managed (Quantitativ gemanagter Prozess): Der Prozess wird, mittels der Steuerung von festgelegten statischen Verfahren gestützt.
- 5 – Optimizing (Optimierender Prozess):Über die statischen Verfahren und dessen Informationen wird der Prozess den Abweichungen zufolge kontinuierlich verbessert. [20, p. 215f]

Dem gegenüber steht die bereits erwähnte stufenförmige Darstellung. Diese kommt ohne einer Stufe Null aus und beschreibt folglich nur fünf Maturity Levels von eins bis fünf. Diese Darstellung konzentriert sich auf die Erreichung eines Fähigkeitsgrades mit welchem eine Vergleich ganzer Unternehmen beziehungsweise deren Bereiche ermöglicht wird. Diese Maturity Levels lauten wie folgt: [20, p. 216]

- 1 – Initial (Initial): Die Organisation verfügt wenn überhaupt, nur mangelhaft und ad hoc über die dargestellten Prozesse. Der Erfolg ist gekoppelt mit der Verfügbarkeit der entsprechenden Ressourcen womit dieser Reifegrad sozusagen in jedem Unternehmen automatisch vorzufinden ist.
- 2 - Managed (Gemanagt): In Abstimmung werden die Prozessaktivitäten mit jenen der Unternehmensrichtlinien geplant und überprüft. Außerdem wird entsprechende Kapazität an Ressourcen bereitgestellt. Die Projekte werden respektive auf deren Erfüllung überprüft.
- 3 – Defined (Definiert): Die Prozesse sind erläutert und werden entsprechend der Ressourcen verstanden. Mittels dokumentierten Methoden und Werkzeugen wird dies sichergestellt. Durch standardisierte Prozesse erfolgt die Ausführung, gleichermaßen wie auch die kontinuierliche Verbesserung.
- 4 – Quantitatively managed (Quantitativ gemanagt): Mittels statischer Verfahren werden die Prozesse ergänzend ausgeführt. Die zugrunde liegende Qualität und Performance der Prozesse wiederfährt einem entsprechenden Management.
- 5 – Optimizing (Optimierend): Über die statisch gewonnen Informationen hinaus erfahren die Prozesse zwecks besserem Verständnis, eine optimierte Verbesserung. [20, p. 216]

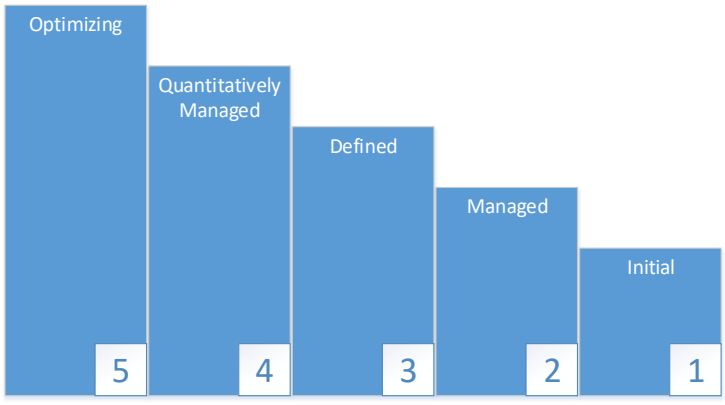

Abbildung 13 CMMI Maturity Levels

Nach CMMI existiert auch eine Weiterentwicklung mit der Bezeichnung ITSCMM, IT-Service-CMM. Durch dieses Modell wird IT-Dienstleistern ermöglicht, eine etappenweise Verbesserung der Erbringung von Services anzubieten. [39, p. 178]

CMMI stellt außerdem Schnittstellen zu weiteren Reifegradmodellen und Frameworks zur Verfügung, weshalb die Attraktivität dieses Modells weiter hervorgehoben wird. Mit der Anpassung an das SPICE Modell oder einer Schnittstelle zu COBIT, entstehen weitere positive Aspekte zu diesem Modell. [39, p. 178]

3.3.2. Process Maturity Framework nach ITIL (PMF)

Wie einführend bereits erwähnt, enthält ITIL 3 ein Reifegradmodell welches hier kurz erläutert wird. Das Modell ist am CMMI als auch dessen Vorgänger CMM, respektive dem CMMI für IT-Services, „CMMI-SVC“ ausgerichtet. Dieses Modell nimmt keine Unterscheidung der Abstufungen von einzelnen Prozessen vor, sondern findet für beide Varianten Anwendung. Die Anpassung erfolgte im Hinblick auf die Betrachtung der ITSM-Prozesse. Die einzelnen Prozesse in diesem Modell sind Vision und Steuerung, Prozesse, Personen/Mitarbeiter, Technologie/Tools sowie Kultur. Diese fünf Bereiche sind die Grundlage für die Auführung des Reifegrades im Modell. [20, p. 217]

Gleichermaßen wie bei CMMI finden fünf festgelegte Stufen, von eins bis fünf, unter der folgenden Bezeichnung Verwendung:

- Initial
- Repeatable
- Defined
- Managed
- Optimizing [20, p. 217]

Wie in den anderen Reifegradmodellen erfordert auch hier die Erreichung einer Stufe immer mindestens das Erlangen der Vorstufen. [20, p. 217]

3.3.3. ISO/IEC 33000 | ISO/IEC 15504 (SPICE)

SPICE ist ein Akronym für „Software Process Improvement and Capability Determination“ und wurde 1992 im Rahmen des Standards ISO/IEC 15504 veröffentlicht. SPICE legt den Fokus auf die Softwareentwicklung und verfolgt dabei zwei wesentliche Punkte: Sowohl die Prozessbewertung- und verbesserung „Process Improvement“, als auch die Ermittlung des Prozessreifegrades „Capability“. [40, p. 44]

Im Jahr 1998 wurde die ISO/IEC TR 15504 Norm als Vorversion entfernt, worauf 2006 der Ersatz durch die ISO/IEC 15504 erfolgte.
Im Gegensatz zum Technical Report 15504 besteht die ISO/IEC 15504 aus fünf wesentlichen Teilen welche wie folgt dargestellt werden:

- ISO/IEC 15504-1: Grundsätzliche Begriffe und Konzepte
- ISO/IEC 15504-2: Anforderungen zu Assessments und Referenzmodellen
- ISO/IEC 15504-3: Guide zur Durchführung von Assessments
- ISO/IEC 15504-5: Guide zur Anwendung von Prozessverbesserungen
- ISO/IEC 15504-6: Beispiel für Prozess-Assessment-Modell [40, p. 44]

Das Konzept hinter der ISO 15504 basiert auf einem Framework zur Messung und Bewertung von Prozessen, vor allem im Softwarebereich. Maßgebend dabei ist das Prozess-Assessment-Modell, welches das Referenzmodell und den Bewertungsrahmen in Einklang bringt. [40, p. 45]

Die ISO 15504 basiert wiederum auf sechs Fähigkeitsstufen, sogenannten „capability levels“, welche aufeinander aufbauend dargestellt werden. Eine Skala von vier Stufen dient der Bewertung der Prozessattribute. [40, p. 45]

Im Jahr 2015 hat die „International Standardization Organization“ die Weiterentwicklung der ISO/IEC 15504 zur ISO 33000 vorangetrieben. [41, p. 224]

Da die bekanntesten Reifegradmodelle und deren Funktionen nun vorgestellt wurden, wird an dieser Stelle zum Hauptteil dieser Arbeit übergegangen. Das nachstehende Kapitel beschreibt sämtliche Funktionen und Eigenschaften des entwickelten Tools und greift darin wieder auf eines der vorgestellten Reifegradmodelle zurück.

4. Assessment Tool

Zielsetzung dieser Arbeit ist ein Assessment Tool, mit welchem Aussagen zu den Wechselwirkungen von Service zu Security Management, beziehungsweise umgekehrt getroffen werden können.
Um die Implementierungen von Standards nicht anhand von Vermutungen abhängig zu machen, soll ein Werkzeug entstehen, mit dem präzise Aussagen zu den Wechselwirkungen ermöglicht werden. Dadurch sollen die Entscheidungen in Organisationen zugunsten der Einführung eines Standards zum einen erleichtert und zum anderen bekräftigt werden.

Als Zwischenergebnis wird dazu eine Einflussmatrix konstruiert, welche die Schnittpunkte der entsprechenden Kapitel beziehungsweise Kontrollen darstellt und diese Beziehung bewertet. Darauf aufbauend, werden weiterführende Aussagen, Prognosen respektive Auswirkungen abgeleitet.

Das genannte Assessment Tool wird nun in den folgenden einzelnen Teilabschnitten, Schritt für Schritt, erklärt.

4.1. Vorgehen der Modell-Erstellung

Ausgangspunkt ist die Entwicklung eines komplett neuartigen Werkzeugs, um fortführende Aussagen bei der Implementierung, eines der folgend genannten Standards und dessen Kontrollen treffen zu können.

Die Grundlage der Entwicklung zum Assessment Tool, basiert auf der Applikation Microsoft Excel. Die Wahl zugunsten dieses Programms wurde dahingehend getroffen, weil Excel weitläufig bekannt ist, nahezu jede nutzende Person damit produktiv arbeiten kann und darin fortführende Berechnungen mit einfachen Mitteln automatisiert abgebildet werden können. Sowohl durch Makros, als auch der Programmiersprache Visual Basic sind die Anwendungsmöglichkeiten praktisch unbegrenzt erweiterbar, wodurch das Produkt dieser Arbeit, das Assessment Tool, für jegliche mögliche Weiterentwicklungen gerüstet ist.

Für jene, die über diese Arbeit hinausreichen, empfiehlt sich, das Tool aufgrund reichhaltiger Überlegungen in eine alleinstehende Applikation zu übertragen.
Gerade im Bereich der Forschung erscheint allerdings Microsoft Excel, aus den zuvor genannten Gründen, als die ideale Wahl zur Erstellung dieser Erstversion. Um bestmögliche IT-Sicherheit anzustreben, wird vorerst auch auf die Verwendung von Makros verzichtet, wodurch das Tool eine .xlsx Endung trägt.

4.2. Tool „ServiceM2SecM.xlsx“

Das Assessment Tool „ServiceM2SecM“ dient als Basis, um Aussagen zu Wechselwirkungen in Unternehmen bei der Einführung, Implementierung beziehungsweise Erweiterung durch Service oder Security Management zu treffen. Hauptaugenmerk sind dabei die folgenden Standards:

- Service Management: ISO 20000-1, siehe Abschnitt 2.2.2
- Security Management: ISO 27001 , siehe Abschnitt 2.3.1.2
- Security Management: ISO 27002, siehe Abschnitt 2.3.1.3

Auf Grundlage der Kapitel und Kontrollen der oben genannten Regelwerke, basieren im Tool weitere Berechnungen. Um diese Auswertungen wissenschaftlich zu bekräftigen dienen Experteninterviews, welche in der sogenannten Einflussmatrix eingearbeitet sind.

Verwendet wurden im Modell folgende Versionen der Standards:

- Service Management: ISO 20000-1, EVS-ISO/IEC 20000-1:2013 [42]
- Security Management: ISO 27001 , 2. Entwurf Ausgabe: 2014-01-15 [43]
- Security Management: ISO 27002, ÖNORM ISO/IEC 27002 Edition: 2014-11-01 [44]

Die folgende Abbildung zeigt eine schematische Übersicht des Konzepts zum Assessment Tool.

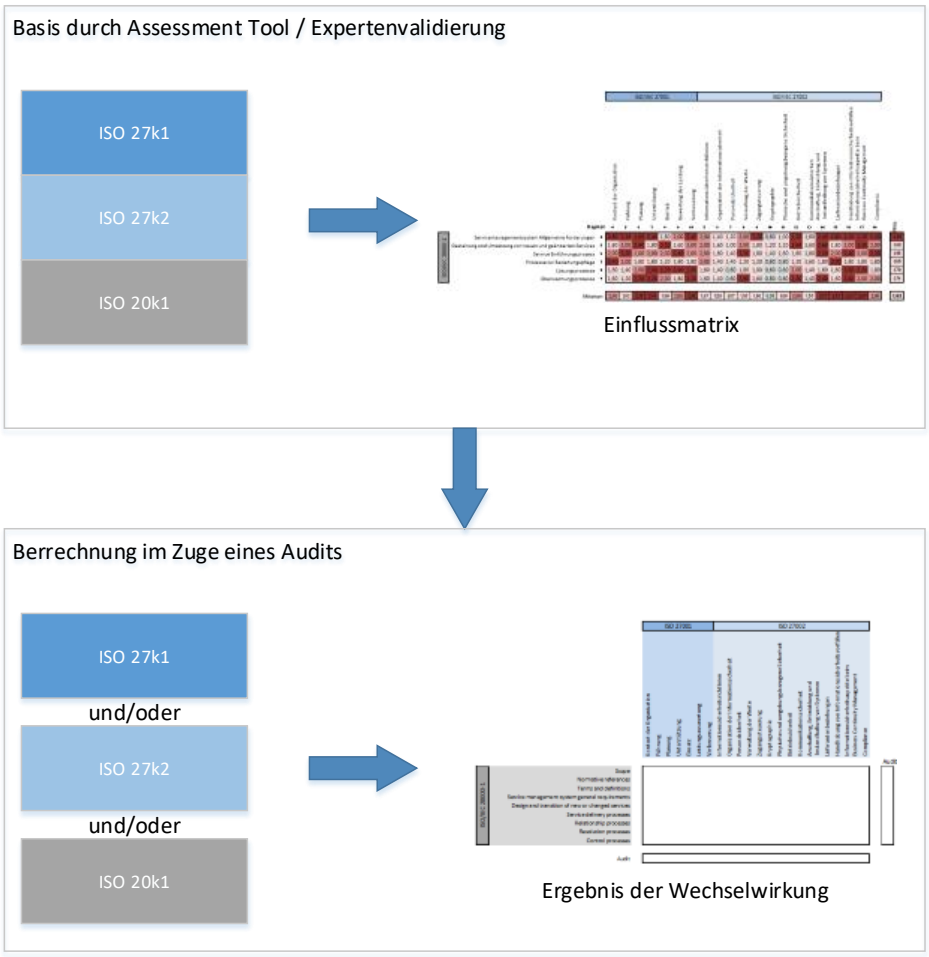

Abbildung 14 Übersicht zum Assessment Tool

Wie in Abbildung 14 ersichtlich, ist die Basis zum Assessment Tool die sogenannte Einflussmatrix. Für diese wird eine Einschätzung der Wechselwirkungen im Zuge dieser Arbeit bewertet und daraufhin durch Experten validiert.
Aufbauend auf diesem Resultat, können weiterführende Kalkulationen mit den Bewertungen im Zuge eines Audits errechnet werden. Dadurch lassen sich weiterführende Aussagen über die Wechselwirkungen und die Beeinflussungen von Implementationen im Unternehmen treffen.

Der nachstehende Abschnitt beschreibt daher die im Tool verwendeten Kapiteln.

4.2.1.1. Verwendete Kapitel und Kontrollen

Wie bereits erwähnt, basiert das Assessment Tool auf den Kapitel und Kontrollen der in Punkt 4.2 genannten Standards. Die nachstehende Tabelle erläutert die verwendeten Kapitel der jeweiligen Normen.

Norm	Kapitel	Bezeichnung
ISO 27001	4	Kontext der Organisation
ISO 27001	5	Führung
ISO 27001	6	Planung
ISO 27001	7	Unterstützung
ISO 27001	8	Betrieb
ISO 27001	9	Bewertung der Leistung
ISO 27001	10	Verbesserung
ISO 27002	5	Informationssicherheitsrichtlinien
ISO 27002	6	Organisation der Informationssicherheit
ISO 27002	7	Personalsicherheit
ISO 27002	8	Verwaltung der Werte
ISO 27002	9	Zugangssteuerung
ISO 27002	10	Kryptographie
ISO 27002	11	Physische und umgebungsbezogene Sicherheit
ISO 27002	12	Betriebssicherheit
ISO 27002	13	Kommunikationssicherheit
ISO 27002	14	Anschaffung, Entwicklung und Instandhaltung von Systemen
ISO 27002	15	Lieferantenbeziehungen
ISO 27002	16	Handhabung von Informationssicherheitsvorfällen
ISO 27002	17	Informationssicherheitsaspekte beim Business Continuity Management
ISO 27002	18	Compliance
ISO 20000-1	4	Servicemanagementsystem allgemeine Forderungen
ISO 20000-1	5	Gestaltung und Umsetzung von neuen und geänderten Services
ISO 20000-1	6	Service Einführungsprozess
ISO 20000-1	7	Prozesse zur Beziehungspflege
ISO 20000-1	8	Lösungsprozesse
ISO 20000-1	9	Überwachungsprozesse

Tabelle 8 Verwendet Kapitel im Assessment Tool

Vernachlässigt wurden dagegen einführende Kapitel der Normen, da diese im Hinblick auf die Wechselwirkungen keine tragende Relevanz mitbringen.
Insbesondere ist die Rede der Kapitel null bis einschließlich drei, der ISO 27001 sowie die Kapitel null bis einschließlich vier in der ISO 27002. In der ISO 20000-1 wurden die Kapitel eins, zwei und drei vernachlässigt, da diese keinen nennenswerten Einfluss bezüglich der Wechselwirkungen zum Security Management darstellen.

Im folgenden Abschnitt werden die verwendeten Kapitel der Tabelle 8 jeweils kurz vorgestellt.

4.2.1.2. Kurzbeschreibung der Kapitel & Kontrollen

Die verwendeten Kapitel der Normen ISO 27001, ISO 27002 und ISO 20000-1 werden nun der Reihe nach vorgestellt und deren Zweck in kurzen, prägnanten Sätzen zusammengefasst.
Mit dieser Beschreibung werden die Kapitel auch im Tool, im jeweiligen Registerblatt, beschrieben. Für detaillierte Informationen zu den Kapiteln, gibt es einen Verweis zum jeweiligen Regelwerk.

Die Kapitel der Norm, wurden im Assessment Tool bis zur jeweils zweiten Stufe aufgeschlüsselt. Das bedeutet beispielsweise, dass ein Kapitel „x“ bis zu „x.y“ beschrieben wurde. Enthält „x.y“ noch weitere Subkapitel, wie

„x.y.z“, wurden diese nicht mehr angeführt. Diese Detailinformationen können dem jeweiligen Standard entnommen werden.

Es folgen die Zusammenfassungen zu den verwendeten ISO 27001 Kapiteln.

- ISO 27001, Kapitel 4: Kontext der Organisation

Die Organisation bestimmt interne und externe Sachverhalte im Zuge der Informationssicherheit. Besonderes Augenmerk liegt dabei auf dem Verständnis für den Kontext der Organisation, den Bedürfnissen und Erwartungen der Stakeholder, sowie dem Geltungsbereich eines Informationssicherheitssystem. Die Organisation verfügt über ein Managementsystem für Informationssicherheit anhand der gegebenen Anforderungen und sorgt darüber hinaus für die Aufrechterhaltung und laufende Verbesserung. [42, p. 6]

- ISO 27001, Kapitel 5: Führung

Die Leitung stellt durch gezielte Maßnahmen wie Führung und Engagement, einer Leitlinie und organisatorischen Aufgaben, Zuständigkeiten und Befugnissen, die Führung zur Informationssicherheit sicher. [42, p. 7]

- ISO 27001, Kapitel 6: Planung

Die Organisation berücksichtigt und ermittelt bezüglich gegebener Risiken und Chancen entsprechend einer Informationssicherheitsrisikoeinschätzungs- und Risikobehandlung. Um die Sicherheitsziele- und pläne zu erreichen werden entsprechende Funktionen festgelegt. [42, p. 8f]

- ISO 27001, Kapitel 7: Unterstützung

Die Organisation unterstützt durch Ressourcen, Kompetenz, Bewusstsein, Kommunikation und Dokumentation bei der Implementierung und laufender Verbesserung des Informationssicherheitssystems. [42, p. 11f]

- ISO 27001, Kapitel 8: Betrieb

Die Organisation plant und kontrolliert die notwendigen Prozesse, die Implementierung und Kontrolle der Informationssicherheit. In regelmäßigen Abständen findet eine Risikoeinschätzung der Informationssicherheit bei wesentlichen Änderungen statt. Für die Risikoeinschätzung der Informationssicherheit hat die Organisation einen entsprechenden Plan implementiert. [42, p. 13]

- ISO 27001, Kapitel 9: Bewertung der Leistung

Die Organisation überwacht, misst, analysiert und bewertet die Performance und Wirksamkeit des Informationssicherheitssystem. In regelmäßigen Abständen finden Audits statt, um Rückmeldungen dazu erhalten. Auch die Leitung prüft planmäßig das Informationssicherheitssystem, um sich bezüglich dessen Wirksamkeit zu überzeugen. [42, p. 14]

- ISO 27001, Kapitel 10: Verbesserung

Die Organisation ist um eine laufende Verbesserung des Managementsystems für Informationssicherheit bemüht. Bei auftretenden Fehlern wird umgehend reagiert und mit entsprechenden Maßnahmen dagegen gearbeitet, um Eignung, Wirksamkeit und Angemessenheit zu gewährleisten. [42, p. 15f]

Folgend stellen die nachstehenden Punkte eine Zusammenfassung zu den jeweiligen verwendeten Kapiteln der ISO 27002 dar.

- ISO 27002, Kapitel 5: Informationssicherheitsrichtlinien

Die Organisation hält Managementanweisungen- und unterstützung für die Informationssicherheit betreffend Geschäftsanforderungen, relevante Gesetzen und Vorschriften bereit. [43, p. 2ff]

- ISO 27002, Kapitel 6: Organisation der Informationssicherheit

Die Organisation schafft einen Steuerungsrahmen zur Einleitung und Kontrolle der Umsetzung sowie zum Betrieb der Informationssicherheit innerhalb der Organisation. Außerdem gewährleistet die Organisation die Sicherheit der Telearbeit und die Nutzung von mobilen Geräten. [43, p. 4ff]

- ISO 27002, Kapitel 7: Personalsicherheit

Die Organisation stellt sicher, dass Mitarbeiter und Auftragnehmer ihre Verantwortlichkeiten verstehen und für jene Rollen geeignet sind, für die sie in Betracht gezogen werden. Außerdem sind sich Mitarbeiter vor, während und mit Beendigung ihrer Verantwortung im Sinne der Informationssicherheit bewusst. Bei einem Wechsel oder bei Beendigung der Anstellung ist der Schutz der Interessen der Organisation sichergestellt. [43, p. 9ff]

- ISO 27002, Kapitel 8: Verwaltung der Werte

Die Organisation identifiziert und definiert organisatorische Vermögenswerte, sowie deren geeignete Schutzverantwortlichkeiten. Es wird sichergestellt, dass Informationen in Übereinstimmung mit ihrer Bedeutung für die Organisation, ein angemessenes Schutzniveau erhalten. Es wird außerdem verhindert, dass Unbefugte eine Offenlegung, Änderung, Entfernung oder Vernichtung von auf Medien gespeicherten Informationen vornehmen können. [43, p. 13ff]

- ISO 27002, Kapitel 9: Zugangssteuerung

Die Organisation verfügt über Beschränkungen des Zugriffs auf Informationen, beziehungsweise deren Einrichtungen, mittels User Access Management. Durch User Responsibilities kann, durch Schutz der Authentifizierungsinformationen, Rechenschaft gezogen werden. Außerdem soll durch Access Control Unbefugten der Zugriff auf bestimmte Systeme und Anwendungen verhindert werden. [43, p. 19ff]

- ISO 27002, Kapitel 10: Kryptographie

Die Organisation verwendet angemessene, wirksame Verwendung von Kryptographie, um Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen gewährleisten zu können. [43, p. 28ff]

- ISO 27002, Kapitel 11: Physische und umgebungsbezogene Sicherheit

Die Organisation verhindert unbefugten Zugriff, Beschädigung und Störungen der Informationen und deren Einrichtungen. Die Organisation sorgt außerdem mit vorbeugenden Maßnahmen vor, um Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit zu unterbinden. [43, p. 30ff]

- ISO 27002, Kapitel 12: Betriebssicherheit

Die Organisation gewährleistet operative Prozesse und Verantwortlichkeiten für den korrekten und sicheren Betrieb von informationsverarbeitenden Einrichtungen. Sämtliche Daten sowie auch Datenverarbeitungseinrichtungen sind gegen Malware geschützt. Zu Verhinderung von Datenverlust ist durch ein Backup der Informationen vorzusorgen. Logging und Monitoring werden durchgeführt, um Ereignisse aufzuzeichnen und Beweise zu sichern. Die Kontrolle von Betriebssoftware gewährleistet

Integrität von Betriebssystemen. Schwachstellenmanagement wird verwendet, um der Ausnutzung technischer Mängel entgegen zu wirken. Abschließend wird mit Hilfe von Audits zu Informationssystemen, eine Minimierung der sicherheitstechnischen Auswirkungen von Aktivitäten auf betriebliche Systeme erreicht. [43, p. 38ff]

- ISO 27002, Kapitel 13: Kommunikationssicherheit

Das Netzwerksicherheitsmanagement und unterstützende Informationsverarbeitung soll sowohl den Schutz von Informationen in Netzwerken, als auch der Anlagen selbst sicherstellen. Die Sicherheit bei der Informationsübertragung von Daten innerhalb einer Organisation sowie auch beim Austausch mit externen Einheiten soll gewährleistet sein. [43, p. 49ff]

- ISO 27002, Kapitel 14: Anschaffung, Entwicklung und Instandhaltung von Systemen

Die Organisation kann sicherstellen, dass die Sicherheitsanforderungen an Systeme über den gesamten Lebenszyklus hinweg einen integralen Bestandteil darstellen. Dies schließt auch die Anforderungen an Informationssysteme mit ein, welche Dienste über öffentliche Netze bereitstellen. In den Entwicklungs- und Supportprozessen wird gewährleistet, dass Informationssicherheit innerhalb des Entwicklungslebenszyklus von Systemen entsprechend entworfen und implementiert wird. Zuletzt wird durch Testdaten der Schutz der Daten geprüft. [43, p. 54ff]

- ISO 27002, Kapitel 15: Lieferantenbeziehungen

Zum Schutz der Vermögenswerte, welche unter dem Einfluss von Lieferanten stehen, nimmt die Organisation die Informationssicherheit bezüglich den Lieferantenbeziehungen wahr. Lieferantenservice- und management werden genutzt, um ein vereinbartes Maß an Informationssicherheit und „Service Delivery“ im Einklang mit Lieferantenvereinbarungen zu erzielen. [43, p. 62ff]

- ISO 27002, Kapitel 16: Handhabung von Informationssicherheitsvorfällen

Die Organisation verfolgt eine konsistente und effektivvolle Strategie für das Management von Vorfällen der Informationssicherheit, einschließlich der Kommunikation über Ereignisse und Schwachstellen derer. [43, p. 67ff]

- ISO 27002, Kapitel 17: Informationssicherheitsaspekte beim Business Continuity Management

Die Kontinuität der Informationssicherheit soll in die Business Continuity Management Systeme der Organisation integriert sein, um Informationen jederzeit schützen zu können und auf etwaige negative Ereignisse vorbereitet zu sein. Darüber hinaus, soll die Verfügbarkeit ausreichend redundanter informationsverarbeitender Einrichtungen garantiert werden. [43, p. 71ff]

- ISO 27002, Kapitel 18: Compliance

Die Organisation gewährleistet die Einhaltung rechtlicher und vertraglicher Anforderungen zur Vermeidung von Verstößen gegen gesetzliche, regulatorische oder vertragliche Verpflichtungen in Bezug auf Informationssicherheit und Anforderungen. Außerdem wird sichergestellt, dass die Informationssicherheitsvorkehrungen entsprechend der organisatorischen Richtlinien und Verfahren implementiert und betrieben werden. [43, p. 74ff]

Zum Ende dieses Abschnitts, werden im Folgenden noch die verwendeten Kapitel der ISO 20000-1 zusammengefasst vorgestellt.

- ISO 20000-1, Kapitel 4: Servicemanagementsystem Allgemeine Forderungen

Die Organisation plant, betreibt, überwacht, pflegt und verbessert das SMS. Vom Serviceanbieter sind sämtliche Prozesse anderer Parteien identifiziert. Der Serviceanbieter muss demzufolge sämtliche Dokumente erstellen und verwalten, um eine effektive Planung und Bedienung des SMS zu gewährleisten. Der Serviceanbieter stellt die benötigten personellen, technischen, informativen und finanziellen Ressourcen zur Verfügung. Außerdem wird der Scope des SMS im Service Management Plan berücksichtig. [44, p. 7ff]

- ISO 20000-1, Kapitel 5: Gestaltung und Umsetzung von neuen und geänderten Services

Die Organisation muss diesen Prozess sowohl für alle neuen Dienste, als auch an deren Änderungen, mit dem Potenzial, einen großen Einfluss auf Dienstleistungen oder den Kunden zu haben, verwenden. Der Serviceanbieter muss die Serviceanforderungen für die neuen oder geänderten Services ermitteln. Neue oder geänderte Services müssen die Serviceanforderungen erfüllen. Dabei muss der Service Provider sämtliche Serviceleistungen entwerfen und dokumentieren. Die neuen oder geänderten Services müssen getestet werden, um sicherzustellen, dass sie die Serviceanforderungen erfüllen. Die neuen oder geänderten Services müssen anhand vorab vereinbarter Kriterien für die Abnahme von Dienstleistungen überprüft werden. [44, p. 13ff]

- ISO 20000-1, Kapitel 6: Service Einführungsprozess

Der Serviceanbieter muss die mit dem Kunden zu erbringenden Leistungen vereinbaren. Für jede gelieferte Dienstleistung sind ein oder mehrere SLAs mit dem Kunden abzustimmen. Der Serviceanbieter muss mit dem Kunden einen Leistungskatalog vereinbaren. Dieser muss die Abhängigkeiten zwischen Services und Servicekomponenten beinhalten. Die Beschreibung jedes Serviceberichts, einschließlich seiner Identität, seines Zwecks, seiner Zielgruppe, Häufigkeit und Details der Datenquelle müssen dokumentiert und vom Serviceanbieter und den interessierten Parteien genehmigt werden. Der Serviceanbieter muss die Risiken für die Kontinuität und die Verfügbarkeit von Services bewerten und dokumentieren. Er identifiziert und stimmt die Servicekontinuität mit den Verfügbarkeitsanforderungen ab. Die vereinbarten Anforderungen müssen die geltenden Geschäftspläne, Serviceanforderungen, SLAs und Risiken berücksichtigen. Es soll eine definierte Schnittstelle zwischen der Budgetierung und der Abrechnung von Serviceprozessen und anderen Finanzmanagement-Prozesse geben. Der Serviceanbieter muss Kapazität und Leistungsanforderungen mit dem Kunden identifizieren und vereinbaren. Das Management muss eine Informationssicherheitspolitik unter Berücksichtigung der gesetzlichen, regulatorischen Serviceanforderungen beziehungsweise den vertraglichen Verpflichtungen gewährleisten. [44, p. 15ff]

- ISO 20000-1, Kapitel 7: Prozesse zur Beziehungspflege

Der Serviceanbieter muss die Kunden, Nutzer und Interessenten der Services identifizieren sowie auch dokumentieren. Für jeden Kunden muss der Dienstleister eine bestimmte Person wählen, die für die Verwaltung der Kundenbeziehung verantwortlich ist. Der Serviceanbieter muss einen Kommunikationsmechanismus mit dem Kunden einrichten. Der Serviceanbieter verwendet Lieferanten, um bestimmte Teile des Service Management Prozesses zu implementieren. Der Serviceanbieter und der Lieferant vereinbaren einen dokumentierten Vertrag. [44, p. 19ff]

- ISO 20000-1, Kapitel 8: Lösungsprozesse

Für alle Vorfälle muss ein dokumentiertes Verfahren bestehen. Dieses Verfahren für die Verwaltung der Erfüllung von Serviceanfragen muss von der Aufzeichnung bis zur Schließung bestehen. Incidents und

Service Requests werden gemäß der Verfahren verwaltet. Es muss ein dokumentiertes Verfahren geben, um Probleme zu identifizieren und die Auswirkungen von Vorfällen zu minimieren oder ganz zu vermeiden. Der Serviceanbieter muss Daten und Trends zu Vorfällen und Problemen analysieren, um deren Ursachen zu ermitteln und potenziell vorbeugende Maßnahmen ergreifen können. [44, p. 21ff]

- ISO 20000-1, Kapitel 9: Überwachungsprozesse

Die Organisation verfügt über Kontrollprozesse sowie dokumentierte CI-Typen und einer Change Management Politik. Außerdem hat der Serviceanbieter mit dem Kunden eine Freigaberichtlinie zu vereinbaren, in der die Häufigkeit der Nutzung und die Art der Releases definiert sind. [44, p. 22ff]

Da nun die einzelnen Abschnitte der verwendeten Standards zusammengefasst wurden, beschreibt der kommende Punkt die wesentlichen Funktionen des Tools.

4.2.1.3. Funktionen des Tools

Ehe die einzelnen Funktionen, welche das Assessment Tool „ServiceM2SecM“ abdecken, genauer beschrieben werden, ist im Folgenden eine kurze Übersicht der wesentlichen Funktionen zusammengefasst:

- Übersichtliche Navigation durch das Tool
- Ausgewählte Kontrollen der ISO 27001
- Ausgewählte Kontrollen der ISO 27002
- Ausgewählte Kontrollen der ISO 20000-1
- Werkzeug zur Protokollierung im Zuge des Audits
- Berechnung der Wechselwirkungen der Kontrollen
- Zusammenfassung als Bericht mit übersichtlicher Darstellung
- Grafische Auswertung des Ergebnisses
- Einberechnung des Reifegrades
- Justierungsmöglichkeit von Parametern zur Auswertung

Die oben angeführten fundamentalen Funktionen werden nun in den darauf folgenden Abschnitten beschrieben. Im nächsten Abschnitt werden dazu ein Überblick und eine Navigationshilfe zum Tool hergestellt.

4.2.2. Überblick zum Assessment Tool

Das Tool ist in sechs grundlegende Bereiche unterteilt. Diese sind wie folgt, in einer für den Ablauf logischen Reihenfolge, benannt:

- 01_Navigation
- 02_SecurityM
- 03_ServiceM
- 04_Konfiguration
- 05_Auswertung
- 06_Bericht

Die zuvor genannten sechs Abschnitte im Tool, sind als farbige Registerblätter gekennzeichnet und charakterisieren die Hauptarbeitsbereiche. Über diese hinaus, existiert für die Standards ein eigenes Registerblatt pro Kapitel beziehungsweise pro Kontrolle.

Im Folgenden werden nun die genannten Hauptbereiche beziehungsweise deren Zweck erläutert.

Im ersten Registerblatt, Navigation, soll eine Übersicht über das Tool und dessen Verwendung geschaffen werden. Sämtliche Funktionen sind von diesem Bereich aus verknüpft. Es besteht demnach die Möglichkeit, direkt einzelne Kapitel per Link anzusteuern. Diese Übersicht bildet den vorgesehen Ablauf des Tool schematisch ab. Zudem fungiert die Übersicht als vorgesehener Ausgangspunkt bei der Verwendung des Tools. Sämtliche Registerblätter führen über das FH St. Pölten Logo zurück zu diesem Startpunkt.

Die nachstehende Grafik zeigt einen Ausschnitt der Navigation. Dieser Bereich ist als Startpunkt zu sämtlichen weiterführenden Bereichen zu betrachten.

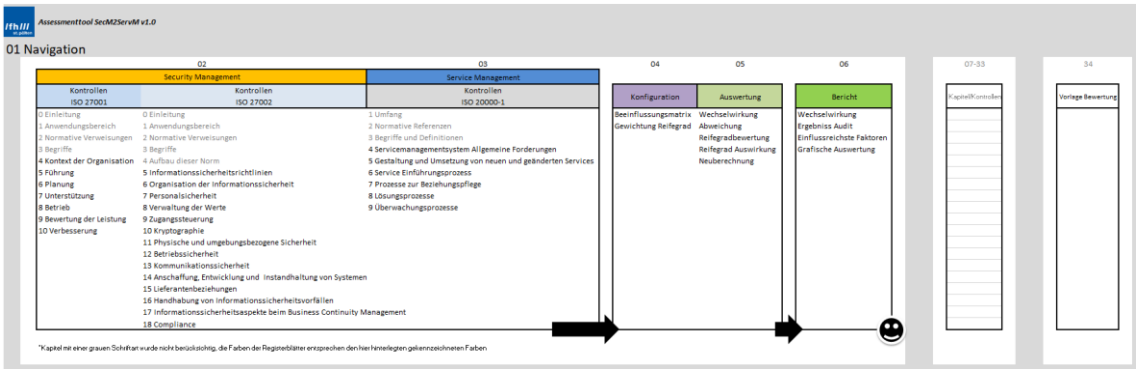

Abbildung 15 Bereich Navigation

Der Bereich „SecurityM“ zeigt eine Zusammenfassung der Kontrollen zum Security Management. Sämtliche Bewertungen darin, sind zu Beginn mit „Default-Werten“ befüllt. Per Klick auf die entsprechende Kontrolle, ist diese im jeweiligen Registerblatt verlinkt. Die festgelegten Bewertungen sind hier zusammengefasst dargestellt.

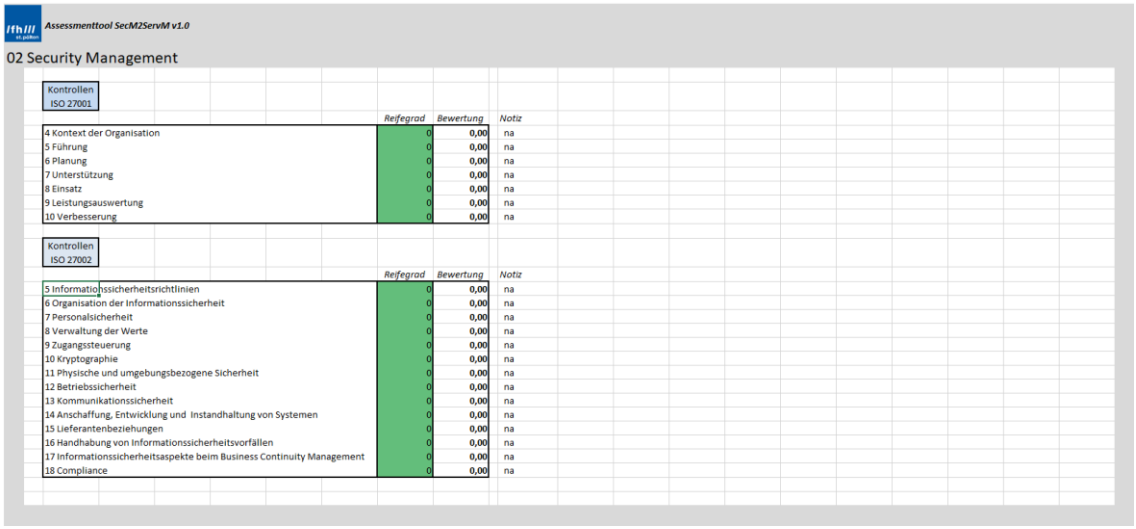

Abbildung 16 Bereich Security Management

Der Bereich „ServiceM“ bildet das Pendant zum vorherigen Registerblatt, in welchem sämtliche Kontrollen und Kapitel zum Service Management zusammengefasst sind. Die Struktur, die darin enthaltenen Elemente und Werte darin, sind nach demselben Prinzip wie zuvor im Security Management Bereich gegliedert.

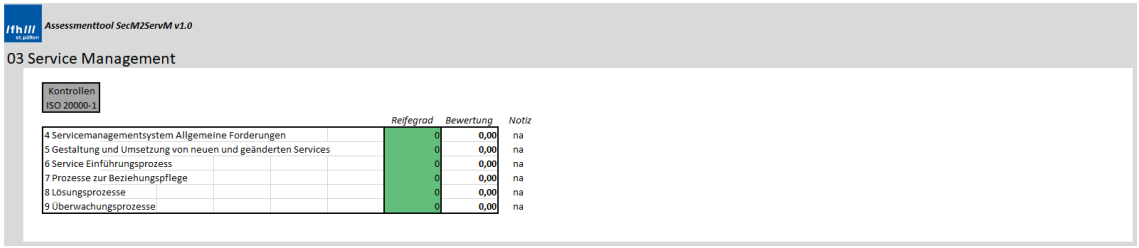

Abbildung 17 Bereich Service Management

Das folgende Registerblatt „Konfiguration“ ermöglicht Anpassungen der Einflussmatrix und fortlaufende Einstellungen im Hinblick auf die folgende Auswertung. Nachstehende Grafik zeigt einen Ausschnitt der Konfiguration.

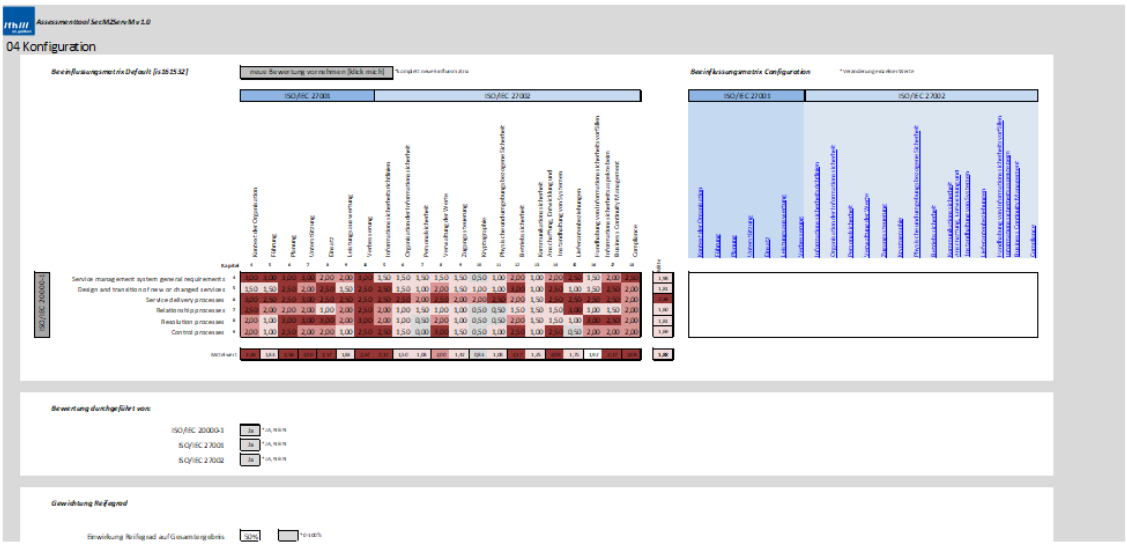

Abbildung 18 Bereich Konfiguration

Die Tabellen in diesem und im nachstehenden Abschnitt umfassen die entscheidenden Kalkulationen. Demzufolge sind diese Tabellen mit einer eindeutigen Nummer gekennzeichnet, um Querverweise zu anderen zu erleichtern. In den dazugehörigen Überschriften ist jeweils ein Kommentar mit Informationen hinterlegt. Darin ist die Berechnung erklärt und mit der entsprechenden Nummer zur eindeutigen Identifikation, ein Verweis auf eine andere Tabelle gegeben.

Im fünften Bereich „Auswertung“ sind die Berechnungen zur Basis der Einflussmatrix in Form von Tabellen ausgewertet. Dieses Registerblatt umfasst fünf Matrixtabellen wie folgt:

- „[3] Wechselwirkung durch Beeinflussungsmatrix [x + y * Basismatrix / 2 / 3]” – Berechnung der Wechselwirkung aufgrund einer erfolgten Bewertung der Kapitel beziehungsweise Kontrollen und der definierten Einflussmatrix.
- „[4] Abweichung Einzeln [Einzelabweichung Bewertung - Basismatrix]“ – Berechnung der Abweichungen in der Einflussmatrix zu den Wechselwirkungen
- „[5] Reifegradbewertung [IF, ELSE Reifegrad x + y / 2]“ – Berechnung des Schnittpunktes zum Reifegrad. Ist nur eines der beiden Kapitel zum Schnittpunkt bewertet, wird dieses übernommen. Sind

beide Werte zum Schnittpunkt gegeben, werden diese addiert und anschließend durch zwei dividiert, um den Mittelwert der Beiden als Schnittpunkt zu erlangen.

- „[6] Reifegrad Auswirkung auf Basismatrix [Reifegrad x Basismatrix]“ – Berechnung einer erneuten Basismatrix mithilfe der zuvor ermittelten Reifegradbewertung.
- „[7] Neuberechnung durch Reifegrad Faktor [x * y = Auswertung * Reifegradfaktor]“ – Berechnung eines Reifegrad-Faktors durch die Multiplikation der Reifegrad-Auswirkung und der Auswertung zu den Wechselwirkungen.

Das vorerst letzte Registerblatt der sechs Hauptbereiche ist eine Zusammenfassung der Ergebnisse. Alle bedeutenden Auswertungen sind darin in Form von Tabellen dargestellt und werden mit dazugehörigen grafischen Analysen bekräftigt. Demzufolge eignet sich der Bericht beispielsweise als zusammenfassende Dokumentation zu Audits, welche der überprüften Organisation und dem Management ausgehändigt werden können. Dieser abschließende Bereich gliedert sich damit wie folgt:

- Grafische Auswertung zu den Wechselwirkungen der Basismatrix
- Grafische Auswertung der einzelnen Bewertungen zu den Kapiteln
- Individuelle Darstellung der einflussreichsten Kapitel, wie beispielsweise die „Top 10 Auswirkungen“
- Grafische Auswertungen zu den Abweichungen der Basismatrix und den Reifegradkreuzungen
- Grafische Auswertungen zur Neuberechnung des Reifegrades

Darauf folgend sind noch die jeweiligen Kapitel beziehungsweise Kontrollen aus den Standards, jeweils in eigenen Registerblättern abgebildet. Darin besteht die Möglichkeit, diese einzeln im Zuge eines Audits zu bewerten und weitere Dokumentationen festzuhalten, beispielsweise in Form von Notizen. Auch der Reifegrad des jeweiligen Kapitel beziehungsweise der Kontrolle kann darin bestimmt werden. Die getätigten Bewertungen zu den einzelnen Kapiteln und Kontrollen nehmen daraufhin Einfluss auf die folgende Auswertung.

Die Folgende Abbildung 19 zeigt die Darstellung dieser Registerblätter anhand eines Beispiels.

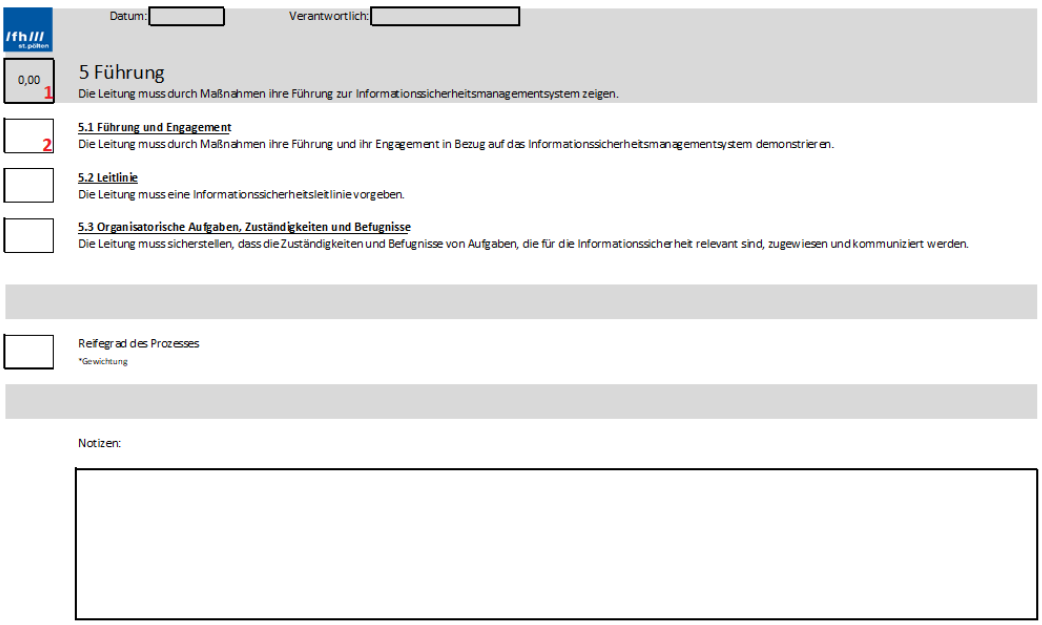

Abbildung 19 Registerblatt zur Kontrolle

Wie in Abbildung 19 zu sehen besteht im jeweiligen Registerblatt die Möglichkeit der Bewertung der einzelnen Kontrollen und Kapitel. Es kann entweder direkt im zusammenfassenden Bereich (in der Abbildung 19 durch die Eins gekennzeichnet) das gesamte Kapitel bewertet werden oder andernfalls werden die einzelnen Unterkapitel (in der Abbildung 19 durch die Zwei gekennzeichnet) bewertet und der zusammenzufassende Bereich errechnet sich durch diese wie folgt.

$$\overline{x} = \frac{x_1 + x_2 + \ldots + x_n}{n} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i$$

Das letzte Registerblatt zur vollständigen Arbeitsmappe ist eine Bewertungsvorlage „Auswertung_Vorlage“ in welcher die Einflussmatrix eigens, neu bewertet werden kann. Die Bewertung darin wird automatisch in die Konfiguration übernommen und kann dort gegebenenfalls nochmals angepasst werden.

Um jederzeit einfach zum Ausgangspunkt, der Übersicht im Navigationsbereich zu gelangen, genügt jeweils am entsprechenden Registerblatt ein Klick auf das „FH St. Pölten Bild“ im linken oberen Arbeitsbereich. Um die Bedienbarkeit zu vereinfachen wurden die Bearbeitungsmöglichkeiten in den Registerblättern äußerst eingeschränkt. Dadurch sollen die Anwenderinnen und Anwender auf die entscheidenden Bereiche hingewiesen werden.
Zur Bearbeitung beziehungsweise Weiterentwicklung des Tools kann die Sperre ohne einem Passwort aufgehoben werden.

Da nun ein Überblick zum Tool vorliegt, beschreibt der nachstehende Bereich die Beurteilungskriterien zur Einflussmatrix, worauf fortlaufende Auswertungen basieren.

4.2.2.1. Beurteilung zur Einflussmatrix

Dieser Abschnitt beschreibt die Beurteilung der sogenannten „Einflussmatrix“ zum Assessment Tool. Diese Matrix basiert auf Kreuzprodukten der Kapitel und Kontrollen aus den Standards. Die Matrix veranschaulicht zusammenfassend die jeweilige Überschneidung einschließlich deren Auswirkung.

Die Beurteilung der Einflussmatrix ermöglicht einen gewissen Raum zur Interpretation. Daher soll an dieser Stelle vorweg darauf hingewiesen werden, dass diese keine Bewertung der reinen Anforderungen darstellt, sondern vielmehr als eine Interpretation zu bewerten ist. Anders ausgedrückt ist zu verstehen, dass sofern in einem Normkapitel X kein direkter Hinweis auf die Notwendigkeit eines „Controls“ zur ISO/IEC 27002 vorhanden ist, dies nicht als negativ zu beurteilen ist. Vielmehr soll hier der Weg der Einschätzung gewählt werden. Die dadurch zusammenhängende Unschärfe der Bewertung soll am Ende durch den Mittelwert der Evaluierungen relativiert werden.
Die einzelnen Bewertungen zum Assessment Tool wurden daher bewusst dezent gestaltet und in drei grundlegende Stufen unterteilt. Eine tiefergreifende Differenzierung in kleinere Einheiten würde eine enorm steigende Komplexität mit sich bringen. Darüber hinaus steigt die Problematik mit einer breiteren Skala um ein Vielfaches, so dass ein soeben erwähntes gleiches Verständnis bei der Bewertung erzielt wird. Demzufolge basiert die Auswertung auf drei wesentlichen Stufen, „leicht - mittel – stark“, sowie zusätzlich der Stufe „Null“, welche keine relevante Abhängigkeit ausdrücken soll.

Die Bewertung der Ausprägung setzt sich daher aus den folgenden Werten zusammen:

- Stufe [0] entspricht „keine relevante Abhängigkeit“

Die Stufe Null, stellt keine nennenswerten Abhängigkeit zwischen den Abschnitten der jeweiligen Norm dar und kann somit im Wesentlichen vernachlässigt werden. An dieser Stelle muss allerdings erwähnt werden, dass eine

hundertprozentige „Nichtauswirkung“ theoretisch in der Praxis nicht vorzufinden sein wird. Dennoch geht dieses Werkzeug davon aus, dass in gewissen Fällen eine bedeutungslose theoretische Abhängigkeit vorherrscht, womit diese hier vernachlässigt werden kann.

- Stufe [1] entspricht „leichte Abhängigkeit“

Stufe Eins beschreibt eine leichte Abhängigkeit. Damit ist nur eine geringe Beeinflussung des Abschnittes auf dessen Schnittpunkt gegeben. Der Bezug zweier Kapitel kann in dieser Stufe nicht mehr vernachlässigt werden, womit dieser gering berücksichtigt werden soll.

- Stufe [2] entspricht „mittlere Abhängigkeit“

Die mittlere Stufe Zwei, zeigt wesentliche Merkmale der Abhängigkeit. Der Schnittpunkt in der Matrix von zwei Kapiteln lässt tragende Abhängigkeiten sowohl positiv als auch negativ erkennen, wenn diese auch nicht vollkommen ausgeprägt sind. Daher verbleibt der Beziehung beider Kapitel noch Platz für eine stärkere Form der Abhängigkeit, welche in der letzten folgenden Stufe abgebildet werden soll.

- Stufe [3] entspricht „starke Abhängigkeit“

Die letzte Stufe Drei, zeigt erhebliche Abhängigkeit und steht für die am stärksten ausgeprägte Interdependenz welche in der Matrix abgebildet werden kann. Mit dieser Stufe wird die bedeutendste Form der Beeinflussung wiedergegeben, wodurch die Umsetzung starke Auswirkung mit sich bringt.

Die nachstehende Grafik zeigt die Lese- und Bewertungsrichtung, mithilfe der zuvor genannten Beurteilungen.

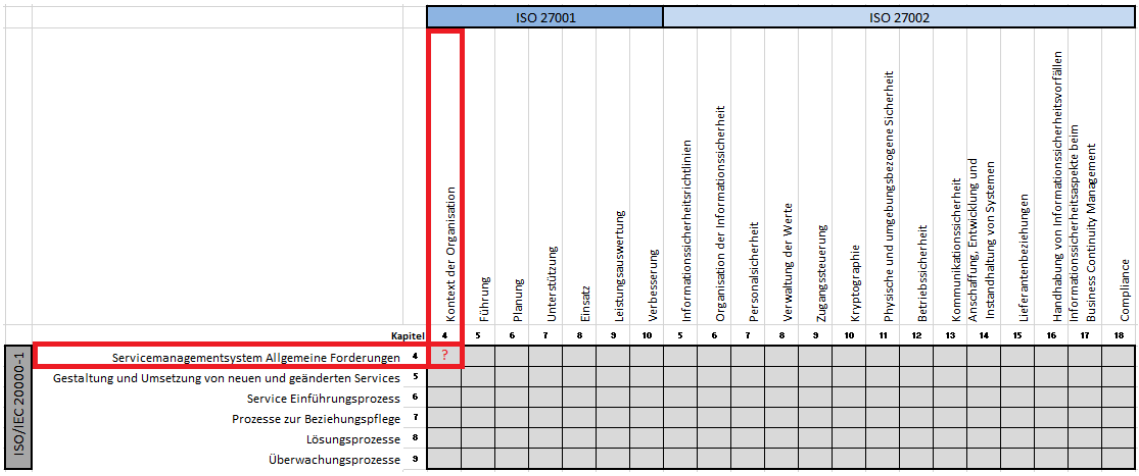

Abbildung 20 Lese- und Bewertungsrichtung der Matrix

Die dargestellte Abbildung 20 bringt die Lesbarkeit der Matrixtabelle nahe. Im Tool wird zur Bewertung jedes Kapitels der ISO 20000-1, horizontal einzeln dargestellt und anschließend, entgegen der Kapitel der ISO 27001 und ISO 27002, vertikal dargestellt, durchgegangen. Das oben abgebildete Muster ist wie folgt zu lesen:
Wie steht „Kontext der Organisation“ mit „->“ „Service management system general requirements“ in Zusammenhang? Zusammengefasst ausgedrückt, ist die Matrix daher vertikal zu horizontal zu verstehen und demnach als unidirektional zu bewerten.

Die jeweiligen Bewertungen werden entsprechend der Auswirkung mit einem aussagekräftigen „Farbcode“ wie folgt gekennzeichnet.

0	Stufe [0] entspricht „keine relevante Abhängigkeit“
1	Stufe [1] entspricht „leichte Abhängigkeit“
2	Stufe [2] entspricht „mittlere Abhängigkeit“
3	Stufe [3] entspricht „starke Abhängigkeit“

Tabelle 9 Farbcode der Bewertung

Das Tool bietet im Bereich der Bewertungsvorlage, Registerblatt „Auswertung_Vorlage“ außerdem die Möglichkeit, anhand der horizontalen, beziehungsweise vertikalen, Plus- und Minussymbole die Unterkapitel zum jeweiligen Kapitel und der Kontrollen ein- und auszublenden.

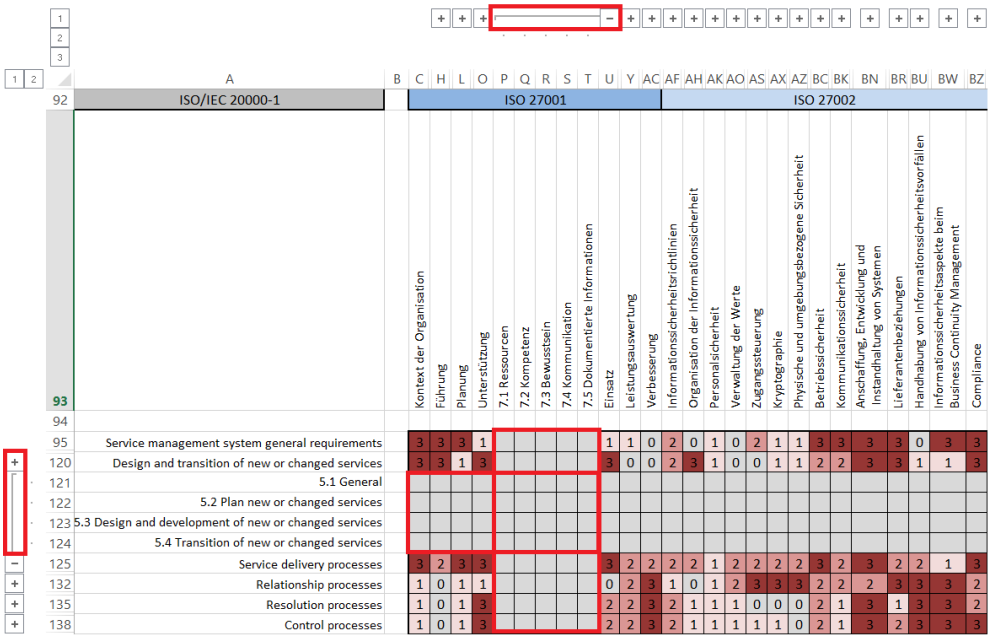

Abbildung 21 Erweiterte Ansicht der Unterkapitel

Da die Einflussmatrix, die Bewertungsschemata und deren Funktionen nun vorgestellt wurden, beschreibt der nachkommende Abschnitt die Evaluation hinter den ermittelten Werten.

4.2.3. Evaluation der Daten zum Modell / Experteninterview

Wie bereits skizziert, bildet die Einflussmatrix die Basis für fortlaufende Berechnungen im Tool.

Aufgrund der zahlreichen Kapitel und Kontrollen der drei Standards ergibt sich eine sehr umfassende Kreuztabelle. Werden lediglich die Grundkapitel multipliziert, bewirkt das die Rechnung der Faktoren 6 und 21 mit dem Produkt von 126 Kreuzungen.
Wird die Kreuzungstabelle mit den beschrieben Plus-Symbolen aus Abbildung 21 erweitert, entsteht eine Matrix mit den Faktoren 76 und 44, wodurch sich das Produkt von 3666 Kreuzungen summiert.
Wie in Abbildung 22 veranschaulicht ist, geht daher ein enormer Bewertungsaufwand bei der Berücksichtigung von Subkapiteln der Standards einher.

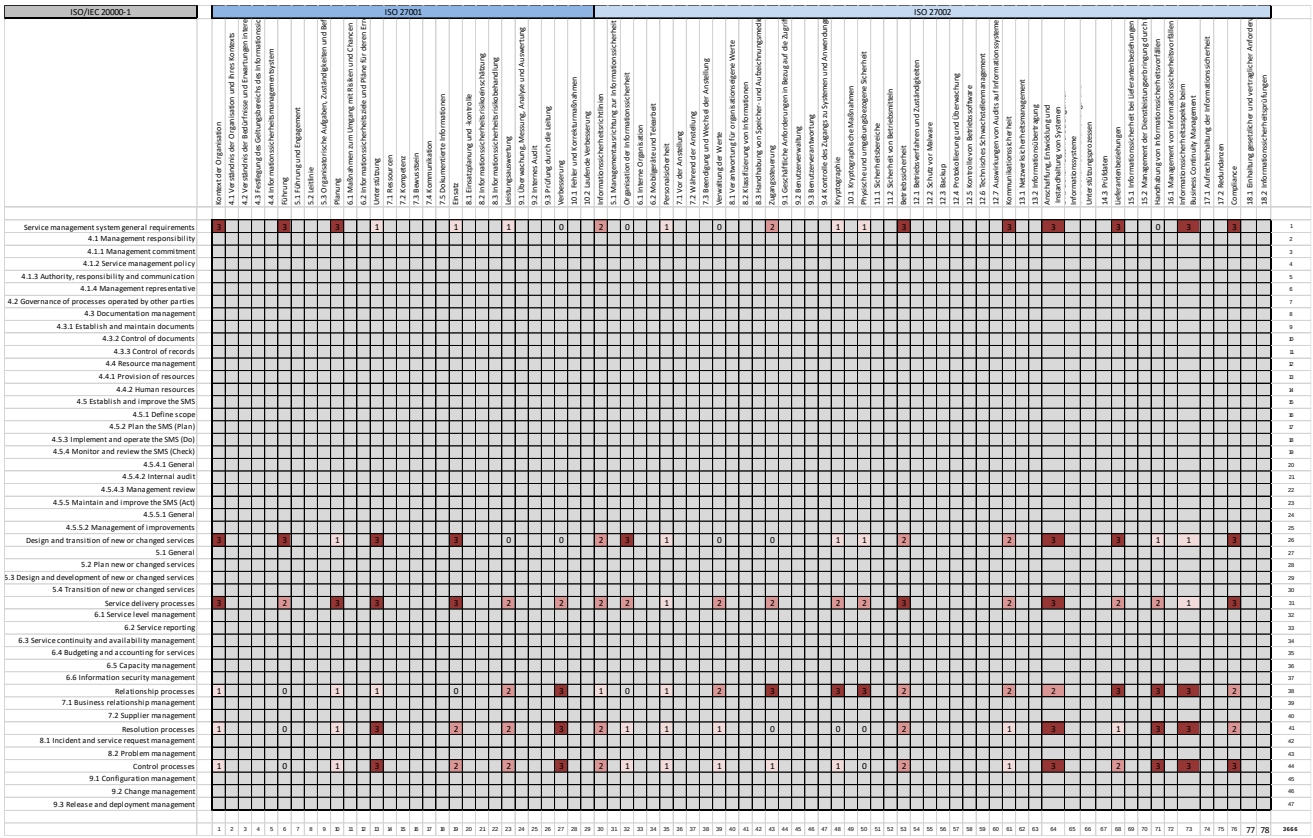

Abbildung 22 Matrix mit Subkapitel

Wird diese ausgedehnte Kreuztabelle und der damit verbundene Bewertungsaufwand mit einem naheliegenden Zeitfaktor zur Bewertung multipliziert, ergibt sich dadurch ein kaum zu realisierender Aufwand für ein Experteninterview mit mehreren Personen für diese Arbeit.

Aus diesem Grund wurde die Bewertung schrittweise pro Kapitel auf oberster Ebene vorgenommen und in erster Instanz, die Kreuzung von 126 Kapiteln der Standards als Ziel verfolgt.
Die Bewertung der einzelnen Schnittpunkte ist in einem separaten Excel-File festgehalten, um die Evaluierung der Werte vom eigentlichen Tool zu trennen. Das zusammengefasste Ergebnis der Auswertung zur Einflussmatrix ist im Tool abgebildet, wobei die einzelnen Werte bei Bedarf individuell angepasst werden können.

Ganz zuerst erfolgt eine Einschätzung der Abhängigkeiten durch den Autor. Demzufolge wird in den nachstehenden Tabellen, pro bewertetem Kapitel der ISO/IEC 20000-1, jeweils die Bewertung und ein kurzer Kommentar mit deren Begründung aufgelistet. Sämtliche Kommentare zu den Bewertungen sind als kurze stichworthaltige Statements zu verstehen.

Im Anschluss ist das Gesamtergebnis nochmals zusammenfassend abgebildet. Zur besseren Lesbarkeit und zum Verständnis der einzelnen Bewertungen wurde die Tabelle transponiert, das heißt Zeilen und Spalten im Hinblick auf das Endergebnis vertauscht.

		ISO 20000-1
		Servicemanagementsystem Allgemeine Forderungen
ISO 27001	Kontext der Organisation	3 — Der Kontext der Organisation muss gut verstanden werden, um den Anforderungen des Service Management gerecht zu werden. Das Verständnis der Bedürfnisse und die Erwartungen interessierter Parteien, müssen sowohl im Bereich Security als auch im Service Management bekannt sein. Selbiges gilt für den Geltungsbereich des IS Systems, dessen Kontext stark mit den Domänen im Service Management korreliert.
	Führung	3 — Führung und Engagement stehen in starkem Zusammenhang mit Management Responsibility. Governance von Prozessen anderer Parteien ist wesentlich mit Führung in Verbindung zu bringen. Führung muss im Sinne der IS geschehen, um diese auch im Service Management entsprechend gewährleisten zu können. Eine Leitlinie muss für die IS gegeben sein und betrifft ebenso sämtliche SM Anforderungen.
	Planung	3 — Maßnahmen zum Umgang mit Risiken und Chancen im Sinne des IS sind in starkem Zusammenhang mit Governance anderer Parteien, Ressourcen Management aber auch bei der Einrichtung eines SMS. Informationssicherheitsrisikoeinschätzung- und Behandlung ist ein nicht weniger wichtiger Aspekt im Hinblick auf Management Verantwortlichkeiten. Ziele und Pläne für die Erreichung der IS sind sehr stark in Verbindung mit den SMS Anforderungen zu setzen.
	Unterstützung	3 — Unterstützung muss durch Ressourcen, Kompetenz, Bewusstsein und Kommunikation geschaffen werden und steht in Zusammenhang mit Ressourcen Management. Es beeinflusst überdies ebenso sehr wesentlich den Betrieb des SMS. Dokumentierte Informationen korrelieren außerdem stark mit dem Dokumenten Management im SMS.
	Betrieb	1 — Einsatzplanung- und Kontrolle, Informationssicherheitsrisikoeinschätzung- und Behandlung haben teilweise Übereinstimmungen im Zuge der Einführung eines SMS.
	Bewertung der Leistung	2 — Messung und Analyse von Leistungen können wesentliche Teile zu den Prozessen in SMS Anforderungen beitragen, vor allem wenn es um eine laufende Verbesserung im SMS geht.
	Verbesserung	3 — Verbesserung von Fehlern, respektive dessen Korrekturmaßnahmen, sind sehr stark in Verbindung zur laufenden Verbesserung des SMS zu setzen.
ISO 27002	Informationssicherheitsrichtlinien	2 — Vorgaben der Leitung zur Informationssicherheit beeinflussen Ressourcen Management, das Governance von Lieferanten sowie den Betrieb des SMS.
	Organisation der Informationssicherheit	2 — Die interne Organisation der IS erhebt essentielle Einflüsse auf den Betrieb des SMS. Zudem ist Governance von anderen Parteien auch entscheidend betroffen.
	Personalsicherheit	1 — Sicherheit des Personals steht in Zusammenhang mit dem Bereich des Ressource Managements. Kleine Überschneidungen sind im Bereich Governance, im Zuge von Prozessen mit anderen Parteien, vorzufinden.
	Verwaltung der Werte	2 — Verwaltung und Verantwortung für Werte korrelieren mit Management Verantwortung im SMS und stimmt zudem mit Ressource Management und dem Betrieb des SMS überein.
	Zugangssteuerung	2 — Etwaige Zugriffskontrollen im IS wirken auf den Betrieb und die Verbesserung zum SMS ein. Bereiche wie Governance von anderen Parteien sind dadurch ebenso betroffen.
	Kryptographie	1 — Kryptographische Maßnahmen streifen in wenigen Aspekten, wie beispielsweise Governance von anderen Parteien sowie im Betrieb des SMS.
	Physische und umgebungsbezogene Sicherheit	1 — Sicherheitsbereiche und Betriebsmittel im IS wirken sich auf den Betrieb des SMS aus. Bereiche wie Ressource Management sind ebenso davon betroffen.
	Betriebssicherheit	2 — Betriebsverfahren und Zuständigkeiten, Schutz vor Malware, Datendiebstahl oder auch Datensicherung haben Auswirkungen auf Governance von Prozessen anderer Parteien, allen voran dem Betrieb und der laufenden Verbesserung des SMS.

Kommunikationssicherheit	2	Sicherheit in der Kommunikation hat Konsequenzen auf Governance von Prozessen anderer Parteien, dem Betrieb und der laufenden Verbesserung des SMS.
Anschaffung, Entwicklung und Instandhaltung von Systemen	2	Anschaffung, Entwicklung und Instandhaltung von Systemen beeinflusst Ressource Management, den Betrieb und die laufende Verbesserung des SMS.
Lieferantenbeziehungen	3	Sicherheit in Lieferantenbeziehungen steht in starkem Zusammenhang zur Governance von Prozessen anderer Parteien des SMS.
Handhabung von Informationssicherheitsvorfällen	2	Management von Informationssicherheitsvorfällen und deren Verbesserungen, beeinflusst vor allem die laufende Verbesserung des SMS.
Informationssicherheitsaspekte beim Business Continuity Management	3	Informationssicherheitsaspekte des Business Continuity Management ist stark verflechtet mit dem Betrieb und der laufenden Verbesserung des SMS.
Compliance	2	Richtlinienkonformität ist ein wichtiger Bereich zur Management Verantwortlichkeit, Ressource Management und vor allem im Betrieb des SMS.

Tabelle 10 Mapping ISO20k Kapitel 4 vs. ISO27k1, ISO27k2

		ISO 20000-1 Gestaltung und Umsetzung von neuen und geänderten Services
ISO 27001		
Kontext der Organisation	1	Kontext und Verständnis der Organisation deckt sich mit Teilbereichen der Phase der Gestaltung und Umsetzung für neue oder geänderte Services.
Führung	2	Führung hat teilweise Überschneidungen zu den Bereichen der Phase der Gestaltung und Umsetzung für neue oder geänderte Services. Besonders im Bereich organisatorische Aufgaben und Zuständigkeiten lassen sich Überkreuzungen zum SMS erkennen.
Planung	3	Maßnahmen zum Umgang mit Risiken und Chancen des IS sind stark im Zusammenhang zum Bereich Gestaltung und Umsetzung für neue oder geänderte Services zu sehen. Informationssicherheitsrisikoeinschätzung- und Behandlung sind davon nicht auszuschließen.
Unterstützung	2	Ressourcen, Kompetenzen, Bewusstsein und vor allem dokumentierte Informationen sind in folgenreichen Zusammenhang zu den Bereichen Gestaltung und Umsetzung für neue oder geänderte Services.
Betrieb	3	Einsatzplanung- und Kontrolle, beziehungsweise die Informationseinschätzung sind wichtige Eckpfeiler bei der Phase Gestaltung und Umsetzung für neue oder geänderte Services.
Bewertung der Leistung	2	Überwachung, Messung, Analyse, Auswertung und Audits zur Bewertung der Leistung können hilfreich sein zum Gestaltung und Umsetzung für neue oder geänderte Services womit eine gewisse Abhängigkeit festzuhalten ist.
Verbesserung	3	Fehler und Korrekturmaßnahmen, beziehungsweise laufende Verbesserung sind in starker Korrelation mit Gestaltung und Umsetzung für neue oder geänderte Services.
ISO 27002		
Informationssicherheitsrichtlinien	2	Vorgaben der Leitung zur Informationssicherheit tragen maßgeblich zum Design und zur Transition für neue oder geänderte Services im SMS bei.
Organisation der Informationssicherheit	1	Die interne Organisation der IS streift gewisse Bereiche zur Gestaltung und Umsetzung der Services im SMS.
Personalsicherheit	1	Die Sicherheit des Personals und weitere Subbereiche dieses Kapitels beeinflussen teilweise die Bereiche der Gestaltung und Umsetzung für neue oder geänderte Services.
Verwaltung der Werte	2	Das Erhalten des angemessenen Schutzes der Werte einer Organisation steht zum Teil in Beziehung zu Gestaltung und Umsetzung für neue oder geänderte Services.
Zugangssteuerung	1	Die Beschränkung des Zugriffs auf Informationen beeinflusst teilweise die Kapitel der Gestaltung und Umsetzung für neue oder geänderte Services.
Kryptographie	1	Die wirksame Verwendung von Kryptographie beeinflusst das Kapitel zur Gestaltung und Umsetzung für neue oder geänderte Services nur teilweise.

Physische und umgebungsbezogene Sicherheit	1	Verhinderung des unautorisierten physischen Zugriffs hat schwache Dependenzen im Hinblick auf die Gestaltung und Umsetzung für neue oder geänderte Services im SMS.
Betriebssicherheit	3	Sicherstellung des ordnungsnahen und sicheren Betriebs ist ein wichtiger Punkt in der Gestaltung und Umsetzung für neue oder geänderte Services.
Kommunikationssicherheit	1	Sicherstellung, des Schutzes von Informationen in Netzwerken hat weniger bedeutende Überschneidungen in besonderer Betrachtung der Phase zur Gestaltung und Umsetzung für neue oder geänderte Services.
Anschaffung, Entwicklung und Instandhaltung von Systemen	3	Die Sicherstellung, dass IS über den gesamten Lebenszyklus wahrgenommen wird, korreliert besonders in Phasen der Veränderung und damit mit Gestaltung und Umsetzung für neue oder geänderte Services.
Lieferantenbeziehungen	1	Die Sicherstellung, des Schutzes der für Lieferanten zugänglichen Informationen hat weniger Einfluss auf Gestaltung und Umsetzung für neue oder geänderte Services, darf aber dennoch nicht außer Acht gelassen werden.
Handhabung von Informationssicherheitsvorfällen	2	Das Management von Informationssicherheitsvorfällen und deren Verbesserungen, ist im wesentlichen Zusammenhang zur Gestaltung und Umsetzung für neue oder geänderte Services eines SMS.
Informationssicherheitsaspekte beim Business Continuity Management	3	Die Kontinuität der IS als Teil des Business Continuity Managements steht in tiefgründigem Zusammenhang mit der Phase Gestaltung und Umsetzung von Services.
Compliance	2	Informationssicherheitsvorkehrungen haben eine wichtige Auswirkung zur Gestaltung und Umsetzung für neue oder geänderte Services.

Tabelle 11 Mapping ISO20k Kapitel 5 vs. ISO27k1, ISO27k2

		ISO 20000-1 Service Einführungsprozess
ISO 27001		
Kontext der Organisation	3	Die Festlegung des Geltungsbereichs und das Verständnis der Bedürfnisse sind in bedeutsamen Zusammenhang mit dem Service Einführungsprozess und Level Management.
Führung	2	Führung, Engagement, Leitlinie, Organisatorische Aufgaben, Zuständigkeiten und Befugnisse korrelieren teilweise mit den Punkten zum Service Einführungsprozess.
Planung	2	Planung der Informationssicherheitsziele sowie der Umgang mit Risiken und den Chancen hat teilweise Berührungspunkte mit den Prozessen der Service Einführung, allen voran denen des Security Management.
Unterstützung	3	Unterstützung durch Ressourcen, Kompetenz, Bewusstsein, Kommunikation und dokumentierte Informationen der IS sind in vielen Punkten zum Bereich Service Einführung stark verbunden.
Betrieb	2	Einsatzplanung- und Kontrolle sowie Informationssicherheitsrisikoeinschätzung- und deren Behandlung, haben teilweise Überschneidungen mit dem Service Einführungsprozess.
Bewertung der Leistung	3	Überwachung, Messung, Analyse und Bewertung der Leistung ist im Kontext des Service Einführungsprozess entscheidend, vor allem in Bereichen des Service Reporting und Capacity Management.
Verbesserung	2	Verbesserung, respektive deren Fehler und Korrekturmaßnahmen, gehören zum Service Einführungsprozess, wenn auch nicht der Hauptfokus darin zu sehen ist. Dennoch gibt es Überschneidungen, vor allem beim Availabiliy und Continuity Management.
ISO 27002		
Informationssicherheitsrichtlinien	2	Vorgaben der Leitung zur Informationssicherheit betreffen in mehreren Punkten auch den Service Einführungsprozess.
Organisation der Informationssicherheit	2	Organisation der Informationssicherheit hat mehrfach Überschneidungen mit den Kapiteln im Service Einführungsprozess.
Personalsicherheit	2	Die Wahrung der Sicherheit des Personals hat ausschlaggebende Auswirkungen im Service Einführungsprozess.

	Verwaltung der Werte	2	Wertemanagement, respektive ein zulässiger Gebrauch dessen, Klassifizierung von Informationen und der Umgang mit Medien sind in Wechselbeziehung mit dem Service Einführungsprozess.
	Zugangssteuerung	2	Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle, Benutzerverwaltung- und Verantwortung haben eine wesentliche Interaktion mit Bereichen im Service Einführungsprozess.
	Kryptographie	3	Kryptographische Maßnahmen haben starken Einfluss im Service Einführungsprozess.
	Physische und umgebungsbezogene Sicherheit	3	Schutz vor physischem Zugang und Umwelteinflüssen hat starke Relationen zu den Bereichen des Service Einführungsprozess.
	Betriebssicherheit	1	Betriebsverfahren, Zuständigkeiten, Datensicherungen, Protokollierung und Überwachung, hat teilweise Überschneidungen mit Prozessen der Service Einführung.
	Kommunikationssicherheit	2	Der Schutz von Informationen in Netzwerken ist in Wechselwirkung mit einzelnen Prozessen des Service Einführungsprozesses.
	Anschaffung, Entwicklung und Instandhaltung von Systemen	3	Anschaffung, Entwicklung und Instandhaltung von Systemen des IS hat mehrfach Überschneidungen mit Prozessen der Service Einführung im SMS.
	Lieferantenbeziehungen	3	Sicherheit in Lieferantenbeziehungen und das Management der Dienstleistungserbringung ist in sehr starker Wechselwirkung mit dem Prozess des Service Einführung im SMS.
	Handhabung von Informationssicherheitsvorfällen	2	Das Management von Informationssicherheitsvorfällen korreliert mit Prozessen des Service Einführung, allen voran mit dem Abschnitt Continuity und Availability Management.
	Informationssicherheitsaspekte beim Business Continuity Management	2	Die Kontinuität der Informationssicherheit ist in Zusammenspiel mit Bereichen des Service Einführungsprozess wie beispielsweise vor allem Continuity Management.
	Compliance	2	Richtlinienkonformität steht in vielen Zusammenhängen zum Service Einführungsprozess, beispielsweise mit dem Service Level Management.

Tabelle 12 Mapping ISO20k Kapitel 6 vs. ISO27k1, ISO27k2

			ISO 20000-1
			Prozesse zur Beziehungspflege
ISO 27001	Kontext der Organisation	2	Der Kontext der Organisation, beziehungsweise vor allem das Verständnis der Bedürfnisse und Erwartungen interessierter Parteien, überschneidet sich mit Bereichen wie dem Beziehungspflege Management des SMS.
	Führung	1	Die Führung und ihr Engagement in Bezug auf das Informationssicherheitsmanagementsystem hat kaum Einfluss auf Bereiche im Beziehungspflege Prozess.
	Planung	1	Die Planung zum Umgang mit Risiken und Chancen, korreliert begrenzt mit den Prozessen im Beziehungspflege Management.
	Unterstützung	2	Unterstützung durch Ressourcen, Kompetenz, Bewusstsein, Kommunikation und dokumentierte Informationen der IS, betrifft Bereiche im Beziehungspflege Prozess.
	Betrieb	0	Betrieb im Sinne der Planung, Kontrolle, Informationssicherheitsrisikoeinschätzung- und behandlung hat keine offensichtlichen Überschneidungen mit den Kernbereichen im Beziehungspflege Prozess.
	Bewertung der Leistung	2	Überwachung, Messung, Analyse und Auswertung der IS kann mit tiefgreifenden Überschneidungen mit den Prozessen zur Beziehungspflege einhergehen.
	Verbesserung	2	Fehler und Korrekturmaßnahmen haben bedeutende Wechselwirkungen auf Bereiche im Beziehungspflege Prozess.
ISO	Informationssicherheitsrichtlinien	2	Vorgaben der Leitung zur Informationssicherheit betreffen auch Bereiche wie Business Relationship und Supplier Management.

Organisation der Informationssicherheit	0	Interne Organisation oder Informationssicherheit bei Telearbeit hat kaum Berührungspunkte mit den Kernaufgaben des Beziehungspflege Managements.
Personalsicherheit	1	Sicherheit des Personals vor, während und nach der Anstellung kann geringe Überschneidungen zu Beziehungspflege Prozessen zeigen.
Verwaltung der Werte	0	Schutz der Werte der Organisation hat wenig nennenswerte Verbindungen zu den Beziehungspflege Prozessen.
Zugangssteuerung	1	Beschränkung des Zugriffs auf Informationen, kann geringe Überschneidungen mit dem Beziehungspflege Prozess haben.
Kryptographie	1	Verwendung von Kryptographie, kann geringe Überschneidungen im Beziehungspflege Prozess mit sich bringen.
Physische und umgebungsbezogene Sicherheit	0	Verhinderung des unautorisierten physischen Zugriffs auf Informationen hat keine bedeutenden Verbindungen zu Bereichen der Beziehungspflege Prozesse.
Betriebssicherheit	1	Betriebssicherheit zur Verarbeitung von Informationen, hat sehr geringe Verbindung zu Business Relationship und Supplier Management.
Kommunikationssicherheit	2	Sicherheit in der Kommunikation betrifft ebenso diverse Kapitel im Beziehungspflege Prozess.
Anschaffung, Entwicklung und Instandhaltung von Systemen	1	Anschaffung, Entwicklung und Instandhaltung von Systemen, zeigt geringe Auswirkungen auf die Bereiche im Beziehungspflege Prozess.
Lieferantenbeziehungen	3	Sämtliche Subkapitel in diesem Bereich sind in starker Verbindung zu den Prozessen der Beziehungspflege.
Handhabung von Informationssicherheitsvorfällen	1	Die Sicherstellung einer wirksamen Strategie bei Informationssicherheitsvorfällen hat Auswirkung auf Bereiche des Beziehungspflege Managements, wenn dies auch nicht der primäre Fokus ist.
Informationssicherheitsaspekte beim Business Continuity Management	2	Kontinuität der Informationssicherheit hat maßgebliche Auswirkungen auf die Bereiche im Beziehungspflege Prozess.
Compliance	2	Richtlinienkonformität kann mitunter Prozesse der Beziehungspflege grundlegend beeinflussen.

Tabelle 13 Mapping ISO20k Kapitel 7 vs. ISO27k1, ISO27k2

		ISO 20000-1
		Lösungsprozesse
ISO 27001 / Kontext der Organisation	1	Das Verständnis der Bedürfnisse, beziehungsweise die Festlegung des Geltungsbereichs zur IS haben teilweise einen Einfluss auf die Lösungsprozesse.
ISO 27001 / Führung	0	Das Kapitel Führung hat kaum nennenswerte Berührungspunkte, lediglich Überschneidungen, welche im Hinblick auf die Kernaufgaben der Lösungsprozesse ignoriert werden können.
ISO 27001 / Planung	3	Sämtliche Maßnahmen zum Umgang mit Risiken und Chancen korrelieren stark mit denen der Lösungsprozesse.
ISO 27001 / Unterstützung	3	Unterstützung mittels Kompetenzen, Bewusstsein, Kommunikation oder dokumentierte Informationen, können mitunter erhebliche Anwendung im Lösungsprozess finden.
ISO 27001 / Betrieb	3	Sämtliche Einsatzplanung- und Kontrolle, wie auch Informationssicherheitsrisikoeinschätzung und dessen Behandlung, haben Dependenzen mit dem Lösungsprozess.
ISO 27001 / Bewertung der Leistung	3	Die Überwachung, Messung, Analyse und Auswertung kann starken Einfluss auf die Bereiche in der Lösungsprozesse-Phase haben.
ISO 27001 / Verbesserung	3	Fehler, Korrekturmaßnahmen sowie laufende Verbesserung sind ebenso fundamentaler Bestandteil im Lösungsprozess.
ISO / Informationssicherheitsrichtlinien	2	Sicherheitsleitlinien zur IS können mitunter wesentliche Beziehungen zum Lösungsprozess haben.
ISO / Organisation der Informationssicherheit	1	Die interne Organisation der IS hat teilweise eine Beziehung mit den Lösungsprozessen.

Personalsicherheit	0	Die Sicherheit des Personals spielt eine weniger beachtenswerte Rolle, in Betracht auf die Aufgaben des Lösungsprozesses.
Verwaltung der Werte	1	Die Prozesse im Wertemanagement im Sinne dessen angemessenen Schutzes, haben teilweise Überschneidungen mit Teilbereichen im Lösungsprozess.
Zugangssteuerung	1	Zugriffskontrolle wie Benutzerverwaltung hat wenig primäre Wechselwirkungen zum Lösungsprozess, diese sind dennoch nicht auszuschließen.
Kryptographie	1	Die Sicherstellung der ordnungsgemäßen Verwendung von Kryptographie hat beschränkte Beziehungen zu den wesentlichen Aufgaben im Lösungsprozess.
Physische und umgebungsbezogene Sicherheit	1	Verhinderung des unerlaubten physischen Zugriffs auf Informationen hat wenig Auswirkung auf die Kernaufgaben im Lösungsprozess.
Betriebssicherheit	2	Die Betriebssicherheit, mitsamt der Unterpunkte, hat wesentliche Rückwirkung auf den Lösungsprozess.
Kommunikationssicherheit	2	Die Sicherheit in der Kommunikation ist ein wesentlicher Bestandteil zu den Prozessen in der Lösungsphase.
Anschaffung, Entwicklung und Instandhaltung von Systemen	2	Die Sicherstellung der Sicherheit über den gesamten Lebenszyklus der IS hat mehrfache Zusammenhänge mit denen im Lösungsprozess.
Lieferantenbeziehungen	0	Die Sicherheit in Lieferantenbeziehungen hat keine nennenswerten Überschneidungen mit den primären Anliegen im Lösungsprozess.
Handhabung von Informationssicherheitsvorfällen	3	Das Management von Informationssicherheitsvorfällen hat starke Korrelation mit den Anliegen im Lösungsprozess.
Informationssicherheitsaspekte beim Business Continuity Management	3	Die Kontinuität der Informationssicherheit hat starke Bedeutung in den Abschnitten zum Lösungsprozess.
Compliance	2	Die Richtlinienkonformität hat grundlegenden Überschneidungen, welche im Lösungsprozess beachtet werden müssen.

Tabelle 14 Mapping ISO20k Kapitel 8 vs. ISO27k1, ISO27k2

		ISO 20000-1	
			Überwachungsprozesse
ISO 27001	Kontext der Organisation	1	Das Verständnis der Organisation, sowie deren Kontext, kann mitunter Einfluss auf Subkapitel im Überwachungsprozess nehmen.
	Führung	0	Führung und Engagement hat keine bemerkenswerten direkten Auswirkungen auf die Kernaufgaben der Überwachungsprozesse.
	Planung	2	Das Planen der IS hat in Abschnitten wie Informationssicherheitsrisikoeinschätzung- und behandlung teilweise Dependenzen zu den Überwachungsprozessen.
	Unterstützung	2	Die Unterstützung der IS durch Ressourcen, Kompetenzen, Bewusstsein, Kommunikation und dokumentierte Information, haben signifikante Einflüsse auf die Prozesse im Überwachungsabschnitt.
	Betrieb	1	Einsatzplanung und -kontrolle sowie Informationssicherheitsrisikoeinschätzung- und behandlung sind teilweise in Beziehung mit den Überwachungsprozessen.
	Bewertung der Leistung	1	Überwachung, Messung, Analyse, Auswertung und Audits haben Überschneidungen mit den Abschnitten im Überwachungsprozess.
	Verbesserung	2	Fehler, Korrekturmaßnahmen und laufende Verbesserung stehen in engem Kontakt zu den Überwachungsprozessen.
ISO 27002	Informationssicherheitsrichtlinien	2	Sicherheitsleitlinien haben fundamentale Wechselwirkungen zu den Überwachungsprozessen.
	Organisation der Informationssicherheit	1	Die Organisation der Informationssicherheit hat kaum erkennbare Wechselwirkungen bezüglich der primären Aufgaben im Überwachungsprozess.
	Personalsicherheit	0	Die Sicherheit des Personals hat keine essentiellen Überschneidungen mit den Kerngebieten im Überwachungsprozess.

Verwaltung der Werte	3	Das Wertemanagement hat folgenreiche Überschneidungen mit den Punkten im Überwachungsprozess.
Zugangssteuerung	2	Die Zugriffskontrolle übt starken Einfluss auf die Prozesse im Überwachungsabschnitt aus.
Kryptographie	1	Die Sicherstellung der wirksamen Verwendung von Kryptographie hat schwache direkte Konsequenzen auf die Überwachungsprozesse.
Physische und umgebungsbezogene Sicherheit	1	Der Schutz vor physischem Zugang und Umwelteinflüssen, kann mitunter Verbindungen zu den Überwachungsprozessen zeigen.
Betriebssicherheit	2	Die Sicherstellung des ordnungsgemäßen Betriebs, beispielsweise des "Änderungsmanagements", hat mitunter wesentliche Dependenzen zu den Prozessen im Bereich Überwachung.
Kommunikationssicherheit	1	Die Sicherheit in der Kommunikation hat Berührungspunkte mit den wesentlichen Aktivitäten der Überwachungsprozesse.
Anschaffung, Entwicklung und Instandhaltung von Systemen	2	Anschaffung, Entwicklung und Instandhaltung von Systemen hat bedeutende Gemeinsamkeiten, wie beispielsweise Änderungskontrollverfahren, mit den Überwachungsprozessen.
Lieferantenbeziehungen	0	Die Lieferantenbeziehungen haben kaum erwähnenswerte Überschneidungen mit den grundlegenden Überwachungsprozessen.
Handhabung von Informationssicherheitsvorfällen	3	Die Handhabung von Informationssicherheitsvorfällen ist gravierend mit dem Überwachungsprozess, allen voran Configuration, Change Release & Deployment Management verbunden.
Informationssicherheitsaspekte beim Business Continuity Management	3	Die Kontinuität der Informationssicherheit hat starke Korrelation mit den Abschnitten im Überwachungsprozess.
Compliance	1	Die Richtlinienkonformität hat nur teilweise Einwirkungen auf die Überwachungsprozesse, beziehungsweise dessen Subkapitel.

Tabelle 15 Mapping ISO20k Kapitel 9 vs. ISO27k1, ISO27k2

Aus den zuvor abgebildeten Tabellen, 10 einschließlich Tabelle 15, ergibt sich folgende erstmalige zusammenfassende Matrix aus den einzeln durchgeführten Einschätzungen und den deshalb enthaltenen Begründungen durch den Autor.

		ISO 27001							ISO 27002														
	Kapitel	4 Kontext der Organisation	5 Führung	6 Planung	7 Unterstützung	8 Einsatz	9 Leistungsauswertung	10 Verbesserung	5 Informationssicherheitsrichtlinien	6 Organisation der Informationssicherheit	7 Personalsicherheit	8 Verwaltung der Werte	9 Zugangssteuerung	10 Kryptographie	11 Physische und umgebungsbezogene Sicherheit	12 Betriebssicherheit	13 Kommunikationssicherheit	14 Anschaffung, Entwicklung und Instandhaltung von Systemen	15 Lieferantenbeziehungen	16 Handhabung von Informationssicherheitsvorfällen	17 Informationssicherheitsaspekte beim Business Continuity Management	18 Compliance	Anzahl	Mittl
ISO/IEC 20000-1	Service management system general requirements	3	3	3	3	1	2	3	2	2	1	2	2	1	1	2	2	2	3	2	3	2	1	2,14
	Design and transition of new or changed services	1	2	3	2	3	2	3	2	1	1	2	1	1	1	3	1	3	1	2	3	2	2	1,90
	Service delivery processes	3	2	2	3	2	3	2	2	2	2	2	2	3	3	1	2	3	3	2	2	2	3	2,29
	Relationship processes	2	1	1	2	0	2	2	2	0	1	0	1	1	0	1	2	1	3	1	2	2	4	1,29
	Resolution processes	1	0	3	3	3	3	3	2	1	0	1	1	1	1	2	2	2	0	3	3	2	5	1,76
	Control processes	1	0	2	2	1	1	2	2	1	0	3	2	1	1	2	1	2	0	3	3	1	6	1,48
	Anzahl	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	126	
	Mittelwert	1,83	1,33	2,33	2,50	1,67	2,17	2,50	2,00	1,17	0,83	1,67	1,50	1,33	1,17	1,83	1,67	2,17	1,67	2,17	2,67	1,83		1,81

Abbildung 23 Wechselwirkung Bewertung is161532

In der darüber liegenden Abbildung 23, ist das Ergebnis der Bewertung zu den Wechselwirkungen zusammengefasst. Horizontal sind die ausgewählten Kapitel der ISO 27k1 und ISO 27k2 repräsentiert. Vertikal sind jene der ISO 20k1 angeführt. Zur Orientierung ist die Nummer des Kapitels vom Standard dargestellt und

außerdem eine Anzahl der Kreuzungen abgebildet, welche im rechten unteren Rand, multipliziert das Kreuzprodukt von 126 Überschneidungen belegt. Außerdem enthält jede Zeile beziehungsweise Spalte einen Mittelwert am äußeren Rand berechnet.

Um diese Einflussmatrix wissenschaftlich zu stützen wurden daraufhin Experteninterviews mithilfe eines Fragebogens, siehe Anhang A, durchgeführt. Die Bewertungsergebnisse der Experten werden nun im folgenden Kapitel vorgestellt.

4.2.3.1. Experteninterviews

Um der erstmalig durchgeführten begründeten Bewertung der Einflussmatrix durch den Autor wissenschaftlich angemessener Bedeutung zuzuweisen, wurden Einschätzungen von Fachexperten eingeholt.

Im Zusammenhang mit den folgenden Expertenevaluierungen wird der Begriff „Experte“ wie folgt verstanden: ExpertInnen werden oftmals ebenso mit den Begriffen wie Berater oder Gutachter gleichgestellt und darüber hinaus dem Laien gegenübergestellt. [45, p. 8]
Unter dem Begriff „Expertin“ beziehungsweise „Experte“ sind somit Personen zu verstehen, welche aufgrund ihrer langjährigen beruflichen Tätigkeit und der damit einhergehenden Erfahrung ein vielfältiges spezifisches Domänenwissen mitbringen. Eine langjährige Erfahrung geht dabei ab einen Zeitraum von 10 Jahren Training und Erfahrung einher. [45, p. 9]

Die genannten Attribute sind bei den folgenden befragten Personen zutreffend, weshalb diese gezielt für die Befragung selektiert wurden. Die befragten Personen sind allesamt Fachkräfte, im Bereich Service und Security Management und können auf aussagekräftige Kenntnisse und Erfahrungen aus der Wirtschaft und Forschung zu den behandelten Themen zurückgreifen.
Zum Zwecke dieser Arbeit wurden dahingehend jeweils zwei wesentliche Gruppen von Experten befragt. Zum einen wurden zwei Fachkräfte, welche vorwiegend in der Wirtschaft tätig sind, interviewt. Anschließend wurden weitere zwei Experten um deren Einschätzung, vorwiegenden basierend auf Eindrücken aus der Forschung, gebeten. Dadurch soll eine optimale Verteilung aus den verschiedenen Blickwinkeln von Wirtschaft und Forschung hergestellt werden.

Die folgenden Evaluierungen wurden in einer separaten Excel-Datei getätigt, weshalb nun die zusammengefassten Auswertungen der Einschätzung durch die Fachkräfte vorgestellt werden:

Befragte Person: ***Markus Schiemer, BSc BSc MSc MSc MBA***
Unternehmen: Microsoft Österreich
Position: Senior Service Delivery Manager

ISO/IEC 20000-1		ISO 27001							ISO 27002														
		Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Kapitel		4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Service management system general requirements	4	3	3	3	3	3	2	3	1	1	2	1	1	0	1	2	0	2	2	1	1	3
Design and transition of new or changed services	5	2	1	2	2	2	1	2	3	2	1	2	2	1	1	3	1	2	1	1	2	2
Service delivery processes	6	3	3	3	3	3	2	3	3	3	2	3	2	1	2	3	1	2	2	3	3	2
Relationship processes	7	3	3	3	2	2	2	3	2	2	2	2	1	0	1	2	1	2	3	1	1	2
Resolution processes	8	3	2	3	3	3	1	3	2	1	1	3	1	0	0	2	1	1	2	3	2	2
Control processes	9	3	2	3	2	3	1	3	3	2	0	3	1	0	1	3	1	3	1	1	1	3

Abbildung 24 Einflussmatrix Markus Schiemer, BSc BSc MSc MSc MBA

Befragte Person: ***Mag. Manfred Spanner, MSc***
Unternehmen: ÖBB-Konzern
Position: Chief Information Security Officer

ISO/IEC 20000-1		ISO 27001							ISO 27002														
		Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Kapitel		4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Service management system general requirements	4	1	1	1	1	1	2	2	3	1	1	3	3	1	1	3	2	3	3	4	3	2
Design and transition of new or changed services	5	1	1	2	1	2	1	2	1	1	1	2	2	2	2	3	2	3	1	3	2	1
Service delivery processes	6	1	1	2	1	1	2	1	1	1	1	3	2	1	1	1	2	2	2	2	2	2
Relationship processes	7	2	2	1	1	1	1	1	2	2	2	1	1	1	2	1	2	2	3	2	2	1
Resolution processes	8	1	1	1	2	1	3	2	1	1	1	3	1	1	1	1	1	2	2	2	2	1
Control processes	9	1	2	2	2	1	2	2	1	1	1	3	2	1	1	2	1	2	2	3	2	1

Abbildung 25 Einflussmatrix Mag. Manfred Spanner, MSc

Befragte Person: ***FH-Prof. Mag. Dr. Simon Tjoa***
Unternehmen: Fachhochschule St. Pölten GmbH
Position: FH-Dozent, Internationaler Koordinator im Department Informatik und Security

			ISO 27001							ISO 27002														
			Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
	Kapitel		4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ISO/IEC 20000-1	Service management system general requirements	4	3	2	3	3	2	2	3	2	2	1	2	3	1	1	2	2	3	3	3	2	2
	Design and transition of new or changed services	5	3	3	3	2	3	2	2	2	2	1	1	2	1	1	2	2	2	3	2	2	3
	Service delivery processes	6	1	2	2	2	3	3	3	2	2	1	1	1	1	1	2	2	2	1	3	2	3
	Relationship processes	7	2	1	2	2	2	2	2	2	2	1	2	2	1	1	1	2	3	3	3	3	2
	Resolution processes	8	2	2	2	3	3	3	3	2	3	1	1	1	1	1	3	2	2	2	3	3	3
	Control processes	9	1	1	2	3	3	3	3	1	1	1	2	2	1	1	2	2	3	3	3	3	3

Abbildung 26 Einflussmatrix FH-Prof. Mag. Dr. Simon Tjoa

Befragte Person: ***Dipl.-Ing. Herfried Geyer***
Unternehmen: Fachhochschule St. Pölten GmbH
Position: FH-Dozent, stellvertretender Studiengangsleiter IT Security (BA) Department Informatik und Security

			ISO 27001							ISO 27002														
			Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
	Kapitel		4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ISO/IEC 20000-1	Service management system general requirements	4	3	2	3	2	2	2	1	2	1	1	2	2	1	1	2	2	2	3	2	2	2
	Design and transition of new or changed services	5	2	3	2	2	1	2	1	2	2	1	3	2	1	1	2	2	3	3	2	2	2
	Service delivery processes	6	2	3	1	1	1	2	1	2	1	1	2	2	1	1	2	2	2	2	2	1	2
	Relationship processes	7	3	3	2	2	1	2	1	2	1	1	1	1	1	0	1	1	1	3	2	1	2
	Resolution processes	8	1	2	1	1	1	2	2	1	1	1	1	1	0	0	2	1	1	2	2	1	1
	Control processes	9	2	1	2	2	2	2	1	1	2	1	2	1	1	0	2	2	2	2	2	1	2

Abbildung 27 Einflussmatrix Dipl.-Ing. Herfried Geyer

Diese einzelnen Bewertungen werden im nachstehenden Abschnitt mit dem Mittelwert ausgewertet zusammengefasst und das Ergebnis als Basis weiterer Berechnungen herangezogen.

4.2.3.2. Zusammenfassung der Einflussmatrix

Die Evaluierungen der Experten des vorhergegangen Kapitels werden nun wie folgt zusammengefasst. Daraus ergibt sich folgende, für diese Arbeit vollständige Einflussmatrix.:

		ISO 27001							ISO 27002															
		Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance		
	Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18		Mittelwert
ISO/IEC 20000-1	Servicemanagementsystem Allgemeine Forderungen 4	2,6	2,2	2,6	2,4	1,8	2,0	2,4	2,0	1,4	1,2	2,0	2,2	0,8	1,0	2,2	1,6	2,4	2,8	2,2	2,2	2,2		2,01
	Gestaltung und Umsetzung von neuen und geänderten Services 5	1,8	2,0	2,4	1,8	2,2	1,6	2,0	2,0	1,6	1,0	2,0	1,8	1,2	1,2	2,6	1,6	2,6	1,8	2,0	2,2	2,0		1,88
	Service Einführungsprozess 6	2,0	2,2	2,0	2,0	2,0	2,4	2,0	2,0	1,8	1,4	2,2	1,8	1,4	1,6	1,8	1,8	2,2	2,0	2,4	2,0	2,2		1,96
	Prozesse zur Beziehungspflege 7	2,4	2,0	1,8	1,8	1,2	1,8	1,8	2,0	1,4	1,4	1,2	1,2	0,8	0,8	1,2	1,6	1,8	3,0	1,8	1,8	1,8		1,65
	Lösungsprozesse 8	1,6	1,4	2,0	2,4	2,2	2,4	2,6	1,6	1,4	0,8	1,8	1,0	0,6	0,6	2,0	1,4	1,6	1,6	2,6	2,2	1,8		1,70
	Überwachungsprozesse 9	1,6	1,2	2,2	2,2	2,0	1,8	2,2	1,6	1,4	0,6	2,6	1,6	0,8	0,8	2,2	1,4	2,4	1,6	2,4	2,0	2,0		1,74
	Mittelwert	2,00	1,83	2,17	2,10	1,90	2,00	2,17	1,87	1,50	1,07	1,97	1,60	0,93	1,00	2,00	1,57	2,17	2,13	2,23	2,07	2,00		**1,82**

Abbildung 28 Vollständige Einflussmatrix

Die Werte der Kreuzungen zu der jeweiligen Zeile, beziehungsweise Spalte, sind der Mittelwert durch das ungewogene arithmetische Mittel und der einzelnen Evaluierungen aus dem Abschnitt 4.2.3.1. Die vollständige Einflussmatrix dieser Arbeit gibt somit den Mittelwert der erstmaligen Selbsteinschätzung, sowie der Bewertung der vier Fachpersonen wieder.
Das Zeilen- und Spaltenergebnis errechnet sich nach demselben Prinzip wie die Kreuzprodukte, wobei die Kreuzprodukte in diesem Fall die Basiswerte sind. Das Rechteckt am rechten unteren Rand zeigt den Mittelwert über die gesamte Matrix. Daher sind die jeweiligen Berechnungen wie folgt zu verstehen:

$$\overline{x} = \frac{x_1 + x_2 + \ldots + x_n}{n} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i$$

Gerundet wurde der jeweilige Mittelwert auf ein beziehungsweise zwei Dezimalstellen genau. Im rechten unteren Bereich der Abbildung ist der Mittelwert, von den Kreuzprodukten über die gesamte Tabelle, dargestellt.

Da die Basismatrix nun ausführlich aufgrund deren Funktion beschrieben wurde, folgt eine Interpretation.

Auf den ersten Blick ist durch die grafische Kennzeichnung horizontal betrachtet, im ersten und letzten Drittel eine maßgebliche Abhängigkeit zu beobachten. Im zweiten Drittel, das heißt horizontal in der Mitte betrachtet ist hingegen eine unterlegene Wechselwirkung zu verzeichnen. Diese Feststellung ist unterstützend anhand der Mittelwerte zu den Spalten festzuhalten. Diese übersteigen horizontal im ersten Drittel dreimal die Schwelle von >2, sowie viermal >2 im letzten Drittel.
Vertikal betrachtet übersteigt der Mittelwert, über die Zeilen betrachtet, nur einmal die Schwelle von >2.
Zusammengefasst ist daher die Wechselwirkung in der dargestellten Matrix in der Mitte als dürr zu betrachten und in den ersten sowie abschließenden dargestellten Kapiteln als beachtlich festzuhalten.

In Summe ergibt dies über die gesamte Einflussmatrix eine Abhängigkeit von 1,82. Diese Zahl errechnet sich aus der Summe der horizontalen und vertikalen Mittelwerte. Das Ergebnis ist im rechten unteren Quadrat dargestellt. Auf der zugrunde liegenden Bewertungsskala von null bis drei, ist der Wert 1,82 als durchaus relevant zu verstehen. Damit wird eine ausschlaggebende Abhängigkeit vom Service und Security Management zum Ausdruck gebracht.

Ein „Extremwert“, das heißt ein eindeutiges Feld in dem alle Personen der Evaluation mit der Bewertung Null oder Drei beurteilt haben, kann einmal verzeichnet werden. Bei dem Kapitel „Relationsship processes“ (ISO 20000, Kapitel 7) zu „Lieferantenbeziehungen“ (ISO 27002, Kapitel 15) waren sich alle Personen einig die „Höchstbewertung“ von Drei zu beurteilen. Der andere „Extremfall“, eine Bewertung einer Kreuzung von Null von allen befragten Fachkräften, wurde nicht erfasst.

Um diese Eindrücke nochmals optisch zu verdeutlichen dient die folgende Abbildung 29, in welcher die Ergebnisse der Beurteilung übersichtlich untereinander dargestellt sind.

Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ergebnis [is161532] 4	3	3	3	3	1	2	3	2	2	1	2	2	1	1	2	2	2	3	2	3	2
5	1	2	3	2	3	2	3	2	1	1	2	1	1	1	3	1	3	1	2	3	2
6	3	2	2	3	2	3	2	2	2	2	2	2	3	3	1	2	3	3	2	2	2
7	2	1	1	2	0	2	2	2	0	1	0	1	1	0	1	2	1	3	1	2	2
8	1	0	3	3	3	3	3	2	1	0	1	1	1	1	2	2	2	0	3	3	2
9	1	0	2	2	1	1	2	2	1	0	3	2	1	1	2	1	2	0	3	3	1

Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ergebnis [Markus Schiemer] 4	3	3	3	3	3	2	3	1	1	2	1	1	0	1	2	0	2	2	1	1	3
5	2	1	2	2	2	1	2	3	2	1	2	2	1	1	3	1	2	1	1	2	2
6	3	3	3	3	3	2	3	3	3	2	3	2	1	2	3	1	2	2	3	3	2
7	3	3	3	2	2	2	3	2	2	2	2	1	0	1	2	1	2	3	1	1	2
8	3	2	3	3	3	1	3	2	1	1	3	1	0	0	2	1	1	2	3	2	2
9	3	2	3	2	3	1	3	3	2	0	3	1	0	1	3	1	3	1	1	1	3

Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ergebnis [Manfred Spanner] 4	1	1	1	1	1	2	2	3	1	1	3	3	1	1	3	2	3	3	3	3	2
5	1	1	2	1	2	1	2	1	1	1	2	2	2	2	3	2	3	1	3	2	1
6	1	1	2	1	1	2	1	1	1	1	3	2	1	1	1	2	2	2	2	2	2
7	2	2	1	1	1	1	1	2	2	2	1	1	1	2	1	2	2	3	2	2	1
8	1	1	1	2	1	3	2	1	1	1	3	1	1	1	1	1	2	2	2	2	1
9	1	2	2	2	1	2	2	1	1	1	3	2	1	1	2	1	2	2	3	2	1

Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ergebnis [Herfried Geyer] 4	3	2	3	2	2	2	1	2	1	1	2	2	1	1	2	2	2	3	2	2	2
5	2	3	2	2	1	2	1	2	2	1	3	2	1	1	2	2	3	3	2	2	2
6	2	3	1	1	1	2	1	2	1	1	2	2	1	1	2	2	2	2	2	1	2
7	3	3	2	2	1	2	1	2	1	1	1	1	1	0	1	1	1	3	2	1	2
8	1	2	1	1	1	2	2	1	1	1	1	1	0	0	2	1	1	2	2	1	1
9	2	1	2	2	2	2	1	1	2	1	2	1	1	0	2	2	2	2	2	1	2

Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Ergebnis [Simon Tjoa] 4	3	2	3	3	2	2	3	2	2	1	2	3	1	1	2	2	3	3	3	2	2
5	3	3	3	2	3	2	2	2	2	1	1	2	1	1	2	2	2	3	2	2	3
6	1	2	2	2	3	3	3	2	2	1	1	1	1	1	2	2	2	1	3	2	3
7	2	1	2	2	2	2	2	2	2	1	2	2	1	1	1	2	3	3	3	3	2
8	2	2	2	3	3	3	3	2	3	1	1	1	1	1	3	2	2	2	3	3	3
9	1	1	2	3	3	3	3	1	1	1	2	2	1	1	2	2	3	3	3	3	3

Abbildung 29 Optische Übereinstimmung der Evaluierungen

Wie in der Abbildung 29 ersichtlich, herrscht über die Kapitel 10, „Kryptographie“ und 11, „Physische und umgebungsbezogene Sicherheit“ von der ISO 27002 über alle Personen hinweg vertikal betrachtet bemerkenswerte Einigkeit.

Hingegen zeigt diese Grafik auch auffallende Wahrnehmungen im ersten Drittel der Matrix bei den Kapitel 4 bis 10 der ISO 27001.
Demzufolge muss allerdings auch darauf hingewiesen werden, dass die Bewertung der Wechselwirkungen aufgrund einer subjektiven Evaluierung erfolgt. Daher unterliegt diese kontinuierlich einem schmalen Grad, sofern es um die Entscheidung zwischen zwei Zahlen geht. Daher beruht die Bewertung beispielsweise von Zwei oder Drei oftmals nur auf einer äußerst minimal unterschiedlichen Wahrnehmung.

Die Ermittlung der Varianz drückt die Unterschiede in den Bewertungen der fünf Matrizen aus. Der Wert Null zeigt eine Einigkeit über alle fünf Tabellen und ist grün hinterlegt. Je höher der Wert, desto unterschiedlicher sind die Bewertungen in den Evaluierungen ausgefallen. Eine hohe Zahl, das heißt große Unterschiede ist rot gekennzeichnet.

		ISO 27001							ISO 27002														
		Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
	Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ISO/IEC 20000-1	Servicemanagementsystem Allgemeine Forderungen 4	0,8	0,7	0,8	0,8	0,7	0	0,8	0,5	0,3	0,2	0,5	0,7	0,2	0	0,2	0,8	0,3	0,2	0,7	0,7	0,2
	Gestaltung und Umsetzung von neuen und geänderten Services 5	0,7	1	0,3	0,2	0,7	0,3	0,5	0,5	0,3	0	0,5	0,2	0,2	0,2	0,3	0,3	0,3	1,2	0,5	0,2	0,5
	Service Einführungsprozess 6	1	0,7	0,5	1	1	0,3	1	0,5	0,7	0,3	0,7	0,2	0,8	0,8	0,7	0,2	0,2	0,5	0,3	0,5	0,2
	Prozesse zur Beziehungspflege 7	0,3	1	0,7	0,2	0,7	0,2	0,7	0	0,8	0,3	0,7	0,2	0,2	0,7	0,2	0,3	0,7	0	0,7	0,7	0,2
	Lösungsprozesse 8	0,8	0,8	1	0,8	1,2	0,8	0,3	0,3	0,8	0,2	1,2	0	0,3	0,3	0,5	0,3	0,3	0,8	0,3	0,7	0,7
	Überwachungsprozesse 9	0,8	0,7	0,2	0,2	1	0,7	0,7	0,8	0,3	0,3	0,3	0,3	0,2	0,2	0,2	0,3	0,3	1,3	0,8	1	1

Abbildung 30 Varianzanalyse der Evaluierung

Wie in Abbildung 30 zu sehen sind im ersten Drittel der Matrix deutliche Uneinigkeiten bei der Bewertung entstanden. Das bedeutet, dass es vor allem bei der ISO 27001 gegensätzliche Wahrnehmungen der Wechselwirkungen zur ISO 20000-1 gibt.
Wie die Abbildung 29 optisch bereits erkennen lässt, bestätigt die Varianzanalyse größere Einigkeit bei der Festlegung der Wechselwirkungen der ISO 27002 Kapitel Sieben bis Vierzehn.
Besondere Unterschiede sind bei der Wechselwirkung „Gestaltung und Umsetzung von neuen und geänderten Services „ zu „Lieferantenbeziehungen“ zu erkennen. Ebenso herrscht deutliche Uneinigkeit zwischen „Lösungsprozesse“ und „Einsatz“ sowie „Lösungsprozesse“ und „Verwaltung der Werte“.
Die größten Unterschiede in der Evaluierung sind bei „Überwachungsprozesse“ zu „Lieferantenbeziehungen“ zu beobachten.

Über die fünf Matrizen hinaus, ergeben sich allerdings auch bedeutende Übereinstimmungen. Nachstehende Abbildung 31 zeigt die eindeutigen Gemeinsamkeiten der Evaluierungen einzeln hervorgehoben. Dabei wird die Zahl Null, rot hinterlegt als Ungleichheit, über die fünf Matrizen hinweg verwendet. Die Zahl 1, grün hinterlegt, symbolisiert wiederrum eine eindeutige Übereinstimmung aller Evaluierungen.

		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
	Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ISO/IEC 20000-1	Servicemanagementsystem Allgemeine Forderungen 4	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
	Gestaltung und Umsetzung von neuen und geänderten Services 5	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
	Service Einführungsprozess 6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Prozesse zur Beziehungspflege 7	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0
	Lösungsprozesse 8	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
	Überwachungsprozesse 9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Abbildung 31 Eindeutige Übereinstimmungen der Experten

Wie in der Grafik zu sehen ist, konnten sechs eindeutige Übereinstimmungen in den Bewertungen erzielt werden. Bereits bei fünf Evaluierungen zeigt die Abbildung die Schwierigkeit exakte Übereinstimmungen zu erzielen. Mit steigender Anzahl an Matrizen, das heißt weiteren Evaluierungstabellen oder verfeinerter Bewertungsskala, würde demnach die Wahrscheinlichkeit sinken, eine gleiche Zahl im gleichen Feld zu erhalten.

Nun muss allerdings an dieser Stelle erwähnt werden, dass es sich bei der Befragung keinesfalls um zufällige Bewertungen handelt. Vielmehr liegen wissenschaftliche Bewertungen aufgrund von standardisierten Kapitel und Kontrollen vor, welche kein Glückspiel oder Ähnliches abbilden. Dennoch soll die geringe Wahrscheinlichkeit zum Ausdruck gebracht werden, da es oftmals durchaus schwierig ist, gleiches Verständnis der Personen der Evaluierung in Bezug auf die Einschätzung mithilfe der Bewertungsskala zu erreichen.
Da der Fokus dieser Arbeit aber nicht auf die Wahrscheinlichkeit dieser Auswertung gerichtet ist, werden nun die eindeutigen Überschneidungen, deren Aussagen und Relevanz im Detail näher betrachtet. Die nachstehende Grafik zeigt dazu die eindeutigen Übereinstimmungen der fünf Evaluierungen mitsamt ihrem Wert. Die in der Matrix enthaltene Abkürzung „kÜ“ bedeutet „keine Übereinstimmung“.

		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
	Kapitel	4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ISO/IEC 20000-1	Servicemanagementsystem Allgemeine Forderungen 4	kÜ	kÜ	kÜ	kÜ	kÜ	2	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	1	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ
	Gestaltung und Umsetzung von neuen und geänderten Services 5	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	1	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ
	Service Einführungsprozess 6	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ
	Prozesse zur Beziehungspflege 7	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	2	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	3	kÜ	kÜ	kÜ
	Lösungsprozesse 8	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	1	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ
	Überwachungsprozesse 9	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ	kÜ

Abbildung 32 Detailwerte der eindeutigen Übereinstimmungen

Wie bereits erwähnt, ist eine Überschneidung besonders hervorzuheben, da „Prozesse zur Beziehungspflege“ (ISO 20000, Kapitel 7) und zu „Lieferantenbeziehungen“ (ISO 27002, Kapitel 15) als einzige Bewertung von allen Fachpersonen die höchste Dependenz von Drei erhalten hat.
Kurz zusammengefasst ist, der Bewertung zufolge, dieser Quadrant als die am meisten entscheidende Wechselwirkung zu interpretieren.
Weitere zwei eindeutige Überschneidungen halten die Evaluierung mit dem Wert Zwei. Zum einen „Servicemanagementsystem Allgemeine Forderungen“ (ISO 20000, Kapitel 1) zu „Bewertung der Leistung“ (ISO 27001, Kapitel 9) und zum anderen „Prozesse zur Beziehungspflege“ (ISO 20000, Kapitel 7) zu „Informationssicherheitsrichtlinien“ (ISO 27002, Kapitel 5).
Zuletzt sind weitere drei eindeutige Überschneidungen in den Matrizen mit der Bewertung Eins „leichte Abhängigkeit“ zu finden. „Servicemanagementsystem Allgemeine Forderungen“ (ISO 20000, Kapitel 1) zu „Physische und umgebungsbezogene Sicherheit“ (ISO 27002, Kapitel 11), „Gestaltung und Umsetzung von neuen und geänderten Services“ (ISO 20000, Kapitel 5) zu „Personalsicherheit“ (ISO 27002, Kapitel 7) und „Lösungsprozesse“ (ISO 20000, Kapitel 8) zu „Zugangssteuerung“ (ISO 27002, Kapitel 9).
Eine eindeutige Übereinstimmung mit der Stufe Null „keine relevante Abhängigkeit“, bleibt über die Matrizen hinweg vorenthalten.

Basierend auf dieser zugrunde liegenden Einflussmatrix der Wechselwirkungen aus Abbildung 28, werden anschließend sämtliche weitere Auswertungen im Tool abgeleitet werden.
Bei einer beabsichtigten kompletten Revision der Basismatrix, stellt das Tool eine Bewertungsvorlage „Auswertung_Vorlage“ in einem eigenen Registerblatt zu Verfügung. Darin kann eine komplette eigene Bewertung der Wechselwirkungen vorgenommen werden, welche anschließend in die Konfiguration automatisch übernommen wird.

Nachstehend wird die Möglichkeit der Auswertung vom Reifegrad im Tool vorgestellt.

4.2.3.3. Auswirkungen durch den Reifegrad

An dieser Stelle werden die, in Abschnitt 3.3 vorgestellten, Reifegradmodelle aufgegriffen. In den Registerblättern zu dem jeweiligen Kapitel, kann im Zuge eines Audits der Reifegrad zum gegenwärtigen Zustand festgelegt werden. Die Reife des Prozesses beeinflusst in späterer Folge das Ergebnis zur Wechselwirkung. Daher wird im Folgenden derer Wirksamkeit beschrieben.

Da das in Abschnitt 3.3.1 beschrieben Modell, CMMI zu den bekanntesten Reifegradmodellen gehört, findet es hier praktische Anwendung. Die Auswahl zugunsten CMMI wurde dahingehend gewählt, da dieses Modell am meisten Anwendung vorfindet. Außerdem soll das Tool an bewährten Modellen und Verfahren angelehnt werden, um optimale Adaption und Weiterentwicklung zu ermöglichen.

Im jeweiligen Registerblatt besteht die Möglichkeit, den Reifegrad zum gegenwärtigen Status zu bestimmen. Die Unterteilung findet in den fünf von CMMI definierten Maturity Levels, „1 – Initial, 2 – Managed, 3 – Defined, 4 – Quantitatively managed, 5 – Optimizing“ statt.

Angesichts der Verständlichkeit, ist der Wert der Nummerierung, eins bis fünf, auch mit demselben Wert als Schwerpunkt hinterlegt. Im Registerblatt „Konfiguration“ können die einzelnen Prioritäten zum Reifegrad allerdings bei Bedarf individuell angepasst werden.

Basierend auf den evaluierten Bewertungen der Reifegrade pro Kapitel, findet im Tool eine entsprechende Auswertung statt.

Der Schnittpunkt berechnet sich jeweils aus der Summe, dividiert durch die Konstante Zwei. Ist lediglich ein Reifegrad der Schnittpunkte bewertet, wird jener übernommen und die Division durch die Konstante Zwei entfällt. Der Reifegrad basiert demnach auf der folgenden beispielhaft dargestellten Berechnung:

$$Reifegrad\ Schnittpunkt = \frac{x + y}{2}$$

Eine exemplarische Bewertung der Kapitel liefert demzufolge eine in Abbildung 33 beispielhafte Auswertung zu den Reifegraden. Die Werte entsprechen den definierten Maturity Levels zwischen eins und fünf, beziehungsweise null sofern keine Bewertung stattgefunden hat.

			ISO 27001							ISO 27002													
			Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
	Kapitel		4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ISO/IEC 20000-1	Service management system general requirements	4	5,0	5,0	5,0	5,0	3,5	5,0	4,0	5,0	5,0	5,0	5,0	4,0	5,0	5,0	5,0	5,0	4,5	5,0	4,0	5,0	3,0
	Design and transition of new or changed services	5	0,0	0,0	0,0	0,0	2,0	0,0	3,0	0,0	0,0	0,0	0,0	3,0	5,0	5,0	0,0	0,0	4,0	0,0	3,0	0,0	1,0
	Service delivery processes	6	5,0	5,0	5,0	5,0	3,5	5,0	4,0	5,0	5,0	5,0	5,0	4,0	5,0	5,0	5,0	5,0	4,5	5,0	4,0	5,0	3,0
	Relationship processes	7	3,0	3,0	3,0	3,0	2,5	3,0	3,0	3,0	3,0	3,0	3,0	3,0	4,0	4,0	3,0	3,0	3,5	3,0	3,0	3,0	2,0
	Resolution processes	8	2,0	2,0	2,0	2,0	2,0	2,0	2,5	2,0	2,0	2,0	2,0	2,5	3,5	3,5	2,0	2,0	3,0	2,0	2,5	2,0	1,5
	Control processes	9	0,0	0,0	0,0	0,0	2,0	0,0	3,0	0,0	0,0	0,0	0,0	3,0	5,0	5,0	0,0	0,0	4,0	0,0	3,0	0,0	1,0

Abbildung 33 Matrix zum Reifegrad der Kapitel

Aufbauend auf dieser erstellten Matrix, erfolgt mit den eruierten Reifegraden mithilfe der Basismatrix eine erneute Multiplikation. Dadurch entsteht eine neue Matrix, welche die Kennzahlen zu den Auswirkungen aufgrund des Reifegrades verdeutlicht. Die folgende Abbildung 34 zeigt eine exemplarische Auswertung davon.

			ISO 27001							ISO 27002													
			Kontext der Organisation	Führung	Planung	Unterstützung	Einsatz	Leistungsauswertung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
	Kapitel		4	5	6	7	8	9	10	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ISO/IEC 20000-1	Service management system general requirements	4	97,9	96	126	58,5	4,55	26	46,8	26	26	6,5	26	20,8	6,5	6,5	26	26	23,4	58,5	20,8	58,5	30,6
	Design and transition of new or changed services	5	0	0	0	0	13,5	0	20,3	0	0	0	0	2,25	3,75	3,75	0	0	27	0	9	0	8
	Service delivery processes	6	69,4	30	43,3	30	9,33	30	10,7	13,3	13,3	13,3	13,3	10,7	30	30	3,33	13,3	27	30	10,7	13,3	23
	Relationship processes	7	10,5	2,5	4,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10
	Resolution processes	8	1,75	0	27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7,5
	Control processes	9	0	0	0	0	1,33	0	8	0	0	0	0	8	3,33	3,33	0	0	10,7	0	18	0	1,92

Abbildung 34 Auswirkung des Reifegrades

Das Ergebnis ist das Produkt der Faktoren zu den Schnittpunkten. Das Produkt ist daher als eine Kennzahl im Verhältnis zu den anderen Werten zu verstehen.

Es besteht die Möglichkeit, die Schwere der Einwirkung des Reifegrades auf das Gesamtergebnis zu bestimmen. Standardmäßig wurde eine Einwirkung von 50% definiert.

$$Schnittpunkt\ Matrix\ a * Schnittpunkt\ Matrix\ b * 0{,}5$$

Im Abschnitt „04_Konfiguration“ kann der Wert der prozentualen Einwirkung, individuell angepasst werden.

Die Evaluation der Daten sowie auch die Effekte und Berechnung der Reifegrade wurden in diesem Kapitel vorgestellt. Auf dieser zugrunde liegenden Basismatrix erfolgt eine Auswertung zu den im Zuge eines Audits ermittelten Daten. Für die Beachtung von situationsbedingten Konfigurationen, beschreibt daher der nachstehende Abschnitt die im Tool vorliegenden Möglichkeiten.

4.2.4. Konfiguration im Tool

Über die festgelegte Konfiguration hinaus, obliegt es der Anwenderin oder dem Anwender diese individuell, situationsbedingt anzupassen. Die betreffende Person kann im Tool an diversen Stellschrauben drehen, um den situativen Faktoren Sorge zu tragen.

Zu allererst besteht die Möglichkeit, die Basismatrix und deren Evaluierung im Zuge dieser Arbeit anzupassen. Diese Basismatrix und dessen Daten über die Wechselwirkungen sind ausschlaggebend für weiterführende Aussagen.
Situationsbedingt können allerdings Abweichungen dazu festgelegt werden. Dazu kann die nutzende Person in der rechten Matrix einzelne Werte korrigieren. Diese werden in der linken Matrix überschrieben und daraufhin in den weiterführenden Berechnungen verwendet. Die Gewichtung der einzelnen Kennzahlen kann somit individuell an die jeweiligen Verhältnisse angepasst werden. Die folgende Grafik zeigt dies anhand einer einzelnen Korrektur.

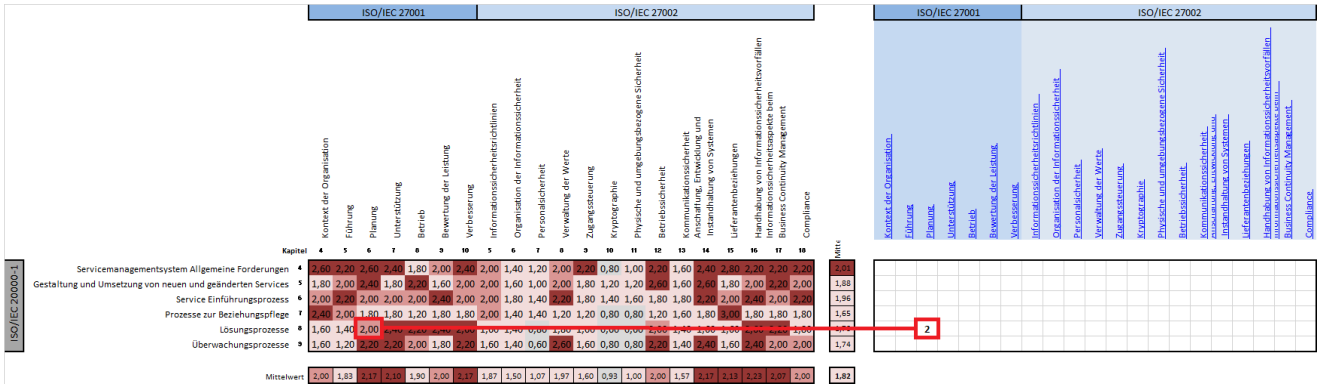

Abbildung 35 Konfiguration der Basismatrix

Erarbeitete Erfahrungswerte können dadurch in weiterer Folge in die Kalkulation und Auswertung der weiteren Ergebnisse miteinbezogen werden, um eine möglichst solide Bestimmung der Wechselwirkungen zu gewährleisten.
Möchte die Anwenderin oder der Anwender eine komplette Überarbeitung der Basismatrix als Ausgangspunkt der Berechnungen vornehmen, gelangt diese über den Button „neue Bewertung vornehmen [klick mich]“ zum vorgefertigten Registerblatt „Auswertung_Vorlage“. Das Resultat dieser komplett neuen Bewertung wird in der rechten und darüber hinaus in der linken Matrix übernommen. Dadurch kann eine erneute einzelne Abweichung an dieser Stelle korrigiert werden.

Im Anschluss an die Basismatrix muss angegeben werden, welche Kapitel im Tool bewertet wurden. Dazu gibt es zu den Standards ISO/IEC 20000-1, ISO/IEC 27001, ISO/IEC 27002 jeweils eine Checkbox, welche mit „Ja“

oder „Nein“ zu kennzeichnen ist. Eine korrekte Angabe dieser Checkboxen ist entscheidend, für die korrekte Berechnung der darauf folgenden Auswertungen.

Zusätzlich kann in der Konfiguration die Gewichtung des Reifegrades angepasst werden. Diese ist mit 50% vorgegeben, kann aber im entsprechend Feld abgestimmt werden.

Sind adäquate Konfigurationen getroffen, beziehungsweise entsprechen die Basiswerte bereits der Zufriedenheit der nutzenden Person, erfolgt der Schritt zum letzten Teil des Tools. In diesem wird eine übersichtliche Zusammenfassung in Form eines Berichtes bereitgestellt. Dieser Bereich wird daher im folgenden Abschnitt beschrieben.

4.2.5. Auswertungen im Tool

Auf Basis der erfolgten Bewertung im Zuge eines Audits, werden automatische Kalkulationen im Tool ausgeführt. Durch diese können in Folge weiterführende Auswertungen getroffen werden.
Dazu sind hier im fünften Hauptbereich „05_Auswertung“ des Tools, sämtliche Kalkulationen zum Audit aufgeschlüsselt. Diese sind in Form von Kreuztabellen dargestellt, womit eine Detailanalyse der zwischenzeitlichen Ergebnisse ermöglicht wird.

- Die Tabelle „[3] Wechselwirkung durch Beeinflussungsmatrix [x + y * Basismatrix / 2 / 3]“ stellt nach erfolgter Bewertung der jeweiligen Kapitel und Kontrollen die Wechselwirkungen auf Basis der festgelegten Einflussmatrix dar.
- Die nächste Auswertung „[4] Abweichung Einzeln [Einzelabweichung Bewertung - Basismatrix]“ ist eine Übersicht in welcher Abweichungen zur Basismatrix repräsentiert werden.
- Anschließend zeigt die folgende Matrix „[5] Reifegradbewertung [IF, ELSE Reifegrad x + y / 2]“ die Bewertung des Reifegrades zum jeweiligen Kapitel beziehungsweise zur Kontrolle.
- In Folge dessen, stellt die nächste Tabelle „[6] Reifegrad Auswirkung auf Basismatrix [Reifegrad x Basismatrix]“ die Bewertung des Reifegrades in Bezug auf die Einflussmatrix dar.
- Die abschließende Tabelle „[7] Neuberechnung durch Reifegrad Faktor [x * y = Auswertung * Reifegradfaktor]“ ist eine Zusammenfassung der Bewertung des Reifegrades mit Einberechnung des festgelegten Schwerpunkts.

Der Auswertung folgt ein Bericht, welcher im nachstehenden Kapitel beschrieben wird.

4.2.6. Zusammenfassender Bericht des Tools

Basierend auf den Auswertungen, dargestellt im Reiter „05_Auswertung“, werden die Daten daraufhin zusammenfassend, unter anderem grafisch, im Abschnitt „06_Bericht“ aufbereitet.
Der Bereich „Bericht“ umfasst damit sämtliche Ergebnisse welche von entscheidender Relevanz sind und dient zum einen als Dokumentation, aber auch zur Berichterfassung für das Management. Der Report kann dem Format DIN A4 angepasst werden und ist damit als ideale Zusammenfassung zu sehen. Der Druckbereich wurde dahingehend standardmäßig soweit abgestimmt, um den Bericht auf vier Seiten im Format DIN A4 zusammenzufassen.

Grundsätzlich ist der Bericht so strukturiert, dass jeweils eine grafische Auswertung am linken oder rechten Bildrand veranschaulicht ist und daneben die Tabelle mit den dazugehörigen Daten dazu angeführt ist. Im Folgenden werden dazu die darin enthaltenen Informationen und Grafiken kurz vorgestellt beziehungsweise deren Bedeutung erläutert.

- Die erste Grafik am Bericht ist eine Auswertung in Form eines Liniendiagramms zur Wechselwirkung durch die Beeinflussungsmatrix.
- Darauf folgen die einzelnen Ergebnisse der Bewertungen auf Basis der Einflussmatrix. Die Spalte Basis zeigt den Basiswert der Einflussmatrix aus dem Bereich „04_Konfiguration“. Die Spalte Auswirkung ist der Mittelwert des jeweiligen Kapitels beziehungsweise der Kontrolle. Der Wert ergibt sich in der jeweiligen Spalte beziehungsweise Zeile der Tabelle [3] im Bereich „05_Auswertung“. Rechts zur tabellarischen Bewertung, verdeutlicht ein Tortendiagramm die Verteilung prozentuell zum Standard.
- Der Abschnitt „Einflussreichste Kapitel und Kontrollen“ ist eine Übersicht über die Standards hinweg. In der Spalte „Wirkung“ können die Werte beispielsweise der Größe nach absteigend sortiert werden, um eine Reihung dieser vorzunehmen. Eine Legende vermerkt die farbliche Kennzeichnung der Werte.
- Der abschließende Bereich ist eine zusammenfassende grafische Auswertung der Daten. Die erste Auswertung ist ein Liniendiagramm mit den Abweichungen zur Basismatrix. Zur Grafik ist rechts die dazugehörige Tabelle festgehalten. Die gleiche Darstellung ist im Anschluss zur Reifegradbewertung in Form eines Balkendiagramms vorhanden. Die Grafik und die dazugehörige Tabelle zeigen die Werte der Reifegradbewertungen. Die letzte Grafik zeigt die erneute Berechnung des Reifegrades in Bezug auf die Wechselwirkungen.

Da die Hauptbereiche des Assessment Tools mit Abschluss des Berichtes grundlegend dargestellt wurden, zeigt nachstehender Abschnitt abschließend eine Zusammenfassung der Arbeit, eine Reflexion der Ergebnisse und einen Ausblick.

5. Abschluss

Die vorliegende Arbeit liefert den Entwurf eines Assessment Tools zur Beurteilung der Wechselwirkungen von Service- und Security Management Standards.
Um den sich ständig vorantreibenden und dynamischen Marktbedingungen Stand zu halten, verlangt es einer entsprechenden Umsetzung von Prozessen und etablierten Modellen. Mithilfe des, im Zuge dieser Arbeit entstehenden, Assessment Tools soll demzufolge eine Hilfestellung entstehen, um fortlaufende Berechnungen und Analysen zu ausgewählten Standards treffen zu können. Die entstandene Einflussmatrix der Wechselwirkungen bildet Einflussfaktoren in einem Tool ab. Die Bewertung der darin enthaltenen Wechselwirkungen wurde durch fachkundige Experten validiert, um dem Ergebnis wissenschaftlichen Ausdruck gewährleisten zu können.
Mit dem zugrunde liegenden Tool können Bewertungen zu Kapitel und Kontrollen von ausgewählten Standards dokumentiert werden. Anhand dieser Bewertungen, lassen sich anschließend entscheidende weiterführende Aussagen treffen, womit die Hebelwirkung bestimmter Einflussfaktoren festgestellt werden kann. Dadurch können Teilbereiche vorausschauend analysiert und deren Auswirkung in Organisationen besser abgeschätzt werden.

Das Tool gestaltet darüber hinaus eine essenzielle Basis und Potenzial für Weiterentwicklung, sei es in Hinsicht auf Anpassung des Tools an sich, oder eine Weiterentwicklung in Betracht auf den Umfang der enthaltenen Standards und der festgelegten Möglichkeiten.

5.1. Zusammenfassung

Themenbereiche rund um IT Service und Security Management gewinnen an zunehmender Aktualität. Es ist davon auszugehen, dass auch in Zukunft der Ruf nach Zertifizierung ein unbedingtes Erfordernis für IT-Organisationen darstellen wird.
Dadurch wird nicht nur die Transparenz und Vergleichbarkeit gefördert, vielmehr wird auch ein Zeichen für Qualität stationiert. Dritten wird es ermöglicht, anhand etwaiger Anforderungen diverse Bereiche wie Planung, Kontrolle und Monitoring besser abzudecken.
Durch die Implementierung von etablierten Standards können Prozesse leichter und transparenter umgesetzt werden. Die Vergleichbarkeit der einzelnen Modelle, Standards und Normen stellen entscheide Aspekte in Aussicht. Unterschiedliche Ansätze verfolgen verschiedene Bereiche in Organisationen. Nicht nur deshalb ist es von grundlegender Bedeutung zu wissen, welche Prozesse mit welchen Standards am besten abgedeckt werden, wie sich die Standards in Kombination auswirken und wo die einzelnen Schnittstellen zwischen diesen zu finden sind. Nicht nur diese wenigen Anhaltspunkte geben Anlass für zahlreiche fortführenden Arbeiten, respektive Modellen.
Beim Einsatz von IT Normen, Frameworks und Standards treten allerdings auch besondere Herausforderungen zu tage. Bei der konsequenten und richtigen Handhabung von Standards können solche nur funktionieren wenn diese auch tatsächlich eingesetzt und richtig gelebt werden. Demnach ist entsprechende Überzeugungsarbeit unabdingbar, um die fortlaufende Umsetzung aufrecht zu halten.
Organisationen sind stetig bemüht, Standards optimal an deren Anforderungen und Bedingungen anzupassen ohne dabei unnötige Ressourcen zu verschwenden.

All jene genannten Erkenntnisse sind vorweg zu überdenken. Dahingehend soll das in dieser Arbeit entwickelte Assessment Tool einen praxisnahen Ansatz darbieten, um die Wechselwirkungen erstmals mit ausgewählten Bereichen beurteilen zu können. Mit den Auswertungen im Tool können dahingehend Entscheidungen zu Standards getroffen und entsprechende Handlungen durchgeführt werden.

Die Vielfalt, Reichweite und Bedeutung der Standards wurde daher am Beginn zum besseren Verständnis in der Arbeit ausführlich dargestellt.

Zu Beginn der Arbeit wurden zunächst Grundlagen zu Normen, Framework und Standards erläutert. Daraufhin die Themenbereiche von IT Service und Security Management jeweils separat näher dargestellt. Darin wurden ausgewählte Standards detaillierter vorgestellt, wobei der Fokus in Richtung der gewählten Standards gelegt wurde. Abschließend zu diesem Abschnitt wurden Kombinationen der ausgewählten Standards laut Literaturrecherche in einer Tabelle gegenübergestellt.
In der zweiten Hälfte der Arbeit, dem praxisorientierten Teil, wurde das Assessment Tool im Detail vorgestellt. Darin sind der Aufbau, die Verwendung und die Interpretation der darin enthaltenen Ergebnisse dokumentiert. Ein besonderes Hauptaugenmerk hat dabei die Evaluierung der Einflussmatrix und deren Ergebnisreflexion erhalten. Abschließend wurde die Arbeit mit einer Zusammenfassung, Reflexion und einem Ausblick abgerundet.

5.2. Ergebnisreflexion

Im eingehenden Kapitel „Einleitung“ wurden die Problemstellung und die Motivation der Arbeit kurz vorgestellt. Abschließend möchten im Besonderen die Fragestellungen an dieser Stelle nochmals aufgegriffen, um zusammenfassend beantwortet zu werden.

Die beiden Hauptfragen „Gibt es Dependenzen zwischen den Domänen des IT Service und Security Managements?“ und „Wie können etwaige Abhängigkeiten dargestellt, ausgewertet und daraufhin fortführende Aussagen auf deren Basis getroffen und prognostiziert werden?“ können damit wie folgt beantwortet werden.
Die erste Frage wurde im Zuge der Recherche mehrmals beantwortet. In der Literatur wurde mehrmals die Abhängigkeit beider Bereiche zum Ausdruck gebracht. Allerdings gibt es kaum Modelle, wie diese Wechselwirkung verdeutlicht dargestellt werden kann. Lediglich die im Abschnitt 3 „Kombinationen“ erarbeitete Tabelle, konnte mithilfe einer Gegenüberstellung die Übereinstimmungen kennzeichnen.
Diesem Umstand zufolge wurde in dieser Arbeit die sogenannte Einflussmatrix mithilfe von Expertinnen und Experten entwickelt. In dieser lässt sich die Fragestellung am besten, wie bereits im Abschnitt 4.2.3.2 „Zusammenfassung der Einflussmatrix“ erwähnt, beantworten. Die Einflussmatrix bringt die Abhängigkeit vom IT Service und Security Management anhand von ausgewählten Standards zum Ausdruck. Mit einem durchschnittlichen Wert von 1,82 über die gesamte Matrix, bei einer Bewertung von null bis drei, kann man von einer keinesfalls unwesentlichen Abhängigkeit sprechen. Punktuelle einzelne Abhängigkeiten in der Tiefe sind der Einflussmatrix zu entnehmen.
Die zweite Frage um etwaige Abhängigkeiten lässt sich ebenso, am besten mithilfe der Einflussmatrix beantworten. Diese schließt die Lücke von bislang kaum vorhandenen Abhängigkeitsmodellen zwischen Service und Security Management und bringt diese mithilfe wissenschaftlicher Methoden zum Ausdruck.
Die daraus abgeleiteten Fragen konnten wie folgt beantwortet werden:
„Welche Kombinationen von Standards des IT Service und Security Management können als sinnvoll betrachtet werden?“ Im Abschnitt 3.2 Zusammensetzungen / Schnittpunkte wurde versucht, Überschneidungen laut Literatur darzustellen. Im Service Management wurde dahingehend, die ISO 20000-1 der ISO 27001 und dem IT-Grundschutz aus der Domain des Security Management in einer Tabelle gegenübergestellt. Eine genaue Überschneidung ist schwer festzumachen, da eine Bewertung oder Evaluierung der einzelnen Punkte darin benötigt werden würde. Dennoch kann am ehesten eine Übereinstimmung bei den sogenannten “shall” Normen wie beispielsweise der ISO 20000-1 und 27001 fixiert werden, da diese zwingende Definitionen vorgeben. Die Überschneidungen der Kapitel laut Literatur sind daher der Tabelle 7 beziehungsweise dem Anhang B zu entnehmen.
Die Frage „Gibt es vordefinierte Kombinationen von Standards des IT Service und Security Management?“ kann schwer eindeutig definiert werden, da dies stark von der individuellen Situation und den Gegebenheiten der Organisation abhängt. Dennoch wurde versucht, anhand von gewissen Standards Überschneidungen laut Literatur zu finden. Diese wenigen Aussagen dahingehend, sind in Tabelle 7 beziehungsweise dem Anhang B zu finden. Jedenfalls ergeben sich bedeutende Synergieeffekte bei gemeinsamer Zertifizierung eines integrierten Managementsystems.

Die vorletzte abgeleitete Frage „Ist eine maßgebliche Abhängigkeit von IT Service und Security Management festzustellen?“ lässt sich wie in Abschnitt 4.2.3.2, mit der Summe über die gesamte Einflussmatrix mit 1,82 als

Mittelwert bei einer Bewertungsskala von null bis drei zum Ausdruck bringen. Damit kann eine maßgebliche Abhängigkeit der Standards belegt werden. Überschneidungen beider Domänen werden in der Literatur oftmals als so groß betitelt, dass beide Managementsysteme bei Organisationen als IMS betrieben werden. Dieser Ansatz wird allem voran im Regelwerk ISO/IEC 27013, wie im Abschnitt 2.3.1.8 beschrieben und als standardisierte Vorgehensweise abgebildet. Darin sind Hilfestellungen dahingehend beschrieben, um beide Ansichten besser verstehen zu können. Synergien sind demnach maßgeblich vorhanden und können, um Doppelarbeiten zu vermeiden, mithilfe eines IMS in Verbindung gebracht werden.

Abschließend wird im letzten Punkt ein Ausblick über folgende Forschungsgebiete, der Weiterentwicklung sowie weiteren Anregungen zum Thema dargestellt.

5.3. Ausblick

Mit dieser Arbeit und dem zugrunde liegenden Tool entstehen zahlreiche Gedanken und Möglichkeiten, sich diesem Gebiet weiter zu widmen und die Forschung auszubauen.

Die erste und evidenteste Überlegung besteht in der Möglichkeit, das Tool in der derzeitigen Ausführung weiter auszubreiten. Gerade im Bereich der Konfigurationen, Auswertung und dem Bericht besteht das Potenzial das Tool weiter zu verfeinern. Dabei können zum einen die Berechnungen und die zugrunde liegenden Algorithmen weiter optimiert, zum anderen aber auch weitere Auswertungen und Grafiken erstellt werden.
Zuallererst ist das entwickelte Tool im Rahmen dieser Arbeit aber auch als dessen erster Entwurf zu betrachten. Eine technische Weiterentwicklung zur Optimierung des Tools ist dahingehend anzudenken, dieses in eine alleinstehende unabhängige Applikation zu übertragen. Umsetzungsmöglichkeiten ergeben sich dabei in zahlreichen Ausprägungsformen, welche an dieser Stelle offen gelassen werden möchten.

Die Bewertung der darin abgebildeten Einflussmatrix kann ausgebaut, verfeinert und optimiert werden, um ein noch genaueres Ergebnis der einzelnen Schnittpunkte zu erreichen. Experten beider Domänen zu erreichen, ist eine schwer zugängliche Herausforderung, womit allerdings noch Möglichkeiten der Weiterentwicklung entstehen. Im Anhang findet sich dazu der Fragebogen, welcher zudem im Tool nochmals abgebildet ist.
Die Erweiterung der Einflussmatrix kann auch mit diversen Optimierungen der Berechnungen geschehen. Damit können, bei Vorhandensein einer gewissen Menge von Befragungen, eventuelle statistische Ausreißer besser behandelt oder gar nichtig gemacht werden.

Darüber hinaus ist anzudenken, mit steigender Anzahl der Befragungen, die Skala der Bewertung Null bis Drei weiter zu unterteilen. Dies würde allerdings eine erhebliche Komplexität mit sich bringen und demzufolge müssten auch bereits vorhandene Evaluierungen nichtig gemacht werden. Eine steigende Komplexität der Evaluierung ist allerdings auch kritisch zu betrachten, da der Bewertungsaufwand für die befragten Personen drastisch steigt. Dadurch wird es zum einen schwieriger, Expertinnen und Experten zur Evaluierung zu überzeugen, andererseits steigt ebenso die Schwankung der subjektiven Einschätzung. Nichts desto trotz ist dieser Ansatz als alleinstehender Forschungsbereich anzudenken, was eine wesentlich detailreichere Bewertung ergeben würde.

Ein weiteres Forschungsthema bringt die Bewertung der in Abbildung 22 dargestellten Matrix mit sich. Auch diese Matrix trägt bei der Evaluierung zu einem enormen Mehraufwand bei, womit diese Bewertung eine eigenständige Forschungsarbeit einschließt. Wie im dazugehörigen Kapitel beschrieben, umfasst diese Matrix 3666 Kreuzungen, mit den jeweiligen Unterkapiteln der ausgewählten Standards miteingeschlossen. Eine Bewertung nach diesem Schema würde eine weitreichendere Unterteilung der Wechselwirkung und eine noch peniblere Auswertung zum Ausdruck bringen.

Eine Erweiterung der Einflussmatrix um weitere Standards und Normen würde ermöglichen, die einzelnen Wechselwirkungen der Basismatrix noch allgemeiner und branchenunabhängiger darzustellen. Zum einen wäre

eine Erweiterung um Standards der Service und Security Domain denkbar, aber auch der Querverweis zu anderen verwandten Bereichen und deren Standards, beispielsweise dem Qualitätsmanagement, ist eine anzudenkende Möglichkeit.

Es besteht demnach noch Forschungsbedarf, womit diese Arbeit zahlreiche weitere Fragen und viel Potenzial zur Weiterentwicklung mit sich bringt. Welcher Standard welche Entwicklung und Auswirkungen mit sich bringt, muss letztlich individuell getroffen werden. Für den optimalen Einsatz können Modelle wie jene dieser Arbeit allerdings wesentlich bei der Entscheidungsfindung beitragen.

Anhang A

Fragebogen

Im Zuge der Diplomarbeit „Interdependencies of service and security management“ soll ein Assessment Tool entstehen wodurch die Beeinflussung von Service und Security Management, genauer der ISO 20000-1 entgegen der ISO 27001 und ISO 27002 festgestellt werden kann.
Zur Evaluierung der Abhängigkeiten soll eine Matrix entstehen, auf Basis derer weitere Berechnungen und Auswirkungen ermöglicht werden sollen.

Zu Bewertung der einzelnen ausgewählten Teilbereiche der Normen sind folgende Stufen der Ausprägung gewählt:

- Stufe [0]
  Entspricht „keine relevante Abhängigkeit“
- Stufe [1]
  Entspricht „leichte Abhängigkeit“
- Stufe [2]
  Entspricht „mittlere Abhängigkeit“
- Stufe [3]
  Entspricht „starke Abhängigkeit“

Folgend ist jeweils horizontal das jeweilige Kapitel aus der ISO 20000-1(grau) angeführt. Vertikal hingegen ausgewählte Kapitel der ISO 27001 (dunkelblaue) und ISO 27002(hellblau).

Kapitel der ISO 20000-1

4 Servicemanagement-system Allgemeine Forderungen

ISO/IEC 20000-1		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Betrieb	Bewertung der Leistung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Servicemanagement-system Allgemeine Forderungen																						

5 Gestaltung und Umsetzung von neuen und geänderten Services

ISO/IEC 20000-1		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Betrieb	Bewertung der Leistung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Gestaltung und Umsetzung von neuen und geänderten Services																						

6 Service Einführungsprozess

ISO/IEC 20000-1		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Betrieb	Bewertung der Leistung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Service Einführungsprozess																						

7 Prozesse zur Beziehungspflege

ISO/IEC 20000-1		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Betrieb	Bewertung der Leistung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Prozesse zur Beziehungspflege																						

8 Lösungsprozesse

ISO/IEC 20000-1		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Betrieb	Bewertung der Leistung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Lösungsprozesse																						

9 Überwachungsprozesse

ISO/IEC 20000-1		ISO 27001							ISO 27002													
		Kontext der Organisation	Führung	Planung	Unterstützung	Betrieb	Bewertung der Leistung	Verbesserung	Informationssicherheitsrichtlinien	Organisation der Informationssicherheit	Personalsicherheit	Verwaltung der Werte	Zugangssteuerung	Kryptographie	Physische und umgebungsbezogene Sicherheit	Betriebssicherheit	Kommunikationssicherheit	Anschaffung, Entwicklung und Instandhaltung von Systemen	Lieferantenbeziehungen	Handhabung von Informationssicherheitsvorfällen	Informationssicherheitsaspekte beim Business Continuity Management	Compliance
Überwachungsprozesse																						

Anhang B

Service Management				Security Management			
ITIL		ISO/IEC 20000-1:2011		ISO/IEC 27001:2013		IT-Grundschutz	
Kapitel	*Bezeichnung*	*Kapitel*	*Bezeichnung*	*Kapitel*	*Bezeichnung*	*Kapitel*	*Bezeichnung*
		0	Introduction		Introduction		
		0.1	General	0.1	General		
		-	-	0.2	Compatibility with other management systems		
		1	Scope	1	Scope		BSI-Standard 100-2, Kapitel 1 Einleitung
		1.1	General	-	-		
		1.2	Application	-	-		
		2	Normative references	2	Normative references		BSI-Standard 100-1, Kapitel 1.5 Literaturverzeichnis
		-	-	-	-		
		-	-	-	-		
		3	Terms and definitions	3	Terms and definitions		IT-Grundschutz-Kataloge, Glossar
		-	-	-	-		
		-	-	-	-		
	Verschiedene ITIL-Prozesse aus Service Strategie, Service Design und Kontinuierliche Service-Verbesserung (CSI)	4.5	Establish and improve the SMS	4	Context of the organization		
		7	Relationship processes				
		4.5.1	Define scope	4.1	Understanding the organization and its context	100-2, 3.2.1	Ermittlung von Rahmenbedingungen
	Business Relationship Management	7.1	Business relationship management				
		4.5.1	Define scope	4.2	Understanding the needs and expectations of interested parties	100-2, 3.2	Konzeption und Planung des Sicherheitsprozesses
	Business Relationship Management	7.1	Business relationship management				
		4.5.1	Define scope	4.3	Determining the scope of the information security management	100-2, 3.3.2, 4	
		-	-	4.4	Information security management system	100-1, 3	ISMS-Definition und Prozessbeschreibung
						100-2, 2	Informationssicherheitsmanagement mit IT-Grundschutz
				5	Leadership		
		4.1.1	Management commitment	5.1	Leadership and commitment	100-2, 3.1	Übernahme von Verantwortung durch die Leitungsebene
		6.6.1 a)	Information security policy (communication and the importance of conformity)				
		4.1.2	Service management policy	5.2	Policy	100-2, 2, 3	
		6.6.1	Information security policy (definition of information security management objectives)				
		4.1.3	Authority, responsibility and communication	5.3	Organizational roles, responsibilities and authorities	100-2, 3.4	Organisation des Sicherheitsprozesses
		4.1.4	Management representative				
	Supplier Management und Service Level Management	4.2	Governance of processes operated by other parties				
	Strategie-Management für IT Services und verschiedene Prozesse aus Kontinuierliche Service-Verbesserung (CSI)	4.1	Management responsibility	6	Planning		
		4.5.2	Plan the SMS (Plan)				
		4.5.5	Maintain and improve the SMS (Act)				
		6.6.1 c) and d)	Information security policy (definition of risk assessment approach and risk assessment realization)				
		-	-	6.1	Actions to address risks and opportunities		
		4.5.5.1	General	6.1.1	General	100-2, 3, 4, 5	
		4.5.2 j) 4.5.3 d)		6.1.2	Information security risk assessment	100-2, 3, 4	
		6.6.1 c) 6.6.2	Approach to be taken for the management of risks and the criteria for accepting risks	6.1.3	Information security risk treatment	100-2, 4, 5	
		4.1.1 6.6.1 b)	Management commitment	6.2	Information security objectives and planning to achieve them	100-2, 3	
		4	Service management system general requirements	7	Support		
		5.2	Plan new or changed services				
		6	Service delivery processes				
		4.4.1	Provision of resources	7.1	Resources	100-2, 3.5	Bereitstellung von Ressourcen für die Informationssicherheit
		4.4.2	Human resources	7.2	Competence	100-2, 3.4.3	Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation
				7.3	Awareness	100-2, 3.6	Einbindung aller Mitarbeiter in den Sicherheitsprozess
	Verschiedene Service-Strategie-, Service-Design- und Service-Transition-Prozesse	5.2 c)	Communication with interested parties	7.4	Communication	100-2, 3.6	Einbindung aller Mitarbeiter in den Sicherheitsprozess
	Service Level Management	6.2	Service reporting				
	Verschiedene Service-Strategie-, Service-Design- und Service-Transition-Prozesse	4.3	Documentation management	7.5	Documented information		
		-	-	7.5.1	General	100-2, 6.2	Informationsfluss im Informationssicherheitsprozess
		-	-	7.5.2	Creating and updating	100-1, 4.3	Kommunikation und Wissen
		-	-	7.5.3	Control of documented information	100-2, 6.2	Informationsfluss im Informationssicherheitsprozess
	IT Service Continuity Management und Availability Management Information Security Management	4.5.3	Implement and operate the ISMS (Do)	8			
		6.3	Service continuity and availability management				
		6.6	Information security management				
		4.5.3 e)	Manage service management processes and interfaces	8.1	Operation and planning control	100-2, 5	Umsetzung der Sicherheitskonzeption
		4.5.3 d)	Identify, assess, and manage service management risks	8.2	Information security risk assessment	100-2, 3, 4	
		6.3.1	Service continuity and availability requirements				
		4.5.3 d)	Identify, assess, and manage service management risks		Information security risk treatment	100-2, 4, 5	
		6.3.2	Service continuity and availability plans	8.3			
		6.6.2	Information security controls				
		6.6.3	Information security changes and incidents				
	IT Service Continuity Management und Availability Management Information Security Management	4.5.4	Monitor and review the SMS (Check)	9	Performance evaluation		
		6.3	Service continuity and availability management				
		6.6	Information security management				
		4.5.4.1	General	9.1	Monitoring, measurement, analysis and evaluation	100-2, 6	Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
		6.3.3	Service continuity and availability monitoring and testing				
		4.5.4.2	Internal audit	9.2	Internal audit	100-2, 6.1.1	Methoden zur Überprüfung des Informationssicherheitsprozesses
		6.6.1 e)	Information security policy (internal audit)				
		4.5.4.3	Management review	9.3	Management review	100-2, 6.1	Überprüfung des Informationssicherheitsprozesses in allen Ebenen
		6.6.1 f)	Information security policy (audit results review)				
		4.5.5	Maintain and improve the SMS (Act)	10	Improvement		
		4.5.5.1	General	10.1	Nonconformity and corrective action	100-2, 6.1	Überprüfung des Informationssicherheitsprozesses in allen Ebenen
		4.5.5.2	Management of improvements	10.2	Continual improvement		

Anhang C

CD-ROM mit .xslx Tool “Assessmenttool SecM2ServM v1.0”

Literaturverzeichnis

[1] M. Stemmer und G. Goldacker, „IT-STANDARDISIERUNG IN DER ÖFFENTLICHEN VERWALTUNG," Frauenhofer Fokus, Juni 2015. [Online]. Available: https://cdn1.scrvt.com/fokus/4cd9b8f6fc302383/5f41cdcaa45a/IT-Standardisierung-in-der-o-ffentlichen-Verwaltung.pdf. [Zugriff am 04 Juli 2017].

[2] Bundesamt für Sicherheit in der Informationstechnik, Informationssicherheit - Ein Vergleich von Standards und Rahmenwerken, 53133 Bonn: Bundesamt für Sicherheit in der Informationstechnik , 2009.

[3] H.-P. Königs, IT-Risikomanagement mit System, Wiesbaden: Springer Vieweg, 2013.

[4] T. W. Harich, IT Sicherheitsmanagement: Arbeitsplatz IT Security Manager, Heidelberg : mitp Verlags GmbH & Co. KG, 2012.

[5] P. Melzer-Klauke , „ITIL in der Praxis," 15 Juli 2010. [Online]. Available: https://de.slideshare.net/sibbev/itil-in-der-praxis. [Zugriff am 02 Oktober 2017].

[6] ISACA, „About ISACA," ISACA, [Online]. Available: http://www.isaca.org/about-isaca/Pages/default.aspx. [Zugriff am 05 November 2017].

[7] W. Bock, G. Macek, T. Oberndorfer und R. Pumsenberger, Praxisbuch ITIL: Erfolgreiche Zertifizierung nach ISO 20000, Bonn: Galileo Computing, 2008.

[8] International Electrotechnical Commission, „IEC - About the IEC," International Electrotechnical Commission, [Online]. Available: http://www.iec.ch/about/. [Zugriff am 11 Dezember 2017].

[9] International Organization for Standardization, „About us," International Organization for Standardization, [Online]. Available: https://www.iso.org/about-us.html. [Zugriff am 11 Dezember 2017].

[10] „https://www.bitkom.org/Bitkom/Publikationen/Kompass-der-IT-Sicherheitsstandards.html," BITKOM, September 2013. [Online]. Available: https://www.bitkom.org/noindex/Publikationen/2013/Leitfaden/Kompass-der-IT-Sicherheitsstandards/Kompass-der-IT-Sicherheitsstandards-it-sa-Broschuere-Web.pdf. [Zugriff am 17 Juli 2017].

[11] EVOLIT , „http://www.evolit.ch/," 23 Novemer 2011. [Online]. Available: http://www.evolit.ch/portals/0/content/04_verifizierung/04-02_iso27000/evl_iso27k-info_v1-00.pdf. [Zugriff am 1 August 2017].

[12] H. Schlegel, Steuerung der IT im Klinikmanagement, Wiesbaden: Vieweg+Teubner Verlag, 2010.

[13] AXELOS Limited 2011, ITIL glossary and abbreviations, AXELOS Limited 2011, 2011.

[14] P. T. Köhler, ITIL: Das IT-Servicemanagement Framework, Berlin Heidelberg: Springer-Verlag , 2005.

[15] ISACA, Basic Foundational Concepts Student Book: Using COBIT 5, Rolling Meadows: ISACA, 2014.

[16] J. Brunnstein, ITIL Security Management realisieren, Wiesbaden: Vieweg & Sohn Verlag | GWV Fachverlage GmbH, 2006.

[17] K.-R. Müller, IT-Sicherheit mit System, Wiesbaden: Vieweg+Teubner Verlag, 2011.

[18] CIS - Certification & Information Security Services GmbH , „CIS | System-Certification/Integrated-Management-Systems/Integration-ISO-27001-ISO-20000-ISO-9001," CIS - Certification & Information Security Services GmbH , [Online]. Available: http://www.cis-cert.com/System-Certification/Integrated-Management-Systems-/Integration-ISO-27001-ISO-20000-ISO-9001.aspx. [Zugriff am 09 Oktober 2017].

[19] H. Kersten, J. Reuter und K.-D. Schröder, IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Wiesbaden: Springer Vieweg, 2013.

[20] M. Beims, IT-Service Management in der Praxis mit ITIL® 3, München: Carl Hanser Verlag GmbH & Co. KG, 2012.

[21] P. Kuntsche und K. Borchers, Qualitäts- und Risikomanagement im Gesundheitswesen, Berlin: Gabler Verlag, 2017.

[22] TSO (The Stationery Office), ITIL® Service Strategy 2011 edition, Belfast: TSO Ireland, 2011.

[23] A. Ehringfeld, ITIL als Methode gegen Attacken eines Social Engineers im IT-Betrieb, Wien: Fakultät für Informatik der Technisches Universität Wien, 2012.

[24] G. Klett, K.-W. Schröder und H. Hersten, IT-Notfallmanagement mit System, Wiesbaden: Vieweg+Teubner Verlag, 2011.

[25] Lynda Cooper, „ISO/IEC 27013 – integrating ISO/IEC 27001 and ISO/IEC 20000-1," Lynda Cooper, 10 July 2017. [Online]. Available: https://apmg-international.com/article/isoiec-27013-integrating-isoiec-27001-and-isoiec-20000-1. [Zugriff am 09 Oktober 2017].

[26] O. Weiss , „IT Service Management sollte COBIT nicht vergessen," computerwelt, 02 März 2011. [Online]. Available: http://www.computerwelt.at/news/technologie-strategie/detail/artikel/47736-it-service-management-sollte-cobit-nicht-vergessen/. [Zugriff am 05 November 2017].

[27] H.-P. Königs, IT-Risiko-Management mit System, Wiesbaden: Vieweg+Teubner Verlag, 2009.

[28] S. Klipper, Information Security Risk Management, Wiesbaden: Springer Vieweg, 2015.

[29] IsecT Ltd, „http://www.iso27001security.com/," Juni 2017. [Online]. Available: http://www.iso27001security.com/ISO27k_Standards_listing.pdf. [Zugriff am 13 August 2017].

[30] ISO copyright office, ISO/IEC 27000:2016 (E) Fourth edition, Vernier: ISO copyright office, 2016.

[31] CIS - Security Information Certification, „CIS | System-Zertifizierung | Informationssicherheit | ISO 27001," CIS - Security Information Certification, [Online]. Available: http://at.cis-cert.com/Pages/de/System-Zertifizierung/Informationssicherheit/ISO-27001/ISO27001.aspx. [Zugriff am 1 August 2017].

[32] Austrian Standards Institute, ISO/IEC 27013:2012, Wien: Austrian Standards Institute/Österreichisches Normungsinstitut (ON), 2013.

[33] Bundesamt für Sicherheit in der Informationstechnik – BSI, „Überblick IT-Grundschutz - Entscheidungshilfe für Manager," Druck- und Verlagshaus Zarbock GmbH & Co. KG, Bonn, 2016.

[34] Bundestamt für Sicherheit in der Informationstechnik, „BSI - IT-Grundschutz Modernisierung," Bundestamt für Sicherheit in der Informationstechnik, [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/itgrundschutz_modernisierung_node.html. [Zugriff am 10 Oktober 2017].

[35] EPPS Services Ltd., „ISO 27001 vs. ISO 20000 matrix," 12 März 2015. [Online]. Available: http://info.advisera.com/27001academy/free-download/iso-27001-vs-iso-20000-matrix. [Zugriff am 05 April 2018].

[36] IT Process Maps GbR, „ISO 20000 | IT Process Wiki," 27 April 2017. [Online]. Available: https://wiki.de.it-processmaps.com/index.php/ISO_20000#ISO-20000-ITIL-Hinweis. [Zugriff am 05 April 2018].

[37] Bundesamt für Sicherheit in der Informationstechnik, „Zuordnungstabelle," 15 August 2011. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile&v=3. [Zugriff am 05 April 2018].

[38] M. Mangiapane und R. P. Büchler, Modernes IT-Management : Methodische Kombination von IT-Strategie und IT-Reifegradmodell, Wiesbaden: Springer Vieweg, 2014.

[39] S. Rudolph, Servicebasierte Planung und Steuerung der IT-Infrastruktur im Mittelstand, 2009: Gabler | GWV Fachverlage GmbH, Wiesbaden .

[40] M. Jungreitmair, Entwicklung eines Kennzahlensystems zur Bestimmung des Reifegrades für eine Zertifizierung nach ISO 20000, Wien: Universität Wien, 2008.

[41] M. Andenmatten, COBIT® 5 Grundlagen: Planung, Umsetzung und Optimierung der IT-Steuerung, Düsseldorf: Symposion Publishing GmbH, 2015.

[42] Austrian Standards Institute/Österreichisches Normungsinstitut, ISO/IEC DIS 27001:2013, Wien: Austrian Standards Institute/Österreichisches Normungsinstitut, 2014.

[43] Austrian Standards Institute/Österreichisches Normungsinstitut, ISO/IEC 27002:2013, Wien: Austrian Standards Institute/Österreichisches Normungsinstitut, 2014.

[44] ISO copyright office, ISO/IEC 20000-1, Geneva: ISO copyright office, 2011.

[45] H. A. Mieg und M. Näf , „Experteninterviews Institut für Mensch-Umwelt-Systeme (HES), ETH Zürich," April 2005. [Online]. Available: http://www.metropolenforschung.de/download/Mieg_Experteninterviews.pdf. [Zugriff am 17 April 2018].

[46] „http://ecinetworks.com/," Clinch Consulting, Mai 2009. [Online]. Available: http://ecinetworks.com/wp-content/uploads/bsk-files-manager/13_ITILV3_and_Information_Security_White_Paper_May09.pdf. [Zugriff am 17 Juli 2017].

[47] K.-R. Müller, IT-Sicherheit mit System, Wiesbaden: Vieweg+Teubner Verlag, 2008.

[48] Wirtschaftslexikon24.com, „ISO (=International Standards Organization)," Wirtschaftslexikon24.com, [Online]. Available: http://www.wirtschaftslexikon24.com/d/iso-international-standards-organization/iso-international-standards-organization.htm. [Zugriff am 11 Dezember 2017].