Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

GEGENÜBERSTELLUNG STANDARDISIERTER VORGEHENSWEISEN ZUR IMPLEMENTIERUNG EINES GESCHÄFTSKONTINUITÄT-MANAGEMENTS MIT SCHWERPUNKT AUF DIE INFORMATIONSTECHNOLOGIE

Eingereicht am: 06. September 2023
von: Simon Lang

Vorwort und Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Anfertigung dieser Masterarbeit unterstützt und motiviert haben. Zuerst gebührt mein Dank Frau Prof. Dr.-Ing. Antje Raab-Düsterhöft für die Betreuung der Master-Thesis und Herrn Prof. Dr. Ahrens für die freundliche Übernahme des Korreferats. Ein großer Dank gilt meinen Freunden und Kollegen für den Rückhalt und die Unterstützung über die Dauer meines gesamten Studiums und vor allem in der Zeit der Erstellung der Masterarbeit. Abschließend möchte ich mich bei meiner Familie bedanken, die immer hinter meiner Entscheidung standen, dieses Studium zu absolvieren und stets mit aller Kraft unterstützt haben.

Simon Lang

Aufgabenstellung

Ziel der Masterthesis ist es eine Übersicht über eine Auswahl von nationalen und internationalen etablierten Geschäftskontinuität-Management Vorgehensweisen mit Schwerpunkt auf die Informationstechnologie zu erstellen, auch IT-Service Continuity Management genannt. Zunächst soll ein grundlegendes Verständnis für Geschäftskontinuität-Management in Hinblick auf aktuellem Forschungsstand, Motivation und Definition bzw. Abgrenzung der Begrifflichkeiten geschaffen werden. Anschließend wird die Auswahl der Vorgehensweisen begründet und eine exemplarische Institution dargestellt, an Hand derer die Implementierung in Grundzügen gezeigt werden soll. Bei den ausgewählten Vorgehensweisen werden die Voraussetzungen und der Ablauf nacheinander präsentiert. Nachdem die Vorgehensweisen bekannt sind, sollen die Unterschiede und Gemeinsamkeiten herausgearbeitet werden und eventuell vorhandene Vor- bzw. Nachteile der einzelnen Vorgehensweisen herausgearbeitet werden. Die Möglichkeit zwei oder mehrere Vorgehensweisen zu kombinieren wird geprüft.

Die Bedeutung der Masterthesis liegt vor allem in dem Vergleich der Vorgehensweisen. Die Auswahl einer passenden Vorgehensweise für die individuellen Bedürfnisse soll durch die Gegenüberstellung der Voraussetzungen, Implementierung und Vorteilen und Nachteilen erleichtert werden.

Kurzreferat

Die Anzahl der IT-Sicherheitsvorfälle steigt jährlich, in 2021 wurde bereits bei 86 Prozent der deutschen Unternehmen ein Schaden durch IT-Sicherheitsvorfälle verursacht. Des Weitern wurde 2022 das erste Mal der Katastrophenfall wegen eines IT-Sicherheitsvorfalles ausgerufen und für 207 Tage aufrechterhalten. Damit die Ausfallzeiten bzw. der entstandene Schaden verringert wird, ist es wichtig zügig zu einem geordneten Unternehmensbetrieb zurückzukehren. Um für den Ernstfall vorbereitet zu sein, ist es wichtig, eine Strategie für ITSCM im Voraus zu entwickeln. Trotzdem steht mit der ISO 27031 nur ein internationaler Standard zur Verfügung, der keine Umsetzungshilfe bietet. Allerdings ist insbesondere bei kleinen und mittelständischen Organisationen die Implementierungsrate eines ITSCM auf Grund mehrerer Herausforderungen gering. Weshalb eine möglichst leicht zu implementierende Vorgehensweise wünschenswert ist. Es werden in der Arbeit deshalb elf IT-Standards auf Eigenschaften von ITSCM geprüft. Anschließend werden der BSI 200-4 und die VdS 10000, anhand eines exemplarischen Unternehmens, ausgearbeitet. Weiterhin werden Vor- und Nachteile der detailliert analysierten Standards und das allgemeine Synergiepotenzial dargestellt. Die Übersicht über die verschiedenen Methoden soll die Auswahl eines geeigneten Standards erleichtern. Es bietet aber auf Grund der Menge an verfügbaren Vorgehensweisen keinen vollständigen Überblick. Beim Vergleich der verschiedenen Standards stellt man fest, dass keiner eine vollständige und detaillierte Implementierung eines ITSCM abbildet. Weiterhin sind insbesondere für kleinste und kleine Organisationen eine weitere Vereinfachung und individuelle Anpassung der Vorgehensweisen ratsam.

Abstract

The number of IT security incidents is increasing every year and by 2021, 86 per cent of German companies had already suffered damage from IT security incidents. In addition, 2022 was the first year that an IT security incident leads to a disaster that lasts for 207 days. In order to reduce downtime or the damage caused, it is important to return swiftly to normal business operations. To be prepared for an emergency, an ITSCM strategy must be developed in advance. ISO 27031 is the only international standard for ITSCM, however is does not provide implementation guidance. The implementation rate of ITSCM is low, especially in small and medium-sized organisations, due to several challenges. Therefore, an approach that is as easy to implement as possible is desirable. For this reason, eleven IT standards are examined for ITSCM characteristics. Subsequently, the BSI 200-4 and the VdS 10000 are eloberated on the basis of an exemplary company. Furthermore, the advantages and disadvantages of the standards considered in detail and general synergy potentials are presented. The overview of the different methods is intended to facilitate the selection of a suitable standard, but does not provide a complete overview due to the number of methods available. A comparison of the various standards shows that none of them represents a complete and detailed implementation of ITSCM. Furthermore, a further simplification and individual adaptation of the procedures is advisable, especially for the tiny and small organisations.

Inhalt

1 Einleitung ... 9
1.1 Entstehung Business Continuity Management ... 9
1.2 Gründe für BCM ... 10
1.3 Forschungstand BCM ... 12

2 Vorbetrachtung ... 14
2.1 Definitionen und Abgrenzungen ... 14
2.1.1 Definitionen ... 14
2.1.2 Abgrenzungen ... 16
2.2 ISO 27031 ... 18
2.3 Auswahlkriterien ... 19

3 Übersicht und Begründung für die Auswahl der Vorgehensweisen ... 23
3.1 BSI-Standard 200-4 Business Continuity Management – Community Draft ... 23
3.2 National Institute of Standards and Technology ... 26
3.2.1 Framework for Improving Critical Infrastructure Cybersecurity ... 26
3.2.2 Security and Privacy Controls for Information Systems and Organizations ... 29
3.2.3 Contingency Planning Guide for Federal Information Systems ... 31
3.3 VdS-Richtlinien für die Informationsverarbeitung ... 33
3.4 Information Technology Infrastructure Library 4th Edition ... 36
3.5 FitSM ... 38
3.6 Good Practice Guidelines Edition 2018 ... 40
3.7 Control Objectives for Information and Related Technology ... 42
3.8 Compliance Informations-Sicherheitsmanagement System in 12 Schritten ... 45
3.9 National Fire Protection Association 1600 ... 47

4 Exemplarische Ausarbeitung ausgewählter Vorgehensweisen ... 51
4.1 Ausarbeitung BSI 200-4 ... 53
4.1.1 Initiierung des Business Continuity Management Systems durch die Institutionsleitung ... 54
4.1.2 Konzeption und Planung des BCMS ... 56
4.1.3 Aufbau und Befähigung der besonderen Aufbauorganisation ... 58
4.1.4 Voranalyse ... 62
4.1.5 Business Impact Analyse ... 64
4.1.6 Soll-Ist-Vergleich ... 71
4.1.7 BCM-Risikoanalyse ... 73
4.1.8 Business-Continuity-Strategien und Lösungen ... 74
4.1.9 Geschäftsfortführungsplanung ... 75
4.1.10 Wiederanlauf- und Wiederherstellungsplanung ... 79
4.1.11 Üben und Testen ... 80

4.1.12 Leistungsüberprüfung und Berichterstattung 83
4.1.13 Aufrechterhaltung und Verbesserung 85
4.1.14 Vergleich von BSI 200-4 mit BSI 100-4 86
4.2 Ausarbeitung VdS 10000 89
4.2.1 Organisation der Informationssicherheit 90
4.2.2 Leitlinie zur Informationssicherheit (IS-Leitlinie) 91
4.2.3 Richtlinien zur Informationssicherheit (IS-Richtlinien) 91
4.2.4 Mitarbeiter 92
4.2.5 Wissen 93
4.2.6 Identifizieren kritischer IT-Ressourcen 94
4.2.7 IT-Systeme 98
4.2.8 Netzwerke und Verbindungen 104
4.2.9 Mobile Datenträger 105
4.2.10 Umgebung 106
4.2.11 IT-Outsourcing und Cloud Computing 107
4.2.12 Zugänge und Zugriffsrechte 108
4.2.13 Datensicherung und Archivierung 109
4.2.14 Störungen und Ausfälle 110
4.2.15 Sicherheitsvorfälle 113
4.2.16 Vergleich VdS 10000 und mit BCM-Standards 114

5 Auswertung der ausgewählten Vorgehensweisen und Einschätzung des Synergiepotenzials 115
5.1.1 Bewertung BSI 200-4 115
5.1.2 Bewertung VdS 10000 116
5.1.3 Synergiepotenzial der betrachteten Vorgehensweisen 117

6 Zusammenfassung und Ausblick 119
6.1 Zusammenfassung 119
6.2 Ausblick 121

Literaturverzeichnis 123

Bilderverzeichnis 132

Tabellenverzeichnis 133

Anlagenverzeichnis und Anlagen 134
Anlage 1: Übersicht Ergebnisse des Vergleichs: 135
Anlage 2: BCMS-Leitlinie der Mustermann GmbH 142
Anlage 3: Definition der Schadenskategorien 145
Anlage 4: IS-Leitlinie der Mustermann GmbH 147
Anlage 5: Definitionen für die Schutzbedarfskategorien vom BSI-Standard 200-2 151
Anlage 6: IS-Richtlinie für IT-Systeme 153

Anlage 7: Risikoeinstufung BSI 200-3 156
Anlage 8: IS-Richtlinie für Störungen und Ausfälle 158
Verzeichnis der Abkürzungen 160
Selbstständigkeitserklärung 161
Thesen 162

1 Einleitung

1.1 Entstehung Business Continuity Management

Der Ursprung des Business Continuity Management (BCM) geht auf den chinesischen General Sun Tzu und sein Buch „Die Kunst des Krieges, Standardwerk der Strategie“ zurück, das ca. 500 v. Chr. veröffentlicht wurde [1]. BCM bei Sun Tzu wird mit Aussagen, wie „Sei auf das Schlimmste vorbereitet!” [1] und „If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” [2] abgeleitet. Da bei militärischen Operationen immer mit Störungen durch den Feind zu rechnen ist, sind robuste Pläne und gut geplante Ausweichoptionen unerlässlich, um sein Ziel zu erreichen [3, p. 16] [1].

Das Konzept wurde über die Jahrhunderte verbessert und weiterentwickelt und später auf andere Bereiche übertragen, z.B. 1950 auf die Zivilverteidigung und den Katastrophenschutz in den USA. Es folgten besonders gefährdete Organisationen wie Kernkraftwerke und Chemieanlagen. Der aktuell letzte Entwicklungsschritt war die Ausdehnung des zunächst im IT-Bereich etablierten BCM auf das gesamte Unternehmen. Damit wurde auch die Entwicklung von Standards und Normen vorangetrieben [1]. Die zeitliche Entwicklung wird in Bild 1 optisch dargestellt.

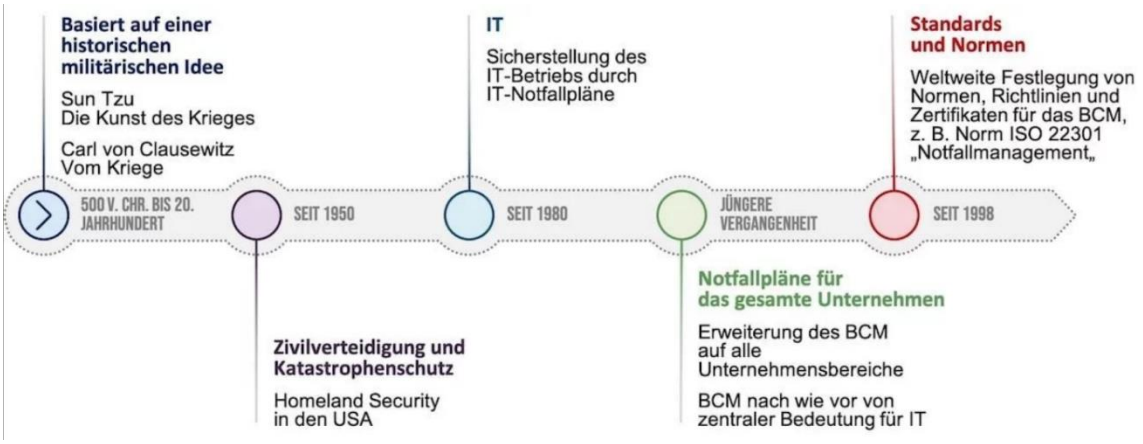

Bild 1: Zeitstrahl BCM-Entstehung [1]

1.2 Gründe für BCM

Die Anzahl der IT-Sicherheitsvorfälle nimmt jährlich zu und 2021 waren bereits 86 Prozent der deutschen Unternehmen von Schäden durch IT-Sicherheitsvorfälle betroffen [4]. Zudem wurde im Jahr 2022 erstmals der Katastrophenfall aufgrund eines IT-Sicherheitsvorfalles ausgerufen und für 207 Tage aufrechterhalten [5]. Im Oktober 2022 kam es zu einem Cyberangriff auf die Verwaltung des Rhein-Pfalz-Kreises, bei dem rund 11.000 Datensätze mit einem Volumen von 100 Gigabyte entwendet wurden. Ein Abfluss weiterer Daten konnte den Angaben zufolge schnell gestoppt werden. Allerdings rechnet die Verwaltung des Rhein-Pfalz-Kreises erst zwischen Mai und Juli 2023 mit einem Normalbetrieb [6]. Diese Beispiele zeigen, dass die Bedrohung für IT-Dienste stetig zunimmt. Gleichzeitig herrscht die gängige Meinung, dass eine hundertprozentige Sicherheit nicht möglich bzw. zu teuer und nicht praxistauglich ist [7] [8] [9] [10]. Daher muss immer mit dem Versagen von Sicherheitsmaßnahmen und den damit verbundenen Risiken gerechnet werden. Ab dem Punkt, an dem diese Bedrohungen das Überleben des Unternehmens gefährden, bietet BCM Strategien zur Überlebenssicherung [11] [12] und im Bereich der IT wird dies durch IT-Service Continuity Management (ITSCM) erfüllt. Die Relevanz von BCM und ITSCM wird durch die Umfrage, in Bild 2, der Controllit AG vom September 2020 zur Wirksamkeit von Notfallstrategien in Bezug auf Covid-19 verdeutlicht.

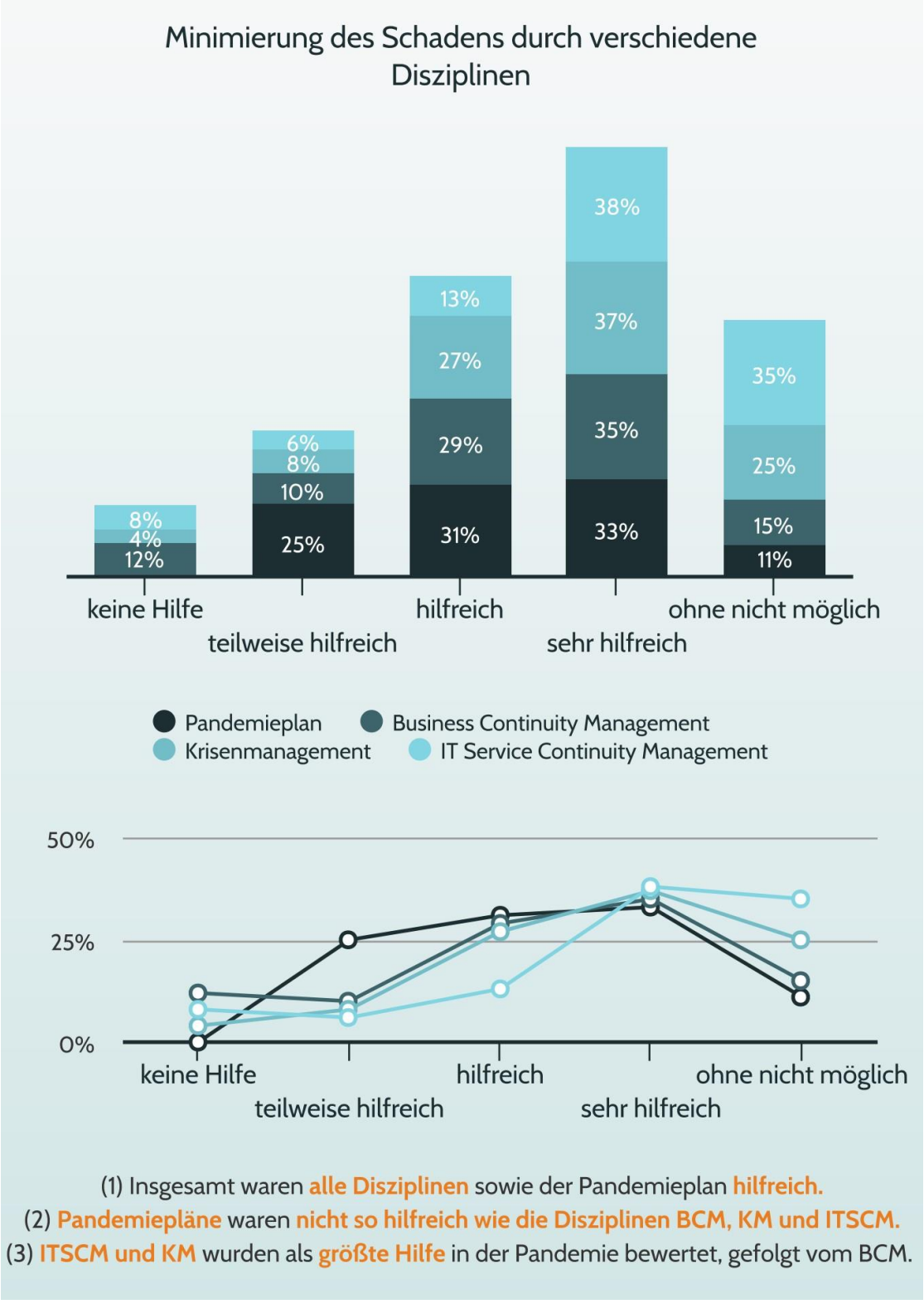

Bild 2: Umfrage zur Wirksamkeit von Notfallstrategien [13]

Hier wird deutlich, dass vor allem ITSCM bei dem Großteil der Unternehmen „sehr hilfreich“ bzw. „ohne nicht möglich“ gewesen wäre, die Krise zu bewältigen.

1.3 Forschungstand BCM

Die zunehmende Relevanz von BCM hat zu einer Reihe von nationalen und internationalen Normen geführt, bis schließlich 2012, mit der International Organization for Standardization (ISO) 22301, die erste ISO-Norm zu BCM veröffentlicht wurde.

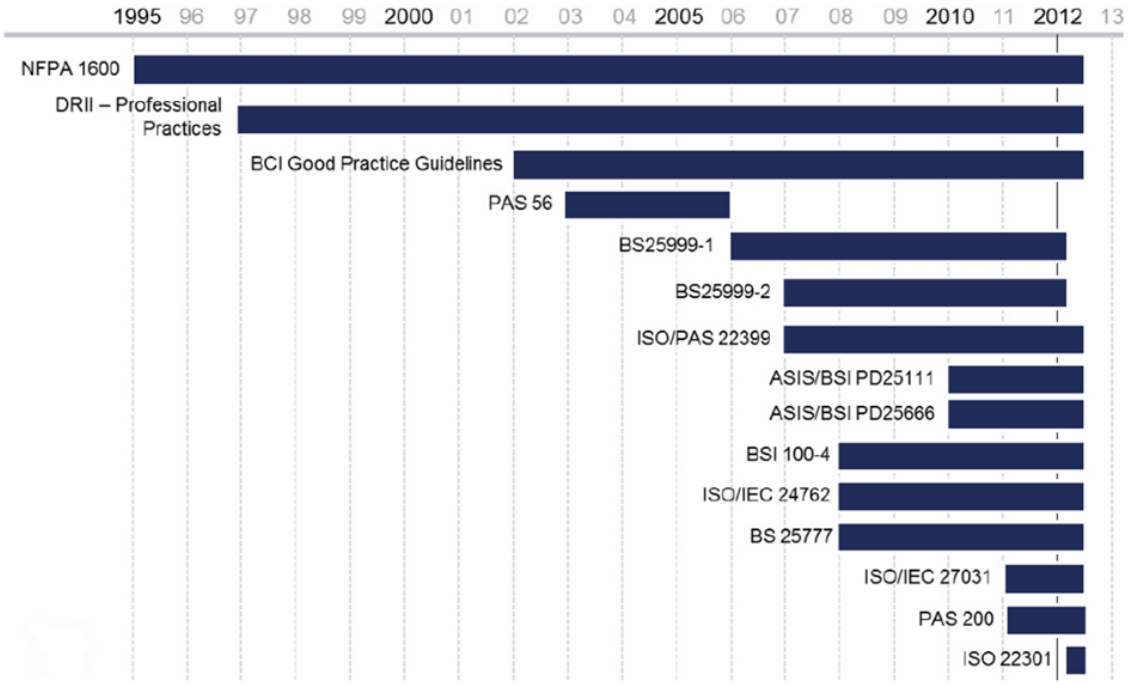

Bild 3: verschiedene Normen im zeitlichen Zusammenhang [14, p. 9]

Bild 3 stellt die Entwicklung dar, die zur Veröffentlichung der ISO 22301 geführt hat. Die ISO 22301 wurde kontinuierlich verbessert und aktualisiert und ist derzeit in der aktuellen Version ISO 22301:2019-10 mit Veröffentlichungsdatum Oktober 2019 gültig [15]. Für ITSCM ist in Bild 3 lediglich BS 25777 und ISO/IEC 27031 relevant, da diese die einzigen Richtlinien sind, die sich auf ITSCM spezialisiert haben. Der BS 25777 wurde 2008, vom British Standard Institute, veröffentlichte und im März 2011 durch die ISO/IEC 27031:2011-03 ersetzt [16]. Dies ist nach wie vor die aktuelle Version [17]. Beim BCM werden nicht nur die internationalen, sondern auch die nationalen Standards, laufend angepasst, z.B. vollzieht das Bundesamt für Sicherheit in der Informationstechnik (BSI) derzeit den Wechsel vom noch gültigen „BSI-Standard 100-4 Notfallmanagement“ zum „BSI-Standard 200-4 Business Continuity Management“, bei dem derzeit die Anmerkungen,

Kommentare etc. zum zweiten Community-Draft eingearbeitet werden [18]. Die BCM-Standards sind, aufgrund der allgemeinen Natur, sowie den grundlegend geschaffenen Strukturen und Prozessen zur Bewältigung von Krisen, langfristig gültig. Es darf jedoch nicht außer Acht gelassen werden, dass auf alle Entwicklungen, wie technologische, politische, wirtschaftliche etc., durch eine ständige Überprüfung der Bedrohungslage reagiert werden muss.

Beim ITSCM sieht der aktuelle Stand anders aus, da in der IT stetige Entwicklung stattfindet und somit auch neue Gefahren und Möglichkeiten ergeben, ist die ISO 27031 von 2011 technisch nicht mehr auf dem aktuellen Stand. Jedoch gibt es im Gegensatz zu BCM für ITSCM aktuell neben der ISO 27031 keine anderen Regelwerke. Meistens wird ITSCM als Teil eines BCM-Standards oder eines andern IT-Sicherheits-Standards erfasst [19] [20] [21] [22].

Gleichwohl stellt bereits BCM vor allem für kleine und mittlere Organisationen (KMO) eine Herausforderung dar. Dies liegt vermutlich an der Komplexität, den Kosten und dem Zeit- und Personalaufwand für die Implementierung [23].

2 Vorbetrachtung

2.1 Definitionen und Abgrenzungen

2.1.1 Definitionen

Business-Continuity-Management ist der Prozess zur Umsetzung und Verwaltung der Aufrechterhaltung der Betriebsfähigkeit [24, p. 8]

Aufrechterhaltung der Betriebsfähigkeit ist die Fähigkeit einer Organisation, die Lieferung bzw. Erbringung von Produkten und Dienstleistungen nach einer Störung innerhalb akzeptabler Zeiträume mit zuvor festgelegter Kapazität fortzusetzen [24, p. 8].

IT-Service-Continuity ist die Fähigkeit, einen Dienst ohne Unterbrechungen oder mit der vereinbarten Verfügbarkeit zu liefern. IT-Service Continuity Management kann ein Teil von BCM sein [25, p. 8]. Im Regelfall wird von ITSCM gesprochen.

Information and Communications Technology (ICT) Readiness for Business Continuity (IRBC) ist die Fähigkeit einer Organisation Geschäftsoperationen durch Verhindern, Erkennen, Reagieren und Wiederherstellen von ICT-Diensten zu unterstützen [26, p. 3]. IRBC und ITSCM können Synonym benutzt werden [19]. Der Begriff ITSCM wurde von der Information Technology Infrastructure Library (ITIL) geprägt und IRBC von der ISO 27031 [27]. In der weiteren Arbeit wird ITSCM verwendet, sofern es sich nicht um eine, aus einem Dokument, übernommene Kapitelüberschrift handelt.

Service-Management ist eine Kombination von Fähigkeiten und Prozessen, um die Aktivitäten und Ressourcen in Bezug auf Planung, Design, Änderung, Bereitstellung und Verbesserung von Diensten, zu steuern und zu kontrollieren, um einen Wert zu erzeugen [25, p. 9]. Im Regelfall wird von IT-Service Management (ITSM) gesprochen.

Informationssicherheit (IS) ist die Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Information im Normalbetrieb [28, p. 11]. Im Regelfall wird von einem Informationssicherheitsmanagementsystem (ISMS) gesprochen.

Information System Contingency Plan (ISCP) befasst sich mit der möglichst schnellen Wiederherstellung des Normalbetriebs von IT-Systemen, indem im Voraus detaillierte Pläne zur Systemwiederherstellung erstellt werden. Hierzu werden verschiedene Ausfallszenarien in Erwägung gezogen [29, p. 10].

Ein **Managementsystem** ist eine Reihe von zusammenhängenden und sich gegenseitig beeinflussenden Elementen einer Organisation, die zur Festlegung der Politik, der Ziele und der Prozesse (zur Erreichung dieser Ziele) dienen. Ein Managementsystem kann eine oder mehrere Disziplinen umfassen. Die Elemente des Systems umfassen die Struktur der Organisation, Rollen mit Verantwortlichkeiten, Planung, Betrieb usw. Der Anwendungsbereich eines Managementsystems kann die gesamte Organisation, bestimmte Funktionen der Organisation, bestimmte Bereiche der Organisation oder eine oder mehrere Funktionen in einer Gruppe von Organisationen umfassen [28, p. 12].

Ein **Informationssicherheitsereignis** ist ein erkannter Zustand eines Systems, Dienstes oder Netzwerkes, der auf eine mögliche Richtlinienverletzung, die Unwirksamkeit von Maßnahmen oder eine vorher nicht bekannte Situation hinweist, die sicherheitsrelevant sein kann [28, p. 11]. Im weiteren Verlauf nur Ereignis genannt, da man sich im Informationssicherheitskontext befindet.

Ein **Informationssicherheitsvorfall** ist ein einzelnes oder eine Reihe von unbeabsichtigten oder unerwarteten Informationssicherheitsereignissen, die mit hoher Wahrscheinlichkeit den Geschäftsbetrieb gefährden und die Informationssicherheit bedrohen [28, p. 12]. Im weiteren Verlauf nur Vorfall genannt, da man sich im Informationssicherheitskontext befindet.

Eine **Störung** ist ein geplantes oder ungeplantes Ereignis, das eine ungeplante, negative Abweichung von der erwarteten Lieferung von Produkten und Dienstleistungen, gemessen an den Zielen einer Organisation, verursacht [24, p. 16].

Notfall ist ein plötzlicher, dringender, normalerweise unvorhergesehener Vorfall oder ein Ereignis, das sofortiges Handeln erfordert; häufig handelt es sich um eine Störung oder einen Zustand, der zwar vorhergesehen wurde oder auf den man sich vorbereitet hat, der aber nicht genau vorhergesagt werden kann [24, p. 18].

Krise ist ein instabiler Zustand, bei dem eine abrupte oder deutliche Veränderung droht, die dringende Aufmerksamkeit und Maßnahmen erfordert, um Leben, Werte, Eigentum oder die Umwelt zu schützen [24, p. 14].

Katastrophe ist eine Situation, in der umfassende menschliche, materielle, wirtschaftliche oder ökologische Verluste eingetreten sind, welche die Fähigkeit der betroffenen Organisation, Gemeinschaft oder Gesellschaft überschreiten, sie mit den eigenen Ressourcen zu bewältigen und sich davon zu erholen [24, p. 16].

2.1.2 Abgrenzungen

Normalbetrieb und Notbetrieb: Der Normalbetrieb bezeichnet die Situation, der vollständigen und planmäßigen Funktionalität aller Prozesse im Unternehmen. Der Notbetrieb hingegen bezeichnet eine Situation, in der nur die wichtigsten Teilschritte eines Prozesses funktionieren oder der Prozess, zwar vollständig, aber mit einem geringeren Durchsatz erbracht wird. Der Notbetrieb muss somit die grundlegende Funktionalität der Organisation sicherstellen.

BCM und IS: Informationssicherheit konzentriert sich auf die Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen im Normalbetrieb. BCM konzentriert sich auf die Aufrechterhaltung der Verfügbarkeit und Integrität der Geschäftsoperationen im Notfall. Dabei können sich die Anforderungen an Verfügbarkeit und Integrität zwischen Normalbetrieb und Notfall unterscheiden [30, p. 22]. Es gibt allerdings Möglichkeiten Synergien zu nutzen, z.B. muss sowohl für das BCM als auch für die Informationssicherheit analysiert werden, welche Geschäftsprozesse welche Ressourcen benutzen, Maßnahmen zur Erhöhung der Verfügbarkeit können positive Auswirkungen für beide Bereiche haben etc. [30, pp. 20,21].

BCM und ITSCM: ITSCM wird meist als Teil eines BCM wahrgenommen [25, p. 8] [31] [30, pp. 20,23]. BCM ist der Prozess, der die zeitkritischen Geschäftsprozesse eines Unternehmens ermittelt und sicherstellt, dass diese im Ereignisfall weitergeführt werden können, jedoch werden für IT-Dienste nur manuelle Überbrückungsmaßnahmen geplant. Das ITSCM befasst sich mit der Aufrechterhaltung der Verfügbarkeit bzw. dem schnellstmöglichen Wiederanlauf von IT-Infrastrukturen, IT-Systemen oder -Anwendungen [32]. Es besteht, die Möglichkeit, dass ein Vorfall ein Notfall für BCM oder ITSCM ist, aber nicht für das andere Managementsystem, z.B. stellt der Ausfall eines redundanten Serversystems zwar einen ITSCM-Notfall dar, aber aufgrund der unterbrechungsfreien Verfügbarkeit des Dienstes kein BCM-Notfall [30, pp. 20,23]. Als Gegenbeispiel kann der Ausfall eines Lieferanten von Rohmaterialien ein BCM-Notfall sein, aber kein ITSCM-Notfall. ITSCM ist daher auf die IT-Dienste bezogen detaillierter und umfassender als BCM.

ITSCM und ITSM: ITSM umfasst den Normalbetrieb und plant auf dessen Basis Maßnahmen, um den IT-Dienst entsprechend den Anforderungen bereitzustellen bzw. den Prozess hinsichtlich Kosten, Zeit, Verfügbarkeit etc. zu optimieren [33]. ITSCM ist für das Notfallmanagement von IT-Systemen ausgelegt, um ein Minimum an Operabilität sicherzustellen und geregelt in den Normalbetrieb zurückzukehren. Gleichwohl können sich die Anforderungen ähnlich, wie zwischen BCM und IS auch hier unterscheiden. Somit werden zwar die gleichen Objekte betrachtet, jedoch mit verschiedenen Zielen, Anwendungszeitpunkten und Gefahren.

BCM und ISCP: BCM beschäftigt sich mit der Überlebensfähigkeit von Organisationen in Notfallsituationen, indem möglichst schnell eine minimale Betriebsfähigkeit wieder erreicht werden soll. Beim ISCP wird die minimale Betriebsfähigkeit nicht berücksichtigt, sondern es soll möglichst schnell die vollständige Funktionalität wieder erreicht werden [34]. ISCP kann, als Teil des BCM zu sehen sein [35].

ISCP und Disaster Revovery: ISCP unterscheidet sich von Disaster Revovery darin, dass die Systemwiederherstellung unabhängig von dem Ort bearbeitet wird [29, p. 10].

Risikomanagement und Kontinuitätsmanagement: Herr Dr. Klaus-Rainer Müller schreibt dazu in seinem Buch „IT-Sicherheit mit System: „Während das Risikomanagement von den Risiken sowie dem geforderten Risikoniveau ausgeht und der Risikostrategie entsprechend entscheidet, wie mit welchen Risiken umzugehen ist, geht das Sicherheits- und Kontinuitätsmanagement von den Sicherheits- und Kontinuitätsanforderungen und dem geforderten Sicherheits- und Kontinuitätsniveau aus. Für das Risikomanagement bildet indessen das Schadenspotenzial den Ausgangspunkt der Analyse, beim Sicherheits- und Kontinuitätsmanagement das Wertniveau. Sowohl das Risiko- als auch das Sicherheits- und Kontinuitätsmanagement identifizieren dann die Bedrohungen, denen das Objekt ausgesetzt ist, und deren Eintrittswahrscheinlichkeiten, um das Bruttorisiko bzw. die Bruttosicherheit zu ermitteln. Bei der weiteren Analyse fließen die ergriffenen Maßnahmen ein, um das Nettorisiko bzw. die Nettosicherheit zu ermitteln.“ [36, p. 217].

2.2 ISO 27031

Der ISO-Standard ISO/IEC 27031 „Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity“ in der „First edition“ vom 01.03.2011 [26, p. i] ist die einzige aktuelle Norm, die sich ausschließlich mit ITSCM befasst. Auf diesen Standard wird in der weiteren Ausarbeitung nicht direkt eingegangen, da die Unterlagen im Wesentlichen vorgeben, was umgesetzt werden soll, jedoch keine Ausarbeitung erfolgt, wie diese Vorgaben erreicht werden sollen. Vereinzelt werden Beispiele angeführt. So wird z.B. im Kapitel „6 IRBC Planning“ der ISO-Norm zum Thema Ressourcen nur geschrieben, dass die Organisation die notwendigen Betriebsmittel identifizieren und bereitstellen muss, um ein ITSCM zu etablieren und zu betreiben. Weiter heißt es, dass ein oder mehrere Verantwortliche für das BCM-System (BCMS) zu benennen sind und diese über die notwendigen Kompetenzen verfügen müssen. Es wird jedoch nicht ausgeführt, wie die benötigten Mittel ermittelt werden können und welche Qualifikationen die Personen benötigen [26, p. 9]. Im Unterkapitel „6.4 Determining IRBC Strategy Options“ [26, pp. 11-14] werden mögliche Notfallmaßnahmen für die erfassten

Objekte, wie Gebäude und Technik, genannt. Es wird jedoch nur darauf hingewiesen, dass in Abhängigkeit von der Gefährdung risikomindernde Maßnahmen ergriffen werden sollten. Es folgt eine Aufzählung von Beispielen ohne weiteren Kontext.

Da, wie in Kapitel 1.3 Forschungsstand BCM dargelegt, BCM bzw. ITSCM insbesondere für KMOs eine Herausforderung darstellt, sind Hinweise und Ausarbeitungen zur Umsetzung von BCM bzw. ITSCM unerlässlich. Die ISO 27031 stellt als internationale Norm dennoch einen wichtigen Baustein dar und eignet sich am besten als Checkliste, um eine vollständige Realisierung zu gewährleisten. Daher werden im Abschnitt 2.3 Auswahlkriterien basierend auf der ISO 27031 beschrieben. Die analysierten Verfahren werden anhand dieser Kriterien überprüft, um festzustellen, ob sie die Anforderungen der ISO 27031 erfüllen oder nicht.

2.3 Auswahlkriterien

Bevor auf die Auswahlkriterien eingegangen wird, ist darauf hinzuweisen, dass im Rahmen der Arbeit nur eine begrenzte Auswahl an Vorgehensweisen betrachtet werden kann. Obgleich die ausgewählten Vorgehensweisen im nächsten Kapitel nicht tiefergehend analysiert werden, erfolgt eine Auswahl von zwei Implementierungsmöglichkeiten, welche anschließend schematisch bearbeitet werden.

Bei der Auswahl der Normen erfolgte eine Orientierung an dem ISO Standard ISO/IEC 27031. Dieser definiert fünf Prinzipien, die zur Erfüllung von ITSCM eingehalten werden sollten. Die fünf Prinzipien sind [26, p. 5]:

1. „Incident Prevention“ - Vorfallprävention: Dabei wird sich mit dem Schutz von ICT-Diensten vor Umgebungsgefahren, Hardwareausfällen, Betriebsfehler, Hackerangriffen und Naturkatastrophen befasst, damit der gewünschte Grad an Verfügbarkeit eingehalten werden kann.
2. „Incident Detection“ – Vorfallerkennung: Vorfällen sollten so früh, wie möglich, erkannt werden, damit die Auswirkungen auf die Dienste reduziert werden, die Wiederherstellungsaufwand verringert wird und die Dienstqualität gehalten wird.

3. „Response“ – Reaktion: Es sollte angemessen auf Vorfälle reagiert werden, um die Ausfallzeit zu verringern und den Wiederherstellungsaufwand zu verringern. Des Weiteren wird durch eine angemessene Reaktion verhindert, dass ein Vorfall sich zur Katastrophe ausweitet.
4. „Recovery“ – Wiederherstellung: Auswahl und Durchführung einer angemessenen Wiederherstellungsstrategie stellt sicher, dass die Dienste innerhalb einer definierten Zeit wieder funktionieren und die Integrität der Daten erhalten bleibt. Hierbei wird im Regelfall zuerst ein Notbetriebsniveau und später die volle Funktionalität wieder erlangt. Außerdem hat eine Priorisierung der Dienste zu erfolgen, damit ein Fokus auf den kritischen Diensten liegt.
5. „Improvement“ – Verbesserung: Erfahrungen durch kleine und große Vorfälle sollten dokumentiert, analysiert und nachbearbeitet werden. Die Erfahrungen sollten zu einer besseren Vorbereitung auf, Kontrolle und Vermeidung von Vorfallen führen.

Die ISO 27031 registriert folgende sechs Objekte als Kernelemente für ein erfolgreiches ITSCM [26, p. 6]:

- „People“ – Mitarbeiter: Spezialisten, mit angemessenen Qualifikationen und Wissen, sowie kompetente Vertretung
- „Facilities“ – Einrichtung: physische Umgebung der ICT, wie Gebäude und Räume
- „Technology“ – Technologie:
    - Hardware: physische Komponenten (ausgenommen Netzwerkkomponenten)
    - Netzwerk: physische Netzwerkkomponenten, Konfiguration des Netzwerkes
    - Software: z.B.: Betriebssystem, Anwendungssoftware, Application Programming Interface
- „Data“ - Daten: alle Arten von Daten, wie Anwendungsdaten und Gesprächsdaten
- „Processes“ - Prozesse: Bezieht sich auf Dokumentation von Konfigurationsdaten, störungsfreier Betrieb, Wiederherstellung und Wartung von ICT Diensten
- „Suppliers“ – Lieferanten: Umfasst alle Leistungen, die von einem Dritten erbracht werden, aber für den ICT Dienst notwendig sind, z.B.: Internetprovider, Mobilfunk

Die Prinzipien des ISO 27031 Standrads werden im folgenden Stufen bewertet:

- nicht betrachtet: Das Auswahlkriterium wird in der Vorgehensweise gar nicht oder nur minimal betrachtet.
- kaum: Das Auswahlkriterium wird betrachtet, erfüllt aber nicht alle Punkte des ISO 27031.

- angemessen: Das Auswahlkriterium wird ausführlich betrachtet und alle Punkte des ISO 27031 werden erfüllt.
- detailliert: Das Auswahlkriterium wird ausführlicher als im ISO 27031 betrachtet.

Außerdem wird für die Kernelemente folgende Bewertungsangaben verwendet:

- Vollständigkeit:
    - vollständig: Für das Kernelement werden alle Prinzipien des ISO 27031 angewendet.
    - unvollständig: Für das Kernelement werden nicht alle Prinzipien des ISO 27031 angewendet.
    - Ausnahmen:
        - Verbesserung: Da dieser Prozess im Regelfall das Unternehmen als Ganzes war nimmt und nicht die einzelnen Elemente, wird es nicht von den Elementen benötigt, um „vollständig“ zu erreichen.
        - Personen: Hier ist im Regelfall nur eine Vorfallprävention möglich, somit muss nur diese für „vollständig“ erreicht werden.
- Detailgrad:
    - nicht betrachtet: Das Kernelement wird nicht betrachtet
    - kaum: Das Kernelement wird nur oberflächlich betrachtet.
    - angemessen: Das Kernelement wird ausreichend betrachtet.
    - detailliert: Das Kernelement wird ausführlich betrachtet.

Als weitere Auswahlkriterien wurde folgende Punkte festgelegt:

- Unternehmensgröße: Ist die Vorgehensweise unabhängig der Unternehmensgröße anwendbar? Anmerkung: Hier wurden die Angaben der Vorgehensweisen übernommen.
- Branchen-Unabhängigkeit: Ist die Vorgehensweise unabhängig der Branche anwendbar? Anmerkung: Es wurden die Angaben der Vorgehensweisen übernommen.
- Technologieunabhängigkeit: Ist die Vorgehensweise neutral gehalten und kann auf jede Technologie angewendet werden, z.B. Windows, Linux, MacOS
- Zertifizierung: Besteht die Möglichkeit, die Verwirklichung der Vorgehensweise zu zertifizieren?
- Umfang: Welchen Umfang besitzt die Richtlinie?
- Veröffentlichung: Wann wurde die Vorgehensweise veröffentlicht. Diese stellt die Aktualität des Standards dar.
- Konzipiert für: Für welche Disziplin wurde die Vorgehensweise ursprünglich konzipiert?
- konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge: Wie detailliert sind die Anforderungen bzw. Vorschläge? Derweil wird angenommen, dass detaillierte Vorschläge besser sind, sofern diese optional sind. Dies

ist damit begründet, dass keine eigene Recherche betrieben werden muss, wie die Anforderung erreicht werden kann. Wenngleich es wichtig ist, dass die Vorgaben nicht zwingend umgesetzt werden müssen, damit die Möglichkeit für passendere Optionen vorhanden bleibt.

- Risikobewertung /Priorisierung: Wie oben genannt, muss eine Priorisierung der ICT Dienste satt finden.
- Preis: Wie viel kosten die Vorgehensweise?

3 Übersicht und Begründung für die Auswahl der Vorgehensweisen

In Tabelle 1 werden die Ergebnisse der nicht tiefergehenden Betrachtung von elf Vorgehensweisen der Kategorien BCM, ISMS, ITSM, ISCP und IS in Bezug auf Verwendbarkeit als ITSCM-Methode dargestellt. Anschließend werden in den Unterkapiteln die Ergebnisse aufgearbeitet präsentiert.

Tabelle 1: Übersicht Ergebnisse des Vergleichs

Bezeichnung des Standards / Kriterien	BSI 200-4	NIST CSF	NIST SP 800-53	NIST SP 800-34	VdS 10000	ITIL	FitSM	Good Practice Guidelines 2018	COBIT	CISIS12	NFPA 1600
Prinziepien von ITSCM											
Vorfallprävention	nicht betrachtet	detailliert	detailliert	detailliert	angemessen	nicht betrachtet	angemessen	angemessen	detailliert	detailliert	kaum
Vorfallerkennung	detailiert	detailliert	detailliert	nicht betrachtet	angemessen	angemessen	kaum	nicht betrachtet	detailliert	detailliert	nicht betrachtet
Reaktion	detailiert	detailliert	detailliert	nicht betrachtet	angemessen	angemessen	kaum	kaum	detailliert	nicht betrachtet	kaum
Wiederherstellung	detailiert	kaum	detailliert	detailliert	kaum	nicht betrachtet	nicht betrachtet	detailliert	detailliert	kaum	detailliert
Verbesserung	detailiert	angemessen	nicht betrachtet	angemessen	angemessen	angemessen	angemessen	detailliert	kaum	angemessen	detailliert
Elemente von ITSCM											
Mitarbeiter	vollständig - angmessen	vollständig – kaum	vollständig – detailliert	vollständig – kaum	vollständig – angemessen	vollständig - kaum	nicht betrachtet	vollständig - detailliert	vollständig - detailliert	vollständig - detailliert	vollständig - kaum
Einrichtungen	unvollständig – kaum	nicht betrachtet	vollständig – detailliert	unvollständig – kaum	unvollständig - kaum	nicht betrachtet	unvollständig - kaum	nicht betrachtet	unvollständig - kaum	unvollständig – detailliert	unvollständig – kaum
Technologie - Hardware - Netzwerk - Software	unvollständig – kaum	vollständig - kaum	vollständig – detailliert	unvollständig – angemessen	vollständig – angemessen	nicht betrachtet	unvollständig - kaum	nicht betrachtet	vollständig - detailliert	unvollständig – detailliert	unvollständig – kaum
Daten	unvollständig – kaum	unvollständig – kaum	unvollständdig - angemessen	unvollständig – kaum	unvollständig - kaum	nicht betrachtet	unvollständig - kaum	nicht betrachtet	unvollständig - angemessen	unvollständig – kaum	unvollständig – kaum
Prozesse	unvollständig - kaum	unvollständig - kaum	vollständig - detailliert	unvollständig – kaum	vollständig - angemessen	vollständig - angemessen	vollständig – angemessen	vollständig – angemessen	vollständig - detailliert	vollständig – detailliert	unvollständig – kaum
Lieferanten	unvollständig – kaum	unvollständig – kaum	vollständig – detailliert	nicht betrachtet	unvollständig – angemessen	unvollständig - kaum	nicht betrachtet	nicht betrachtet	vollständig - detailliert	unvollständig – detailliert	unvollständig – kaum
Priorisierung	vorhanden	nicht betrachtet	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden
Allgemein:											
Unternehmensgröße	jede	jede	jede	jede	KMO	jede	jede	jede	keine Angabe	KMO	jede
Branche	jede	jede	jede	jede	jede	jede	jede	jede	keine Angabe	jede	jede
Technologieunabhängig	ja	ja	zum Großteil	ja	ja	ja	ja	ja	ja	ja	ja
Zertifizierung	nach ISO 22301:2019 möglich	nein	nein	nein	durch VdS	einzelne Personen sind zertifizierbar	nein	nein	nein	ja	möglich
Umfang	234 Seiten + 576 Anforderungen	55 Seiten	492 Seiten	129 Seiten	43 Seiten	260 Seiten	87 Seiten	108 Seiten	326 Seiten	1072 Seiten	97 Seiten
Veröffentlichung	Entwurfsphase aktulle Version Community Draft 2; August 2022	16.04.2018	12.10.2020	Mai 10	01.12.2018	Feburar 2019	14.06.2016, teilweise 17.08.2022 aktualisiert	08.11.2017	eng.:Dezember 2018 deut.: Dezember 2020	01.06.2021	05.11.2018
Konzipiert für	BCM	IS	IS	ISCP	ISMS	ITSM	ITSM	BCM	Unternehmensstrategie	ISMS	BCM
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	konkret, teilweise Zwang	allgemein	konkret	allgemein	konkret, teilweise Zwang	keine	allgemein	allgemein	zum Teil: allgemeine zum Teil: konkret	allgemein	allgemein
Preis	kostenlos	kostenlos	kostenlos	kostenlos	83,18 €	85,00 €	kostenlos	30,00 £ ~ 35,00 €	kostenlos	150,00 € Behörden kostenlos	11,99$ pro Monat 84,00$ einmalig

In Anlage 1: „Übersicht Ergebnisse des Vergleichs“, wird die Tabelle aufgeteilt, aber größer dargestellt.

3.1 BSI-Standard 200-4 Business Continuity Management – Community Draft

Das BSI, gegründet am 1. Januar 1991, ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. Um seinen Auftrag nachzukommen, stellt das BSI verbindliche Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen auf, erstellt verbindliche Sicherheitsstandards für die Beschaffung und den Einsatz von IT für Bundesbehörden darüber hinaus ist es Ansprechpartner und Berater in allen Fragen der Informationssicherheit für natürliche Personen sowie juristische

Personen [37]. Im Rahmen seiner Aufgaben hat das BSI den BSI-Standard 100-4 Notfallmanagement im Jahr 2006 veröffentlicht [38] und ist aktuell in der Entwicklung des Nachfolgestandards „BSI-Standard 200-4 Business Continuity Management“, der einen Anforderungskatalog (bei der Quellenangabe entspricht „p“ dabei Zeilen) besitzt [18].

Die Vorfallprävention wird indirekt im Abschnitt „8 Soll-Ist-Vergleich (R+AS)“ aufgegriffen, allerdings nur in dem Rahmen, dass bereits vorhandene Maßnahmen erfasst werden und geprüft wird, ob damit die wirkliche Wiederanlaufzeit (wWAZ) unter der geforderten Wiederanlaufzeit (gWAZ) liegt.

Für die Vorfallerkennung wird im Abschnitt „5.2. Detektion, Alarmierung und Eskalation (R+AS)“ ein Prozess etabliert, der alle Aspekte der ISO 27031 erfüllt und ausführlich auf den Meldeweg und die Eskalationsstufen eingeht. Ergänzt wird der Abschnitt, insbesondere durch die Anforderungen des Katalogs. Somit ist der BSI 200-4 hier detaillierter als die ISO 27031.

Reaktionsmaßnahmen werden im Abschnitt „5.3. Definition von Sofortmaßnahmen (R+AS)“ mit Beispielen abgebildet und alle Aspekte der ISO 27031 erfüllt, zugleich wird auch auf evtl. bereits bestehende Sofortmaßnahmen, z.B. aus dem Brandschutz, hingewiesen. Dieser Abschnitt wird durch die Anforderungen des Katalogs und dem Kapitel „11 Geschäftsfortführungsplanung (R+AS)“ ergänzt. Damit ist der BSI 200-4 hier detaillierter als die ISO 27031.

Für die Wiederherstellung wird im Abschnitt „11 Geschäftsfortführungsplanung (R+AS)“ auf das Erreichen des Notbetriebsniveaus eingegangen. Dies wird im Kapitel „12 Wiederanlauf- und Wiederherstellungsplanung (AS)“ ausgebaut und um den Aspekt des Wiederherstellens des Normalbetriebs ergänzt. Simultan werden alle Aspekte der ISO 27031 erfüllt, und mit ausführlichen Umsetzungshilfen erleichtert. Ergänzt wird der Abschnitt durch die Anforderungen des Katalogs. Somit ist die BSI 200-4 hier detaillierter als die ISO 27031.

Für die Verbesserung wird im Abschnitt „15 Aufrechterhaltung und Verbesserung (R+AS)“ ein Prozess etabliert, der alle Aspekte der ISO 27031 erfüllt. Der

Abschnitt wird durch die Anforderungen des Katalogs ergänzt. Die BSI 200-4 beschreibt die Verbesserung somit ausführlicher als die ISO 27031. Daraus ergibt sich folgendes Gesamtbild:

- Vorfallprävention: nicht betrachtet [30, p. 142]
- Vorfallerkennung: detailliert [30, pp. 75-82] [39, pp. 128-177]
- Reaktion: detailliert [30, pp. 83,84,165-178] [39, pp. 178-182]
- Wiederherstellung: detailliert [30, pp. 165-186] [39, pp. 359-391]
- Verbesserung: detailliert [30, pp. 224-230] [39, pp. 557-577]

Der BSI Standard 200-4 beinhaltet alle Elemente des ITSCM. Bei Mitarbeitern wird insbesondere auf die Eigenschaften der Beschäftigten mit besonderen Rollen eingegangen, sowie deren Aufgabe im BCM, allgemeine Sensibilisierungen und Schulungen für alle Angestellten. Dabei wird sogar ein Beispiel für die Erkennung eines Personalmangels gegeben.

Einrichtungen und Technologie werden vor allem in Beispielen erwähnt, aber es wird sich nicht einzeln mit den Objekten befasst.

Daten spielen vor allem im Rahmen des Maximal tolerierbaren Datenverlustes (MTD) eine Rolle, der für alle Geschäftsprozesse und damit verbundenen IT-Systemen definiert werden muss. Die Daten werden kaum direkt behandelt.

Da der BSI 200-4 die IT-Systeme nicht ausführlich inspiziert, sind keine spezifischen Prozesse zur Dokumentation von Konfigurationsdateien oder zur Wartung vorhanden. Auch die Prozesse zur Reaktion und Wiederherstellung sind nur indirekt für IT auslegbar, die IT ist aber als eine der Ressourcenkategorie immer ein Teil davon. Da das Dokument aktuell keine Präventionsmaßnahmen enthält, ergibt sich daraus:

- Mitarbeiter: vollständig – kaum [30, pp. 44,64,65,70-74,79,94,125]
- Einrichtung: unvollständig – kaum [30, pp. 125,142,171-172]
- Technologie: unvollständig – kaum [30, pp. 79,125,171]
- Daten: unvollständig – kaum [30, pp. 115,125] [39, p. 301]
- Prozesse: unvollständig – kaum [30, pp. 83,84,165-186]
- Lieferanten: unvollständig – kaum [30, pp. 79,125,142]

Im Abschnitt „7 Business Impact Analyse (R+AS)“ [30, pp. 114-140] wird die Priorisierung der Prozesse vorgenommen.

Die kostenfreie [18] und technologieunabhängige Norm ist für jede Unternehmensgröße und Branche anwendbar [30, p. 9]. Die Richtlinie kann in den drei Ausprägungen „Reaktiv-BCMS“, „Aufbau-BCMS“ und „Standard-BCMS“ angewendet werden. Allerdings ist das „Standard-BCMS“ die umfassendste Variante und kann nach ISO 22301 zertifiziert werden [30, pp. 9,10]. Der aktuelle Entwurf vom August 2022 [18] umfasst derzeit 236 Seiten und 576 konkrete Anforderungen, die teilweise zwingend für einen zertifizierten Abschluss nachzuweisen sind.

Trotz der fehlenden Präventionsmaßnahmen wird der BSI 200-4 in Kapitel „4.1 Ausarbeitung BSI 200-4“ ausführlicher bearbeitet, da die anderen Prinzipien beschrieben sind und detaillierte Realisierungshilfen bereitgestellt werden. Zusätzlich spricht die Aktualität für eine nähere Betrachtung.

3.2 National Institute of Standards and Technology

Das National Institute of Standards and Technology (NIST) wurde 1901 zur Steigerung der industriellen Konkurrenzfähigkeit der USA gegründet. Um dieses Ziel zu erreichen, förderte und standardisierte das NIST technologische Innovationen. Als Auftrag der NIST definiert die Institution selbst, die Innovationsfähigkeit und Konkurrenzfähigkeit der U.S. durch Voranbringen der Transformation von metrischen Einheiten für U.S.-Unternehmen [40], Standards und Technologien zu steigern und die wirtschaftliche Sicherheit und Lebensqualität zu erhöhen [41].

3.2.1 Framework for Improving Critical Infrastructure Cybersecurity

Das Framework for Improving Critical Infrastructure Cybersecurity (CSF) ist ein Sicherheitsstandard des NIST, der seit dem 16.04.2018 mit der aktuell gültigen Versionsnummer 1.1 veröffentlicht ist [42, p. i]. Derzeit arbeitet das NIST an der neuen Version 2.0 [43]. Das CSF ist prinzipiell für alle Unternehmensgrößen und Branchen adaptierbar. Der Fokus liegt jedoch auf Unternehmen der kritischen Infrastruktur [42, p. V]. Das CSF wurde als technologieunabhängige Vorgehensweise entwickelt [42, p. 2]. Eine Zertifizierungsmöglichkeit für das CSF

ist nicht vorhanden.

Das CSF berücksichtigt alle relevanten Aspekte des ITSCM. Diese werden durch die sogenannten „Framework Functions“ abgebildet. Die fünf Funktionen sind:

1. „Identify“ – Dabei soll ein grundlegendes Verständnis für IT-Sicherheitsrisiken geschaffen werden, damit diese identifiziert und eingeschätzt werden können.
2. „Protect“ – In diesem Schritt sollen Sicherheitsmaßnahmen eingerichtet werden, die die Wahrscheinlichkeit oder die Auswirkungen eines IT-Sicherheitsrisikos verringern.
3. „Detect“ – Die Funktion stellt sicher, dass IT-Sicherheitsereignisse rechtzeitig erkannt werden.
4. „Respond“ – Hier wird die Entwicklung von Maßnahmen zur Eindämmung von Sicherheitsereignissen vorgenommen.
5. „Recover“- Im letzten Schritt werden Wiederanlaufpläne erstellt, damit die IT-Dienste zeitnah wieder zur Verfügung stehen.

Darüber hinaus ist ein Prozess zur kontinuierlichen Optimierung des Sicherheitsprozesses zu implementieren.

Die „Framework Functions“ lassen sich auf die ITSCM-Prinzipien übertragen, wobei sich die Vorfallprävention aus „Protect“ und teilweise aus „Identify“ zusammensetzt. Der wesentliche Teil des Dokuments, ist ein Anforderungskatalog am Ende des Dokuments, der jedoch keine Umsetzungshilfen bietet, sondern auf weitere Referenzdokumente verweist. Allerdings ist dieser Anforderungskatalog ausführlicher als die ISO 27031. Damit ergibt sich folgendes Gesamtbild:

- Vorfallprävention: detailliert [42, pp. 7,25,28-33.36]
- Vorfallerkennung: detailliert [42, pp. 7,37-40]
- Reaktion: detailliert [42, pp. 8,41-43]
- Wiederherstellung: kaum [42, pp. 8,43]
- Verbesserung: angemessen [42, pp. 14,15,42,43]

Mitarbeiter werden nur kurz erwähnt. Nebenbei wird als Anforderung genannt, dass die Angestellten geschult und trainiert sein sollten, sowie ihre Rolle verstehen müssen. Als ergänzende Anforderung wird lediglich genannt, dass IS bei der Personaleinstellung z.B. in Form von Sicherheitsüberprüfungen zu beachten ist.

Einrichtungen werden lediglich in Zusammenhang mit Zutrittskontrollen und Überwachungen der physischen Umgebung indirekt erwähnt.

Mit der Technologie wird sich, über den gesamten Anforderungskatalog im Anhang verteilt, vollständig auseinandergesetzt, jedoch erfolgt auch hier außer der Nennung von Anforderungen keine ausführlichere Ausarbeitung.

Daten werden fast gar nicht erfasst, z.B. wird in Bezug auf Daten sinngemäß geschrieben „Daten sind geschützt“ [42, p. 32]. Darüber hinaus wird nur geschrieben, dass Backups vorhanden sein sollen und funktionieren sollen.

Prozesse werden über das Gesamtdokument hinweg etabliert. Für das ITSCM sind derweil insbesondere der Schutzprozess, der Erkennungsprozess und der Wiederherstellungsprozess im Anhang relevant. Diese werden aber nur genannt werden.

Lieferanten werden im Anhang im Punkt „Supply Chain Risk Management“ betrachtet. Jedoch wird im Wesentlichen nur darauf hingewiesen, dass IS-Maßnahmen und Wiederherstellungsmaßnahmen mit dem Lieferanten festgehalten sein sollten. Zudem wird bei der Erkennung aufgerührt, dass die Leistungserbringung überwacht werden soll. Für die Objekte des ITSCM ergeben sich folgende Werte:

- Mitarbeiter: vollständig – kaum [42, pp. 31,35]
- Einrichtungen: nicht betrachtet [42, pp. 29,30,39]
- Technologie: vollständig – kaum [42, pp. 24,29,30,37,38,39,42,43]
- Daten: unvollständig – kaum [42, pp. 32, 34].
- Prozesse: unvollständig – kaum [42, pp. 4,7,9-11,28,33,34,40,43]
- Lieferanten: unvollständig – kaum [42, pp. 16,28,29,39]

Das CSF ist mit 55 Seiten zwar kompakt, dies führt aber zu allgemeinen Anforderungen und Verweisen auf weiterführende Literatur, für ausführlichere Informationen [42, pp. 22-45]. Somit wäre ein erheblicher additionaler Rechercheaufwand erforderlich, um detaillierte Informationen zu erhalten. Darüber hinaus wird eine Priorisierung, der kritischen Systeme, als vorhanden vorausgesetzt [42, p. 14]. Aus den genannten Gründen wird auf eine detailliertere Ausführung des CSF verzichtet.

3.2.2 Security and Privacy Controls for Information Systems and Organizations

Die Security and Privacy Controls for Information Systems and Organizations (NIST SP: 800-53r5) ist eine Sammlung von Vorgaben der NIST, die weitgehend technologie- und branchenunabhängig [44, p. 16] das IT-Sicherheitsniveau von Unternehmen jeder Größe [44, p. 2] , erhöhen sollen. In der aktuellen Version vom 12.10.2020 lassen sich einige Anforderungen der ISO 27001 auf die NIST SP: 800-53r5 abbilden [45]. Parallel ist auf die genaue Zuordnung der Anforderungen zu achten, da die Anforderungen des ISO 27001 teilweise durch mehrere Anforderungen des NIST SP: 800-53r5 erfüllt werden. Allerdings werden nicht alle Anforderungen des ISO 27001 abgedeckt, so dass eine Zertifizierung nicht möglich ist [45].

Zunächst wird in dem Dokument die Grundlagen der Vorgehensweise erläutert. Anschließend folgt eine Anforderungsliste mit Diskussionsabschnitt, die entweder den Grund, zusätzliche Informationen, Realisierungshilfen oder Bewertungen beinhalten.

Der NIST SP: 800-53r erfüllt alle Prinzipien des ITSCM. Während über das gesamte Dokument verteilt Anforderungen an präventive Maßnahmen gestellt werden, sind diese meistens nach der IT-Systemart unterteilt.

Ebenso werden in allen Bereichen Anforderungen an die Erkennung von Sicherheitsvorfällen gestellt, dies erfolgt im gleichen Schema, wie die Vorfallprävention.

Der Reaktion auf Sicherheitsvorfälle wird ein eigenes Kapitel gewidmet. Dabei werden alle Aspekte der Reaktion, wie Planung, Training, Testen, eigentliche Vorfallbehandlung, Dokumentation und Meldung des Vorfalls abgedeckt.

Der Wiederanlaufplanung ist ebenso ein eigenes Kapitel gewidmet. Es umfasst ebenfalls alle Anforderungen des ITSCM und besitzt eigene Unterpunkte, für z.B. System Backup [44, pp. 125-127]

Auf die kontinuierliche Verbesserung wird nur im Rahmen eines

Beschwerdemanagements zur IT-Sicherheit eingegangen. In der Gesamtschau ergibt sich damit folgendes Bild:

- Vorfallprävention: detailliert; z.B. für Speichermedien [44, pp. 171-178]
- Vorfallerkennung: detailliert; z.B. Denial of Service Schutz [44, pp. 296-300]
- Reaktion: detailliert [44, pp. 149-161]
- Wiederherstellung: detailliert [44, pp. 116-130]
- Verbesserung: nicht betrachtet [44, p. 217]

Alle fünf Elemente des ITSCM werden berücksichtigt. In Bezug auf das Personal werden die Sensibilisierung und Schulung sowie die Sicherheitsanforderungen an das Personal berücksichtigt, nicht jedoch die Eignung des Personals für die jeweilige Position.

Einrichtungen werden als physischer Umgebungsschutz wahrgenommen. Dazu wird von Zugangskontrolle über Kabel und Stromversorgung alle Sicherheitsaspekte betrachtet. Unterdessen wird stets auch auf Erkennung von Ereignissen geachtet und mit alternativen Arbeitsstätten auch auf Redundanz eingegangen.

Anforderungen an Technologie und Daten sind über das gesamte Dokument verteilt. Dennoch wird insgesamt umfassend auf Hardware, Netzwerk und Software eingegangen.

Die Implementierung eines Prozesses wird bei fast jedem Anforderungspunkt genannt. Für das ITSCM ist bei alldem das Konfigurationsänderungsmanagement, Reaktionsmanagement und die Wartung am relevantesten. Die Wartung erhält bei der NIST SP: 800-53r in Form von „Maintanance“ ein eigenes Kapitel.

Die Softwarelieferanten werden in einem eigenen Kapitel vollständig und detailliert behandelt. Daraus ergibt sich:

- Mitarbeiter: vollständig – detailliert [44, pp. 59-64,222-228]
- Einrichtungen: vollständig – detailliert [44, pp. 179-193]
- Technologie: vollständig – detailliert; z.B. [44, pp. 292-362]
- Daten: unvollständig – angemessen; z.B. [44, pp. 97,116,121,122,125]
- Prozesse: vollständig – detailliert [44, pp. 110,111,152,153,162-170]
- Lieferanten: vollständig – detailliert [44, pp. 363-373]

Es erfolgt eine Priorisierung der Objekte auf Basis einer Risikobewertung [44, pp. 238-248], allerdings werden hier direkt die IT-Systeme und die damit verarbeiteten Daten gesichtet. Im Vergleich zu den anderen Ansätzen wird nicht der Prozess bewertet, der das ermittelte Risiko auf die benötigten Ressourcen überträgt. Daher ist dieser Ansatz für ein BCM eher unüblich. Insbesondere an dem Kapitel „PHYSICAL ACCESS CONTROL“, wird deutlich, dass der Standard, trotz der Angabe für alle Organisationen geeignet zu sein, eher für große bzw. hochsicherheitsrelevante Organisationen gedacht ist, z.B. Wachpersonal, physische Blockaden, wie hydraulische Fahrzeugsperren, und alternative Arbeitsstätten [44, pp. 182,191]. Außerdem ist die Ausrichtung auch auf U.S.-amerikanische Behörden konzentriert, vgl. z.B. [44, p. 168].

Die NIST SP: 800-53r5 wird im Weiteren, auf Grund des Fokus auf hochsicherheitsrelevante Organisationen und auf die USA, nicht weiter ausgearbeitet.

3.2.3 Contingency Planning Guide for Federal Information Systems

Die Richtlinie Contingency Planning Guide for Federal Information Systems (NIST SP:800-34) beschäftigt sich mit der Notfallplanung für Bundesbehörden in den USA [29, p. 2], soll aber auch branchen- und größenunabhängig Vorgaben für grundlegende Sicherheit bieten [29, p. 1]. Für die aktuelle Fassung vom Mai 2010 [29, p. Deckblatt 2] ist keine Zertifizierungsmöglichkeit vorhanden.

Das Dokument behandelt die Prävention vor allem in Bezug auf Backups, alternative Arbeitsstätten und Ersetzen von Ausstattung.

Detektion wird lediglich in Zusammenhang mit präventiven Maßnahmen kurz erwähnt.

Die Vorgaben zur Reaktion auf Sicherheitsvorfällen werden kurz behandelt, wobei der Fokus auf den Benachrichtigungsmechanismus der relevanten Personen im Notfall abzielt. Maßnahmen zur Eindämmung des Vorfalles werden nicht genannt.

Der Ablauf der Wiederanlaufphase wird detailliert in dem Kapitel „Recovery

Phase“ festgehalten und gibt skizzenhaft alle zu beachtenden Schritte der Phase an. Im Verlaufe dessen wird ein Fokus auf den abschließenden Funktionstest der Wiederherstellungsphase gelegt.

Kontinuierliche Überprüfung und Verbesserung sollen durch intensives Testen, Trainieren und Anpassen erreicht werden. Das Ergebnis für NIST SP:800-43 ist:

- Vorfallprävention: detailliert [29, pp. 19-25,44-58]
- Vorfallerkennung: nicht betrachtet [29, p. 19]
- Reaktion: nicht betrachtet [29, pp. 27,36-39]
- Wiederherstellung: detailliert [29, pp. 39-42]
- Verbesserung: angemessen [29, pp. 27-31]

Bezüglich des Personals wird erwartet, dass die Verantwortlichkeiten bekannt sind, eine Grundsensibilisierung vorhanden ist und das Personal für die entsprechenden Positionen qualifiziert ist, was aus dem Punkt „Plan Testing, Training, and Exercises“ herauszulesen ist.

Bei den Einrichtungen geht es vor allem um Ausweichgebäude, es werden aber auch Beispiele für die Detektion, wie Rauchmelder, genannt.

Die Maßnahmen für die Technologie beziehen sich im Wesentlichen auf Backups und Redundanzen. Dies gilt auch für die Daten.

Prozesse zum Erreichen, der Umsetzung der Anforderungen sollen bei den meisten Kapiteln implementiert werden. Für ITSCM relevante Prozesse, wie Konfigurationsänderungsmanagement werden, aber nur erwähnt, ohne konkret ausgeführt zu werden.

Lieferanten werden vereinzelt erwähnt, aber es werden keine näheren Informationen zu diesen genannt. Somit ergibt sich insgesamt folgende Bewertung:

- Mitarbeiter: vollständig – kaum [29, pp. 26-28]
- Einrichtungen: unvollständig – kaum [29, pp. 19,21-24,46-48]
- Technologie: unvollständig – angemessen [29, pp. 23,46-58]
- Daten: unvollständig – kaum [29, pp. 21,44,45]
- Prozesse: unvollständig – kaum [29, pp. 24,27,28,44,49,50]
- Lieferanten: nicht betrachtet [29, p. 56]

Die Anforderungen sind allgemein gehalten und betreffen organisatorische Punkte, wie z. B. institutsinterne Sicherheitsrichtlinien und Wartungsverträge z.B. [29, pp. 24,25,E-1 - E-8]. Da die Richtlinie mehrere ITSCM-Prinzipien nicht erfasst und auf keines der Kernelemente im Detail eingeht, wird der Ansatz nicht weiter untersucht.

3.3 VdS-Richtlinien für die Informationsverarbeitung

Der Verband der Sachversicherer (VdS) Schadenverhütung GmbH ist eine 100-prozentige Tochtergesellschaft des Gesamtverbandes der Deutschen Versicherungswirtschaft und wurde 1997 gegründet. Die VdS Schadenverhütung GmbH ist ein Dienstleister für Risikobeurteilungen, Prüfungen von Anlagen, Zertifizierungen von Produkten, Firmen und Fachkräften und bietet Bildungsangebote an. Zusätzlich berät die VdS Schadenverhütung GmbH zur Unternehmenssicherheit mit den Schwerpunkten Brandschutz, Security, Naturgefahrenprävention und Cyber-Security. Nach eigenen Angaben gehören alle DAX-Konzerne zum Kundenkreis [46]. Darüber hinaus ist die VdS Schadenverhütung GmbH u.a. zur Zertifizierung von Sicherheitsdienstleistern nach DIN EN ISO/IEC 17065 und von Managementsystemen nach DIN EN ISO/IEC 17021 berechtigt [47].

Die VdS-Richtlinien für die Informationsverarbeitung (VdS 10000) behandelt ISMS für KMOs und den gehobenen Mittelstand, Verwaltungen, Verbände und sonstige Organisationen. Die VdS 10000 ist seit dem 01.12.2018 gültig und kann von der VdS Schadenverhütung GmbH zertifiziert werden [48, p. 6]. Die VdS 10000 ist eine Vorgehensweise zur Implementierung eines ISMS und beinhaltet aufgrund der Überschneidungen zwischen ISMS und ITSCM auch Aspekte zur Geschäftskontinuität.

Die Anforderungen zur Vorfallvorsorge sind über die gesamte Richtlinie verteilt und zielen neben der Sicherstellung der Verfügbarkeit auch auf die Sicherstellung der Integrität und Vertraulichkeit ab. Indem ein Basisschutz definiert wird, der für alle IT-Systeme umzusetzen ist und bei kritischen IT-

Systemen erweitert wird, ist ein Minimum an Schutz sichergestellt.

Bei der Vorfallerkennung wird darauf hingewiesen, dass überwacht werden muss, ob sich kritische IT-Systeme im Regelbetrieb befinden. Hierzu sind einige Beispiele für Erkennungsmaßnahmen angegeben.

Bei der Reaktion werden einzelne Schritte aufgelistet, die bei der Durchführung beachtet werden sollten. Diese Schritte umfassen neben Schadenseindämmung und Nachbearbeitung, die für ITSCM am wichtigsten sind, auch Sicherung von Beweismittel.

Zur Wiederherstellung wird im Wesentlichen nur angegeben, dass Wiederanlaufpläne für kritische IT-Systeme zu erstellen sind.

Dass eine kontinuierliche Verbesserung stattfinden soll, wird nur in einem Satz erwähnt. Diese ist in der Anforderungsangabe für Prozesse hinterlegt. Dennoch werden Prozesse bei mehreren Schritten der VdS 10000 implementiert und somit eine weitreichende Grundlage für Verbesserungen geschaffen. Für ITSCM ist aber vor allem die Dokumentation und die Nachbearbeitung aus dem Reaktionsabschnitt relevant. Daraus folgt:

- Vorfallprävention: angemessen; z.B. [48, pp. 22-26,28,29,33-35]
- Vorfallerkennung: angemessen [48, pp. 26,27,38]
- Reaktion: angemessen [48, pp. 36,38]
- Wiederherstellung: kaum [48, p. 37]
- Verbesserung: angemessen [48, pp. 36,38,39]

Bei Mitarbeitern wird bei der Einstellung auf die Eignung der Person geachtet, sowie die Sensibilisierung und Verpflichtung zur Einhaltung der Vorschriften gefordert.

Auf Einrichtungen wird kurz im Zusammenhang, mit Umweltbedingungen für Server und aktive Netzwerkkomponenten eingegangen. Ansonsten spielen diese nur im Rahmen von Aufbewahrung von Sicherungen und Dokumenten in verschiedenen Brandschutzabschnitten eine Rolle.

Mit der Technologie wird sich ausführlicher auseinandergesetzt, wobei der Fokus auf vorbeugende Maßnahmen liegt. Konzentriert wird sich, auf einen Basisschutz

für IT-Systeme und das Netzwerk, der immer umgesetzt werden muss. Für kritische Systeme muss außerdem eine Risikobewertung und Risikobehandlung durchgeführt werden.

Daten sind im Rahmen des MTD relevant für den Standard, werden aber ansonsten nur im Rahmen von Datensicherungen betrachtet.

Prozesse werden in dieser Norm durch zentrale Anforderungen im Anhang definiert, auf die regelmäßig im Text verwiesen wird. In diesem Fall muss die Zuweisung der Verantwortlichkeiten, klare Formulierung und Bekanntgabe, Behebung von Mängeln und kontinuierliche Verbesserung beachtet werden.

Lieferanten werden insbesondere im Rahmen der Planung von Auslagerungen als relevant erkannt. Dazu wird darauf hingewiesen, dass bei der Vertragsgestaltung darauf zu achten ist, dass Ansprüche bei Vertragsverletzungen durchsetzbar sind und eine vollständige Herausgabe der IT-Ressourcen bei Beendigung des Vertragsverhältnisses gewährleistet ist.

Dabei sind die Anforderungen kurzgehalten, beinhalten aber die wichtigen Sicherheitsaspekte. Somit ergibt sich:

- Mitarbeiter: vollständig – angemessen [48, pp. 17-19]
- Einrichtungen: unvollständig - kaum [48, pp. 30,31,34,37]
- Technologie: vollständig – angemessen [48, pp. 21-29]
- Daten: unvollständig – kaum [48, pp. 19,20,25,26,35]
- Prozesse: vollständig – angemessen [48, pp. 35-39]
- Lieferanten: unvollständig – angemessen [48, pp. 31,32]

Eine Priorisierung erfolgt anhand von Prozessen und Daten [48, pp. 20-21]. Die VdS 10000 ist zwar ein Ansatz für ein ISMS, erfüllt aber grundlegend alle Aspekte eines ITSCM und stellt über das gesamte Dokument hinweg knappe, aber konkrete Anforderungen z.B. an IT-Systeme [48, pp. 20-27]. Des Weiteren bildet die Richtlinie, die 83,18 Euro [48] kostet, mit ihrem expliziten Fokus auf KMOs eine Ausnahme und wird im Kapitel „4.2 Ausarbeitung VdS 10000“ genauer untersucht.

3.4 Information Technology Infrastructure Library 4th Edition

Untersucht wurde die „ITIL® Foundation ITIL 4 Edition“ von Axelos. Axelos wurde 2014 als ein gemeinsames Unternehmen von der britischen Regierung und dem Unternehmen Capita gegründet und 2021 von PeopleCert, einem Unternehmen für Prüfung und Akkreditierung in Bereich IT, übernommen [49].

Information Technology Infrastructure Library 4th Edition (ITILv4) ist eine Vorgehensweise für ITSM, mit dem aktuellen Stand von Februar 2019 [50, p. 4], und für alle Unternehmensgrößen und Branchen geeignet [50, p. 10]. ITILv4 kann nicht direkt für ein Unternehmen zertifiziert werden. Es kann lediglich einer Person bescheinigt werden, dass sie über die notwendigen Kenntnisse zur Umsetzung von ITILv4 verfügt [51] [52].

Es ist anzumerken, dass im Punkt „5.2.12 Service continuity management“ [50, pp. 190-193] das ITSCM explizit von der restlichen Vorgehensweise abgetrennt wird. Da dieser Abschnitt lediglich aus vier Seiten besteht und im Wesentlichen nur darauf hinweist, dass ein ITSCM vorhanden sein sollte, wurde das restliche Schriftstück auf weitere Aspekte des ITSCM geprüft.

Allerdings wird die Prävention ohne konkrete Ausführung lediglich erwähnt.

Die Vorfallerkennung wird in dem Kapitel „5.2.7 Monitoring and event management“ kurz bearbeitet. Indem die Erkennung möglichst automatisch ablaufen und auch Zusammenhänge zwischen den Ereignissen registrieren soll, wird eine zeitnahe Erkennung gewährleistet. Ferner wird ein Fokus auf die Klassifizierung von den Ereignissen gelegt, um falsche Alarme zu vermeiden.

Die Reaktion wird in „5.2.5 Incident management“ behandelt. Hierbei wird vor allem darauf hingewiesen, dass die Informationen zu den Vorfällen dokumentiert werden müssen. Die Vorfallbearbeiter müssen regelmäßig den Sachstand aktualisieren und bei Fremdprodukten einen engen Kontakt zu Lieferanten pflegen.

Überdies gibt es in der ITILv4 sogenannte Probleme, die als Folge von Vorfällen definiert werden. Probleme erfordern eine Analyse der Ursache, Erstellen eines

Workarounds und finden einer langfristen Lösung. Somit kann der Workaround als eine Art Notbetriebsniveau verstanden werden. Eine genauere Betrachtung von Wiederherstellung findet außerhalb von dem ITSCM Kapitel nicht statt.

Die Verbesserung hingegen wird ausführlich behandelt. Dennoch ist für das ITSCM der wichtigste Aspekt, dass durch eine Dokumentation und Verständnis der aufgetretenen Vorfälle, die Eintrittshäufigkeit, Identifizierung und Lösung von zukünftigen Vorfällen verbessert wird. Somit ergibt sich:

- Vorfallprävention: nicht betrachtet [50, pp. 114-116,175]
- Vorfallerkennung: angemessen [50, pp. 171-174, 176]
- Reaktion: angemessen [50, pp. 163-166]
- Wiederherstellung: nicht betrachtet [50, pp. 174-178]
- Verbesserung: angemessen [50, pp. 92-103,110-114,163,179]

Die Mitarbeiter müssen über die entsprechenden Qualifikationen verfügen und durch ein Talentmanagement gefördert werden.

Einrichtungen sind in der ITILv4 überhaupt nicht auszumachen. Während Technologie, Daten und Lieferanten zwar erwähnt werden. Aber es können keine bzw. kaum ITSCM-relevante Aspekte ausgemacht werden.

Prozesse zum Konfigurationsänderungsmanagement oder Vorfallbehandlung, werden in „5.2.4 Change control“ bzw. „5.2.5 Incident management“ ausführlich behandelt, wobei beim Änderungsmanagement der Fokus auf der Gewinnmaximierung liegt. Daraus folgt:

- Mitarbeiter: vollständig – kaum [50, pp. 40,41,147-150]
- Einrichtungen: nicht betrachtet
- Technologie: nicht betrachtet [50, pp. 41-46]
- Daten: nicht betrachtet [50, pp. 41-46]
- Prozesse: vollständig – angemessen [50, pp. 160-166]
- Lieferanten: unvollständig – kaum [50, pp. 46-48,142-146,165]

Darüber hinaus wird eine Priorisierung durch eine Risikobewertung vorgenommen [50, pp. 33,54,132-135]. Es werden jedoch keinerlei Anforderungen gestellt, sondern nur Hinweise gegeben. Die technologieunabhängige Vorgehensweise kostet 85,00 Euro [53] und ist nicht geeignet, um ein ITSCM zu etablieren. Weshalb der ITILv4 nicht weiter studiert wird.

3.5 FitSM

Die IT Education Management Organisation (ITEMO) ist ein eingetragener Verein und ein Zusammenschluss von Spezialisten auf dem Gebiet des IT-Managements. ITEMO schult und zertifiziert IT- und Managementpersonal [54]. Des Weiteren hat ITEMO FitSM, das ursprünglich aus einem, von der EU, gefördertem Projekt mit dem Namen FedSM hervorgegangen ist [55], entwickelt. Der aktuelle Stand wurde am 17.08.2022 für „FitSM-0 Overview and vocabulary“ und „FitSM-1 Requirments“ [56, p. Deckblatt 2] [57, p. Deckblatt 2] bzw. 14.06.2016 für „FitSM-2 Objectives and activities“ und „FitSM-3 Role model“ [58, p. Deckblatt 2] [59, p. Deckblatt 2] veröffentlicht. FitSM wurde speziell für KMOs [60] entwickelt, ist aber auch für große Unternehmen adaptierbar und branchen- und technologieunabhängig [56, p. 1]. Eine Zertifizierung der FitSM Implementierung ist nicht möglich.

FitSM deckt alle Tätigkeitsbereiche des ITSCM ab, indem in „FitSM-1 Requirments“ die Anforderungen kurz aufgelistet und in „FitSM-2 Objectives and activities“ diese konkretisiert werden. In diesem Fall handelt es sich bei den weiterführenden Informationen eher um eine Checkliste der erforderlichen Informationen und der durchzuführenden Schritte als um eine Beschreibung, der Maßnahmen. Es erfolgt keine Ausführung, wie die einzelnen Informationen beschafft oder die Schritte durchgeführt werden können.

Vorbeugende Maßnahmen können in den Kapiteln „PR4 Service Availability & Continuity Management (SACM)“, „PR5 Capacity Management (CAPM)“ und „PR6 Information Security Management (ISM)“ ermittelt werden. Im Wesentlichen wird gefordert, dass eine Planung erstellt wird, die den jeweiligen Aspekt identifiziert und Anforderungen dokumentiert, zusätzlich muss der Plan stets aktuell gehalten werden.

In den genannten Plänen, von „PR5“ und „PR6“, wird auch die Überwachung und Erkennung von Abweichungen der aufgestellten Anforderungen verlangt. Darüber hinaus erfolgt keine weitere Ausführung.

Reaktion wird in dem Kapitel „PR9 Incident & Service Request Management

(ISRM)“ behandelt. Der Schwerpunkt liegt auf dem Prozess bzw. Prozessen zur Meldung, Klassifizierung und Schließung einer Vorfallmeldung. Die eigentliche Behandlung wird nur im Rahmen von „Resolve an incident or service reques“ [58, p. 15] ausgearbeitet.

Bei FitSM gibt es wie bei der ITILv4 noch die Kategorie Problem, die in „PR10 Problem Management (PM)“, behandelt wird. Dies stellt auf Grund von Workaroundmaßnahmen, wieder eine Art Notbetriebsnievau dar. Wiederherstellung an sich wird aber nur in „PR4“, ohne weitere Ausführungen, erwähnt.

Eine kontinuierliche Verbesserung soll durch einen eigenen Prozess, „PR14 Continual Service Improvement Management (CSI)“ erreicht werden. In Bezug auf ITSCM sind jedoch die Hinweise in „PR9“ und „PR10“ zur Bearbeitung von Vorfällen relevanter. Daraus folgt:

- Vorfallprävention: angemessen [57, pp. 6,7] [58, pp. 9-12]
- Vorfallerkennung: kaum [57, pp. 6,7] [58, pp. 10,12]
- Reaktion: kaum [57, p. 8] [58, pp. 15-16]
- Wiederherstellung: kaum [57, pp. 6,8] [58, pp. 9,17]
- Verbesserung: angemessen [57, pp. 8,10] [58, pp. 15-17,21]

Personen werden lediglich in „FitSM-3 Role model“ behandelt. Hierbei liegt der Fokus auf der Zuteilung von Verantwortlichkeiten und Aufgaben, jedoch wird nicht auf Qualifikationen oder Sicherheitsmaßnahmen eingegangen. Somit sind für ITSCM keine relevanten Informationen enthalten.

Einrichtungen, Technologie und Daten werden nicht als eigene Objekte erfasst. Es wird der Begriff „Konfigurationsobjekte“ verwendet. Konfigurationsobjekte sind bei der Erbringung eines Dienstes beteiligt. Somit können IT-Geräte, Gebäude und ähnliches darunterfallen.

Bei fast jeden Anforderungspunkt wird ein standardisierter und wiederholbarer Prozess gefordert. Für das ITSCM sind in diesem Zusammenhang insbesondere, neben den Prozessen für die Durchführung der Prinzipien, das Konfigurations- und das Konfigurationsänderungsmanagement relevant, die beide definiert werden. Es erfolgt aber keine Ausführung, wie ein Prozess definiert werden kann.

Für Lieferanten sollen Kontaktdaten und weitere wichtige Informationen gesammelt werden. Dies ist für ITSCM nur minimal von Relevanz. Das Gesamtbild ist somit, wie folgt:

- Mitarbeiter: nicht betrachtet [59, pp. 1-33]
- Einrichtungen: unvollständig – kaum [56, p. 7] [57, pp. 7,9,10] [58, pp. 11,12,18-20]
- Technologie: unvollständig – kaum [56, p. 7] [57, pp. 7,9,10] [58, pp. 11,12,18-20]
- Daten: unvollständig – kaum [56, p. 7] [57, pp. 7,9,10] [58, pp. 11,12,18-20]
- Prozesse: vollständig – angemessen z.B. [57, pp. 8,9] [58, pp. 15-19]
- Lieferanten: nicht betrachtet [57, p. 7] [58, p. 14]

Die Prozesse werden priorisiert [57, p. 5] [58, p. 7]. Allgemeine Anforderungen sind über das gesamte Dokument verteilt, z.B. [57, pp. 1-10] [58, pp. 1-21] [59, pp. 1-30]. FitSM ist ein kostenloser ITSM-Ansatz mit 87 Seiten Umfang, im „Core Standard“, mit Fokus auf KMOs. Da es aber kaum Überschneidungen in Bezug auf ITSCM gibt, wird FitSM nicht weiter analysiert.

3.6 Good Practice Guidelines Edition 2018

Die Good Practice Guidelines Edition 2018 (GPG2018) werden vom Business Continuity Institute (BCI) veröffentlicht. Das BCI ist, nach eigenen Angaben, seit 1994 das führende Institut für Geschäftskontinuität und Widerstandsfähigkeit im Geschäftsbereich [61]. Die aktuelle Version GPG2018, vom 8.11.2017 [62], gibt eine strukturierte Vorgehensweise zur Implementierung eines BCM vor und beinhaltet Erklärungen, Tipps und Beispiele [63, p. 6]. Es wird darauf hingewiesen, dass die Maßnahmen an die Unternehmensgröße anzupassen sind, z.B. [63, p. 41].

Der GPG2018 enthält alle Prinzipien des ITSCM. Es werden jedoch keine konkreten Maßnahmen oder Vorgaben gemacht, sondern der Fokus liegt auf der Definition und Implementierung von Prozessen für Prävention, Reaktion, Wiederherstellung und Verbesserung. Die Detektion wird als Teil der Reaktion betrachtet.

Bei der Prävention werden die einzelnen Schritte des zu implementierenden Prozesses kurz erklärt. Währenddessen wird auch auf die Kosten-Nutzen-Analyse der Maßnahmen eingegangen.

Die Vorfalldetektion wird nur als Auslöser der Reaktionsmaßnahmen ohne weitere Ausführungen erwähnt.

Für die Reaktion werden drei verschiedene Teams definiert, die je nach Schwere des Vorfalls aktiviert werden. Diese sind aber für die gesamte Organisation vorgesehen und für ein reines ITSCM überdimensioniert.

Zur Wiederherstellung wird ausführlich die Erstellung von Plänen beschrieben. Es wird zwischen drei Ebenen unterschieden, von der Geschäftsführung, über den Verantwortlichen für die Ressource bis zu dem Verantwortlichen der die eigentliche Wiederherstellung durchführt.

Zur kontinuierlichen Verbesserung muss ein Prozess zur Überprüfung von selbst vorgebenden Leistungsmerkmalen, Anpassung bei Änderungen, Behebung von Mängeln implementiert werden sowie ein Entwicklungs- und Trainingsprozess angestoßen werden. Daraus ergibt sich:

- Vorfallprävention: angemessen [63, pp. 66,67]
- Vorfallerkennung: nicht betrachtet [63, pp. 70,71]
- Reaktion: kaum [63, pp. 70-75]
- Wiederherstellung: detailliert [63, pp. 76-85]
- Verbesserung: detailliert [63, pp. 88-98]

Von den nach ITSCM relevanten Objekten, werden Maßnahmen bezüglich der Mitarbeiter ausführlicher beschrieben und zusätzlich mit Beispielen versehen. Für Einrichtungen, Technologie, Daten und Lieferanten gibt es teilweise kurze Beispiele.

Prozesse werden für jeden Bereich definiert und schrittweise kurz erklärt. Durch die mangelhafte Betrachtung der Technologie werden keine spezifischen Prozesse für Konfigurationsänderungsmanagement usw. gefordert. Es werden nur allgemeine Prozesse etabliert, von denen für das ITSCM, nur die Prozesse für die fünf Prinzipien relevant sind.

Somit ergibt sich folgendes Gesamtbild:

- Mitarbeiter: vollständig – detailliert [63, pp. 28-35] [63, p. 71]
- Einrichtungen: nicht betrachtet [63, pp. 59-61,63,67]
- Technologie: nicht betrachtet [63, pp. 59-61,63,67]
- Daten: nicht betrachtet [63, pp. 59-61,63,67]
- Prozesse: vollständig – angemessen; z.B. [63, pp. 73,77,89,93]
- Lieferanten: nicht betrachtet [63, pp. 59-61,63,67]

Die GPG2018 stellt etablierte Methoden für die Implementierung eines BCM zur Verfügung, konzentriert sich aber mehr auf die Implementierung von allgemeinen Prozessen. Das Dokument kostet ca. 35 Euro [64] und umfasst 108 Seiten. Die Hinweise und Anregungen sind allgemein gehalten. GPG2018 ist nicht zertifizierbar und wird in der weiteren Arbeit, auf Grund des begrenzten Umfanges, bezüglich der ITSCm-Elemente, nicht weiter untersucht.

3.7 Control Objectives for Information and Related Technology

Die Information Systems Audit and Control Association (ISACA) ist eine globale Vereinigung von 170.000 Menschen aus 188 Ländern, die sich, seit über 50 Jahren, auf die IT und Informationssicherheit spezialisiert hat [65]. ISACA hat Control Objectives for Information and Related Technology (COBIT) als IT-Verwaltungs- und Managementrichtlinie in der aktuellen Version „2019“ im Dezember 2018 [66] und in deutscher Sprache im Dezember 2020 [67] veröffentlicht. COBIT2019 ist ein Konzept, das die IT als entscheidenden Faktor zum Erreichen der Unternehmensstrategie definiert und diesen Faktor effizient und optimiert zur Verfügung stellen möchte [68].

Hierbei werden sogenannte Managementziele, wie „Betrieb ist gemanagt“, mit dazugehörigem Zweck, Unternehmenszielen und IT-bezogene Zielen definiert. Anschließend wird für jedes Managementziel Anforderungen für einen Prozess, Organisationsstruktur, Informationen, Mitarbeiter, Richtlinien, Unternehmenskultur und benötige Dienste, Infrastruktur und Anwendungen identifiziert. Es erfolgt eine Unterteilung der Anforderungen, nach Fähigkeitsstufe, die angibt, wie weit die Verwirklichung von COBIT vorangeschritten ist.

Die Vermeidung von Vorfällen wird im gesamten Dokument, insbesondere aber im Kapitel „Managementziel: DSS01 – Betrieb ist gemanagt“, erfasst. Bei diesem Managementziel, wird z.B. darauf eingegangen, dass ein reibungsloser Ablauf gewährleistet sein muss und die Zuverlässigkeit der Dienste durch Maßnahmen erhöht werden soll.

Maßnahmen zur Erkennung von Vorfällen können insbesondere in den Kapiteln „Managementziel: BAI04 – Verfügbarkeit und Kapazität sind gemanagt“ und „Managementziel: DSS01 – Betrieb ist gemanagt“ registriert werden. Dadurch wird eine ständige Überwachung der IT-Komponenten erwartet.

„Managementziel: DSS02 – Serviceanfragen und Störungen sind gemanagt“ bilden Reaktionsmaßnahmen detailliert ab. Hierbei wird auf eine Klassifizierung, Anleitungen, mit Sofortmaßnahmen, für häufig auftretende Störungen, Eskalation und Dokumentation eingegangen.

Wiederherstellungsmaßnahmen werden in „Managementziel: BAI04 – Verfügbarkeit und Kapazität sind gemanagt“ erwähnt und „Managementziel: DSS04 – Kontinuität ist gemanagt“ behandelt. Zusammen erfolgt eine detaillierte Auflistung der zu erfolgenden Schritte zur Erstellung eines Wiederherstellungsplans.

Eine anzustrebende Verbesserung wird bei fast jedem Kapitel in COBIT2019 und insbesondere in „MEA01- Überwachung von Leistung und Konformität wird gemanagt“ erwähnt. Jedoch erfolgt keine Ausführung, wie die Verbesserung erreicht werden soll.

Für ITSCM sind vor allem die Abschnitte zum Störungs- und Problemmanagement relevant. Daraus ergibt sich:

- Vorfallprävention: detailliert; z.B. [69, pp. 249-252]
- Vorfallerkennung: detailliert [69, pp. 191-196,249-252]
- Reaktion: detailliert [69, pp. 255-260]
- Wiederherstellung: detailliert [69, pp. 191-196,267-270]
- Verbesserung: kaum [69, pp. 257, 294, 295, 298, 299]

Bei den zu ITSCM-relevanten Elementen werden nur Mitarbeiter, Technologie und Lieferanten ausführlicher bearbeitet, darüber hinaus finden sich über das

gesamte Dokument verstreut Aspekte zu den drei Elementen.

Einrichtungen und Daten werden nur punktuell, für ITSCM relevanten Aspekten, dargestellt.

Wie bereits erwähnt werden für jedes Managementziel Anforderungen an einen Prozess gestellt. Somit wird auch bei jedem Managementziel ein Prozess implementiert. Für ITSCM werden zusätzlich zu den fünf Prinzipen, z.B. in „IT-Änderungen sind gemangt“ relevante Prozesse etabliert.

Damit ergibt sich folgendes Gesamtbild:

- Mitarbeiter: vollständig – detailliert; z.B. [69, pp. 103-110]
- Einrichtungen: unvollständig – kaum [69, pp. 251,252]
- Technologie: vollständig – detailliert, z.B. [69, pp. 249-289]
- Daten: unvollständig – angemessen [69, pp. 154,179,213,271]
- Prozesse: vollständig – detailliert; z.B. [69, pp. 205-209]
- Lieferanten: vollständig – detailliert; z.B. [69, pp. 25,123-128,250]

Eine Priorisierung der Objekte findet vor allem im „Managementziel: APO12 – Risiko ist gemanagt“ statt. Vereinzelt wird im Dokument von einer weiteren Priorisierung gesprochen [69, pp. 135-142,192,268]. Die Vorgaben zielen eher darauf ab, Anforderungen an einen Prozess zu formulieren, als konkrete Hinweise zu geben, wie das Ziel erreicht werden kann, z.B. „2. Identifizieren und verfolgen Sie sämtliche Störungen, die auf eine inadäquate Leistung oder Kapazität zurückzuführen sind.“ [69, p. 191]. Es wird die Anforderung gestellt, alle Störungen zu identifizieren, aber nicht wie dies erreicht werden kann. Des Weiteren variiert der Detailgrad der Anforderungen zwischen allgemein [69, pp. 267-274] und konkret [69, pp. 275-282], wobei sich die konkreten Anforderungen ausschließlich auf präventive Maßnahmen beziehen. COBIT2019 bietet, kostenlos, mit seinen 326 Seiten eine solide Vorgehensweise, die viele Aspekte des ITSCM abdeckt. COBIT2019 wird allerdings auf Grund des begrenzten Rahmens der Arbeit nicht weiter betrachtet.

3.8 Compliance Informations-Sicherheitsmanagement System in 12 Schritten

Compliance Informations-Sicherheitsmanagement System in 12 Schritten (CISIS12) ist ein Rahmenwerk des IT-Sicherheitscluster e.V., der die Weiterentwicklung und Erforschung von Datenschutz, IT-Sicherheit und Informationssicherheit fördert und vom Bundesministerium für Bildung und Forschung, sowie dem Bundesministerium für Wirtschaft und Klimaschutz, gefördert wird [70]. CISIS12 wurde speziell für KMOs zur Implementierung eines ISMS entwickelt und ist branchenunabhängig anwendbar [71, p. 2]. CISIS12 liegt derzeit in der Version 1.0 vom 01.06.2021 [71, p. II] vor und stellt den Nachfolger des ISIS12-Regelwerkes dar. CISIS 12 umfasst 1072 Seiten in drei Dokumenten, kostet 150 Euro und kann zertifiziert werden [72]. Jedoch ist anzumerken, dass 976 Seien davon auf einen Anforderungskatalog entfallen, indem je Seite eine Anforderung mit einem kurzen Umsetzungshinweis gelistet ist. Die Norm stellt die Anforderungen weniger umfassend in Fließtext dar. Im Handbuch ist die Durchführung in zwölf Schritte gliedert und erläutert.

Die Prävention bildet den größten Teil und ist über die gesamten Dokumente verteilt, was mit der Ausrichtung auf ISMS zu begründen ist.

Bezüglich der Erkennung wird in vielen Abschnitten darauf hingewiesen, dass Maßnahmen zur Erkennung von Vorfällen zu implementieren sind, wobei anzumerken ist, dass hier auch Erkennungsmaßnahmen genannt werden, die nicht direkt IT-bezogen sind, z.B. Branderkennung [73, p. 844].

Reaktionsmaßnahmen werden nur im Kapitel „B2.170-M010 - Notfallkonzept“ als Sofortmaßnahmen erwähnt.

Bezüglich der Wiederherstellung wird im gesamten Dokument auf die Notwendigkeit von funktionierenden Backup-Lösungen hingewiesen. Insbesondere aber in den Kapiteln „B2.170-M010 - Notfallkonzept“ und „B2.380-M040 - Wiederherstellung nach einem Sicherheitsvorfall“ wird auf Wiederherstellungspläne eingegangen. In diesem Fall werden Übungen zur sofortigen Einleitung der Wiederherstellung nach einem Vorfall fokussiert.

Kontinuierliche Verbesserungen werden durch ständige Überprüfungen, Information des Managements und Nachbereitung von Vorfällen sichergestellt. Daraus ergibt sich:

- Vorfallprävention: detailliert; z.B. [73, pp. 170,234-241]
- Vorfallerkennung: detailliert; z.B. [73, pp. 236,361,417,428,435,454, 553,844]
- Reaktion: nicht betrachtet [73, pp. 159,160]
- Wiederherstellung: kaum [73, pp. 159,165,245,262,364,362,410,412, 418,429,431,436,455]
- Verbesserung: angemessen [73, pp. 166-168,366]

Bei Mitarbeitern wird die Schulung bzw. Sensibilisierung, Qualifikationsprüfung bei Einstellung, der Eingliederungsprozesse mit Hinweisen auf Einhaltung der IS-Regelungen, Rollenverteilung und Regelungen zum Einsatz von Fremdpersonal geregelt.

Einrichtungen werden beginnend von Inventarisierung, über Definition von Sicherheitsbereiche, Einführung von Erkennungsmaßnahmen, wie Brandmeldeanlage, bis Regelungen zum Schließen von Fenstern ausführlich analysiert.

Bei der Technologie wird die Hardware, die Software und das Netzwerk ausführlich im jeweiligen Abschnitt erfasst. Dadurch werden außer der Reaktion alle Aspekte des ITSCM dargestellt.

Daten können ausschließlich in präventiven Maßnahmen wie Datensicherungen registriert werden.

Prozesse werden für mehrere Bereiche gefordert und beinhalten neben übergeordneten Prozessen, wie IS-Prozess, auch direkt für das ITSCM relevante Bereiche, wie Änderungsmanagement, Meldeprozess für IS-Vorfälle oder Einarbeitungs- und Schulungsprozess für neue Mitarbeiter.

Mit Lieferanten wird sich über die gesamten Unterlagen hinweg und schwerpunktmäßig in den Bausteinen „Outsourcing (Nutzung)“ und „Lieferantenmanagement“ auseinandergesetzt.

Es werden somit Maßnahmen zu allen Elementen des ITSCM wahrgenommen,

dadurch ergibt sich folgende Bewertung:

- Mitarbeiter: vollständig - detailliert [73, pp. 48-51,110-136]
- Einrichtungen: unvollständig – detailliert [73, pp. 839-952]
- Technologie: unvollständig – detailliert [73, pp. 224-267,374-538,552-838]
- Daten: unvollständig – kaum [73, pp. 553,565,571,599,614,657]
- Prozesse: vollständig – detailliert; z.B. [73, pp. 51,83,112,186,224-233,351,361]
- Lieferanten: unvollständig – detailliert; z.B. [73, pp. 169,268-311,353-360,538-552]

Bis auf wenige Anforderungen handelt es sich jedoch aufgrund der Ausrichtung auf das ISMS um präventive und allgemeine Maßnahmen, wie z.B. Backups, weshalb mit Ausnahme der Mitarbeiter und Prozesse keine vollständige Betrachtung erfolgt.

Es findet eine Risikobewertung statt [73, pp. 149-159] und bietet mit dem Katalog eine Vielzahl von allgemein gehaltenen Anforderungen. Aufgrund der fehlenden Reaktionsmaßnahmen und dem für ITSCM mangelhaften Wiederherstellungsmaßnahmen, wird der Standard nicht weiter ausgeführt.

3.9 National Fire Protection Association 1600

Anmerkung: Die Online-Version der Norm enthält zusätzliche Informationen, vgl. Bild 4 und 5. Im Folgenden wird von der Online-Version der Norm ausgegangen, die über das Abo-Modell zugänglich ist [74], da diese jedoch keine Seitenzahlen enthält, werden für die Quellenangaben die Seitenzahlen der PDF-Version verwendet.

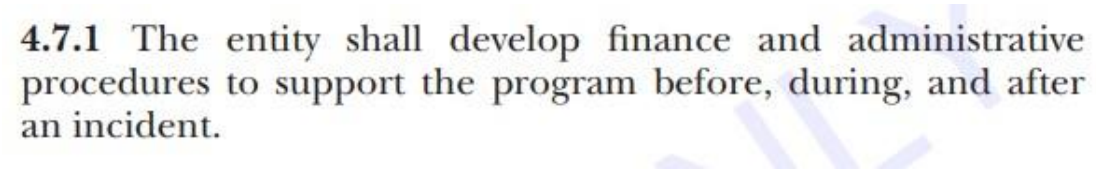

Bild 4: Bsp. PDF-Version NFPA 1600 [75, p. 7]

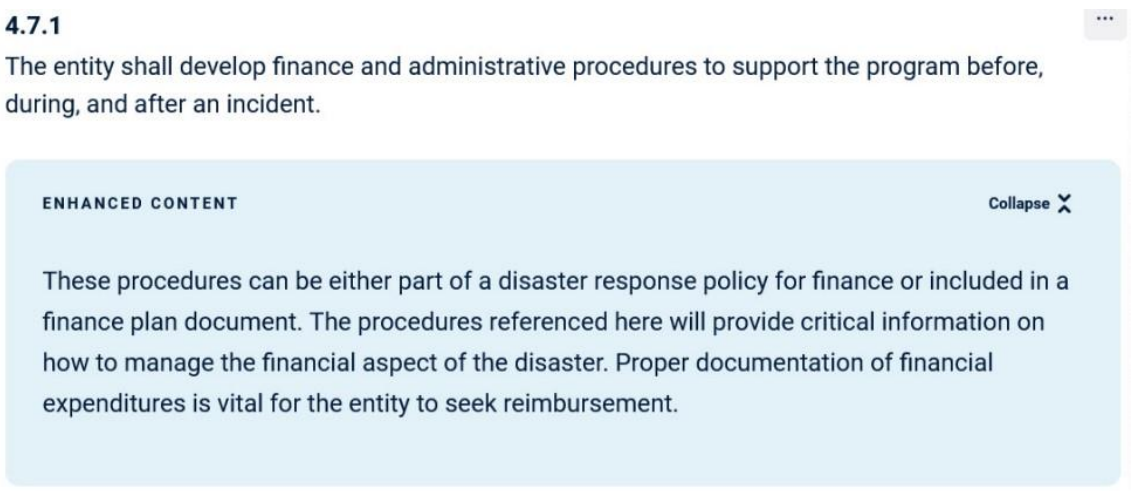

Bild 5: Bsp. Online-Version NFPA 1600 [74]

Die National Fire Protection Association (NFPA) ist eine gemeinnützige Organisation, die 1896 mit dem Ziel gegründet wurde, Todesfälle, Verletzungen, Sachschäden und wirtschaftliche Verluste durch Feuer, Elektrizität und verwandte Gefahren zu reduzieren. Um dieses Ziel zu erreichen, entwickelt die NFPA verschiedene Richtlinien [76]. Einer dieser Normen ist der NFPA 1600 „Standard on Continuity, Emergency, and Crisis Management“. Dieser wird von der US-amerikanischen Kommission für Terrorangriffe auf die US als nationaler Bereitschaftsstandard anerkannt [77]. Die Unterlagen können entweder über ein monatliches Abonnement für 11,99 $ oder über einen einmaligen Kauf für 84,00 $ in der aktuellen Version 2019 [74], vom 05.11.2018 [75, p. 1], bezogen werden. Die Realisierung des 97 Seiten umfassenden Dokuments kann nicht zertifiziert werden. Die Implementierung kann aber von der lokalen zuständigen Behörde in den USA gefordert sein [75, pp. 5,16]. Die technologieunabhängige Vorgehensweise ist für alle Branchen und Unternehmensgrößen anwendbar [75, p. 5].

Zum Thema Prävention werden über das gesamte Dokument verteilt Aspekte genannt. Der Hauptpunkt ist jedoch „6.2 Prevention“ und „A.3.3.22 Prevention“, der nur die Punkte Unfallprävention, Informationen von möglichen Vorfällen sammeln und Implementierung von IS-Maßnahmen beinhaltet.

Die Detektion wird im Zusammenhang von Krisenmanagement erwähnt, da zum Auslösen des Krisenfalls, zunächst eine Krise erkannt werden muss. Es erfolgt

aber keinerlei Ausführung, wie dies zu erfolgen hat.

Reaktionsmaßnahmen werden zwar in einem eigenen Kapitel „6.3 Mitigation“ und vereinzelt auch in anderen Punkten berücksichtigt, allerdings wird nur darauf hingewiesen, dass ein Plan für Reaktionen vorhanden sein sollte und in diesem Maßnahmen zur Schadenseindämmung definiert sein müssen.

Die Wiederherstellung wird in „6.10 Continuity and Recovery“ und dem dazugehörigen Anhang behandelt. Dabei handelt es sich im Wesentlichen, aber um eine reine Anforderungsliste, die zwar detaillierter ist als die ISO 27031, aber keine weitere Umsetzungshilfe bietet.

Die Verbesserung wird ebenfalls in mehreren Punkten angesprochen, wobei vor allem Kapitel „9.1 Program Evaluation“ und Kapitel 10 „Program Maintenance and Improvement“ zu beachten sind. Für das ITSCM ist gleichwohl die Verbesserung auf Basis der Nachbearbeitung von Vorfällen insbesondere relevant. Somit ergibt sich:

- Vorfallprävention: kaum [75, pp. 7,9,12,17]
- Vorfallerkennung: nicht betrachtet; z.B. [75, p. 10]
- Reaktion: kaum [75, pp. 8,9]
- Wiederherstellung: detailliert [75, pp. 11,26-27]
- Verbesserung: detailliert [75, pp. 12,13]

Mitarbeiter werden vor allem in Bezug auf Verantwortlichkeiten und Rollen betrachtet. Sie werden auch als Ressource mit Expertenwissen zum Betrieb von Geschäftsprozessen anerkannt. Des Weiteren sieht der NFPA 1600 vor, Beschäftigte inklusive der Familie im Krisenfall zu unterstützen, geht aber außer auf Kommunikationsmitteln, in einem eigenen Abschnitt, nicht weiter darauf ein. Der einzige für ITSCM wichtige Aspekte ist die Qualifikation, die man aus dem Expertenwissen ableiten muss.

Einrichtungen, Technologie, Daten und Lieferanten werden über den gesamten Text als Arbeitsmittel immer mit erwähnt, sind aber nur mit einigen Beispielen für Redundanz bzw. Ausweicheinrichtungen weiter ausgeführt.

Prozesse werden mehrmals erwähnt und sollen auch regelmäßig verbessert werden. Jedoch ist keiner der erwähnten Prozesse, außer der kontinuierlichen

Verbesserung, für ITSCM relevant. Daraus ergibt sich folgende Bewertung:

- Mitarbeiter: vollständig - kaum [75, pp. 7,9,27]
- Einrichtungen: unvollständig – kaum [75, pp. 9,10,13,24-27]
- Technologie: unvollständig – kaum [75, pp. 9,13,25-27]
- Daten: unvollständig – kaum [75, pp. 9, 25-27]
- Prozesse: unvollständig – kaum [75, pp. 9,12,13] 9 12 13
- Lieferanten: unvollständig – kaum [75, pp. 9,25-27]

Eine Priorisierung der Geschäftsprozesse und damit verbunden Objekte findet in Rahmen einer Business Impact Analyse (BIA) statt. [75, pp. 9,10].

Da mit der Vorfallprävention, Vorfallerkennung und der Reaktion drei von fünf Schritten gar nicht oder nur kaum für ITSCM-relevant bearbeitet werden, wird der NFPA1600 im Folgenden nicht näher untersucht.

4 Exemplarische Ausarbeitung ausgewählter Vorgehensweisen

Im Folgenden wird ein kleines Unternehmen vorgestellt, anhand dessen in den nächsten Kapiteln die Implementierung, der zwei ausgewählten Verfahren, exemplarisch dargestellt wird. Allerdings ist zu beachten, dass aufgrund der begrenzten Zeit und des begrenzten Umfangs das Unternehmen nicht in seiner Gesamtheit betrachtet werden kann.

Das fiktive Unternehmen Mustermann GmbH ist ein 1987 gegründetes Familienunternehmen mit insgesamt 30 Angestellten. Das Unternehmen stellt Spezialspritzmaschinen für Kunststoffe her. Sitz des Unternehmens ist Musterstadt in Bayern. Auf dem Firmengelände befinden sich die Produktionshalle, eine Lagerhalle sowie ein Bürogebäude. Darüber hinaus beschäftigt das Unternehmen zwei Servicemitarbeiter, die in Nord- und Mitteldeutschland im Home-Office und im Außendienst tätig sind. Die GmbH erwirtschaftet einen Jahresumsatz von 5,5 Millionen Euro und einen Gewinn von 500.000 Euro. Der größte Teil des Umsatzes wird durch den Verkauf der Spritzmaschinen erzielt. Durch die im letzten Jahr eingeführte Fernwartung wächst der Umsatz im Servicebereich stark an und ist somit der zweitstärkste Geschäftsbereich. Herr Mustermann möchte zwar die Wiederstandfähigkeit seines Unternehmens erhöhen, zielt aber nicht zwangsläufig auf eine Zertifizierung ab.

In Bild 6 folgt eine Darstellung der Mitarbeiterzahl und der Organisationsstruktur der Mustermann GmbH sowie eine Darstellung des aktuellen Netzwerkes in Bild 7. Weitere Informationen werden bei der Bearbeitung der Verfahren ermittelt.

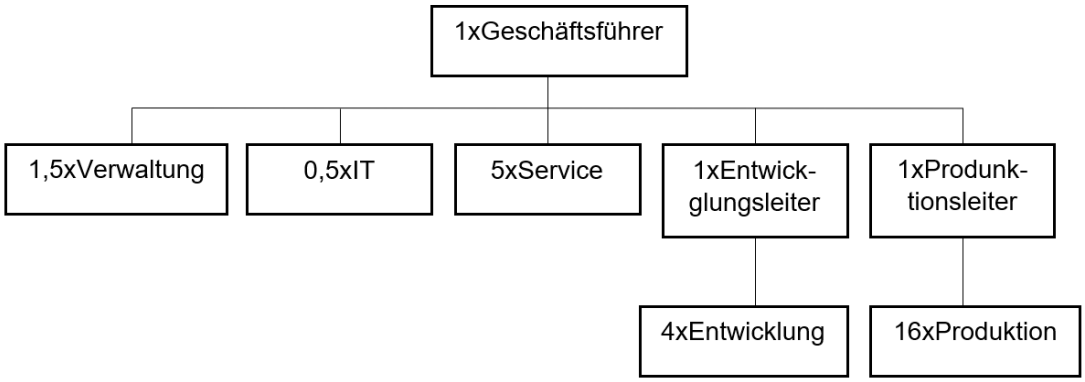

Bild 6: Organigramm mit Personenanzahl der Mustermann GmbH

Ein Beschäftigter bringt 50 Prozent seiner Arbeitszeit für die IT und 50 Prozent für die Verwaltung auf.

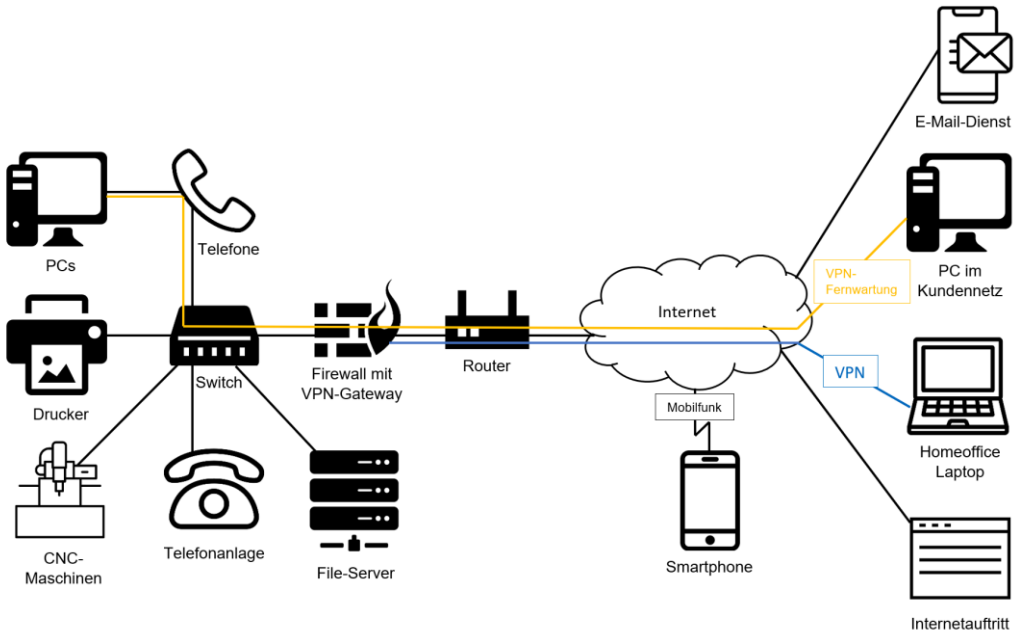

Bild 7: Netzplan der Mustermann GmbH

Die Smartphones besitzen keine Verbindung zum Unternehmensnetz. Die Mobilfunkverbindung dient zur Navigation, der externen Arbeitnehmer, und zum Zugriff auf den E-Mail-Dienst.

4.1 Ausarbeitung BSI 200-4

Bei der Verwirklichung des BSI 200-4 stellt sich zunächst die Frage: In welchen Umfang und Detailgrad eine Absicherung stattfinden soll, da zwischen drei Umsetzungsstufen unterschieden wird.

Eine Stufe stellt das sogenannte „Reaktiv-BCMS“ dar. Hierbei wird auf Grundlage der bereits vorhandenen Sicherheits- und Vorsorgemaßnahmen eine Absicherung der wichtigsten Geschäftsprozesse vorgenommen. Dazu werden nicht alle Schritte des BSI 200-4 angewendet und es findet kein wiederholter Durchlauf des Prozesses statt. Dies schafft zwar schnell die Kompetenz zur Notfallbewältigung, jedoch ist diese aufgrund der eingeschränkten Betrachtung sowohl für die ausgewählten Prozesse als auch für die gesamte Organisation unvollständig [30, p. 29].

Die nächste Stufe ist das „Aufbau-BCMS“, bei dem eine vollständige Abarbeitung des BSI 200-4 auf einen ausgewählten Teilbereich erfolgt. Der Teilbereich wird so gewählt, dass möglichst viele der kritischen Prozesse in diesem Bereich liegen. Das hat gegenüber dem „Reaktiv-BCMS“ den Vorteil, dass die kritischen Prozesse ausführlicher und vollständig abgesichert werden, jedoch gibt es auch hier Teilbereiche der Organisation, die nicht erfasst werden. Das „Aufbau-BCMS“ ist vor allem darauf ausgelegt, mit begrenzten Ressourcen eine solide Basis zu schaffen, die durch regelmäßige Aktualisierung und Erweiterung zu einem „Standard-BCMS“ heranwächst [30, pp. 28-30].

Die letzte Stufe ist das „Standard-BCMS“, das eine vollständige Untersuchung der Organisation vorsieht. Da eine vollständige Bearbeitung stattfindet, wird der Schritt „Voranalyse“ nicht durchgeführt. Diese Stufe ist nach ISO 22301 zertifizierbar und wird vom BSI empfohlen, auch langfristig anzustreben. Jedoch besteht hier der größte Mittelbedarf [30, pp. 28-30].

Zur Auswahl der geeigneten Einstiegsstufe gibt das BSI mit Bild 8 eine Hilfestellung.

Kriterien bzw. Stufen	Aufbau-BCMS	Standard-BCMS
Es existieren gesetzliche bzw. regulatorische Anforderungen	X (sofern alle regulierten GPs im Prozessumfang liegen	X
Es existiert solide Vorerfahrung mit Managementsystemen	X	
Es existiert Vorerfahrung in einzelnen Aspekten des BCM oder der Krisenbewältigung	X	
BCMS ist bereits etabliert		X
Ressourcenausstattung ist gut	X	X

Bild 8: „Aufbau-BCMS“ im Vergleich zu „Standard-BCMS“ [30, p. 31]

Das BSI empfiehlt, die jeweilige Stufe nur dann zu wählen, wenn alle mit „X“ gekennzeichneten Kriterien in der Organisation erfüllt sind. Da es für das „Reaktive BCMS“ keine Voraussetzungen gibt, kann dieses immer angewendet werden. Der Vollzug der einzelnen Schritte kann mit Hilfe des Anforderungskatalogs dokumentiert und überprüft werden, vgl. [39].

Für die exemplarische Skizzierung der Mustermann GmbH wird daher die Methode des „Reaktiv-BCMS“ angewendet. Die beim „Reaktiv-BCMS“ ausgelassenen Schritte werden nur kurz beschrieben. In den folgenden Abschnitten „4.1.1“ bis „4.1.13“ wird das entsprechende Kapitel der BSI 200-4 mit der gleichen Überschrift behandelt [30].

4.1.1 Initiierung des Business Continuity Management Systems durch die Institutionsleitung

Beim BSI 200-4 muss bei der Initiierung des BCMS folgendes festgelegt werden:

- Verantwortlichkeit der Leitungsebene
- Zielsetzung
- Geltungsbereich
- Umsetzungsstufe
- BCM-Beauftragter

Die Unternehmensleitung ist für den ordnungsgemäßen Betrieb des Unternehmens, auch in Notfallsituationen, verantwortlich. Aufgrund dieser Verantwortung kann auch nur die Geschäftsführung Entscheidungen zur Bewältigung bzw. Nutzung von Risiken treffen und die dafür notwendigen

Arbeitsmittel sicherstellen. Für die Mustermann GmbH bedeutet dies, dass Herr Peter Mustermann, als Inhaber und Geschäftsführer der GmbH, die Implementierung eines BCM veranlassen muss, was durch die später von ihm unterzeichnete „Leitlinie BCMS“ schriftlich dokumentiert wird. Vorher sollte die Geschäftsführung ein Grundverständnis für BCM besitzen bzw. sich durch Schulungen aneignen. Des Weiteren hat sie sich aufgrund ihrer Vorbildfunktion an alle aus dem BCM resultierenden Regelungen zu halten.

In der Zielsetzung werden die Gründe für ein BCMS, die Ziele und der abzusichernde Zeitraum festgelegt. Die Gründe für die Einführung eines BCMS bei der Mustermann GmbH sind auf die Corona-Pandemie zurückzuführen. Dadurch wurde Herrn Mustermann bewusst, dass sein Unternehmen bereits auf kleinere Ausnahmefälle nicht vorbereitet ist und somit bereits bei kleineren Ausfällen mit erheblichen finanziellen Schäden zu rechnen ist.

Der Hauptfokus für das BCMS ist die Absicherung der Geschäftsprozesse, die für die Bestandskunden relevant sind. Dies sind die Bereiche Service und Produktion, zudem drohen Vertragsstrafen bei Nichteinhaltung dieser Verpflichtungen. Als existenzbedrohend wird ein Schaden in Höhe von 300.000 € angesehen. Diese Summe wäre nach geschätzten sechs Wochen erreicht. Daher wird für das BCM ein Zeitraum von 21 Tagen festgelegt, bis ein Normalbetrieb wieder möglich ist. Grundsätzlich wird für das Unternehmen ein niedriges Risikoakzeptanzniveau angestrebt, jedoch sind die zur Verfügung stehenden Ressourcen begrenzt, so dass auch ein höheres Risiko, im Einzelfall, akzeptabel wäre.

Da bei der Mustermann GmbH derzeit keine Vorkenntnisse in Bezug auf BCM vorhanden sind, wird zunächst ein „Reaktiv-BCMS“ eingeführt, das später zu einem „Aufbau-BCMS“ ausgebaut werden soll.

Für die Implementierung des BCMS wird ein Verantwortlicher, der Business Continuity Beauftragter (BCB), benannt. Dieser sollte sich mit dem BCMS auskennen und im besten Fall gute Kenntnisse über das Unternehmen haben.

Kein Angestellter der Mustermann GmbH kommt derzeit als BCB in Frage. Da

das BCMS als langfristiger Prozess geplant ist und ein externer Berater sich erst in das Unternehmen einarbeiten müsste, entscheidet Herr Mustermann, dass der dienstälteste Mitarbeiter, der Leiter der Entwicklung ist, geschult und anschließend BCB wird. In der Einführungsphase ist geplant, dass der BCB drei Tage pro Woche für das BCM zur Verfügung steht. Die Schulungen sollte, vor der weiteren Erledigung des Standards erfolgen, da hierfür bereits Kenntnisse im BCM erforderlich sind. Außerdem ist zu beachten, dass der BCB nur eine Rolle der Business Continuity -Vorsorgeorganisation ist [30, p. 73].

4.1.2 Konzeption und Planung des BCMS

In der Konzeptionsphase werden acht Teilaufgaben unterschieden:

- Definition und Abgrenzung
- Analyse der Rahmenbedingungen (nicht beim „Reaktiv-BCMS)
- Definition der BCM-Aufbauorganisation
- Dokumentation
- Ressourcenplanung
- Schulung
- Sensibilisierung
- Leitlinie

Bei der Definition und Abgrenzung würde das BCM von bereits bestehenden Sicherheitskonzepten, wie ITSCM oder ISMS, abgrenzt werden. Da bei der Mustermann GmbH keine Managementsysteme existieren und im Rahmen dieser Arbeit explizit die Anwendbarkeit von ITSCM untersucht werden soll, findet hier keine Abgrenzung statt. Wichtig ist, dass eine einheitliche Definition wichtiger Begriffe wie Störung und Notfall verwendet wird. Diese wurden in „Kapitel 2.1.1 Definitionen“ definiert und werden von der Mustermann GmbH übernommen. Außerdem ist zu prüfen, ob bereits vorhandene Schutzmaßnahmen zum BCM beitragen. Im Beispielfall sind dies der Brandschutz und der Arbeitsschutz, da durch diese die physischen Werte und die Menschen geschützt werden.

Bei der Analyse der erweiterten Rahmenbedingungen werden die Einflussfaktoren auf das BCMS untersucht. Dies können gesetzliche Vorgaben, Auflagen/Erwartungen von Kunden, Vorgaben von Versicherungen oder interne Interessenten, wie Betriebsrat oder Führungskräfte, sein. Nach der Identifikation

der Interessengruppen ist zu klären, ob und wie mit diesen über das BCMS kommuniziert wird. Im letzten Schritt der Voranalyse werden mögliche Schnittstellen und Synergiepotenziale identifiziert. Beispielsweise wird das Facility-Management für den physischen Schutz der Gebäude benötigt oder bei einem bereits vorhandenen ISMS kann auf bereits erhobene Daten zurückgegriffen werden.

Bei kleineren Unternehmen, wie im Beispielfall, besteht die Aufbaustruktur in der Regel nur aus der Geschäftsleitung und dem BCB, wobei die Geschäftsleitung für die Rahmenbedingungen und der BCB für die Umsetzung des BCMS verantwortlich ist. In größeren Unternehmen können weitere Personen erforderlich sein, z.B. BCM-Koordinatoren, die über ein ausgeprägtes Fachwissen in einem Geschäftsbereich verfügen.

Der BCB muss für jeden durchgeführten Schritt einen kurzen Abschlussbericht erstellen, der von ihm und der Geschäftsführung unterzeichnet wird. Dieser Bericht soll die getroffenen Entscheidungen mit einer kurzen Begründung sowie die getroffenen Maßnahmen und deren Kosten enthalten. Beim „Aufbau-BCMS“ und „Standard-BCMS“ erfolgt eine ausführlichere und stärker reglementierte Dokumentation. Bei diesen beiden Stufen ist das wichtigste Dokument das Notfallhandbuch, in dem alle für die Reaktion wichtigen Informationen gesammelt werden.

Bei der Mittelplanung kann in dieser Phase der Realisierung nur grob geschätzt werden, wie hoch der Ressourcenbedarf ist. Dabei spielen vor allem die Größe und Komplexität des Unternehmens, der gewählte Geltungsbereich und die gewählte Stufe eine Rolle. Des Weiteren muss entschieden werden, ob die Finanzen zentral oder dezentral verwaltet werden und für welchen Zeitraum diese ausgelegt sind, z.B. ob bereits Kapital für eine Erweiterung zum „Aufbau-BCMS“ eingeplant wird. Bei der Mustermann GmbH werden die Mittel zentral verwaltet und sind nur für die Erreichung der definierten Ziele vorgesehen. Da ein „Reaktiv-BCMS“ gewählt wurde, das im Wesentlichen auf dem Istbestand aufbaut, werden zunächst, 60 Prozent der Arbeitszeit des Entwicklungsleiters und 15.000 € als Budget zur Verfügung gestellt. Aus diesem Budget werden auch die im vorigen Kapitel erwähnten BCB-Schulungen bezahlt.

Eine Grundsensibilisierung aller Angestellten erfolgt durch den BCB, der den IT-Mitarbeiter und den Produktionsleiter intensiver schult, da die Beiden seine technischen Ansprechpartner im jeweiligen Bereich sind.

Nachdem all diese Punkte festgelegt wurden, müssen die wichtigsten davon in der BCMS-Richtlinie als übergeordnetes und zentrales Dokument festgehalten werden. Diese Punkte sind [30, p. 67]:“

- Motivation für den Aufbau des BCMS inklusive der rechtlichen und regulatorischen Anforderungen
- Ziele für den Aufbau des BCMS
- Abzusichernder Zeitraum durch ein BCM
- Geltungsbereich des BCMS
- Übernahme der Gesamtverantwortung der Institutionsleitung
- institutionsspezifische Definition des Begriffs BCM und der Eskalationsstufen Störung, Notfall und Krise
- zentrale Rollen der BC-Vorsorgeorganisation erläutern
- die Selbstverpflichtung der Institutionsleitung dokumentieren, angemessene Ressourcen für das BCMS bereitzustellen“

Im BSI 200-4 wird als Musterrichtlinie auf den „Umsetzungsplan Bund - Leitlinie BCMS für Informationssicherheit in der Bundesverwaltung, Bundesministerium des Innern“ verwiesen [30, p. 234]. Die exemplarische BCMS-Richtlinie der Mustermann GmbH ist in den Anlagen zu finden, vgl. Anlage 2: BCMS-Leitlinie der Mustermann GmbH. Anzumerken ist, dass in Realität eine praxisnähere Definition von Störung, Notfall und Krise besser geeignet wäre. Davon wurde auf Grund einer einheitlichen Definition in der Arbeit abgesehen.

4.1.3 Aufbau und Befähigung der besonderen Aufbauorganisation

Die besondere Aufbauorganisation (BAO) wird sogenannt, da sie im Normalbetrieb nicht aktiv ist, sondern nur in besonderen Fällen, hier im Notfall, mit weitreichenden Weisungsbefugnissen zur Verfügung steht. Man unterscheidet die drei Ebenen in strategisch, taktisch und operativ. Die strategische Ebene legt Ziele und Prioritäten fest, die dann von der taktischen Ebene analysiert werden. Die taktische Ebene beschließt Maßnahmen, die von der operativen Ebene umgesetzt werden. Darüber hinaus gliedert sich die BAO in ein Kernteam, das im Krisenfall immer anwesend ist, eine situationsbedingte

Erweiterung, die je nach Krisensituation ihr Fachwissen einbringen kann, und eine Stabsassistenz, von der der Protokollführer immer Teil der BAO sein sollte. In der Stabsassistenz befindet sich in der Regel auch der BCB, der aber nur bei Bedarf hinzugezogen wird.

Bei der Mustermann GmbH ist jedoch der BCB als BCM-Experte der Leiter der BAO. Weiterhin sollten im Kernteam die Aspekte, IT, Personal, Gebäudemanagement und Kommunikation vertreten sein. Sofern diese ausgelagert wurden, sind die Verantwortlichen für das Outsourcing in das Kernteam aufzunehmen. Herr Mustermann ist als Vertreter für Personal, Gebäudemanagement und Kommunikation im Kernteam, zusätzlich ist dadurch der enge Kontakt zur Geschäftsführung gewährleistet. Der IT-Mitarbeiter ist als IT-Ansprechpartner anwesend sowie der Verwaltungsmitarbeiter als Protokollführer.

Als situative Erweiterung werden der Produktionsleiter sowie einer der drei Servicemitarbeiter vor Ort hinzugezogen. Damit ist die strategische und taktische Ebene abgebildet.

Auf der operativen Ebene sind die Notfallbewältigungsteams entsprechend dem Organigramm zu betrachten, d.h. für das Notfallmanagement in der IT ist der IT-Mitarbeiter verantwortlich, sowie für Entwicklung und Produktion der jeweilige Leiter und für Verwaltung und Service direkt die Geschäftsführung. Eine fehlende oder nicht geeignete Vertretung ist zwar nicht empfehlenswert, aber noch zulässig, weshalb aufgrund der begrenzten Ressourcen Herr Mustermann, der Stellvertreter für alle anderen Mitglieder des Kernteams ist. Der Leiter der Entwicklung ist der Stellvertreter von Herrn Mustermann Bei einer Erweiterung auf das „Aufbau-BCMS“ oder das „Standard-BCMS“ ist dies zu korrigieren.

Außerdem müssen Pläne für die Meldung und Bewertung von Vorfällen erstellt werden. Da der Fokus auf der IT liegt, wird diese nur exemplarisch skizziert. Bei internen Problemen mit IT-Anwendungen und Systemen ist der IT-Mitarbeiter erster Ansprechpartner. Der IT-Mitarbeiter ist auch Ansprechpartner für den Web-Hoster und den E-Mail-Provider. Bei ihm laufen also alle IT-bezogenen Vorfälle zusammen. Er muss entscheiden, ob es sich um eine Störung mit

Notfallpotenzial handelt oder nicht. Falls ein Notfallpotenzial vorliegt, muss dies dem BAO-Management gemeldet werden. Die Ersteinschätzung kann anhand, der in Bild 9, vorgegebener Listen erfolgen.

Meldestelle IT-Help Desk (1st bzw. 2nd Level Support)

Leitfragen für Schadensereignisse mit Notfallpotenzial - IT	Ja/Nein
• Ist das betroffene IT-System oder die betroffene Anwendung wesentlicher Bestandteil der Sicherheitsinfrastruktur (Viren-Management, Firewall etc.)? Für nähere Details siehe IT-Servicekatalog oder IT-Anwendungsliste. • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen Anwendung Auswirkungen auf einen großen Benutzerkreis oder den wesentlichen Geschäftsbetrieb der Institution? • Besteht ein dringender Verdacht auf vorsätzliche Daten- oder Systemmanipulationen (Datenabfluss), unerlaubte Ausübung von Rechten oder eines gezielten Angriffs (physisch oder virtuell) auf IT-Komponenten? • Ist zu erwarten, dass die Auswirkungen des Ereignisses einen Zeitraum > 8 Stunden übersteigen werden? (Gegebenenfalls die Information im 2nd Level Support erfragen.) • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen IT-Anwendung Auswirkungen auf externe Interessengruppen, wie z. B. Kunden, Medien, Aufsichtsbehörden? Gegebenenfalls die Information beim Anwender erfragen.	

Sobald mindestens eine Frage mit JA beantwortet werden kann, bitte umgehend an den Leiter des Stabes melden: Telefon 1234567890

Bild 9: Beispiel einer Ersteinschätzung eines Schadensereignisses in der IT [30, p. 79]

Die BAO-Leitung entscheidet dann, ob eine Störung, ein Notfall oder eine Krise eingetreten ist.

Zum Schutz von Leben, Sachwerten und um eine mögliche Ausbreitung des Ereignisses zu verhindern, können Sofortmaßnahmen erforderlich sein. Hierfür können bereits Regelungen, z.B. aus dem Brandschutz, bestehen. Diese Sofortmaßnahmen müssen auch geregelt werden, damit kein weiterer Schaden entsteht. Im IT-Bereich können Sofortmaßnahmen darin bestehen, einen infizierten PC vom Netzwerk zu trennen oder den Serverraum mit einem CO2-Feuerlöscher zu löschen.

Die Arbeitsweise der BAO muss geplant werden. Dazu gehört auch die Festlegung einer Arbeitsmethode, wenn kein Notfallhandbuch als Leitfaden vorhanden ist, wie dies beim „Reaktiv-BCMS“ der Fall ist. Als Beispiel nennt das BSI den Führungszyklus FOR-DEC [30, p. 85], der kurz in Bild 10 dargestellt wird.

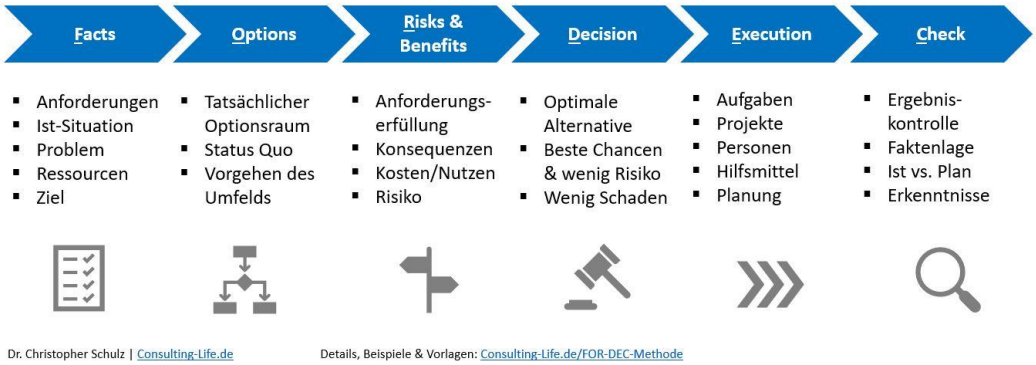

Bild 10: FOR-DEC Führungszyklus [78]

Außerdem müssen klare Arbeits- und Besprechungsphasen definiert werden. Die Arbeitsbedingungen, Protokollierung sowie ein klar definierter Arbeitsbeginn und -ende für die BAO, müssen festgelegt werden. Die beiden höheren Stufen, des BSI 200-4, sind detaillierter und enthalten weitere Punkte wie „Festlegung besonderer Befugnisse“.

In diesem Kapitel wird auch darauf hingewiesen, dass alle Mitglieder des BAO über die notwendigen Kompetenzen verfügen müssen. Darüber hinaus sind geeignete Räumlichkeiten für die BAO zur Verfügung stellen.

Die Regeln für die Kommunikation im Notfall müssen festgelegt werden. Trotzdem ist zu berücksichtigen, wer, wann, welche Informationen benötigt und wie die Kommunikation bei Ausfall der im Normalbetrieb vorhandenen Kommunikation möglich ist.

Schließlich muss festgelegt werden, dass nach der Bewältigung des Notfalls oder der Krise eine Analyse der Bewältigung stattfindet und Verbesserungen vorgenommen werden.

Am Beispiel der Mustermann GmbH könnte eine kurze Regelung wie folgt aussehen.

Die BAO tritt in Kraft, nachdem der BCB einen Notfall festgestellt hat, und folgt dem Führungszyklus FOR-DEC (Anmerkung: Es erfolgte keine Prüfung des Führungszyklus.). Danach sind alle diensthabenden Mitglieder des Kernteams unverzüglich im Aufenthaltsraum zu versammeln und die abwesenden Mitglieder

zu informieren. Diese haben sich unverzüglich, während der Rahmenarbeitszeit (zwischen 7:00 Uhr und 18:00 Uhr) im Dienstgebäude einzufinden. Sobald alle Mitglieder eingetroffen sind, beginnt die erste Lagebesprechung. Eine Lagebesprechung findet alle 4 Stunden statt und dauert maximal 30 Minuten. Zu Beginn einer Besprechung, erfolgt ein kurzer Lagebericht. Jede Besprechung muss Vollständig protokolliert werden. Nach jeder Lagebesprechung erfolgt eine kurze Information aller anwesenden Arbeitnehmer. Eine Information der Kunden bzw. der Öffentlichkeit erfolgt, je nach Lage, per E-Mail oder Website auf Anweisung der Geschäftsleitung. Eine ständige Erreichbarkeit ist durch ein unabhängiges Netzwerk und Mobiltelefon mit Datenübertragung gewährleistet. Alle BAO-Mitglieder müssen regelmäßige Pausen einlegen. Die maximale Arbeitszeit an einem Tag darf 12 Stunden nicht überschreiten. Der Notfall gilt als beendet, wenn die Funktionsfähigkeit weitestgehend wiederhergestellt ist und kein Grund zu der Annahme besteht, dass sich die Situation wieder verschlechtert. Spätestens mit der Wiederherstellung der vollen Funktionsfähigkeit ist der Notfall beendet.

4.1.4 Voranalyse

Die Voranalyse erfolgt nur für das „Reaktiv-BCMS“ und das „Aufbau-BCMS“, da bei diesen der Umfang des BCMS während der Initiierung eingeschränkt wird.

Zu nächst erfolgt eine Einschränkung ohne genaue Analyse und sehr grob, durch die Festlegung des Geltungsbereiches durch die Geschäftsführung. Um die potenziell zeitkritischen Prozesse im eingeschränkten Bereich zu identifizieren, wird eine Voranalyse durchgeführt, die auch den Vorteil hat, dass die anschließende aufwändige BIA nur für eine begrenzte Anzahl von Prozessen durchgeführt werden muss.

Das BSI unterscheidet grundsätzlich, bei der Voranalyse, zwischen drei Methoden. Die erste orientiert sich an Geschäftsprozessen, die zweite an Organigrammen und die dritte an Produkten und Dienstleistungen.

Unabhängig dem gewählten Ansatz muss der Begriff zeitkritisch für das Unternehmen definiert werden, wobei dieser kürzer als der für das BCMS

festgelegte Zeitraum und kürzer als sieben Tage sein sollte. Weiterhin muss für die fünf Bereiche, Beeinträchtigung der persönlichen Integrität, Beeinträchtigung der Aufgabenerfüllung, Verletzung von Gesetzen, Vorschriften und Verträgen, negative interne und externe Wirkung (Imageschaden) und finanzielle Auswirkungen, festgelegt werden, ab wann der Schaden zu hoch ist. Als Orientierungshilfe kann auf die BIA verwiesen werden, da diese Aspekte dort weiter ausgeführt werden. Im nächsten Kapitel wird dieser Punkt konkretisiert.

Das BSI empfiehlt die Auswahl auf Basis von Geschäftsprozessen, wenn bereits eine starke Geschäftsprozessorientierung bzw. eine Prozesslandkarte vorliegt. Die Auswahl anhand des Organigramms bietet sich bei hierarchischen Organisationen an, sowie anhand von Produkten oder Dienstleistungen, wenn ein Produkt- oder Dienstleistungskatalog vorliegt. Das weitere Vorgehen ist identisch. Die Geschäftsleitung legt entweder fest, welcher Prozess, welche Organisationseinheit oder welches Produkt zeitkritisch ist. Die nächste Ebene bestimmt dann, welche Teilobjekte, der von der darüber liegenden Ebene identifizierten Objekte, zeitkritisch sind. Der Detaillierungsgrad sollte unterdessen in der Voranalyse noch nicht sehr hoch sein.

Bei der Mustermann GmbH wurde der Umfang auf die Bereiche Service und Produktion beschränkt. Die Auswahl anhand des Organigramms ist eher schlecht geeignet, da die hierarchische Struktur zu flach ist und somit eine Differenzierung in zeitkritisch und nicht zeitkritisch kaum möglich ist. Eine Differenzierung nach Prozessen bzw. Produkten oder Dienstleistungen würde sich je nach vorhandener Dokumentation anbieten. Die Mustermann GmbH entscheidet sich für die Produkt- bzw. Dienstleistungsmethode.

Als zeitkritischer Zeitraum werden sieben Tage definiert. Des Weiteren wird für die fünf Aspekte, der „zu hohe Schaden definiert“, wobei auf das Kapitel „Festlegung der BIA-Parameter und betrachtete Zeithorizonte“ verwiesen wird [30, pp. 122,123]:

- Beeinträchtigung der persönlichen Unversehrtheit: Die Verletzungswahrscheinlichkeit ist gering und beschränkt sich auf leichte Verletzungen.

- Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb ist stark eingeschränkt, die Wiederaufarbeitung davon dauert mehr als 14 Tage.
- Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird gegen Gesetze oder Verträge mit hohen Strafen verstoßen.
- negative Innen- und Außenwirkung (Imageschaden): Ein nachhaltiger Imageschaden ist extern zu erwarten.
- finanzielle Auswirkungen: Die finanziellen Auswirkungen sind erheblich.

In Bild 11 werden die zeitkritischen Produkte und Services orange hervorgehoben.

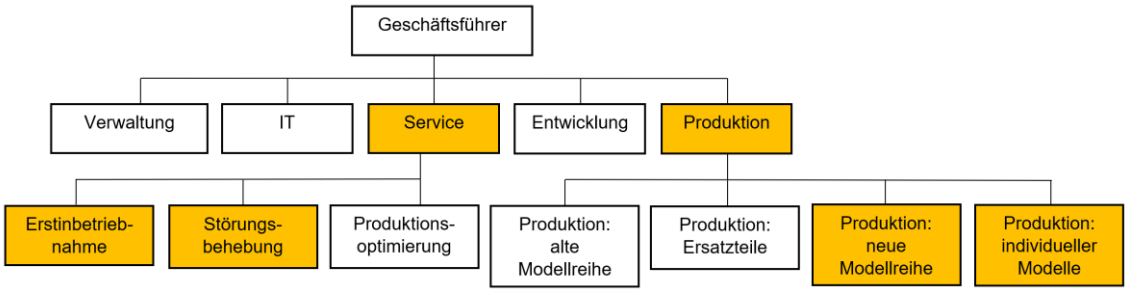

Bild 11: zeitkritische Produkte und Services der Mustermann GmbH

4.1.5 Business Impact Analyse

Bei der BIA wird abschließend festgestellt, welche konkreten Prozesse zeitkritisch sind und ab wann ein Ausfall dieser Prozesse zu inakzeptablen Auswirkungen führt. Die Ursache des Ausfalls ist indessen unerheblich. Für jeden Prozess sind vier Kennzahlen zu ermitteln:

1. maximal tolerierbare Ausfallzeit (MTA) gibt die maximale Ausfallzeit an, bevor inakzeptable Auswirkungen auftreten, hierbei wird das Schadenspotenzial zur Ermittlung verwendet.
2. gWAZ gibt den Zeitraum zwischen Ausfall und Anlaufen des Notbetriebs an. Die gWAZ muss kürzer als die MTA sein, zusätzlich sollte ein zeitlicher Puffer eingeplant werden.
3. maximal zulässiger Datenverlust oder auch MTD gibt an, wie alt die Daten für den Notbetrieb maximal sein dürfen. Daraus leiten sich Back-up Anforderungen ab.
4. Notbetriebsniveau gibt an, ab welchem Arbeitsniveau ein grundlegender Geschäftsbetrieb möglich ist. Die Angaben können prozentual erfolgen oder durch Priorisierung von Aufgaben.

Zunächst muss eine Liste aller Geschäftsprozesse vorliegen. Falls keine Liste vorhanden ist, muss diese erstellt werden, wobei auf eventuell vorhandene

Daten, wie die Strukturanalyse eines ISMS oder das Verzeichnis der Verarbeitungstätigkeiten des Datenschutzes, zurückgegriffen werden kann. Die Auflistung der Geschäftsprozesse sollte nicht zu kleinteilig sein, z.B. „Kündigung eines Arbeitnehmers“ sollte als ein Prozess erfasst werden und nicht mit: Kündigungsschreiben verfassen, Kündigungsschreiben versenden, ..., Personaldaten nach Ablauf der Aufbewahrungsfrist löschen.

Um einheitlich zu bestimmen, ob ein Geschäftsprozess zeitkritisch ist müssen Betrachtungszeiträume, Schadenskategorien und das Untragbarkeitsniveau definiert werden. Dadurch wird gleichzeitig die MTA einheitlich bestimmt.

Der Betrachtungszeitraum ist mindestens so lang, wie der bei der Initiierung definierte Zeitraum für das BCMS. Davor gibt es sinnvolle Abstufungen, die nicht gleich groß sein müssen.

Die Schadenskategorien sollten in Stufen unterteilt werden, die angeben, ob es sich um ein geringes, mittleres oder hohes Schadenspotenzial handelt. Das BSI empfiehlt drei bis fünf Abstufungen. Darüber hinaus müssen Schadenskategorien mindestens für die fünf bereits in der BIA erwähnten Aspekte definiert werden.

Das Untragbarkeitsniveau gibt an, ab welchem Schadenspotenzial die Auswirkungen nicht mehr akzeptable sind.

Der vorletzte Schritt der Vorbereitung ist die Definition der Ressourcenkategorien. Hier werden die für die Durchführung der Prozesse relevanten Ressourcenarten identifiziert, da diese später mit den Prozessen verknüpft werden und deren Kategorisierung übernehmen. Gemäß BSI sind immer IT, Personal, Infrastruktur sowie Dienstleistungen zu erfassen, hinzu kommen je nach Branche z.B. Maschinen, Fahrzeuge und Betriebsmittel.

Abschließend ist die BIA organisatorisch vorzubereiten. Das BSI empfiehlt, bei geringem BCM-Kenntnisstand im Unternehmen, Workshops des BCB mit dem Fachexperten zur Durchführung der BIA. Bei höherem Kenntnisstand können Hilfestellungen ausreichend sein, so dass die Fachexperten die BIA eigenständig durchführen und diese abschließend vom BCB verifiziert wird.

Bei der Durchführung der BIA wird für jeden Geschäftsprozess eine Tabelle erstellt und jede Schadenskategorie zu jedem Zeitpunkt analysiert. Gleichzeitig ist zu beachten, dass das Schadenspotenzial über die Zeit nur ansteigen kann. Das Ergebnis wird dann so zusammengefasst, dass für jeden Zeitpunkt nur das höchste Schadenspotenzial relevant ist. Erreicht das Schadenspotenzial innerhalb der gewählten Zeiträume die Untragbarkeitsschwelle, so gilt der Prozess als zeitkritisch.

Aus dem Zeitpunkt der Überschreitung des Untragbarkeitsniveaus kann die MTA abgeleitet werden, da diese vor diesem Zeitpunkt liegen muss. Die Festlegung der MTA sollte mit der Schadenskategorie begründet werden, die zuerst das Untragbarkeitsniveau erreicht. Da die gWAZ ohne Erfahrungswerte nur geschätzt werden kann, ist es zunächst ausreichend, diese mit kleiner als die MTA zu dokumentieren. Als letzter Parameter ist das Notbetriebsniveau festzulegen. Hier ist stichpunktartig zu dokumentieren, welche Teilschritte des Geschäftsprozesses aufrechterhalten werden müssen.

Der letzte Schritt besteht darin, die Abhängigkeiten zwischen den Objekten der Prozesse zu bestimmen, um dann die MTA und gWAZ auf diese zu vererben. Wenn ein Element von mehreren Prozessen benötigt wird, ist die niedrigste MTA und gWAZ ausschlaggebend. Bei unterschiedlichen MTD kann es zu Konflikten kommen, wenn ein Prozess mit geringer gWAZ mit hohen Verlusten leben kann, ein Prozess mit höherer gWAZ aber nur bei geringerem Datenverlust sinnvoll ist. Hier muss entschieden werden, wie damit umzugehen ist. Dadurch wird sichergestellt, dass jedes Teilstück rechtzeitig wiederhergestellt werden kann.

Beim „Aufbau-BCMS“ und beim „Standard-BCMS“ erfolgt zudem eine Verknüpfung der Prozesse untereinander, wenn Abhängigkeiten bestehen. Ebenso werden Single Points of Failures identifiziert.

Für die Mustermann GmbH werden nun, in Tabelle 2, exemplarisch die Geschäftsprozesse für den Service ermittelt. Für die BIA eignet sich der Detaillierungsgrad „Prozessebene 3“, für die in Kapitel 4.1.4 durchgeführte Voranalyse eignen sich „Prozessebene 1“ und „Prozessebene 2“.

Tabelle 2: Darstellung der ermittelten Geschäftsprozesse der Mustermann GmbH

Prozessebene 1	Prozessebene 2	Prozessebene 3
Service	Erstinbetriebnahme	Termin vereinbaren
		Inbetriebnahme vorbereiten
		Einbau des Spritzkopfes
		Testen der Funktionen
		Einweisung des Kunden
	Störungsbehebung	Entgegennahme der Störung (Telefon oder E-Mail)
		Kategorisierung der Störung
		1st Level-Anfragen lösen
		Analyse des Problems
		2nd Level-Anfragen lösen
		3rd Level-Anfragen lösen

Als Betrachtungszeiträume werden 1 Tag, 3 Tage, 7 Tage, 14 Tage und 21 Tage gewählt.

Für die Schadenskategorien wird ein Ansatz mit drei Stufen gewählt, vgl „Anlage 3: Definition der Schadenskategorien“.

Das Untragbarkeitsniveau wird, von Herrn Mustermann, auf „hoch“ festgelegt.

Es folgt, in Tabelle 3, die exemplarische Bewertung des Schadenpotenzials für jeden Zeitraum anhand des Geschäftsprozesses: „3rd Level-Anfragen lösen“.

Tabelle 3: Bewertung des Schadenpotenzials „3rd Level-Anfragen lösen“

Schadenspotenzial: 3rd Level-Anfragen lösen					
Schadensszenario	1 Tag	3 Tage	7 Tage	14 Tage	21 Tage
Beeinträchtigung der persönlichen Unversehrtheit	1	1	1	1	1
Beeinträchtigung der Aufgabenerfüllung	1	1	2	3	3
Verstoß gegen Gesetze, Vorschriften und Verträge	1	2	3	3	3
Negative Innen- und Außenwirkung	1	2	2	3	3
Finanzielle Auswirkungen	1	1	3	3	3
Höchstwert je Zeitraum	1	2	3	3	3

Eine Beeinträchtigung der persönlichen Unversehrtheit ist in keinem Fall zu erwarten, da „3rd Level-Anfragen“ in keinem Bereich Einfluss auf die persönliche Unversehrtheit haben könnte.

Die Beeinträchtigung der Aufgabenerfüllung steigt langsam an, bis sie nach 14 Tagen inakzeptabel wird. Der Anstieg erfolgt langsam, da die Anzahl der „3rd Level-Anfragen“ an einem Tag gering sind und deshalb der Wiederaufarbeitungszeitraum nur allmählich ansteigt.

Die Verstöße gegen Gesetze, Vorschriften und Verträge steigt langsam an, bis sie nach sieben Tagen inakzeptabel werden. Der Anstieg erfolgt langsam, da keine Verstöße gegen Gesetze und Vorschriften stattfinden und die Anzahl Verstöße gegen Verträge, an einem Tag, auf Grund der geringen Anzahl an der „3rd Level-Anfragen“ gering ist.

Die negative Innen- und Außenwirkung wird erst ab 14 Tagen kritisch, da nur

einzelne Kunden betroffen sind und bei „3rd Level-Anfragen“, die Kunden mit einer längeren Bearbeitungszeit rechnen.

Die finanziellen Auswirkungen stehen in direktem Zusammenhang mit der Nichteinhaltung von Wartungsverträgen und erreichen daher auch nach sieben Tagen einen kritischen Wert.

Anhand der Höchstwerte je Zeitraum lässt sich eine MTA von sieben Tagen ableiten, da bei diesem Zeitraum das erste Mal das Untragbarkeitsniveau erreicht wird. Da keine Erfahrungswerte zur gWAZ vorhanden sind, wird diese lediglich als „kleiner als MTA“ definiert.

Als Notbetriebsniveau wird 40 Prozent der normalen Bearbeitungsrate festgelegt. Damit können die schlimmsten Auswirkungen vermieden werden und ist somit als Notbetriebsniveau geeignet. Zugleich muss auf jeden Fall die Fernwartung und die Kommunikation mit dem Kunden funktionieren.

Als Ressourcenkategorien werden IT, Personal, Infrastruktur, Dienstleistungen und Maschinen/Geräte/Anlagen/Fahrzeuge mit den Beschreibungen des BSI [30, p. 125] definiert. In Tabelle 4 erfolgt eine Zuordnung der benötigten Ressourcen zu dem Prozess „3rd Level-Anfragen lösen".

Tabelle 4: Ressourcen: „3rd Level-Anfragen lösen"

Ressourcen: „3rd Level-Anfragen“ lösen	
IT	- PC - Laptop - Router - Firewall mit VPN-Gateway - Switch - Telefone mit Telefonanlage oder Smartphones - Fileserver - Fernwartungssoftware
Personal	3 Service-Mitarbeiter am Hauptstandort oder 1 Service-Mitarbeiter am Hauptstandort und 1er auswärts.
Infrastruktur	Hauptstandort mit kleinem Serverraum
Dienstleistungen	
Maschinen/Geräte /Anlagen/Fahrzeuge	Autos für evtl. vor Ort Termine: 2 Autos am Hauptstandort oder 1 Auto am Hauptstandort und 1 beim Auswärtigen-Mitarbeiter

Anmerkungen zu den Ressourcen:

- Die Unterscheidung zwischen Telefonen mit Telefonanlage und Smartphones erfolgt, da eine Option für die Kommunikation mit dem Kunden ausreichend ist. Außerdem kann der PC, anders als im Netzplan dargestellt, im Notfall auch direkt an den Switch angeschlossen werden.
- Die Unterscheidung zwischen Hauptstandort und Außendienst erfolgt, da 40 Prozent einem Angestellten am Hauptstandort und einem Außendienstmitarbeiter oder allen drei Servicemitarbeitern am Hauptstandort entspricht. Begründet wird dies mit den längeren Anfahrtszeiten, wenn bei „3rd Level-Anfragen“ eine Lösung vor Ort stattfinden muss.

Ein MTD wird für den Fileserver auf eine Woche festgelegt, da dort die Lösungsanleitungen nur bei Bedarf aktualisiert werden und bei „3rd Level-Anfragen lösen" wenig hilfreich sind. Eine „3rd-Level-Anfrage“ wird immer von einem Beschäftigten bearbeitet, diese treten eher selten auftreten und können somit von den Angestellten aus dem Gedächtnis nachvollzogen werden. Dadurch

ist das Ticketsystem weder zeitkritisch noch muss ein MTD definiert werden.

Die gWAZ von weniger als sieben Tagen wird an alle Objekte vererbt. Damit ist die BIA für „3rd Level-Anfragen lösen" abgeschlossen. Dabei ist zu beachten, dass für die Elemente die niedrigste gWAZ des Prozesses relevant ist, für die sie benötigt werden, z.B. könnte bei „1st Level-Anfragen lösen" die gWAZ auf Grund der größeren Anfragezahl geringer sein.

4.1.6 Soll-Ist-Vergleich

Beim Soll-Ist-Vergleich wird die gWAZ mit der wWAZ verglichen. Dazu müssen die Ressourcenverantwortlichen die wWAZ anhand von Erfahrungswerten, Tests, Serviceverträgen und realen Ausfällen ermitteln. Ebenso ist zu prüfen, ob die Anforderungen an den MTD eingehalten werden. Damit der Mittelbedarf für die Maßnahmen nicht extrem ansteigen, sollte von einem durchschnittlichen Ausfall ausgegangen werden. Falls die BCM-Expertise bei den Verantwortlichen nicht vorhanden ist, sollte die Ermittlung der wWAZ in Zusammenarbeit mit dem BCB erfolgen. Nach Abschluss des Soll-Ist-Vergleichs sind die Ergebnisse dem Management vorzulegen, wobei eine Übersicht über die zeitkritischen Prozesse und Objekte sowie deren gWAZ und wWAZ enthalten sein sollte. Insbesondere sind Abweichungen der wWAZ von der gWAZ und beim MTD aufzuzeigen und auf daraus resultierende Risiken hinzuweisen. In Tabelle 5 werden die IT-Ressourcen der Mustermann GmbH erfasst.

Tabelle 5: Vergleich der gWAZ mit der wWAZ der IT-Ressourcen

Ressource	gWAZ	wWAZ	Nachweis bzw. Erfahrungswerte	wWAZ ≤ gWAZ	Getestet
PC	< 7 Tage	8 Tage	Erstbereit-stellung	nein	nein
Laptop	< 7 Tage	8-10 Tage	Erstbereit-stellung	nein	nein
Router	< 7 Tage	3 Tage	vorherigem Ausfall	ja	ja
Firewall mit VPN-Gateway	< 7 Tage	?	nicht vorhanden	?	nein
Switch	< 7 Tage	21 Tage	Schätzung	nein	nein
Telefon	< 7 Tage	6 Tage	Schätzung	ja	nein
Telefonanlage	< 7 Tage	?	nicht vorhanden	?	nein
Smartphone	< 7 Tage	5-8 Tage	Erstbereit-stellung	nein	nein
Fileserver	< 7 Tage	4 Tage	vorherigem Ausfall	ja	ja
Fernwartungs-software	< 14 Tage	1 Tag	Erstbereit-stellung	ja	ja

Die Schätzung der wWAZ erfolgt für PC, Laptop, Router, Switch, Telefon und Smartphone auf Basis der Zeit, die erfahrungsgemäß benötigt wird, um die erforderliche Anzahl an Geräten zu beschaffen und zu konfigurieren. Die Spanne bei den Laptops und Smartphones ergibt sich aus dem zusätzlichen Versand bzw. der Lieferzeit bei der externen Belegschaft. Das BSI macht keine Angaben dazu, ob es sich z.B. bei den PCs um die Zeit für einen oder mehrere PCs

handelt. Daher wurden hier die Zeiten für die Anzahl der Geräte ermittelt, die für den Prozess „3rd Level Anfragen lösen" benötigt werden, also z.B. drei PCs. In Tabbele 6 wird der Soll-IST-Vergleich für den MTD durchgeführt.

Tabelle 6: Soll-Ist-Vergleich des maximalen Datenverlustes der Mustermann GmbH

Ressource	MTD	tatsäch-licher Daten-verlust	Nachweis	Daten-verlust tragbar	Getestet
Fileserver	7 Tage	5 Tage	Eine automatische Sicherung wird jedes Wochenende erstellt	ja	ja

Die Ergebnisse werden anschließend Herrn Mustermann vorgestellt. Besonders wird darauf hingewiesen, dass die Lieferzeiten für die Switches sehr lang sind und die gWAZ derzeit nicht eingehalten werden können. Der Ausfall des Switches hat weitreichende Auswirkungen auf andere Geschäftsprozesse. Für die Firewall und die Telefonanlage kann der IT-Mitarbeiter keine Einschätzung abgeben, da er diese nicht eingerichtet hat. Diese Abweichung wird in diesem Schritt nur zur Kenntnis genommen und im Schritt "Geschäftsfortführungsplanung" für das "Reaktiv-BCMS" und im Schritt "BCM-Risikoanalyse" für das "Aufbau-BCMS" und das "Standard-BCMS" näher ausgeführt.

4.1.7 BCM-Risikoanalyse

Die „BCM-Risikoanalyse“ wird für das „Reaktive BCM“ nicht durchgeführt.

Die Methode für die Risikoanalyse kann sich, sofern vorhanden, an anderen Managementsystemen orientieren. Im BCM liegt der Fokus auf der Verfügbarkeit, jedoch muss bei der Risikoanalyse berücksichtigt werden, dass auch der Verlust der Integrität oder der Vertraulichkeit dazu führen kann, dass ein Prozess nicht

mehr im Normalbetrieb ablaufen kann.

Zu Beginn müssen Kriterien zur Bewertung der Eintrittshäufigkeit und des Schadensausmaßes erarbeitet werden. Ein Stufenmodell ähnlich der BIA hat sich bewährt. Anschließend muss eine Liste der möglichen Gefährdungen erstellt werden. In diesem Zusammenhang kann eine Orientierung am BSI-Standard „200-3 Risikomanagement“ erfolgen. Als Nächstes muss für alle Elemente eine Priorisierung der Gefährdungen erfolgen, dabei wird zwischen "direkt relevant", "indirekt relevant" und "nicht relevant" unterschieden. Als vorletzter Schritt sind für die Gefährdungen, die Eintrittswahrscheinlichkeit und das Schadensausmaß zu ermitteln und zu einem Risikopotenzialwert zu verknüpfen. Abschließend ist zu klären, ob die jeweiligen Risikopotenzialwerte akzeptabel sind. Ist dies nicht der Fall, werden sie im Schritt „Business Continuity Strategien und Lösungen“ näher analysiert und durch Maßnahmen reduziert.

4.1.8 Business-Continuity-Strategien und Lösungen

Der Schritt „Business Continuity Strategien und Lösungen" ist für das „Reaktiv-BMCS“ nicht anwendbar.

In diesem Schritt werden Maßnahmen identifiziert, um die Eintrittswahrscheinlichkeit bzw. die Schwere von Ausfällen zu reduzieren, die wWAZ zu verbessern oder die maximal mögliche Notbetriebsdauer zu erhöhen.

Zunächst sollte der BCB zusammen mit den Ressourcenverantwortlichen eine Maßnahmenliste erstellen, in der keine Maßnahme ausgeschlossen wird. Im Anschluss sind die Maßnahmen auf ihre Wirksamkeit und Angemessenheit hinsichtlich der Kosten im Verhältnis zur Risikominderung zu prüfen. Hierbei ist zu beachten, dass eine Maßnahme, sofern die Wirksamkeit und die Angemessenheit gegeben sind, auch bei Überschreitung der in „4.1.2 Konzeption und Planung des BCMS“ veranschlagten „Ressourcenplanung“ weiter betrachtet werden sollte. Dies ist mit der groben und ungenauen Möglichkeit der Mittelplanung zu Beginn des BCMS zu begründen. Der BCB sollte dann die ausgewählten Maßnahmen einer genaueren Erörterung unterziehen und mögliche Synergien identifizieren. Synergien können sich positiv auf den

Normalbetrieb auswirken oder mehrere Objekte gleichzeitig schützen. Es sollte auch berücksichtigt werden, dass nach der Umsetzung einer Maßnahme ein Restrisiko bestehen bleibt oder neue Risiken entstehen können. Der finanzielle Aufwand sollte abgeschätzt werden und weitere Aspekte wie „organisatorischer Aufwand“ können in die Bewertung einfließen.

Nachdem das BCB eine Vorauswahl getroffen hat, werden diese der Geschäftsführung vorgelegt, die entscheiden muss, welche davon umgesetzt werden sollen. Zum Schluss muss die Durchführung geregelt und durchgeführt werden.

4.1.9 Geschäftsfortführungsplanung

Die Geschäftsfortführungspläne (GFP) sind die Dokumentationen, der in einem Notfall zu ergreifenden Maßnahmen. Für jeden zeitkritischen Geschäftsprozess muss ein GFP vorhanden sein. Bei den GFPs ist zu unterscheiden zwischen „Reaktiv-BCMS“ und „Aufbau-BCMS“ bzw. „Standard-BCMS“. Beim „Reaktiv-BCMS“ werden konkrete Maßnahmen dokumentiert, mit denen die Prozesse innerhalb der gWAZ das Notfallbetriebsniveau erreichen, wobei der Istbestand oder schnell umsetzbare Maßnahmen genutzt werden. Im Gegensatz dazu wird im „Aufbau-BCMS“ oder „Standard-BCMS“ dokumentiert, wie die im Schritt „Business Continuity Strategien und Lösungen“ identifizierten Maßnahmen im Notfall umgesetzt werden sollen. In der Praxis werden die GFPs häufig nach Organisationseinheiten getrennt und dann für jeden zeitkritischen Prozess in der Organisationseinheit ein GFPs erstellt. Es kann aber auch ein organisationsübergreifender GFP pro Prozess erstellt werden.

Der BCB sollte eine Vorlage für die GFPs erarbeiten, um sicherzustellen, dass diese einheitlich und vollständig ausgefüllt werden. Der BCB sollte alle bereits bekannten Informationen eintragen, d.h. Geltungsbereich, zeitkritische Geschäftsprozesse (mit gWAZ und Notbetriebsniveau), zeitkritische Objekte (mit wWAZ, gWAZ, tatsächlichem und gefordertem MTD), falls ermittelt, Abhängigkeiten zwischen zeitkritischen Geschäftsprozessen. Hinzukommend müssen die Zielsetzung des GFP, der Aktivierungsprozess, besondere Rechte

und Pflichten der Angestellten, besondere Melde- und Berichtspflichten, relevante Kontakte und Dokumente festgelegt werden. Das Ziel gibt an, was mit dem GFP erreicht werden soll. Der Aktivierungsprozess orientiert sich am Schritt „Aufbau und Befähigung der BAO“, indem bereits festgelegt wurde, wann der Stab zusammentritt und wie die notwendigen Personen informiert werden.

Beim Aktivierungsprozess des GFP müssen alle benötigten Mitarbeiter mit Kontaktdaten hinterlegt werden, je nach Festlegung auch extra mit privaten Kontaktdaten. Sollten die Angestellten im Rahmen des Notfallmanagements besondere Berechtigungen erhalten, wie z.B. Zugriff auf die Dateiablage mit vertraulichen Informationen, müssen diese ebenfalls im GFP definiert werden. Zuletzt sind relevante Zusatzdokumente mit Ablageort anzugeben. Dies können z.B. Raum- oder Verkabelungspläne sein.

Der letzte Schritt bei der Erstellung eines GFPs ist die Entwicklung von Maßnahmen, um die Einhaltung der gWAZ und des Notfallbetriebsniveaus gleichzeitig zu erfüllen, wobei die Möglichkeit besteht, die GFPs nach unterschiedlichen Schweregraden des Ausfalls zu unterteilen. Nach Erstellung der GFPs sind diese vom BCB auf Vollständigkeit, Plausibilität und Aktualität zu prüfen. In diesem Fall werden die GFPs freigegeben, was durch den Leiter der Organisationseinheit erfolgen sollte.

Die Mustermann GmbH hat sich dafür entschieden, für jeden Prozess einen organisationsübergreifenden GFP zu erstellen, da aufgrund des familiären Umfeldes und der flachen Hierarchie eine gute Zusammenarbeit zwischen allen Kollegen besteht. Nun wird beispielhaft ein GFP für „3rd Level-Anfragen lösen“ skizziert. Allerdings wird nur der für die IT-Abteilung relevante Teil betrachtet.

Geltungsbereich: Absicherung des Geschäftsprozesses „3rd Level-Anfragen lösen“ im gesamten Unternehmen.

Zielsetzung GFP: Der GFP soll den gleichzeitigen Ausfall mehrerer IT-Objekte für „3rd Level-Anfragen lösen“ absichern und innerhalb der gWAZ, von 7 Tagen, das Notbetriebsniveau von 40 Prozent erreichen. Ein gleichzeitiger Ausfall aller relevanten IT-Geräten sowie höhere Gewalt werden nicht in Erwägung gezogen.

Ausfälle öffentlicher Infrastrukturen werden ebenfalls nicht abgesichert.

Aktivierungsprozess: Der IT-Mitarbeiter, als Teil des Kernteams, wird sofort informiert, wenn ein Notfall ausgerufen wird. Dadurch ist kein weiterer Benachrichtigungsprozess notwendig. Die Aktivierung des GFP erfolgt unmittelbar nach Feststellung des Ausfalls eines der IT-Objekte des Prozesses.

Sonderrechte und -bestimmungen: Der IT-Mitarbeiter kann eigenständig Ausgaben in Höhe von 5.000 € für Ersatzbeschaffungen tätigen, falls Herr Mustermann nicht innerhalb einer Stunde erreichbar ist. Der IT-Mitarbeiter nutzt 100 Prozent seiner Arbeitszeit für die IT und stellt seine 50 Prozent als Verwaltungsmitarbeiter ein.

Zeitkritische Prozesse: 3rd Level-Anfragen lösen

Zeitkritische Ressourcen:

- PC: gWAZ: < 7 Tage, wWAZ: 8 Tage
- Laptop: gWAZ: < 7 Tage, wWAZ: 8 Tage
- Router: gWAZ: < 7 Tage, wWAZ: 3 Tage
- Firewall mit VPN-Gateway: gWAZ: < 7 Tage, wWAZ: ? Tage
- Switch: gWAZ: < 7 Tage, wWAZ: 21 Tage
- Telefone: gWAZ: < 7 Tage, wWAZ: 6 Tage
- Telefonanlage: gWAZ: < 7 Tage, wWAZ: ? Tage
- Smartphones: gWAZ: < 7 Tage, wWAZ: 6 Tage
- Fileserver: gWAZ: < 7 Tage, wWAZ: 5- 8 Tage
- Fernwartungssoftware: gWAZ: < 7 Tage, wWAZ: 1 Tage
- nicht IT relevanten Objekte außen vor gelassen

Melde- und Berichtspflichten an interne und externe Stellen: keine, da Herr Mustermann im Rahmen seiner Tätigkeit im Kernteam bereits informiert ist

Notfallkontakte: IT-Mitarbeiter:

- dienstlich Tel.: 012345/ 6789
- dienstliche E-Mail: IT.Mitarbeiter@mustermann.de
- private Tel.: 09876/ 54321 oder 0151123456789
- private E-Mail: Hans.Meier@besipiel.de

Notfallmaßnahmen: Maßnahmen zur Reduzierung der wWAZ, falls diese über der gWAz liegen:

PC:

- im Notfall: Belegschaft der Entwicklung müssen ihre PCs die Service-Abteilung am Hauptstandort bereitstellen. Die Installation der benötigten Software kann innerhalb eines Tages erfolgen.
- neue geschätzte wWAZ: 2 Tage

Laptop:

- es werden keine Maßnahmen ergriffen, da durch die geringe wWAZ der PCs das Erreichen des Notbetriebsniveaus sichergestellt ist.
- neue geschätzte wWAZ: 8- 10 Tage

Firewall mit VPN-Gateway:

- vorbeugend: Eine Sicherung und eine Dokumentation der Konfiguration erstellen.
- im Notfall: Ersatzgerät beschaffen und anschließend Sicherung einspielen bzw. Konfiguration gemäß Dokumentation. Falls kein baugleiches Gerät verfügbar ist, muss die Konfiguration per Dokumentation des Gerätes und Dokumentation des alten Geräts manuell durchgeführt werden.
- Ein Ersatzgerät, kann aufgrund des finanziellen Rahmens des aktuellen BCMS nicht vorgehalten werden.
- Nach aktuellen Recherchen zum Beschaffungszeitraum ist die neue geschätzte wWAZ: 8 Tage

Switch:

- vorbeugend: Sicherung und Dokumentation der Konfiguration erstellen. Den ausgelaufenen Wartungsvertrag erneuern und in den SLAs eine maximale Ausfallzeit von 6 Tagen vereinbaren.
- im Notfall: Service kontaktieren und je nach Ausfall den Switch anschließend neu konfigurieren.
- neue geschätzte wWAZ: 6 Tage

Telefonanlage:

- Es werden keine Maßnahmen getroffen, da mit den Smartphones eine leichter umzusetzende Alternative vorhanden ist.
- neue geschätzte wWAZ: ? Tage

Smartphones:

- Die wWAZ liegt bei den Smartphones vor Ort innerhalb der gWAZ.

- im Notfall: Die auswärtigen Mitarbeiter werden angewiesen, mit Ihren Privatgeräten Telefonate zu führen und sich anschließend die Kosten erstatten zu lassen.
- neue geschätzte wWAZ: 5 Tage
- Anmerkung: Der Notbetrieb wäre zwar ohne die auswärtigen Beschäftigten möglich, jedoch wird durch diese Maßnahme das Notbetriebsniveau deutlich erhöht.

Der GFP wird vom BCB geprüft und durch Herrn Mustermann freigegeben.

4.1.10 Wiederanlauf- und Wiederherstellungsplanung

Die „Wiederanlauf- und Wiederherstellungsplanung“ findet beim „Reaktiv-BMCS“ nicht statt.

Der Unterschied zwischen Wiederanlauf und Wiederherstellung besteht darin, dass beim Wiederanlauf „nur“ der Notbetrieb und bei der Wiederherstellung der Normalbetrieb erreicht wird.

In der Wiederanlaufplanung (WAP) werden die Maßnahmen für jedes Objekt detailliert aufgeführt, so dass im Notfall eine Person mit gleichem Fachwissen das Erreichen des Notbetriebs sicherstellen kann. Dabei sind für jeden WAP der Zweck, der Geltungsbereich bzw. das abgesicherte Element, der Aktivierungsprozess, die relevanten Dokumente, die Voraussetzungen für die Wiederinbetriebnahme der Ressource und die Notfallmaßnahmen zu erfassen.

Der Schwerpunkt liegt hier auf dem Ablauf der Notfallmaßnahmen, der schrittweise und detailliert zu dokumentieren ist. Voneinander abhängige oder parallel ablaufende Schritte sind zu kennzeichnen. Des Weiteren ist festzulegen, welche Personen (nicht namentlich, sondern als Funktion) diesen Schritt durchführen und in welchem zeitlichen Rahmen die Durchführung des Schrittes zu erfolgen hat. Dies kann durch Checklisten, bebilderte Dokumentationen oder Ähnliches erfolgen, wobei immer sichergestellt sein muss, dass diese Dokumente im Notfall zugänglich sind.

Nach der Erstellung eines WAP für jedes Objekt, sollte ein übergeordneter WAP erstellt werden, in dem alle Abhängigkeiten klar ersichtlich sind. Anschließend müssen die vollständigen, plausiblen und aktuellen WAPs freigegeben werden.

Die Wiederherstellungsplanung ist optional und beschreibt die Vorgehensweise von der Notfallstufe bis zum Erreichen des Normalbetriebs. Da diese Pläne von Notfall zu Notfall sehr unterschiedlich sein können, sollte hier der Detaillierungsgrad geringgehalten werden und eher grobe Überlegungen angestellt werden. Das BSI nennt als Beispiele [30, p. 186]:“

- Übersicht zu Möglichkeiten der Beschaffung neuer Ressourcen, inklusive einer gewählten Präferenz und gegebenenfalls schon im Vorfeld geregelter Aspekte wie Vorverträge, etc.
- Anleitung zur Inbetriebnahme, Integration der Ressource und entsprechende Funktionstests vor Inbetriebnahme (Häufig bereits in Betriebshandbüchern abgedeckt und kann hier referenziert werden.
- Technischer Wechsel von der Ersatzlösung auf die neue Lösung
- Abgleich oder Migration wiederhergestellter Datenstände mit dem im Notbetrieb abweichend erstellten Datenbestand
- Ergänzende organisatorische Maßnahmen (z. B. Erstellung von Migrationshilfen, notwendige Schulungen/Trainings, Anpassung von Prozessaktivitäten/Prozessdokumentation)“

4.1.11 Üben und Testen

Übungen und Tests sind notwendig, um die Funktionsfähigkeit der BAO und möglichst realistische Bedingungen sicherzustellen. Tests sind unterdies Sonderformen von Übungen, die abschließend mit „bestanden“ oder „nicht bestanden“ bewertet werden. Grundsätzlich sind im BSI fünf Arten von Übungen vorgesehen:

- Planbesprechung, optional beim „Reaktiv-BCMS“
- Stabsübung
- Stabsrahmenübung, nicht für „Reaktiv-BCMS“ vorgesehen
- Alarmierungsübung
- Funktionstest, optional für „Reaktiv-BCMS“

Für alle Übungen ist im Vorfeld ein Übungsleiter zu benennen, der mindestens den Zeitraum, den Ort mit Raum, die Übungsziele, die Übungsteilnehmer und das Übungsszenario festlegt.

In der Planbesprechung werden die einzelnen Pläne des BCMS mit allen an der Umsetzung des Plans beteiligten Personen besprochen. Dazu sollte der Plan auf Vollständigkeit, Plausibilität und Aktualität überprüft werden, was durch die

Anwendung des Plans auf ein theoretisches Szenario geschieht. Bei der Planübung stehen Ziele wie Sensibilisierung, Klärung von Zuständigkeiten und Überprüfung der GFPs im Vordergrund.

Die Stabsübung soll die Funktionsfähigkeit des Stabes sicherstellen. Zu diesem Zweck sollte ein realistisches Übungsszenario ausgearbeitet werden, das der Stab zu bewältigen hat. Das Übungsszenario sollte detailliert ausgearbeitet werden und neben dem Ausgangsereignis mehrere weitere Ereignisse beinhalten, auf die reagiert werden muss. Des Weiteren müssen Regeln für die Übung definiert werden. Diese sollten Mindestkriterien für den Abbruch der Übung beinhalten, zudem kann auch die Kommunikation der Stabsmitglieder nach außen oder die Kennzeichnung von Übungsdokumenten geregelt werden. Zuletzt muss das notwendige Personal sichergestellt sein. Neben den Übungsteilnehmern, wird mindestens ein Protokollant, benötigt, um die spätere Auswertung zu erleichtern. Zudem sollte, wenn möglich, mehrere Unterstützungskräfte als „Statisten“ teilnehmen, um realitätsnah, z.B. Kunden zu simulieren, und je nach personellen Möglichkeiten auch zusätzliche Personen als Beobachter teilnehmen, um neutrale Verbesserungsvorschläge zu erhalten.

Die Stabsrahmenübung ist eine Erweiterung der Stabsübung, die neben dem Stabsteam auch die Notfallbewältigungsteams mit einbezieht.

Bei Alarmierungsübung wird die Erreichbarkeit und Reaktionszeit der Stabsmitglieder oder anderer Notfallkontakte getestet. Je nach Festlegung im BCMS kann dies auch zu ungünstigen Zeiten, wie nachts, kurz nach Feierabend oder an Sonntagen, erfolgen. Hierdurch soll sowohl die Zeit bis zur Bestätigung des Informationseingangs als auch die Zeit bis zum Eintreffen im zugewiesenen Raum ermittelt und dokumentiert werden.

Beim Funktionstest werden die Vorsorge- und Notfallmaßnahmen auf ihre Durchführbarkeit überprüft. Der Schwerpunkt liegt auf dem Erreichen der Notfallstufe innerhalb der gWAZ. Insbesondere bei dieser Übungsform besteht die Möglichkeit von Auswirkungen auf den Normalbetrieb, weshalb diese immer in Absprache mit dem Management oder einer Testumgebung durchgeführt werden sollten.

Jede Übung muss nach Abschluss evaluiert und nachbereitet werden. Dabei sind Übungen, die Mängel aufzeigen, ebenso als Erfolg zu werten wie fehlerfreie Übungen. Bei festgestellten Mängeln müssen Maßnahmen zu deren Beseitigung erarbeitet werden.

Es ist ein Übungs- und Testplan zu erstellen, der mindestens die nächsten zwölf Monate umfasst.

Für die Mustermann GmbH wurde in Tabelle 7 ein Übungs- und Testplan erstellt, verantwortlich ist für jede Übung der BCB.

Tabelle 7: Übungs- und Testplan Mustermann GmbH

Nr.	Übungsart	Datum/ Zeitraum	Ziel und Umfang der Übung	Ressourcen
01	Alarmier-ungstest	15.08.23 10:00 Uhr	Überprüfung der Meldewege und der Reaktionszeit der Stabsmitglieder	Stabsmitglieder, je 2 Stunde
02	Stabs-übung	06.11.23 8-12 Uhr	Abläufe des Szenarios „Ausfall der CNC-Maschinen“ üben	Mitglieder des Stabs, Szenario-Ablaufplan, ca. 7 Tage Vorbereitung 1 Tage Nachbereitung je Teilnehmer
03	Funktions-test	29.01 – 02.02.24	Test der Notfallmaßnahmen für die Firewall	Firewall-Leihgerät, IT-Mitarbeiter 5 Tage
04	Alarmier-ungstest	14.04.24 16:00 Uhr	Überprüfung der Meldewege und der Reaktionszeit der Stabsmitglieder	Stabsmitglieder, je 2 Stunde

4.1.12 Leistungsüberprüfung und Berichterstattung

Der Schritt „Leistungsüberprüfung und Berichterstattung“ findet beim „Reaktiv-BMCS“ nicht statt.

Leistungsüberprüfung und Berichterstattung dient der kontinuierlichen Verbesserung und Aufrechterhaltung des BCMS sowie der frühzeitigen Erkennung von eventuell auftretenden Mängeln und Abweichungen. Dazu müssen zunächst Messziele definiert werden, die den aktuellen Zustand des BCMS angemessen darstellen und Vollständigkeit, Aktualität, Angemessenheit, Wirksamkeit, Plausibilität und Wirtschaftlichkeit umfassen. Die Messziele müssen durch Kennzahlen darstellbar sein. Die Leistungskennzahlen können quantitativer Natur, d.h. die im BCMS betrachteten Prozesse werden ins Verhältnis aller Prozessen gesetzt, oder qualitativer Natur sein, d.h. Abweichungen des Ist-Zustandes von den Vorgaben des BCMS werden ermittelt. In Bild 12 und 13 werden Beispiele für Leistungskennzahlen gemäß BSI dargestellt.:

Geschäfts-prozess	In BIA be-trachtet?	Zeitkritisch?	Im GFP vorhanden?	Qualität des GFP?	Anhand des GFP geübt?
A	Ja	Ja	Ja	Angemessen und plausibel	GFP ist funktions-fähig und wirksam
B	Nein	*Fehlende Daten*	*Fehlende Da-ten*	*Fehlende Daten*	*Fehlende Daten*
...	...	...	...	...	...
Z	Ja	Nein	Nicht relevant	Nicht vorhanden	Nicht vorhanden
Gesamt	25/26 (96 % aller Geschäfts-prozesse)	6/26 (23 % aller Geschäftspro-zesse)	6/6 (100 %) 1 unbekannt	4/6 (66,6 % aller GFP aktuell, angemes-sen und plausibel) 1 unbekannt	3/6 (50 % aller GFP wirksam) 1 unbekannt

Bild 12: Beispiele für quantitative Leistungskennzahlen [30, p. 216]

Kennzahl	BCM-Prozess-schritt	Zielwert
Abdeckungsgrad der Geschäftsprozesse gemäß Prozess-landkarte in der BIA	BIA	N = 100 %
Aktualität der BIA-Daten	BIA	Letzte Aktualisierung < 365 Tage
Anteil zeitkritischer Geschäftsprozesse	BIA	N < 50%
Abdeckungsgrad zeitkritischer Geschäftsprozesse in den GFP	GFP	N = 100 %
Aktualität der GFP	GFP	Letzte Aktualisierung < 365 Tage
Abdeckungsgrad zeitkritischer Ressourcen in der Übungsplanung	Üben und Testen	N = 100 % über 3 Jahre
Abdeckungsgrad der Wiederanlaufpläne in der Übungs-planung	Üben und Testen	N = 100 % über 3 Jahre
Abdeckungsgrad der Geschäftsfortführungspläne in der Übungsplanung	Üben und Testen	N = 100 % über 3 Jahre
Termintreue in der Bearbeitung offener Maßnahmen der Maßnahmenliste	Kontinuierliche Verbesserung	N = 100 %

Bild 13: Beispiele für qualitative Leistungskennzahlen [30, p. 217]

Nachdem alle Leistungsindikatoren gesammelt wurden, sind diese auf Abweichungen und Mängel im BCMS zu untersuchen. Falls Probleme identifiziert wurden, ist die Ursache zu ermitteln und der Schweregrad abzuschätzen. Abschließend ist eine Prioritätenliste zur Behebung der Probleme zu erstellen.

Soweit möglich, sollte auch eine Überwachung der externen Dienstleister erfolgen, z. B. durch Vor-Ort-Kontrollen oder durch Berichte der Dienstleister.

Das BCMS sollte regelmäßig oder aus gegebenem Anlass, durch eine interne oder externe Revision oder durch ein Audit überprüft werden. Dazu wird das gesamte BCMS oder ein vorher definierter Ausschnitt detailliert geprüft und die Ergebnisse in einem Abschlussbericht dokumentiert.

Die gesammelten Daten über den aktuellen Stand des BCMS sind vom BCB regelmäßig aufzubereiten und der Geschäftsleitung vorzulegen, da diese die Gesamtverantwortung trägt. Die Geschäftsführung kann dann auf Basis des Berichtes die notwendigen Entscheidungen bezüglich des BCMS treffen.

4.1.13 Aufrechterhaltung und Verbesserung

In der Phase „Aufrechterhaltung und Verbesserung“ werden die in den Phasen „Übung und Testen“ und „Leistungsüberprüfung und Berichterstattung“ festgestellten Mängel behoben. Dazu müssen konkrete Maßnahmen erarbeitet, umgesetzt und auf ihre Wirksamkeit überprüft werden. Dabei ist für jeden Mangel die Ursache zu ermitteln und zu dokumentieren. Des Weiteren sind die Maßnahmen zu priorisieren, ein Verantwortlicher zu benennen, die benötigten Ressourcen zu dokumentieren und ein Realisierungszeitraum festzulegen.

Darüber hinaus ist für das „Reaktiv-BCMS“ festzulegen, ob es erst zum „Aufbau-BCMS“ oder direkt zum „Standard-BCMS“ weiterentwickelt werden soll. Ein Umsetzungszeitplan, für die Weiterentwicklung, ist zu erstellen. Eine Weiterentwicklung des „Reaktiv-BCMS“ ist zu empfehlen, da aufgrund der ausgelassenen Schritte und des begrenzten Mitteleinsatzes nur ein unzureichender Schutz erreicht wird. Je größer die Abweichung des Ist-Zustandes des BCMS vom Soll-Zustand ist und je kleiner die prozentuale Anzahl an abgesicherten Geschäftsprozessen ist, desto größer ist der Weiterentwicklungsbedarf des BCMS.

Bei der Mustermann GmbH hat sich Herr Mustermann aufgrund des BCB-Reports und der darin identifizierten Probleme, wie z.B. Nichteinhaltung der wWAz bei der Firewall, nicht optimale Lösungen, wie z.B. die Nutzung privater Geräte, und teilweise nicht vorhandene GFPs-Maßnahmen, z.B. für Laptops, dazu entschlossen, das BCMS zu einem „Aufbau-BCMS“ und langfristig zu einem „Standard-BCMS“ auszubauen. Als Ablaufplan dient Tabelle 8.

Tabelle 8: Zeitplan der BCMS-Weiterentwicklung der Mustermann GmbH

Zeitraum	Schritt
ab 01.08.23 – 01.03.24	Weiterentwicklung des „Reaktiv-BCMS“ zu einem „Aufbau-BCMS“ bei gleichem Geltungsbereich
ab 01.06.24 – 31.09.24	Erweiterung des Geltungsbereiches um „Entwicklung“
ab 01.10.24 – 31.12.24	Erweiterung des Geltungsbereiches um „Verwaltung“
ab 01.02.25 – 01.06.25	Externes Review
ab 01.07.25 – 31.10.25	Erweiterung des Geltungsbereiches um „IT“
31.12.2025	Erreichen des Niveaus „Standard-BCMS“

4.1.14 Vergleich von BSI 200-4 mit BSI 100-4

Der, in der Entwicklung befindliche, Standard BSI 200-4 wird nun mit dem noch aktuell gültigen Standard BSI 100-4 verglichen.

Der wesentliche Unterschied besteht darin, dass der BSI 100-4 kein Stufenmodell für den Reifegrad des BCMS enthält. Der BSI 100-4 gibt diesbezüglich lediglich an, dass eine Anpassung an die jeweilige Organisation stattfinden muss und somit auch für KMOs geeignet ist [38, p. 2]. Der BSI 200-4 arbeitet mit dem PDCA-Zyklus [30, p. 15], dieser wird im BSI 100-4 nicht explizit erwähnt, jedoch wird auch hier deutlich, dass die einzelnen Schritte zu wiederholen sind [38, p. 10]. Ein weiterer Vorteil der BSI 200-4 ist die Zertifizierbarkeit des „Standard-BCMS“ nach ISO 22301 [30, p. 10]. Dies ist mit dem BSI 100-4 nicht möglich, da dieser zeitlich vor der ISO 22301 erschienen ist, siehe Bild 3. Der BSI 200-4 ist als Managementsystem konzipiert, während die BSI 100-4 als Prozess konzipiert ist. Ein Managementsystem ist umfassender als ein Prozess und erfordert

zusätzliche organisatorische Maßnahmen. Dafür wird das Synergiepotenzial mit anderen Managementsystemen, z.B. ISMS, durch den BSI 200-4 erhöht. Die Kapitelstruktur wurde bei der Aktualisierung von BSI 100-4 zu 200-4 grundsätzlich überarbeitet.

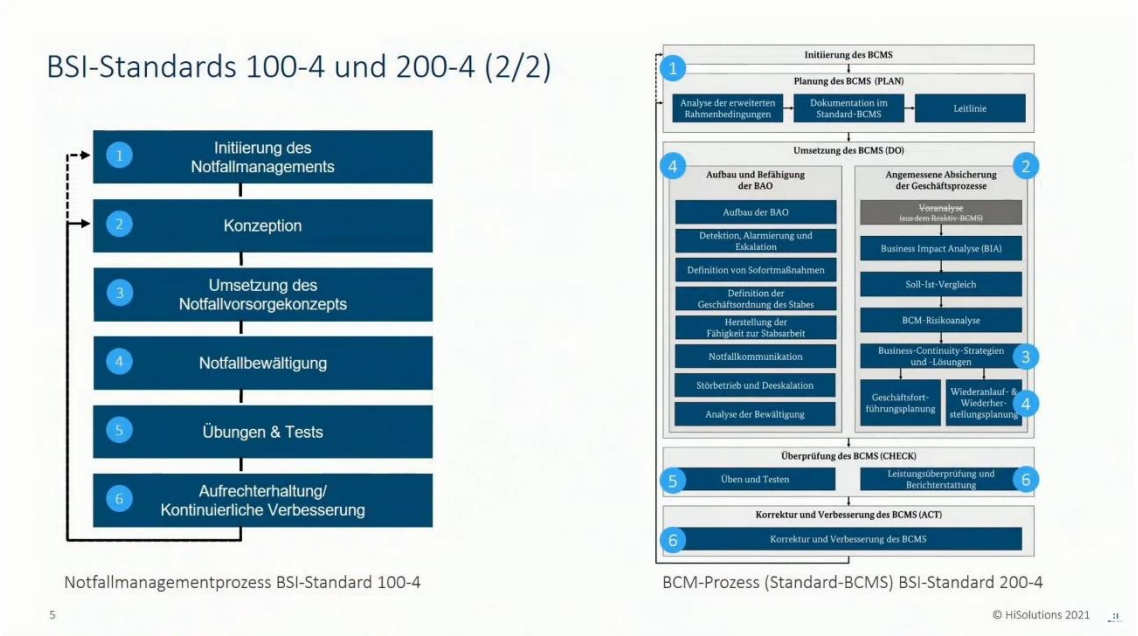

Bild 14: logische Zuordnung der BSI 100-4 Schritte zu BSI 200-4 [79]

Die dargestellte Zuordnung, im Bild 14, entspricht der logischen Zugehörigkeit. Allerdings erfolgt die schriftliche Abbildung davon wie folgt.

Die Kapitel „Initiierung des BCMS durch die Institutionsleitung“, „Konzeption und Planung des BCMS“ und „Aufbau und Befähigung der BAO“, des BSI 200-4, sind im BSI 100-4 in „Initiierung des Notfallmanagement-Prozesses“ zusammengefasst.

Die Kapitel „Voranalyse“, „Business Impact Analyse“, „Soll-Ist-Vergleich“, „BCM-Risikoanalyse“ und teilweise „Business-Continuity-Strategien und Lösungen“, des BSI 200-4, ist beim BSI 100-4 in „Konzeption“ zusammengefasst.

Das Unterkapitel „Umsetzung der BC-Strategien und Lösungen“, des BSI 200-4, ist beim BSI 100-4 durch „Umsetzung des Notfallvorsorgekonzepts“ dargestellt.

Der BSI 200-4 bildet durch die Kapitel „Geschäftsfortführungsplanung“ und „Wiederanlauf- und Wiederherstellungsplanung“ das Kapitel „Notfallbewältigung

und Krisenmanagement“ des BSI 100-4 differenzierter ab.

„Üben und Testen“ wird bei beiden in einem eigenen Kapitel abgebildet.

Beim BSI 200-4 erfolgte mit „Leistungsüberprüfung und Berichterstattung“ und „Aufrechterhaltung und Verbesserung“ eine Aufteilung des Kapitels „Aufrechterhaltung und kontinuierliche Verbesserung“ des BSI 100-4.

Die Ressourcenkategorie „Dienstleistungen“, die beim BSI 200-4 in allen Aspekten integriert ist, wird im BSI 100-4 in einem eigenen Kapitel „Outsourcing und Notfallmanagement“ dargestellt.

Beim BSI 100-4 ist ein Kapitel „Tool-Unterstützung“ erfasst, was nicht im BSI 200-4 abgebildet wird. Hier wird auf die Möglichkeit eingegangen, Software zum Planen, Erledigung von Maßnahmen und Bewältigung von Notfällen einzusetzen.

Die grundlegenden Aufgaben, Konzepte und die Struktur sind gleich, was den Vorteil hat, dass der Übergang von BSI 100-4 zu BSI 200-4 mit wenigen Anpassungen möglich ist. Die BSI 200-4 ist mit 234 Seiten im Vergleich zu 123 Seiten bei der BSI 100-4 deutlich umfangreicher. Die extra Seiten resultieren aus Praxisbeispielen, Synergiepotenzialen zu anderen Managementsystemen und ausführlicheren Beschreibungen. Durch die ausführlicheren Beschreibungen ist die erste Auseinandersetzung mit dem BSI 200-4 zwar aufwendiger, aber die anschließende Durchführung leichter. Das Stufenmodell erleichtert zudem den Einstieg in das BCM.

4.2 Ausarbeitung VdS 10000

Die VdS 10000 ist ein Standard für ISMS und explizit für KMOs konzipiert. Die VdS wurde vom BSI 2019 mit den Worten: „Das Regelwerk VdS 10000 „Informationssicherheitsmanagementsystem für KMU“ stellt ebenso wie die Basis-Absicherung des IT-Grundschutzes einen geregelten Prozess zur Einführung eines ISMS dar. Ebenfalls vergleichbar sind die beschriebenen Handlungsfelder. Unterschiede ergeben sich jedoch in der Ausprägung der einzelnen Anforderungen, die das VdS-Regelwerk in einigen Handlungsfeldern weniger konkret ausformuliert. Somit stellen die Anforderungen der VdS 10000 eine Teilmenge der Basis-Absicherung des IT-Grundschutzes dar und bilden eine gute Basis zur Implementierung eines ISMS gemäß IT-Grundschutz oder ISO 27001.“ beschrieben [80] [81]. In Bild 15 ist der geschätzte Aufwand für die Einführung verschiedener ISMS-Ansätze dargestellt.

Bild 15: Aufwandsvergleich zwischen ISMS-Vorgehensweisen [80]

Es zeigt sich, dass der Aufwand zur Realisierung der VdS 10000 deutlich geringer ist als bei anderen ISMS-Ansätzen. Der Geltungsbereich der VdS 10000 kann eingeschränkt werden. Durch die Unterscheidung zwischen verpflichtenden und empfohlenen Maßnahmen, kann der Aufwand teilweise nochmals reduziert werden [48, p. 6].

Es ist jedoch zu beachten, dass ISMS primär auf den Schutz von IT-Systemen

im Normalbetrieb ausgerichtet ist und nur bedingt Elemente für den Notfall enthält. ISMS-Normen decken daher vor allem die präventiven Maßnahmen eines ITSCM ab. Dennoch erfolgt eine beispielhafte Ausarbeitung, damit KMOs, die bereits ein ISMS eingeführt haben oder dies planen, die Auswirkungen auf ITSCM abschätzen können. Im ISMS wird üblicherweise neben der Verfügbarkeit auch die Integrität und Vertraulichkeit von Objekten ermittelt. Da hier jedoch untersucht werden soll, inwieweit das Regelwerk bereits Aufgaben des ITSCM erfüllt, werden Integrität und Vertraulichkeit nur am Rande betrachtet.

Die Unterkapitel „4.2.1“ bis „4.2.15“ entsprechen den Überschriften der VdS 10000 und behandeln, das entsprechende Kapitel [48].

4.2.1 Organisation der Informationssicherheit

Zu Beginn der Implementierung müssen die Verantwortlichkeiten definiert, zugewiesen und dokumentiert werden. Indem für jeden Verantwortungsbereich die Ziele, Aufgaben, Berechtigungen, benötige Mittel, die Kontrollinstanz und wahrnehmende Organisationseinheit zugeordnet werden, sind die wichtigsten Punkte abgedeckt. In begründeten Ausnahmefällen, darf von den Prinzipen der Funktionstrennung abgewichen werden. Funktionstrennung bedeutet, dass nicht die gleiche Person sowohl für Umsetzung als auch die Kontrolle von Maßnahmen zuständig ist. Die Abweichung muss durch adäquate Kontrollinstanzen kompensiert werden. Dabei sieht die VdS 10000 folgende Verantwortungsverteilung vor.

Das Topmanagement, muss die Gesamtverantwortung übernehmen, die IR-Richtlinie erlassen, die Arbeitsmittel bereitstellen, die IS in die Organisation zu integrieren und nachgeordnete Verantwortlichkeiten zuzuweisen.

Der Informationssicherheitsbeauftragte (ISB) steuert, koordiniert und prüft die Verwirklichung des ISMS mit Hilfe der IS-Leitlinie und Überprüfung der darin enthaltenen Ziele. Der ISB ist gegenüber dem Informationssicherheitsteam (IST) berichtspflichtig.

Das IST setzt sich aus Führungsebene, ISB, IT-Verantwortliche,

Mitarbeitervertretung und Datenschutzbeauftragter zusammen, mit der Aufgabe den ISB, bei der Implementierung, zu unterstützen.

Der IT-Verantwortliche ist für die Gestaltung der IS-Richtlinie in seinem Bereich zuständig, indem er in Abstimmung mit dem ISB technische und organisatorische Maßnahmen festlegt.

Darüber hinaus ist ein Administrator zu benennen, der für die technische Umsetzung der Maßnahmen verantwortlich ist.

Darüber hinaus listet die VdS 10000 noch folgende Personenkategorien auf:

- Vorgesetzter, der für die Einhaltung der IS-Maßnahmen von seiner Belegschaft zuständig ist.
- Mitarbeiter, die die IS-Maßnahmen einzuhalten bzw. umsetzen haben und Störungen melden müssen.
- Projektverantwortliche, die Rücksprache mit dem ISB halten, falls das Projekt Auswirkungen auf die IS haben könnte.
- Externe, die Zutritt, Zugang oder Zugriff auf IT-Systemen haben, müssen ebenfalls die IS-Maßnahmen einhalten bzw. umsetzen.

Die einzelnen Positionen werden in der IS-Leitlinie definiert.

4.2.2 Leitlinie zur Informationssicherheit (IS-Leitlinie)

Die IS-Leitlinie muss von der Geschäftsführung verfasst und erlassen werden. Die IS-Leitlinie ist jährlich auf ihre Aktualität zu überprüfen und gegebenenfalls anzupassen. Neben den Definitionen der Rollen muss die Leitlinie die Ziele und den Stellenwert des IS in der Organisation hervorheben und Konsequenzen bei Nichteinhaltung der Leitlinie beinhalten.

Eine kurze IS-Leitlinie für die Mustermann GmbH findet sich in Anlage 4, auch hier liegt der Schwerpunkt auf ITSCM.

4.2.3 Richtlinien zur Informationssicherheit (IS-Richtlinien)

Die IS-Richtlinien sind konkretere Vorgaben als die IS-Leitlinie und müssen vom ISB in Zusammenarbeit mit dem IST erstellt und aktualisiert werden. Die Inkraftsetzung erfolgt durch das Management und alle Arbeitnehmer, die sie zu

befolgen haben, werden rechtzeitig in Kenntnis gesetzt. Eine IS-Richtlinie muss mindestens die Zielgruppe, den Grund für die Richtlinie, die Übereinstimmung mit anderen Leit- und Richtlinien sowie die Konsequenzen bei Verstößen beinhalten. Alle gesetzlichen, vertraglichen und behördlichen Anforderungen sind zu beachten. Mindestens eine Regelung muss für den Nutzer vorhanden sein, die das Arbeiten mit IT-Systemen grundsätzlich regelt. Ein konkretes Beispiel findet sich in der VdS 10000, vgl. [48, pp. 16-17]. Je nach Struktur und eingesetzten IT-Systemen können weitere spezifische Regelungen erforderlich sein, z. B. für:

- Mobile IT-Systeme
- Mobile Datenträger
- IT-Outsourcing und Cloud-Computing
- Datensicherung
- Störungen und Ausfälle
- Sicherheitsvorfälle

Eine exemplarische Ausarbeitung für „IT-Systeme“ sowie „Störungen und Ausfälle“ befinden sich in Anlage 7 und 8.

4.2.4 Mitarbeiter

Die Mitarbeiter spielen im IS eine zentrale Rolle. Deshalb sind von der Auswahl des Mitarbeiters bis zur Beendigung des Arbeitsverhältnisses Maßnahmen in Bezug auf die IS zutreffen.

Bei der Auswahl der Angestellten sind Qualifikation und Vertrauenswürdigkeit die entscheidenden Faktoren.

Zu Beginn des Arbeitsverhältnisses sollte ein geregelter Prozess implementiert werden, der sicherstellt, dass der Beschäftigte zur Vertraulichkeit, Einhaltung der IS-Leit- und Richtlinien verpflichtet und eingewiesen wird. Eine Schulung zu den relevanten IS-Maßnahmen hat, während der Aushändigung der erforderlichen IT-Ausstattung, zu erfolgen.

Im Fall eines Arbeitsplatzwechsels oder der Beendigung des Arbeitsverhältnisses muss ebenfalls ein Verfahren existieren, dass die erforderlichen Änderungen zuverlässig umsetzt und ggf. über die Änderungen

informiert.

Darüber hinaus wird im Anhang der VdS darauf hingewiesen, dass ein Verfahren festlegen muss, wer für die Umsetzung verantwortlich ist und wie die Dokumentation und eine kontinuierliche Verbesserung zu erfolgen hat.

Bei der Mustermann GmbH könnte das Verfahren grob wie folgt aussehen:

Der Vorgesetzte ist dafür verantwortlich, dass Personalveränderungen frühzeitig (mindestens zwei Wochen vorher) an die IT gemeldet werden. Dabei ist anzugeben, welche IT-Systeme und Berechtigungen benötigt werden (am besten durch Angabe eines Kollegen mit gleichen Voraussetzungen). Darüber hinaus ist der Vorgesetzte verpflichtet, der IT mitzuteilen, was mit den Daten und dem E-Mail-Verkehr geschehen soll, wenn der Angestellte die Organisationseinheit verlässt.

Die IT ist dafür verantwortlich, dass alle erforderlichen IT-Systeme und Berechtigungen bis zum Dienstantritt des Arbeiters eingerichtet sind. Es dürfen keine Berechtigungen vergeben werden, die über den Antrag hinausgehen. Bei Dienstantritt wird der Kollege in die IT-Systeme und IS-Maßnahmen eingewiesen. Bei Beendigung des Arbeitsverhältnisses werden alle vorhandenen IT-Materialien eingezogen und alle Berechtigungen gelöscht. Bei einem Wechsel der Organisationseinheit werden alle nicht mehr benötigten IT-Ressourcen eingezogen und alle Berechtigungen vollständig gelöscht. Um anschließend die neuen Berechtigungen zu vergeben. Hierdurch wird verhindert, dass alte Berechtigungen vergessen werden.

Eine Verbesserung, des darüber beschriebenen Prozesses, wird durch regelmäßiges Feedback zwischen Vorgesetzten, IT und Mitarbeitern sichergestellt.

4.2.5 Wissen

Mangelndes Wissen und Verständnis über Bedrohungen und Störfallmanagement stellt ein erhebliches Risiko dar, deshalb muss ein Prozess etabliert werden, der sicherstellt, dass die gesamte Belegschaft über einen

angemessenen Wissensstand verfügt. Dieser Wissensstand ist je nach Tätigkeitsbereich unterschiedlich. So sollten sich insbesondere IT-Mitarbeiter regelmäßig über neue Bedrohungen und deren Abwehr informieren. Für andere Organisationseinheiten kann es hingegen ausreichend sein, über Grundlagen, Sofortmaßnahmen und verantwortliche Ansprechpartner informiert zu sein. Die Wirksamkeit der Schulungen sollte getestet und durch Feedback verbessert werden.

Bei der Mustermann GmbH ist festgelegt, dass sich der IT-Mitarbeiter mindestens einmal täglich auf der Website des BSI über Cyber-Sicherheitswarnungen informiert [82]. Zudem wird das Unternehmen der „Allianz für Cyber-Sicherheit“ beitreten, um sich in den dortigen Foren auszutauschen [83].

Für Kollegen aus anderen Organisationseinheiten führt der IT-Mitarbeiter zweimal jährlich IS-Schulungen durch. Die Teilnahme an einer der Schulungen ist verpflichtend. Die Schulung wird mit einem Multiple-Choice-Test beendet, bei dem mindesten 75 Prozent der Fragen richtig beantwortet sein müssen. Bei nicht bestehen, muss die Schulung bei nächster Gelegenheit wiederholt werden. Anonyme Verbesserungsvorschläge zur Schulung können eingereicht werden. Neue Mitarbeiterinnen und Mitarbeiter werden bei der Ersteinweisung in die IT-Systeme mit den Grundlagen der IS vertraut gemacht.

4.2.6 Identifizieren kritischer IT-Ressourcen

Der ISB muss die kritischen IT-Ressourcen identifizieren und die Aufstellung mindestens einmal jährlich überprüfen und aktualisieren. Für die Realisierung verweist die VdS 10000 auf die ISO/IEC 27001 oder den BSI-Standard 200-2. Weiterhin wird festgelegt, dass bei der Wahl einer alternativen Methode diese mindestens die Prozesse mit hohem Schadenspotenzial, die kritischen Informationen und die kritischen IT-Mittel identifizieren und dokumentieren muss.

Bei den Prozessen ist es wichtig mindestens, eine Beschreibung, die Begründung des Schadenspotenzials, den Verantwortlichen sowie die maximal MTA zu definiert.

Für Informationen müssen zunächst Auswahlkriterien definiert werden, wobei zwischen qualitativen und quantitativen Kriterien unterschieden wird. Qualitative Kriterien geben Merkmale an, wie z.B. personenbezogene Daten besonderer Kategorie, quantitative Kriterien geben eine Menge an, z.B. wenn 30 Prozent der Datensätze betroffen sind. Anhand dieser Kriterien wird die Auswahl begründet.

Ausgehend von den Prozessen und Informationen können die kritischen IT-Objekte bestimmt werden. Indem betrachtet wird, welche IT-Elemente von den Prozessen mit hohem Schadenspotenzial benötigt werden bzw. von welchem IT-System die Informationen verarbeitet werden. Jetzt muss, eine Beschreibung, Begründung der Kritikalität und die MTA der IT-Objekte dokumentiert werden. Hierbei muss die MTA der IT-Systeme kleiner als die MTA der darauf laufenden Prozesse sein und Abhängigkeiten zu anderen IT-Ressourcen berücksichtigt werden.

Alle ermittelten Ergebnisse werden vom Management freigegeben. In Bezug auf die Bewertung sind die Auswirkungen der Beeinträchtigungen auf Vertraulichkeit, Integrität und Verfügbarkeit zu prüfen. Im Folgenden wird nur eine Bewertung der Verfügbarkeit vorgenommen. Die Bewertung der Vertraulichkeit und Integrität würde analog erfolgen.

Für die Mustermann GmbH wurde entschieden, sich am BSI-Standard 200-2 zu orientieren, im Wesentlichen werden die Kapitel „7.3 Identifikation und Festlegung der kritischen Assets (Kronjuwelen)“, „7.5 Schutzbedarfsfeststellung“ und „8.2 Schutzbedarfsfeststellung“ als relevant identifiziert [84, pp. 70-73,104-132].

Folgende Prozesse definiert Herr Mustermann als Kronjuwelen (wichtigste Prozesse und Informationen), Erstinbetriebnahme, Störungsbehebung, Produktion der neuen Modellreihe sowie von Einzelmodellen. In den Informationen werden die Konstruktionspläne der zukünftigen, aktuellen und individuellen Spritzgießmaschinen als Kronjuwelen identifiziert.

Die Definitionen der Schutzbedarfskategorien werden aus dem BSI-Standard 200-2 übernommen, siehe Anlage 5, mit Ausnahme der Kategorie

„Beeinträchtigung der Aufgabenerfüllung“, die in Tabelle 9 definiert wird. Dennoch ist zu beachten, dass sich die MTA, trotz der Ausrichtung des ISMS auf den Normalbetrieb, auf Ausfälle bzw. Wiederanlaufpläne und nicht auf Störungen bezieht [48, p. 37].

Tabelle 9: Definition „Beeinträchtigung der Aufgabenerfüllung“

Stufe	Beschreibung
normal	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die MTA liegt zwischen 7 und 14 Tagen.
hoch	• Die Beeinträchtigung würde von einigen Betroffenen als nicht tolerabel eingeschätzt werden. • Die MTA liegt zwischen 3 und 7 Tagen.
sehr hoch	• Die Beeinträchtigung würde von den Betroffenen als nicht tolerabel eingeschätzt werden. • Die MTA liegt unter 3 Tagen.

Im Übrigen wird für die Schadenskategorien, die beim aktuellen Objekt nicht betroffen sind, „nicht relevant“ angegeben.

In Tabelle 10 erfolgt die beispielhafte Ausarbeitung, wiederum anhand des Prozesses „Störungsbehebung“.

Tabelle 10: Bewertung des Schadenpotenzials „Störungsbehebung“

Schadensszenario	Schutzbedarfsstufe
Verstoß gegen Gesetze/ Vorschriften/Verträge	sehr hoch
Beeinträchtigung des informationellen Selbstbestimmungsrechts	nicht relevant
Beeinträchtigung der persönlichen Unversehrtheit	nicht relevant
Beeinträchtigung der Aufgabenerfüllung	hoch
Negative Innen- oder Außenwirkung	hoch
Finanzielle Auswirkungen	sehr hoch

Anschließend wird der bestimmte Schutzbedarf an die IT vererbt. Die Vererbung erfolgt meistens in der Kette: Prozess bzw. Information -> Anwendung -> IT-System -> Netz -> Infrastruktur

Außerdem kann eine direkte Vererbung erfolgen, falls ein Objekt in der Kette fehlt.

In Tabelle 11 werden die Objekte aufgelistet, die von dem Prozess „Störungsbehebung“ benötigt werden und somit auch die Schutzbedarfsstufe erben.

Tabelle 11: Vererbung des Schutzbedarfs: „Störungsbehebung“

Anwendung	- Windows - Fernwartungssoftware - Fileserver (als Dienst) - iOS
IT-System	- PC bzw. Laptop - Router - Firewall mit VPN-Gateway - Switch - Telefone mit Telefonanlage - Smartphone - Server
Netz	- internes Netz - VPN - Mobilfunk
Infrastruktur	- Bürogebäude am Hauptstandort - Serverschrank - Büro - Homeoffice-Büro - Fahrzeug

4.2.7 IT-Systeme

Für jedes IT-System ist eine Bestandsaufnahme und Dokumentation eines eindeutigen Identifikationsmerkmales, des Standortes und der Funktion durchzuführen. Wichtige Zusatzinformationen wie Versionen, Lizenzen sowie Konfigurationsmerkmale und Serviceverträge sollten ebenfalls erfasst werden.

Ein Prozess für die Erstinbetriebnahme und Konfigurationsänderungen muss implementiert werden. Dieser stellt sicher, dass die Kritikalität geprüft sowie der Basisschutz eingehalten wird. Zusätzlich muss eine Inventarisierung und Aktualisierung des Netzwerkplans erfolgen. Die Dokumentation der Inbetriebnahme bzw. Änderung muss gewährleistet sein.

Bei der Außerbetriebnahme von IT-Systemen ist ein Verfahren zu implementieren, das sicherstellt:

- erforderlichen Daten zusichern
- alle Informationen sicher aus dem System zu löschen bzw. zu vernichten

- eine Aktualisierung der Inventarisierung und des Netzplans erfolgt
- eine Dokumentation erstellt wird

Die VdS 10000 sieht einen Basisschutz für alle IT-Systeme vor. Die Nichteinhaltung des Basisschutzes muss durch eine Analyse des daraus resultierenden Risikos kompensiert werden. Der Basisschutz setzt sich aus folgenden Aspekten zusammen.

Ein Basisschutz der Software ist gegeben, wenn nur die notwendige Software mit möglichst wenig Rechten sowie Sicherheitsupdates installiert sind. Die Sicherheitsupdates müssen durch ein Verfahren freigegeben und aus einer vertrauenswürdigen Quelle bezogen sein.

Der Netzwerkverkehr wird auf ein notwendiges Minimum beschränkt, wenn eine nicht behebbare Schwachstelle vorliegt oder das IT-System aus dem Internet erreichbar ist. IT-Systeme, für die die Organisation keine Administrationsrechte hat, sollten vermieden werden.

Eine zentrale Protokollierung von fehlgeschlagenen Anmeldeversuchen, Fehlern und IS-relevanten Ereignissen muss erfolgen. Dazu muss die Systemzeit der IT-Systeme synchronisiert sein. Es besteht eine Aufbewahrungspflicht von sechs Monaten.

Externe Schnittstellen sind auf ein Minimum zu reduzieren und der Bootvorgang von nicht freigegebenen Medien ist zu unterbinden.

Ein Virenschutzprogramm muss eingesetzt werden, dass die Ausführung von Schadprogrammen verhindert und in kurzen Zyklen nach aktualisiertem Pattern sucht. Darüber hinaus sollte ein Echtzeitschutz eingesetzt werden.

Der Zugang zu IT-Systemen muss durch ein Authentifizierungsverfahren gesichert werden, das Brute-Force-Angriffe erschwert, Sitzungen bei Inaktivität automatisch beendet oder sperrt und sichere Protokolle für die Netzwerkauthentifizierung verwendet. Darüber hinaus sollten Zugänge zentral verwaltet sowie komplexe Passwörter verwendet werden. Dabei müssen Standardpasswörter geändert und Mehr-Faktor-Authentifizierung als Möglichkeit geprüft werden. Darüber hinaus sollten Zugangs- und Zugriffsrechte auf, das für

die Aufgabenerfüllung notwendige Minimum, reduziert werden.

Für mobile IT-Systeme, wie z.B. Laptops, ist eine weitere IS-Richtlinie zu erlassen, die den Umgang mit diesen festlegt. In diesem Zusammenhang sollten Themen, wie die zur Verarbeitung freigegebenen Daten, Ortungsmöglichkeiten, Fernlöschungsoptionen und weitere wichtige Aspekte, vgl. [48, p. 25], geregelt werden. Der Meldeweg und Sofortmaßnahmen bei Verlust des Systems müssen festgelegt werden sowie der Schutz der Daten vor Zugriff durch Dritte, z.B. durch Verschlüsselung.

Bei Umsetzung aller genannter Maßnahmen ist der Basisschutz der VdS 10000 erfüllt. Bei kritischen IT-Systemen sind darüber hinaus folgende Aspekte zu berücksichtigen.

Die Risikoanalyse und -behandlung muss durchgeführt werden, die sicherstellt, dass alle Gefährdungen identifiziert und nach Schadenspotenzial und Eintrittswahrscheinlichkeit bewertet und priorisiert werden. Die Behandlung muss eine Risikominderung gewährleisten. Der Prozess muss regelmäßig wiederholt und angepasst werden. Auf BSI 200-3 wird als mögliche Vorgehensweise verwiesen. Das Notbetriebsniveau muss definiert werden. Das System ist von Entwicklungs- und Testsystemen zu trennen und alle nicht benötigten Netzwerkdienste sind zu deaktivieren. Änderungen müssen vorher in einem Testsystem überprüft werden und es muss möglich sein, im Produktivsystem zu einem funktionierenden Zustand zurückzukehren. Eine Dokumentation erfasst, wer für das IT-System verantwortlich ist, wie und mit welchen Authentisierungsmerkmalen die Autorisierung erfolgt, der Hintergrund von der Inbetriebnahme und warum, wer und wann Änderungen vorgenommen hat. Das kritische IT-System muss auch über ein Datensicherungs- und Überwachungssystem verfügen. Falls die MTA des Systems nicht eingehalten werden kann, müssen Ersatzsysteme oder -verfahren vorhanden sein, um einen Notbetrieb zu erreichen. Wird kritische Individualsoftware eingesetzt, muss durch vertragliche oder organisatorische Maßnahmen die Nutzung und Anpassung, bei zukünftigen Änderungen am zugrunde liegenden System, sichergestellt werden.

Bei der Mustermann GmbH wird eine IS-Richtlinie für IT-Systeme erstellt, siehe

„Anlage 6: IS-Richtlinie für IT-Systeme“.

Am Beispiel einer der im letzten Kapitel identifizierten kritischen Ressource werden nun die zusätzlichen Maßnahmen für kritische IT-Systeme behandelt, vgl Tabelle 12. Als Gefährdungen wird die Liste des BSI herangezogen, vgl. BSI 200-3 [85, pp. 13-15]. Der Fokus liegt auf den Gefährdungen, die die Verfügbarkeit des Systems einschränken. Es wird nur eine Auswahl der Gefährdungen betrachtet, da die Bearbeitung immer gleich abläuft. Zuerst wird festgelegt, ob die Gefährdung direkte, indirekte oder keine Auswirkungen hat und anschließend, ob sie relevant ist oder nicht. Es ist zu beachten, dass „relevant“ in diesem Fall bedeutet, ob es auf dieser Ebene Maßnahmen gibt, um die Gefährdung zu reduzieren. Anschließend wird die Einstufung begründet. Es erfolgt noch keine Auswahl von Maßnahmen.

Tabelle 12: Zuordnung der verfügbarkeitsbeeinträchtigenden Gefährdungen zum Router

Gefährdung	Wirkung und Relevant	Kommentar
G 0.1 Feuer	Direkte Wirkung/ nicht relevant	Ein Feuer kann direkt die Verfügbarkeit des Routers gefährden, allerdings bestehen keine Schutzmaßnahmen vom System selbst, um die Gefahr zu verringern.
G 0.2 Ungünstige klimatische Bedingungen	Direkte Wirkung/ nicht relevant	Die Gefahr kann direkt die Verfügbarkeit des Routers beeinträchtigen, allerdings bestehen keine Schutzmaßnahmen vom System selbst, um die Gefahr zu verringern.
G 0.21 Manipulation von Hard- und Software	Direkte Wirkung/ relevant	Die Gefahr kann direkt die Verfügbarkeit des Routers beeinträchtigen, Es sind Maßnahmen zu prüfen.
G 0.26 Fehlfunktion von Geräten oder Systemen	Direkte Wirkung/ relevant	Die Gefahr kann direkt die Verfügbarkeit des Routers beeinträchtigen, Es sind Maßnahmen zu prüfen.

Abschließend muss für jede Gefährdung eine Abschätzung der Eintrittswahrscheinlichkeit und des möglichen Schadens vorgenommen werden, exemplarisch vgl. Tabelle 13. Daraus wird die Risikokategorie bestimmt. Die Mustermann GmbH übernimmt die Definitionen des BSI, siehe Anlage 7.

Tabelle 13: Bewertung einer Gefährdung des Routers

<table>
<tr><td colspan="3">Router: Verfügbarkeit: sehr hoch</td></tr>
<tr><td colspan="2">Gefährdung: Fehlfunktion von Geräten oder Systemen</td><td>Beeinträchtigte Grundwerte: Verfügbarkeit</td></tr>
<tr><td>Eintrittshäufigkeit ohne zusätzliche Maßnahmen: sehr häufig</td><td>Auswirkungen ohne zusätzliche Maßnahmen: begrenzt</td><td>Risiko ohne zusätzliche Maßnahmen: hoch</td></tr>
<tr><td colspan="3">Beschreibung: Der gesamte Datenverkehr des Unternehmens läuft über den zentralen Router. Der Datenverkehr über den Router wird mehrmals im Monat ohne ersichtlichen Grund langsam oder die Verbindung wird vollständig unterbrochen.

Bewertung: Das Problem kann meistens zügig durch einen Neustart des Routers gelöst werden, jedoch ist insbesondere in Rahmen der Fernwartung Verbindungsabbrüche problematisch, da in dieser Zeit die Maschinen der Kunden nicht Betrieben werden können.</td></tr>
</table>

Bei der Behandlung von Risiken muss zunächst festgelegt werden, welche Risikokategorie nicht mehr akzeptabel ist, um dann Maßnahmen für die darüber liegenden Gefährdungen zu ergreifen. Risiken können vermieden, vermindert oder übertragen werden. AM Beispiel des Routers wird eine Reduktion vorgenommen, vgl. Tabelle 14.

Tabelle 14: Risikobehandlung einer Gefährdung beim Router

Router: Verfügbarkeit: sehr hoch		
Gefährdung	Risikokategorie	Risikobehandlungsoption
Fehlfunktion von Geräten oder Systemen	hoch	Reduktion: Es wird ein zweites Gerät beschafft und eine Redundanz mit automatischer Umschaltung implementiert.

4.2.8 Netzwerke und Verbindungen

Die Analyse der Daten auf Schadsoftware hat zu erfolgen und eine jährliche Überprüfung der Konfiguration ist durchzuführen. Bei sicherheitsrelevanten Einstellungen muss eine Dokumentation mit folgenden Punkten, wer, wann, warum die Konfiguration vorgenommen hat und welche Wirkung daraus resultiert, erfolgen.

Der Basisschutz für das Netzwerk umfasst die Deaktivierung bzw. den Schutz nicht benötigter Netzwerkzugänge, eine Netzwerksegmentierung mit möglichst weitgehender Verbindungseinschränkung und Protokollierung fehlgeschlagener Verbindungsversuche, die Reduzierung von Remote-Zugängen zum Netzwerk, Absicherung der verbliebenen Remote-Zugänge und schließlich die Absicherung bzw. Vermeidung von Netzwerkkopplungen über unsichere Netzwerke.

Bei kritischen Verbindungen muss eine Risikoanalyse und -behandlung durchgeführt werden, siehe „Kapitel 4.2.7 IT-System“.

Die aktiven Komponenten wären bei vollständiger Ausführung bereits in den vorherigen Kapiteln abgesichert, weshalb hier nicht weiter darauf eingegangen wird.

Bei der Mustermann GmbH liegt ein aktueller Netzplan vor, vgl. „Bild 7: Netzplan der Mustermann GmbH“. Eine Segmentierung des Netzes wurde bisher nicht durchgeführt, weshalb die logische und die physikalische Netzstruktur identisch sind.

Eine Segmentierung des Netzwerkes mittels VLAN soll eingeführt werden, wobei das Routing durch die Firewall zur Zugriffsbeschränkung erfolgen soll. Im Bild 16 sind die geplanten VLANs durch farbige Rahmen dargestellt.

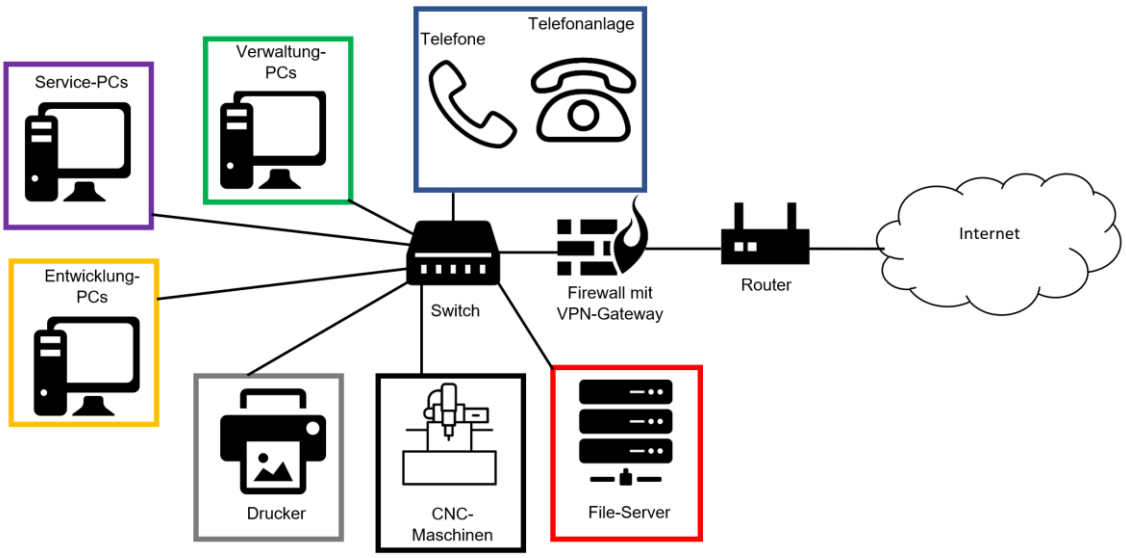

Bild 16: Darstellung der geplanten VLANs der Mustermann GmbH

Außerdem wird festgelegt, dass alle unnötigen Netzwerkzugänge deaktiviert werden. Künftige Freischaltungen sind zu beantragen. Ein Fernzugriff durch Fremdfirmen zur Fehlerbehebung bei den CNC-Maschinen erfolgt per TeamViewer und stetiger Aufsicht durch einen Verantwortlichen. Eine Verbindung der externen Belegschaft, mit dem internen Netz, erfolgt über eine VPN-Verbindung und Zwei-Faktor Authentifizierung.

Des Weiteren wird festgelegt, dass jede Konfigurationsänderung dokumentiert wird. Die Dokumentation muss beinhalten, wer, wann und warum die Konfiguration vorgenommen wurde sowie welche Wirkung diese entfaltet und evtl. wer die Konfigurationsänderung beantragt und genehmigt hat.

4.2.9 Mobile Datenträger

Für mobile Datenträger ist eine eigene IS-Richtlinie zu erlassen, die regelt, welche Daten darauf gespeichert werden dürfen. Darüber hinaus sind die Nutzer auf die besonderen Risiken mobiler Datenträger hinzuweisen und für die Vertraulichkeit, der darauf befindlichen Daten, verantwortlich zu machen. Dabei sollte die Vertraulichkeit durch weiterführende Maßnahmen wie Verschlüsselung sichergestellt werden. Eine Risikoanalyse und -behandlung ist für kritische Datenträger erforderlich, siehe „Kapitel 4.2.7 IT-System“.

Bei der Mustermann GmbH gibt es eine Richtlinie, die zwischen zwei Datenträgern unterscheidet. Das erste Speichermedium ist verschlüsselt und darf nur bei dienstlichen Geräten verwendet werden, hat aber keine Datenbeschränkung. Der zweite Datenträger ist ein Datenträger für den Datenaustausch mit Kunden vor Ort. Auf diesem dürfen nur Daten gespeichert werden, die für den Vertragspartner freigegeben sind.

4.2.10 Umgebung

Die IT-Systeme sind vor negativen Umwelteinflüssen zu schützen. Dies sollte nach einer etablierten Richtlinie oder einem Verfahren erfolgen, das zumindest die Benennung eines Verantwortlichen für die Umsetzung, eine angemessene Dokumentation, eine kontinuierliche Optimierung und eine jährliche Überprüfung der Ergebnisse sicherstellt.

Insbesondere sind Server, aktive Netzwerkkomponenten und Netzwerkverteiler vor unbefugtem Zugriff, Umgebungsbedingungen, wie Temperatur oder Wasser, Stromschwankungen und Verlust bzw. Zerstörung zu schützen. Bei Niederspannungsanlagen sind die gängigen Normen zu beachten. Bei kritischen IT-Systemen ist zudem die Preisgabe vertraulicher Informationen zu verhindern und möglichst alle kritischen IT-Systeme in einer besonders geschützten Sicherheitszone unterzubringen.

Bei der Mustermann GmbH ist festgelegt, dass Strom- und Datenleitungen (bis zum Anschluss im Zimmer) nur von zertifizierten Handwerkern verlegt werden dürfen. Im Keller des Hauptgebäudes befindet sich ein kleiner, fensterloser und abschließbarer Serverraum mit Fileserver, Router, Firewall und Switch. Der Serverraum ist mit einer Klimaanlage und einem Rauchmelder ausgestattet, ein CO2-Feuerlöscher befindet sich ebenfalls im Raum. Weitere Schutzvorkehrungen gegen Feuer, Blitzschlag und Wasser sind durch die allgemeinen Schutzvorkehrungen des Hauptgebäudes, wie z.B. Blitzableiter, gegeben.

Für die Überwachung und Optimierung des Umgebungsschutzes für den Serverraum ist Herr Mustermann als Gesamtverantwortlicher, in

Zusammenarbeit mit dem IT-Mitarbeiter, zuständig. Mängel oder Änderungen werden dokumentieren.

Für andere IT-Systeme, wie z.B. Computer, ist kein besonderer Schutz vor Umwelteinflüssen und -bedingungen erforderlich. Ein unbefugter Zutritt und damit verbundene Diebstähle sind tagsüber eher unwahrscheinlich, da sich alle Kollegen kennen und eine betriebsfremde Person in den nicht öffentlichen Bereichen verdächtig ist. Für den nächtlichen Diebstahlschutz beschließt Herr Mustermann als Verantwortlicher für den Gebäudeschutz, einbruchhemmende Fenster und Türen einbauen zu lassen. Mobile IT-Systeme sind stets im Auge zu behalten und falls dies nicht möglich ist, mit einem Schloss zu sichern. Eine Trennung in verschiedene Sicherheitszonen wird nur für den Serverraum und den Rest des Gebäudes als praktikabel erachtet.

4.2.11 IT-Outsourcing und Cloud Computing

Es muss eine separate IS-Richtlinie für das Outsourcing erlassen werden, in der die Bedingungen und Anforderungen für das Outsourcing reglementiert sind. Bei der Planung einer externen Vergabe ist festzulegen, welche IT-Bestandteile ausgelagert werden soll, welche Bedingungen hinsichtlich Verfügbarkeit, Integrität und Vertraulichkeit erfüllt sein müssen und ob es sich um ein kritisches Element handelt. Bei Vertragsabschluss ist darauf zu achten, dass Vertragsverletzungen durchsetzbar sind und die IT-Ressource bei Vertragsbeendigung an die Organisation zurückgegeben wird. Bei kritischen IT-Objekten sind zusätzlich folgende Anforderungen zu erfüllen:

- Die Leistungserbringung muss definiert und überwacht werden.
- Die Standorte der Leistungserbringung sind definiert.
- Sicherheitsmaßnahmen zum Schutz der IT-Ressourcen sind definiert.
- Die Schnittstellen zur Organisation sind definiert.
- Ansprechpartner auf beiden Seiten sind benannt.
- Eine Geheimhaltungsverpflichtung wird vereinbart.
- Die Weitergabe von Daten an Dritte ist zu regeln.
- Eine Informationspflicht bei Sicherheitsvorfällen ist zu definieren.
- Eine Informations- und Dokumentationspflicht bei Vertragsänderungen ist erforderlich.

Die Auslagerung der Website und des E-Mail-Dienstes erfolgte bei der

Mustermann GmbH durch Herrn Mustermann selbst in Abstimmung mit dem IT-Mitarbeiter. Bei der Auswahl der Vertragspartner wurde darauf geachtet, dass die Datenverarbeitung innerhalb der EU erfolgt und ein Gerichtsstand innerhalb der EU gegeben ist. Da insbesondere eine hohe Verfügbarkeit der Dienste wichtig ist, wurde bei den Vertragsbedingungen darauf geachtet, dass eine Verfügbarkeit von 99 Prozent gegeben ist. Die Wahl fiel für das Webhosting auf AWS und für den E-Mail-Dienst auf 1&1. Die weiteren Anforderungen sind in den Verträgen geregelt, können aber aufgrund des Abhängigkeitsverhältnisses nicht vollständig umgesetzt werden.

4.2.12 Zugänge und Zugriffsrechte

Bei der Verwaltung von Zugängen und Zugriffsrechten ist sicherzustellen, dass beantragte Berechtigungen nur nach Genehmigung erteilt werden. Im Zuge der Genehmigung ist zu prüfen, ob die Berechtigungen für die Aufgabenerfüllung erforderlich sind. Während bei der Vergabe von Berechtigungen eine Begründung für den Bedarf unverzüglich mitzuteilen ist, kann dies beim Entzug unterbleiben. Vor dem Entzug von Berechtigungen ist zu prüfen, ob Daten weitergegeben, gesichert oder gelöscht werden müssen. Bei administrativen Berechtigungen ist der Bedarf detailliert zu begründen und vom IT-Verantwortlichen zu prüfen. Alle Vorgänge im Zusammenhang mit Berechtigungen sind zu dokumentieren. Berechtigungen für kritische IT-Systeme sind jährlich auf ihre Notwendigkeit zu überprüfen.

Im Kapitel „6.2.4 Mitarbeiter“ wurde bereits festgelegt, wie die Berechtigungen bei Dienstantritt, Wechsel der Organisationseinheit und Austritt bei der Mustermann GmbH gehandhabt werden. Dieser Prozess wird nun um die Vergabe bzw. den Entzug von Berechtigungen ohne Stellenwechsel ergänzt.

Um neue Berechtigungen zu erhalten, muss der Angestellte einen begründeten Antrag beim Vorgesetzten stellen, der diesen prüft und an den IT-Mitarbeiter weiterleitet. Wenn möglich, sollte die Berechtigung mit einem Ablaufdatum versehen werden. Der IT-Mitarbeiter führt ebenfalls eine kurze Plausibilitätsprüfung durch, stimmt sich bei Auffälligkeiten mit dem

Genehmigenden ab, und richtet die Berechtigungen ein. Darüber hinaus erfolgt die Vergabe von administrativen Rechten nur nach Freigabe durch Herrn Mustermann, als Gesamtverantwortlicher, da auf Grund der personellen Lage der IT-Mitarbeiter gleichzeitig IT-Verantwortlicher ist und somit ein Interessenkonflikt besteht.

Nicht mehr benötigte Berechtigungen sind unverzüglich dem IT-Verantwortlichen zu melden. Darüber hinaus ist jeder Beschäftigte verpflichtet, seine bestehenden Berechtigungen jährlich auf Notwendigkeit zu überprüfen und nicht mehr benötigte Berechtigungen dem IT-Mitarbeiter zu melden. Der IT-Mitarbeiter prüft quartalsweise, ob alle abgelaufenen Berechtigungen entzogen wurden. Ferner erfolgt einmal jährlich gemeinsam mit Herrn Mustermann einer Prüfung der Berechtigungen für kritische IT-Systeme. Es folgt jeweils eine Aktualisierung der Dokumentation durch den IT-Mitarbeiter.

4.2.13 Datensicherung und Archivierung

Für die Datensicherung und Archivierung empfiehlt die VdS 1000 die Umsetzung des BSI 200-2. Ansonsten ist eine gesonderte IS-Richtlinie für die Speicherorte der Daten zu erlassen. Darüber hinaus ist zu prüfen, welche Daten aufgrund betrieblicher, gesetzlicher und vertraglicher Vorgaben archiviert werden müssen. Ein Datensicherungs- und Datenwiederherstellungsprozess muss eingerichtet werden, der sicherstellt, dass die Daten gegen Verlust, Beschädigung und Einsichtnahme während der Übertragung geschützt sind, die Sicherung in einem anderen Brandabschnitt erfolgt, die Wiederherstellung getestet und das Testergebnis dokumentiert wird. Darüber hinaus sollte geprüft werden, ob eine regelmäßige Auslagerung von Sicherungen an einen entfernten Ort und mehrere Versionsstände der Daten erforderlich sind. Das Datensicherungs- und Wiederherstellungskonzept ist jährlich vom ISB zu überprüfen und anzupassen.

Als Basisschutz fordert die VdS 10000, dass Speicherorte, Server, Systemsoftware und Konfiguration der aktiven Netzwerkkomponenten mindestens alle 24 Stunden gesichert werden. Darüber hinaus sind Vorgaben für die Datensicherung mobiler IT-Systeme zu machen.

Bei kritischen IT-Systemen muss sichergestellt werden, dass die in der Risikoanalyse ermittelte MTD und MTA nicht überschritten wird.

Bei der Mustermann GmbH wird festgelegt, dass dienstliche Daten nur auf dem Fileserver und nicht auf der lokalen Festplatte gespeichert werden dürfen. Zusätzlich wird das Sicherungsintervall, des Fileservers, von einmal wöchentlich auf einmal täglich umgestellt. Die Daten der aktiven Komponenten werden vor und nach Änderungen manuell gesichert. Betriebsrelevante Daten dürfen nicht ausschließlich auf mobilen Geräten gespeichert werden. Deshalb müssen Daten, vor der Übertragung auf mobilen Geräten, auf den Fileserver gesichert sein. Daten, die im Außendienst erzeugt werden, müssen bei nächster Gelegenheit auf dem Fileserver übertragen werden.

Derzeit besteht keine Möglichkeit, die Backups in einem anderen Brandabschnitt zu lagern. Daher ist geplant, in der Produktionshalle in einem geschützten Raum einen Serverschrank mit Festplatten für Backups einzurichten. Nach der Einrichtung dieses Raumes sollen verschiedene Versionen von Backups erstellt werden. Im Ringspeicherverfahren sollen Backups von einer Woche vorhanden sein. Zusätzlich soll das Backup vom Monatsersten einen Monat lang aufbewahrt werden. Eine Auslagerung an einen anderen Ort ist nicht vorgesehen.

4.2.14 Störungen und Ausfälle

Die VdS 10000 empfiehlt zur Absicherung von Störungen und Ausfällen die Implementierung einer etablierten BCM-Norm, wie z.B. BSI 100-4. Die zweite Möglichkeit ist die Entwicklung eines eigenen Vorgehens, wobei die VdS 10000 eine IT-Richtlinie, einen Reaktionsprozess und Wiederanlaufpläne für kritische IT-Objekte fordert.

In der IT-Richtlinie müssen die Begriffe „Störung“ und „Ausfall“ definiert werden, ebenso wie der Meldeweg, die Untersuchungsvorgaben und die Kommunikationsvorgaben.

Der Reaktionsprozess muss sicherstellen, dass ein Überblick über die Situation gewonnen wird, Leib und Leben geschützt werden, Sofortmaßnahmen zur

Schadensbegrenzung eingeleitet werden, der Schaden dokumentiert wird, Beweise gesichert werden, der Regelbetrieb wieder aufgenommen wird und eine Nachbearbeitung erfolgt.

Die Wiederanlaufpläne müssen Informationen enthalten, die es den zuständigen Personen ermöglichen, das IT-System oder das Ersatzsystem innerhalb der MTA auf das Notfallbetriebsniveau zu bringen. Der Plan muss die erforderlichen Mittel definieren, übersichtlich sowie jederzeit schnell verfügbar sein. Darüber hinaus muss das Dokument in einem anderen Brandabschnitt, als das IT-System, aufbewahrt werden. Ergänzend ist zu dokumentieren, von welchen IT-Elementen das aktuell betrachtete IT-System abhängig ist.

Die IS-Richtlinie der Mustermann GmbH für Störungen und Ausfälle ist in Anlage 8 enthalten. Für Störung wird hier die gleiche Definition gewählt, wie in Kapitel 4.1.1 Definitionen, damit eine einheitliche Definition in der gesamten Arbeit gewährleistet ist. In der Praxis wäre eine, je nach Wissensstand der Belegschaft, angepasste Definition von Vorteil.

Als Reaktionsprozess ist festgelegt, dass der IT-Mitarbeiter nach der Alarmierung Informationen vom Melder einholt und eine erste Einschätzung vornimmt. Weitere Informationen, falls benötigt, werden aus Logdateien und Fehlermeldungen gewonnen. Maßnahmen zum Schutz von Leib und Leben sind nicht erforderlich, da diese bei der Mustermann GmbH nicht durch IT-Systeme beeinträchtigt werden können. Entsprechende Sofortmaßnahmen werden je nach Situation durch den IT-Mitarbeiter eingeleitet. Sollte der IT-Mitarbeiter nicht erreichbar sein, muss das IT-System durch Trennung vom Netzwerk isoliert werden. Die Ausfallzeit und eventuelle physische Schäden werden dokumentiert. Der IT-Mitarbeiter sichert alle Logdateien auf zwei externen Datenträger. Anschließend wird der Wiederanlaufplan für das IT-System gestartet. Nach Erreichen des Normalbetriebs erfolgt innerhalb der nächsten zwei Wochen zwingend eine Aufarbeitung des Ausfalls.

Ein Wiederanlaufplan wird exemplarisch für den Router dargestellt:

Anleitung:

Falls der Router physisch unbeschädigt ist, dann:

1. Fritzbox vom Netzwerk und Strom trennen
2. Telefon mit Tonwahlverfahren holen
3. Fritzbox an den Strom anschließen und Telefon an den Router anschließen
4. Warten bis mindestens Power-LED leuchtet
5. Folgende Nummer eingeben**:** #991*15901590* und auf Ton warten
6. anschließend weiter machen wie unter „neu Aufsetzen“

Falls der Router physisch beschädigt ist, dann:

1. gleiches Gerät im nächsten Elektronikgeschäft kaufen
2. falls kein gleiches Gerät verfügbar ist, recherchieren welches Gerät kompatibel ist
3. kompatibles Gerät kaufen, muss vom gleichen Hersteller sein
4. anschließend weiter vorgehen, wie unter „neu Aufsetzen“ beschrieben

neu Aufsetzen:

1. Fritzbox an Strom und Netzwerk anschließen
2. http://fritz.box, http://192.168.178.1 oder http://169.254.1.1 aufrufen
3. mit Daten auf der Rückseite der Fritzbox anmelden
4. „Sicherung“ auswählen
5. „Wiederherstellung“ auswählen und die gesicherte Konfigurationsdatei auswählen
6. Ort der Konfigurationsdatei: „File-Server“: fileserver/Backup/Router/conf.txt oder grüner USB-Stick mit Beschriftung „Backup“: Router/conf.txt
7. vollständig auswählen
8. Konfiguration auf Funktionalität testen
    a. interne IP-Adressen: 10.87.23.112, 10.87.23.115, 10.87.23.117 pingen
    b. Verbindung zum Internet testen durch Aufrufen von: mustermanngmbh.de
    c. Verbindung zum E-Mail-Dienst durch Aufrufen von: https://account.1und1.de/
    d. Test von Fernwartungssoftware durch die externen Kollegen mit einer Remote-Sitzung auf einen internen PC

Ressourcen:

- IT-Mitarbeiter:
    - dienstlich Tel.: 012345/ 6789
    - dienstliche E-Mail: IT.Mitarbeiter@mustermann.de

    - private Tel.: 09876/ 54321 oder 0151123456789
    - private E-Mail: Hans.Meier@besipiel.de
- Telefon mit Tonwahlverfahren
- Evtl. bis zu 500 € für neuen Router
- funktionierender Rechner mit Netzwerkverbindung
- Kennwort der Sicherungsdatei
- Externer Mitarbeiter

Abhängigkeiten:

- Mindestens ein funktionierender Rechner
- Netzwerkverbindung
- Funktionierendes Laptop eines externen Mitarbeiters
- Funktionalität des E-Mail-Dienstes und der Webseite

4.2.15 Sicherheitsvorfälle

Für Sicherheitsvorfälle ist eine eigene IS-Richtlinie zu erlassen, die den Begriff „Sicherheitsvorfall“ definiert, die Angestellten zur Meldung an den ISB verpflichtet, die Untersuchungsmaßnahmen regelt und die Art und Weise der Kommunikation festlegt.

Es sollten Maßnahmen zur automatischen Erkennung von Sicherheitsvorfällen implementiert werden, z.B. Intrusion Detection Systeme.

Ein Prozess muss implementiert werden, um auf einen Sicherheitsvorfall zu reagieren. Dabei muss zunächst ein Überblick über die Situation geschaffen, Leib und Leben geschützt sowie Sofortmaßnahmen eingeleitet werden. Es folgen die Dokumentation des Schadens, die Beweissicherung, die Wiederaufnahme des Normalbetriebs gemäß Wiederanlaufplan und die Nachbereitung des Vorfalls.

Bei geringfügigen Vorfällen können einzelne Punkte ausgelassen werden. Bei Abwesenheit des ISB muss auch eine angemessene, zeitnahe Reaktion gewährleistet sein.

Bei der Mustermann GmbH wird eine entsprechende IS-Richtlinie erlassen. Diese definiert „Sicherheitsvorfall“ wie in Kapitel 4.1.1 dieser Arbeit.

Zur zusätzlichen automatischen Erkennung entscheidet sich Herr Mustermann für die Implementierung eines Intrusion Detection Systems.

Der Prozess zur Reaktion auf IT-Sicherheitsvorfälle entspricht dem Vorgehen bei Störungen und Ausfällen.

4.2.16 Vergleich VdS 10000 und mit BCM-Standards

Die VdS 10000 als ISMS-Norm sieht im Vergleich zu BCM-Normen eine detailliertere Vorsorge zur Vermeidung von Störungen und Ausfällen vor. Die Wiederherstellungsmaßnahmen werden aber nur knapp behandelt. Dies wird im Verhältnis des Umfangs deutlich. Die VdS 10000 behandelt Wiederherstellungsmaßnahmen nur auf ca. zwei Seiten [48, pp. 35-37]. In der BSI 200-4 werden die Geschäftskontinuität und die Wiederanlauf- und Wiederherstellungsplanung auf insgesamt 21 Seiten erfasst [30, pp. 165-186]. In der VdS 10000 werden bei den Wiederherstellungsmaßnahmen nur die IT-Systeme erfasst. Ein möglicher Ausfall anderer Ressourcen, wie z.B. Gebäude, wird nicht abgedeckt. Abschließend lässt sich festhalten, dass die Stärken der VdS 10000 vor allem in präventiven Maßnahmen für IT-Systeme liegen, während andere Prinzipien und Elemente nur grundlegend Behandelt werden.

5 Auswertung der ausgewählten Vorgehensweisen und Einschätzung des Synergiepotenzials

5.1.1 Bewertung BSI 200-4

Der BSI 200-4 ist grundsätzlich geeignet, ein ITSCM zu implementieren. Die Richtlinie beschreibt detailliert die einzelnen Schritte und gibt Hinweise zur Durchführung. Da es sich um einen BCM-Standard handelt, wird die IT nicht tiefgehend behandelt oder in Beispielen aufgegriffen. Daraus folgt, dass für die Realisierung als ITSCM bereits ausreichend IT-Fachwissen vorhanden sein muss bzw. ein zusätzlicher Rechercheaufwand betrieben werden muss, um die Schritte adäquat auf die IT zu übertragen. Dies beginnt bereits in der Initiierungsphase, bei der möglichen Festlegung des Geltungsbereiches. Hier muss bereits grundlegendes Wissen vorhanden sein, was die IT zur Aufrechterhaltung des Betriebes beiträgt, damit sie nicht direkt ausgeschlossen wird. Ein weiterer Aspekt, der tiefergehende Kenntnisse voraussetzt, ist die BIA, da die Verknüpfungen der IT und Prozesse mit den anderen Objekten, wie Einrichtungen, bekannt sein müssen. Als letztes Beispiel für nötiges Hintergrundwissen, ist der Soll-Ist-Vergleich anzuführen, bei dem ohne entsprechende Erfahrung und Kenntnisse keine Bewertung der wWAZ vorgenommen werden kann. Auch in Bezug auf die automatische Alarmierung und mögliche Schutzmaßnahmen, muss das Know-How vorhanden sein, was theoretisch und praktisch umsetzbar ist, aber auch die Fähigkeit zu bestimmen, was für das jeweilige Unternehmen geeignet ist. Größter Nachteil ist der geringe Fokus bzw. die mangelhafte Ausarbeitung auf/für präventive Maßnahmen, vgl. Kapitel 3.1.

Formell ist die Ausarbeitung noch nicht perfekt. z.B.: Durchführung des Soll-Ist-Vergleichs [30, pp. 142-143], keine genaue Definition, ob die wWAZ für ein einzelnes Gerät, oder alle für den Notbetrieb benötigten Geräte definiert werden. Geräte und wWAZ können sich je nach Prozess für das einzelne Objekt unterscheiden. Bei Betrachtung einzelner Geräte, können Synergien, die bei mehreren Geräten auftreten, nicht bedacht werden, z.B., wenn man ein Gerät mit

zwei Tagen ansetzt, aber drei davon braucht. Würde sich dies sechs Tage Wiederanlaufzeit summieren. Wenn aber ein Tag davon auf die Lieferzeit entfällt, würde die Wiederanlaufzeit in der Realität, bei drei Geräten, auf 4 Tage fallen.

5.1.2 Bewertung VdS 10000

Die VdS 10000 ist umfangreicher als die 43 Seiten der eigentlichen Norm, da an mehreren Stellen empfohlen wird, andere Normen als Hilfestellung heranzuziehen:

- ISO/IEC 27001 bzw. BSI Standard 200-2 durchführen [48, p. 19]
- VdS 2007 [48, p. 30]
- BSI 200-2 mit IT-Grundschutzkatalog [48, p. 33]
- BSI-Standard 100-4 bzw. DIN EN ISO 22301 [48, p. 36]

Es besteht zwar die Möglichkeit, jeweils ein eigenes Verfahren einzusetzen, das den Anforderungen der VdS 10000 entsprechen muss. Eigene Verfahren können individuell an die Bedürfnisse der Organisation angepasst werden. Es besteht aber auch die Gefahr, dass wichtige Aspekte ausgelassen werden, was zu einem unzureichenden Schutz führt. Aufgrund der Kürze der Norm werden teilweise keine Umsetzungshinweise gegeben, z.B. wird im Kapitel „9 Identifizierung kritischer IT-Ressourcen“ [48, pp. 19-21] nicht beschrieben, wie die MTA oder das Schadenspotenzial von Prozessen und IT-Systemen ermittelt werden kann. Dies führt dazu, dass zur Ermittlung genauer Daten entweder auf weitere Literatur zurückgegriffen werden muss oder ein erfahrener IT-Mitarbeiter vorhanden sein muss. Ansonsten können nur grobe Schätzungen vorgenommen werden. Die VdS 10000 ist grundsätzlich ungeeignet, um ein ITSCM zu implementieren, da keine adäquate Erörterung von Einrichtungen und Daten erfolgt. Bezüglich der Frage, ob und welche Auswirkungen eine Erfüllung der VdS 10000 auf das ITSCM hat, ist aus Kapitel 6.2 Ausarbeitung VdS 10000 zu schließen, dass insbesondere für die IT-Systeme ein solider Schutz und angemessene Wiederherstellungsmaßnahmen implementiert sind. Darauf aufbauend könnte eine Erweiterung der Wiederherstellungsmaßnahmen für die verbleibenden ITSCM-Elemente erfolgen, wobei für die Realisierungshilfen und Anforderungen auf andere Literatur zurückgegriffen werden muss.

5.1.3 Synergiepotenzial der betrachteten Vorgehensweisen

Das Synergiepotenzial der verschiedenen Ansätze ist je nach Kombination erheblich. Das BSI listet in BSI 200-4, als BCM-Standard, über 20 Synergieoptionen mit verschiedenen Vorgehensweisen wie ISMS und ITSCM auf [30, pp. 38,41,43,47,57,66,83,117,124,126,128,142,143,147,148,154,156,183, 190,192,200,202,208,225]. Die meisten Synergieoptionen können bei allen Ansätzen genutzt werden, da es sich um grundlegende Aspekte wie Organisationsstrukturen, Organisationsanalyse oder allgemein anwendbare Regeln handelt. Diese Aspekte werden bei allen Vorgehensweisen benötigt, so dass z.B. bei der Kombination mehrerer Vorgehensweisen die Analyse der Organisation nur einmal durchgeführt wird und nur vereinzelt nachtäglich Informationen ermittelt werden müssen.

Das Synergiepotential zwischen ITSCM und BCM ist aufgrund der Tatsache, dass ITSCM oft als Teil von BCM gesehen wird, schwer zu definieren, vgl. Kapitel 4.1.2 Abgrenzungen. Im Wesentlichen bestehen die Synergieeffekte in gemeinsamen Strukturen, Definitionen, Methoden und vor allem in der Erhöhung der BCM-Fähigkeit eines Unternehmens durch ein IT-spezifisches BCM in Form eines ITSCM. Dabei ist zu beachten, dass in den geprüften BCM-Standards die IT nicht im Detail abgebildet wird. Für die Verwirklichung eines ITSCM, innerhalb eines BCM, ist zusätzliche Recherchen oder ausreichendes Fachwissen eine Voraussetzung.

Das Synergiepotenzial zwischen BCM bzw. ITSCM und ISMS ist besonders hoch, da das ISMS den präventiven Aspekt des ITSCM durch den Schutz des IT-Normalbetriebs vollständig beinhaltet. Gleichzeitig werden die Aspekte der Wiederanlaufplanung im ISMS durch das ITSCM abgedeckt. Auch bei den betroffenen Objekten gibt es eine weitreichende Schnittmenge. Für beide Managementsysteme sind Mitarbeiter, Daten, Prozesse, Infrastruktur, IT-Systeme und Lieferanten relevant [26, p. 6] [86, pp. 44,45]. Auch hier ergeben sich die oben genannten generellen Synergieeffekte [87].

Es besteht die Möglichkeit, mehrere BCM-Ansätze zu kombinieren, da alle untersuchten BCM ähnliche Grundvoraussetzungen benötigen, vergleichbare

Einzelschritte haben und gleiche Ziele verfolgen, z.B. BIA des BSI 200-4 und der GPG2018 [30, pp. 114-140] [63, pp. 38-53]. Damit besteht die Möglichkeit, für jeden Einzelschritt eine für die Organisation passende Anleitung zu finden und umzusetzen.

6 Zusammenfassung und Ausblick

6.1 Zusammenfassung

BCM und insbesondere ITSCM stellen vor allem für KMOs eine Herausforderung in der Realisierung dar. Verstärkt wird dies durch das Fehlen von Normen und Umsetzungshilfen für ITSCM. Daher muss, bei der Implementierung, auf Vorgehensweisen zurückgegriffen werden, die eigentlich für andere Bereiche wie z.B. ISMS entwickelt wurden.

Vergleicht man verschiedene Vorgehensweisen auf Merkmale von ITSCM, so wird deutlich, dass viele Methoden Aspekte von ITSCM adressieren. Dennoch variieren die Vollständigkeit und der Detaillierungsgrad in Bezug auf ITSCM erheblich. Daher ist die Wahl der Orientierungshilfe entscheidend für einen erfolgreichen Vollzug.

Aus diesem Grund wurden in dieser Arbeit elf Vorgehensweisen, die Schnittmengen mit ITSCM aufweisen, nicht tiefgehender, verglichen. Zwei davon werden anhand eines fiktiven Kleinunternehmens exemplarisch ausgearbeitet. Damit soll die Auswahl einer geeigneten Implementierungsgrundlage erleichtert werden.

Allerdings wird deutlich, dass mit keiner der untersuchten Vorgehensweisen eine vollständige und detaillierte Abwicklung eines ITSCM möglich ist. Auf Basis der detailliert analysierten Methoden lässt sich festhalten, dass der gewählte BCM-Standard zwar solide organisatorische Strukturen schafft, um auf Notfälle und Katastrophen zu reagieren, jedoch keine detaillierte Durchführung im IT-Bereich erfolgt. Dies hat zur Folge, dass für die Umsetzung entweder ein IT-Mitarbeiter mit entsprechendem Fachwissen, ein externer IT-Experte oder weiterführende Literatur benötigt wird. Im geprüften ISMS-Standard werden vor allem die präventiven Maßnahmen für IT-Systeme umfassend behandelt. Auch der Notfall und die Wiederherstellung von IT-Systemen werden angemessen berücksichtigt. Die anderen Aspekte wie Organisation, Daten und Prozesse werden jedoch

weitestgehend ausgeklammert.

Daher wäre eine Kombination mehrerer Orientierungshilfen eine Option, die gegenüber einer unabhängigen Verwirklichung, Vorteile durch Synergieeffekte oder zumindest eine deutliche Ressourceneinsparung, bietet.

Die Realisierung von Normen wie der VdS 10000 oder der BSI 200-4 als „reaktives BCM“ stellt aber auch für KMOs eine große Herausforderung dar. Da nur zwölf Prozent der Unternehmen mit zehn bis 49 Beschäftigten und 43 Prozent der Unternehmen mit 50 bis 250 Angestellten einen eigenen IT-Mitarbeiter beschäftigen [88], müsste für die Durchführung eines ITSCM oder einer anderen IT-Richtlinie externes Fachwissen eingekauft werden.

Meiner Einschätzung nach ist es für Kleinstorganisationen, nach Definition Statistisches Bundesamt [89], nicht realistisch, ein BCM oder ITSCM gemäß einem der untersuchten Methoden einzuführen. Diese sollten sich auf Maßnahmen gegen die gefährlichsten Angriffsvektoren als präventive Maßnahmen und auf die Wiederherstellungsmaßnahmen mit der höchsten Kosten-Nutzen-Bilanz konzentrieren. Die fünf häufigsten Auslöser für Cybersicherheitsvorfälle sind in absteigender Reihenfolge Phising, Ausnutzen von Schwachstellen, Fehlkonfigurationen, kompromittierte Anmeldeinformationen und Anbieter in der Lieferkette [90]. Zumindest für die ersten beiden Schwachstellen, kann mit Schulungen, E-Mail-Filtern und regelmäßigen Updates aller Systeme, relativ leicht ein erhöhtes Schutzniveau erreicht werden. Für die Wiederherstellung der Betriebsfähigkeit sind bei IT-Systemen Backups der Daten und Konfiguration sowie eine detaillierte Dokumentation der Konfiguration als wichtigste Maßnahme anzusehen [91] [92] [93].

Für Kleinorganisationen, nach Definition Statistisches Bundesamt [89], ist es, meines Erachtens, sinnvoll, sich an einem Standard, z.B. BSI 200-4, zu orientieren. Die Vorgaben sollten aber an die eigenen Bedürfnisse angepasst bzw. vereinfacht werden, wenn keine Zertifizierung notwendig oder gewünscht ist. Damit dies möglich ist, muss jedoch ein gewisses Grundwissen vorhanden sein. Im Beispielunternehmen dieser Arbeit könnten die Organisation und die

Definitionen der Verantwortlichkeiten vereinfacht werden, da aufgrund der flachen Hierarchie und des einzelnen IT-Mitarbeiters, die Geschäftsführung immer involviert ist und der IT-Mitarbeiter mehrere der vorgegebenen Rollen innehat. Weitere Erleichterungen könnten sein, dass auf Basis des Hintergrundwissens einige Aspekte von vornherein ausgeschlossen werden können, um keine Kapazitäten bei der Implementierung zu binden. Beispielsweise wird es für ein kleines Unternehmen kaum möglich sein, einen Ausweichstandort zur Verfügung zu stellen oder man stellt fest, dass der Ausfall des Betriebsstandortes und der damit verbundene Schaden durch eine Versicherung abgedeckt ist. Eine genauere Betrachtung dieser beiden Sachverhalte kann damit schon ausgeschlossen werden.

Wird die IT-Infrastruktur bereits durch einen externen Dienstleister bereitgestellt, kann es sinnvoll sein, das ITSCM weitestgehend an diesen auszulagern, was jedoch ein hohes Vertrauen in den externen Dienstleister voraussetzt und mit höheren Kosten verbunden ist.

Bei mittelgroßen Organisationen, im Sinne des Statistischen Bundesamtes [89], sollte die Gestaltung nach einer Norm erfolgen, ohne diesen weiter zu vereinfachen. Hierbei sollte eine „Einstiegsstufe“, wie das „Reaktiv-BCMS“ gewählt werden und eine anschließende kontinuierliche Verbesserung zu einer vollständigen Umsetzung erfolgen.

6.2 Ausblick

Die Ergebnisse der Arbeit geben einen groben Überblick über die Vielfalt der IT-Standards der verschiedenen Teildisziplinen und stellen die Anwendbarkeit für die Durchführung eines ITSCM übersichtlich dar. Im Rahmen der Arbeit wurden jedoch nicht alle aktuellen Vorgehensweisen untersucht und es konnte nur eine kleine Auswahl exemplarisch ausgearbeitet werden. Außerdem wurden im Rahmen der Arbeit nur Vorgehensweisen analysiert, die allgemein gültig sind. In der Realität gibt es jedoch neben diesen Normen eine Reihe von branchen- oder länderspezifischen Vorgehensweisen, die teilweise verpflichtend sind, wie z.B. die „High-level principles for business continuity“ für Banken [94] [22]. Eine

Erweiterung könnte daher durch die Aufnahme weiterer allgemeiner Richtlinien oder durch den Vergleich branchenspezifischer Anforderungen erfolgen.

Zudem entwickeln sich die genannten Dokumente regelmäßig weiter oder werden durch neue ersetzt, z.B. die Entwicklung des in dieser Arbeit betrachteten BSI 200-4 aus dem BSI 100-4. Zudem hat die ISO am zwölften April 2023 einen neuen Entwurf der ISO 27031 zur Abstimmung freigegeben [95]. Der wesentliche Unterschied besteht jedoch nur in einer neuen Strukturierung der Norm. Weitere erwähnenswerte Änderungen sind die engere Zusammenarbeit mit dem BCM [95, pp. 7,15,21] und der Hinweis, dass bei zu großen Abweichungen zwischen gewünschtem und tatsächlich realisierbarem Notfallbetriebsniveau aus Kostengründen eine Überprüfung des Notfallbetriebsniveaus bzw. der gesetzten Ziele notwendig ist [95, p. 29].

Die in dieser Arbeit gewonnenen Erkenntnisse sind daher nur für einen begrenzten Zeitraum gültig und könnten in Zukunft durch neue Orientierungshilfen aktualisiert werden. Dabei ist zu erwarten, dass diese, sofern es sich nicht um eine spezifische Ausarbeitung für ITSCM handelt, ITSCM auch nicht vollständig und detailliert dargestellt werden kann.

Abschließend ist daher festzuhalten, dass die Entwicklung eines spezifischen ITSCM-Standards wünschenswert ist. Eine andere Option wäre, dass eine vorhandene Norm erweitert wird bzw. weitere ITSCM spezifische Hilfsmaterialien erhält. Dies könnte beim BSI 200-4 der Fall sein, da bereits mehrere Hilfsmittel für diesen existieren [96]. Mit einer spezifischen Richtlinie mit Umsetzungshilfen könnte die Implementierung insbesondere für KMOs erleichtert werden.

Literaturverzeichnis

[1] Marhel Group, „Business Continuity Management," [Online]. Verfügbar: https://www.marhelgroup.de/wiki/business-continuity/. [Zugriff am 06 Mai 2023].

[2] M. Santunione, „Risk Management: benefits in the business battlefield - mentoring by Sun Tzu," 20 März 2023. [Online]. Verfügbar: https://www.thebci.org/news/risk-management-benefits-in-the-business-battlefield-mentoring-by-sun-tzu.html. [Zugriff am 06 Mai 2023].

[3] S. Erb, Business Continuity, Wiesbaden: Springer Gabler, 2017.

[4] A. Streim und S. Mann, „Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr," [Online]. Verfügbar: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr#_. [Zugriff am 06 Mai 2023].

[5] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2022," [Online]. Verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8. [Zugriff am 06 Mai 2023].

[6] M. Holland, „Nach Cyberangriff: Rhein-Pfalz-Kreis erwartet Normalbetrieb im Frühsommer," 12 Januar 2023. [Online]. Verfügbar: https://www.heise.de/news/Nach-Cyberangriff-Rhein-Pfalz-Kreis-erwartet-Normalbetrieb-im-Fruehsommer-7457667.html. [Zugriff am 06 Mai 2023].

[7] C. Raum, „Hundertprozentige Sicherheit ist unmöglich," 16 März 2001. [Online]. Verfügbar: https://www.faz.net/aktuell/wirtschaft/it-sicherheit-hundertprozentige-sicherheit-ist-unmoeglich-124350.html. [Zugriff am 06 Mai 2023].

[8] T. Haase und P. Schmitz, „Entlastung durch Schulungen und Outsourcing Unternehmen haben IT-Sicherheit selbst in der Hand," 21 November 2019. [Online]. Verfügbar: https://www.security-insider.de/unternehmen-haben-it-sicherheit-selbst-in-der-hand-a-884335/. [Zugriff am 06 Mai 2023].

[9] Allianz SE, „100-prozentige Sicherheit gibt es nicht," 10 Dezember 2014. [Online]. Verfügbar: https://www.allianz.com/de/presse/news/unternehmen/standpunkte/141210-100-prozentige-sicherheit-gibt-es-nicht.html. [Zugriff am 06 Mai 2023].

[10] C. Louie, „Closing The Gap: The Quest to Achieve One Hundred Percent Cyber Coverage," Dezember 2016. [Online]. Verfügbar: https://www.chrislouie.net/blog/2018/12/16/closing-the-gap-the-quest-to-achieve-one-hundred-percent-cyber-coverage. [Zugriff am 06 Mai 2023].

[11] Controllit AG, „BCM-Beratung," [Online]. Verfügbar: https://www.controll-it.de/de/bcmberatung. [Zugriff am 06 Mai 2023].

[12] CONSUVATION GmbH, „Business Continuity Management - Notfallmanagement," [Online]. Verfügbar: https://www.consuvation.com/ISO22301/. [Zugriff am 06 Mai 2023].

[13] Controllit AG, „Wirksamkeit des BCM während der COVID-19-Pandemie," [Online]. Verfügbar: https://www.controll-it.de/source/PDF/COVID-19_Umfrage_de.pdf. [Zugriff am 06 Mai 2023].

[14] S. Spörrer, Business Continuity Managment ISO 22301 und weitere Normen im Rahmen der Informationstechnologie, Wiesbaden: Springer Gabler, 2018.

[15] „EN ISO 22301:2019," *Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (ISO 22301:2019); Deutsche Fassung EN ISO 22301:2019*, Berlin, Beuth Verlag GmbH.

[16] M. Hämmerle, „Aus BS 25777 wurde ISO/IEC 27031:2011," [Online]. Verfügbar: https://www.bcm-news.de/2011/04/28/aus-bs-25777-wurde-isoiec-270312011/. [Zugriff am 01 Juni 2023].

[17] „ISO/IEC 27031:2011-03," [Online]. Verfügbar: https://www.beuth.de/de/norm/iso-iec-27031/140332996. [Zugriff am 06 Mai 2023].

[18] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-4," [Online]. Verfügbar: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html. [Zugriff am 06 Mai 2023].

[19] BCM Academy GmbH, „ITSCM - IT Service Continuity Management," [Online]. Verfügbar: https://www.bcmacademy.de/de/ausbildung/itscm. [Zugriff am 06 Mai 2023].

[20] D. Antonicelli, „Vergleich von IS-Frameworks: Übersicht, Gemeinsamkeiten, Unterschiede," [Online]. Verfügbar: https://www.fhnw.ch/plattformen/iwi/2019/04/15/vergleich-von-is-

frameworks-uebersicht-gemeinsamkeiten-unterschiede/. [Zugriff am 12 Mai 2023].

[21] D. Kosutic, „Information security & business continuity standards," [Online]. Verfügbar: https://advisera.com/27001academy/knowledgebase/information-security-business-continuity-standards/. [Zugriff am 12 Mai 2023].

[22] BCM Institute, „Standards," [Online]. Verfügbar: https://www.bcmpedia.org/wiki/Standards. [Zugriff am 27 Juli 2023].

[23] M.-A. Kaufhold, T. Riebe, C. Reuter, J. Hester, D. Jeske, L. Knüver und V. Richert, „Business Continuity Management in Micro Enterprises: Perception, Strategies, and Use of ICT," [Online]. Verfügbar: https://www.peasec.de/paper/2018/2018_KaufholdRiebeReuteretal_BusinessContinuityManagementinMicroEnterprises_IJISCRAM.pdf. [Zugriff am 10 Mai 2023].

[24] „EN ISO 22300:2021," *Resilienz– Begriffe (ISO 22300:2021); Deutsche Fassung EN ISO 22300:2021*, Berlin, Beuth Verlag GmbH, 2021.

[25] „ISO/IEC 20000-1," *Information technology — Service management- Part 1: Service management system requirements*, Genf, International Organization for Standardization, 2018.

[26] „ISO/IEC 27031:2011-03," *Information technology— Security techniques— Guidelines for information and communication technology readiness for business continuity*, Genf, International Organization for Standardization, 2011.

[27] M. Hämmerle, „ITSCM Essentials," [Online]. Verfügbar: https://www.bcm-news.de/tag/irbc/. [Zugriff am 06 Mai 2023].

[28] „EN ISO/IEC 27000:2020," *Informationstechnik - Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020*, Berlin, Beuth Verlag, 2020.

[29] „NIST Special Publication 800-34 Rev. 1," *Contingency Planning Guide for Federal Information Systems*, Gaithersburg, National Institute of Standards and Technology.

[30] „BSI 200-4," *BSI-Standard 200-4 Business Continuity Management -Community Draft 2.0-*, Bonn, Bundesamt für Sicherheit in der Informationstechnik.

[31] J. Kobeleff, „Den IT-Notfall richtig managen Mit ITSCM für den Notfall gewappnet," 22 Januar 2020. [Online]. Verfügbar: https://www.security-insider.de/mit-itscm-fuer-den-notfall-

gewappnet-a-897816/. [Zugriff am 06 Mai 2023].

[32] Controllit AG, „IT Service Continuity Management," [Online]. Verfügbar: https://www.controll-it.de/de/itscm. [Zugriff am 06 Mai 2023].

[33] SysAid, „What is ITSM?," [Online]. Verfügbar: https://www.sysaid.com/resources/what-is-itsm. [Zugriff am 06 Mai 2023].

[34] T. Njogu, „Difference Between Business Continuity and Contingency Plan," [Online]. Verfügbar: http://www.differencebetween.net/business/difference-between-business-continuity-and-contingency-plan/. [Zugriff am 06 August 2023].

[35] P. Kirvan, „Definition contingency plan," [Online]. Verfügbar: https://www.techtarget.com/whatis/definition/contingency-plan. [Zugriff am 06 2023 August].

[36] K.-R. Müller, IT-Sicherheit mit System Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement - Sichere Anwendungen - Standards und Practices, Wiesbaden: Springer Vieweg, 2018.

[37] Bundesamt für Sicherheit in der Informationstechnik, „Auftrag," [Online]. Verfügbar: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html. [Zugriff am 08 Mai 2023].

[38] „BSI 100-4," *BSI-Standard 100-4 Notfallmanagement*, Bonn, Bundesamt für Sicherheit in der Informationstechnik.

[39] Bundesamt für Sicherheit in der Informationstechnik, „Anforderungskatalog zum BSI-Standard 200-4," [Online]. Verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Anforderungskatalog.xlsx?__blob=publicationFile&v=2. [Zugriff am 08 Mai 2023].

[40] National Institute of Standards and Technology, „Definition of Measurement Science," [Online]. Verfügbar: https://www.nist.gov/system/files/documents/el/isd/Definition_of_Measurement_Science-handout_v2.pdf;. [Zugriff am 04 April 2023].

[41] National Institute of Standards and Technology, „About NIST," [Online]. Verfügbar: https://www.nist.gov/about-nist. [Zugriff am 06 Mai 2023].

[42] National Institute of Standards and Technology, „Framework for Improving Critical

Infrastructure Cybersecurity," [Online]. Verfügbar: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Zugriff am 06 Mai 2023].

[43] National Institute of Standards and Technology, „Cybersecurity Framework," [Online]. Verfügbar: https://www.nist.gov/cyberframework. [Zugriff am 06 Mai 2023].

[44] „NIST Special Publication 800-53 Revision-5," *Security and Privacy Controls for Information Systems and Organizations*, Gaithersburg, National Institute of Standards and Technology.

[45] National Institute of Standards and Technology, „SP 800-53 Rev. 5," [Online]. Verfügbar: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx. [Zugriff am 06 Mai 2023].

[46] VdS Schadenverhütung GmbH, „Unternehmenssicherheit," [Online]. Verfügbar: https://vds.de/ueber-vds. [Zugriff am 06 Mai 2023].

[47] VdS Schadenverhütung GmbH, „Akkreditierungen und Notifizierung," [Online]. Verfügbar: https://vds.de/ueber-vds/akkreditierungen-und-notifizierung. [Zugriff am 06 Mai 2023].

[48] „VdS 10000," *Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), Anforderungen*, Köln, VdS Schadenverhütung GmbH.

[49] Axelos, „About Axelos," [Online]. Verfügbar: https://www.axelos.com/about-axelos. [Zugriff am 07 Mai 2023].

[50] AXELOS, „ITIL," *ITIL Doundation ITIL 4 Edition*, Norwich, The Stationery Office, 2020.

[51] PeopleCert, „ITIL Certifications," [Online]. Verfügbar: https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1. [Zugriff am 07 Mai 2023].

[52] essendi it GmbH, „Informationssicher-heits-Standards im Vergleich," [Online]. Verfügbar: https://www.essendi.de/wichtige-informationssicherheits-standards-im-vergleich/. [Zugriff am 10 Mai 2023].

[53] RANDUS IT CONSULTING, „ITIL 4 Foundation ITIL 4 Edition Buch Book Publication," [Online]. Verfügbar: https://www.randus.at/index.php/shop/itil4fd-book-axelos. [Zugriff am 16 Mai 2023].

[54] ITEMO, „ITEMO," [Online]. Verfügbar: https://itemo.org/. [Zugriff am 07 Mai 2023].

[55] CORDIS, „Service Manahement in Federated e-Infrastructures," [Online]. Verfügbar: https://cordis.europa.eu/project/id/312851/de. [Zugriff am 07 Mai 2023].

[56] „FitSM," *Part 0: Overview and vocabulary*, München, ITEMO, 2016.

[57] „FitSM," *Part 1: Requirements*, München, ITEMO, 2022.

[58] „FitSM," *Part 2: Objectives and activities*, München, ITEMO, 2016.

[59] „FitSM," *Part 3: Recommended role model*, München, ITEMO, 2016.

[60] ITEMO, „Schlankes IT Service Management mit FitSM," [Online]. Verfügbar: https://itemo.org/fitsm. [Zugriff am 07 Mai 2023].

[61] The Business Continuity Institute, „About the BCI," [Online]. Verfügbar: https://www.thebci.org/about-bci.html. [Zugriff am 07 Mai 2023].

[62] M. Hämmerle, „BCI Good Practice Guidelines 2018 Edition erschienen," [Online]. Verfügbar: https://www.bcm-news.de/2017/11/08/bci-good-practice-guidelines-2018-edition-erschienen/. [Zugriff am 18 Mai 2023].

[63] The Business Continuity Institute/ The BCI Forum, Good Practice Guidelines 2018 Edition, Salisbury: The Business Continuity Institute, 2017.

[64] Business Continuity Institute, „Good Practice Guidelines 2018 Edition - Download," [Online]. Verfügbar: https://www.thebci.org/product/good-practice-guidelines-2018-edition---download.html. [Zugriff am 16 Juni 2023].

[65] ISACA, „Our mission is simple: the pursuit of digital trust," [Online]. Verfügbar: https://www.isaca.org/about-us. [Zugriff am 07 Mai 2023].

[66] auditnet, „COBIT 2019 veröffentlicht," [Online]. Verfügbar: https://www.audit-net.net/de/themen/95-cobit-2019-veroeffentlicht. [Zugriff am 07 Mai 2023].

[67] ISACA Germany Chapter e.V., „Deutsche Version des Rahmenwerks COBIT 2019 ist online!," [Online]. Verfügbar: https://www.isaca.de/sites/default/files/isaca_germany_-_cobit_2019_uebersetzung.pdf. [Zugriff am 18 Mai 2023].

[68] D. Antonicelli, „Vergleich von IS-Frameworks: Übersicht, Gemeinsamkeiten, Unterschiede," [Online]. Verfügbar: https://www.fhnw.ch/plattformen/iwi/2019/04/15/vergleich-von-is-frameworks-uebersicht-gemeinsamkeiten-unterschiede/. [Zugriff am 21 Juni 2023].

[69] „COBIT2019," *COBIT 2019-RAHMENWERK: Governance- und Managementziele*, Berlin, ISACA Germany Chapter, 2029.

[70] IT-Sicherherheitscluster e.V., „Willkommen beim IT-Sicherheitscluster e.V.," [Online]. Verfügbar: https://www.it-sicherheitscluster.de/wer-sind-wir/. [Zugriff am 07 Mai 2023].

[71] „CISIS12_NormV10," *Compliance und Informationssicherheit in 12 Schritten*, Regensburg, IT-Sicherheitscluster e.V., 2021.

[72] IT-Sicherheitscluster e.V., „Audit und Zertifizierung," [Online]. Verfügbar: https://cisis12.de/zertifizierung/. [Zugriff am 18 Mai 2023].

[73] „CISIS12_KatalogV10," *Compliance und Informationssicherheit in 12 Schritten*, Regensburg, IT-Sicherheitscluster e.V., 2021.

[74] National Fire Protection Association, „NFPA 1600, Standard on Continuity, Emergency, and Crisis Management," [Online]. Verfügbar: https://catalog.nfpa.org/NFPA-1600-Standard-on-Continuity-Emergency-and-Crisis-Management-P1438.aspx?icid=D729. [Zugriff am 22 Mai 2023].

[75] „NFPA 1600," *NFPA 1600 Standard on Continuity, Emergency, and Crisis Management 2019*, Quincy, National Fire Protection Association, 2018.

[76] National Fire Protection Association, „NFPA overview," [Online]. Verfügbar: https://www.nfpa.org/overview. [Zugriff am 22 Mai 2023].

[77] National Fire Protection Association, „NFPA 1600®," [Online]. Verfügbar: https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600. [Zugriff am 22 Mai 2023].

[78] C. Schulz, „Die FOR-DEC Methode – die optimale Entscheidung fällen," [Online]. Verfügbar: https://www.consulting-life.de/wp-content/uploads/2017/11/FOR-DEC-Methode-Struktur.jpg. [Zugriff am 05 Juni 2023].

[79] M. Herder, „ISO 22301 und BSI 100-4 zu BSI 200-4, Marcel Herder (HiSolutions AG)," 19 Januar 2021. [Online]. Verfügbar: https://www.youtube.com/watch?v=OEcwEHH-_1k. [Zugriff am 15 Juni 2023].

[80] M. Semmler, „Das Portal rund um die VdS 10000.," [Online]. Verfügbar: https://www.vds10000-portal.de/doku.php. [Zugriff am 21 Juni 2023].

[81] H. Stüber, „VdS 10000 – Informationssicherheits-Managementsystem für KMU," [Online]. Verfügbar: https://www.datenschutz-notizen.de/vds-10000-informationssicherheits-managementsystem-fuer-kmu-5930086/. [Zugriff am 21 Juni 2023].

[82] Bundesamt für Sicherheit in der Informationstechnik, „Suche: Cyber-Sicherheitswarnungen," [Online]. Verfügbar: https://www.bsi.bund.de/SiteGlobals/Forms/Suche/BSI/Sicherheitswarnungen/Sicherheitswarnungen_Formular.html?nn=133020&cl2Categories_DocType=callforbids. [Zugriff am 27 Juni 2023].

[83] Geschäftsstelle der Allianz für Cyber-Sicherheit, „Allianz für Cyber-Sicherheit: Viele Teilnehmer - ein starkes Netzwerk - ein Ziel.," [Online]. Verfügbar: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html. [Zugriff am 27 Juni 2023].

[84] „BSI 200-2," *BSI-Standard 200-2 IT-Grunschutz-Methodik*, Bonn, Bundesamt für Sicherheit in der Informationstechnik.

[85] „BSI 200-3," *BSI-Standard 200-3 Risikoanalyse auf Basis von IT-Grundschutz*, Bonn, Bundesamt für Sicherheit in der Informationstechnik.

[86] Bundesamt für Sicherheit in der Informationstechnik, „BSI 200-1," *BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)*, Bonn, Bundesamt für Sicherheit in der Informationstechnik.

[87] L. Daus und P. Przybylski, „Business Continuity Management und Informationssicherheit," *Datenschutz und Datensicherheit Volume 47,* pp. 417-419, 27 Juni 2023.

[88] Statista Research Department, „Anteil von Unternehmen in Deutschland mit Beschäftigung eigener IT-Fachkräfte im Jahr 2020 nach Unternehmensgröße," [Online]. Verfügbar: https://de.statista.com/statistik/daten/studie/612803/umfrage/beschaeftigung-eigener-it-fachkraefte-in-unternehmen-in-deutschland/. [Zugriff am 25 Juli 2023].

[89] Statistisches Budnesamt, „Kleine und mittlere Unternehmen (KMU)," [Online]. Verfügbar: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Glossar/kmu.html. [Zugriff am 25 Juli 2023].

[90] Artic Wolf, „Die fünf wichtigsten Cyber-Angriffsvektoren," [Online]. Verfügbar: https://arcticwolf.com/resources/blog-de/die-funf-wichtigsten-cyber-angriffsvektoren/. [Zugriff am 18 August 2023].

[91] BREKOM, „Datensicherung – Warum Backups so wichtig sind, wie sie lückenlos funktionieren,“ [Online]. Verfügbar: https://brekom.de/ratgeber-it-sicherheit/datensicherung/. [Zugriff am 18 August 2023].

[92] THE BRISTOL GROUP Deutschland GmbH, „Back-up – Lebensversicherung für Unternehmensdaten und Konfigurationen,“ [Online]. Verfügbar: https://www.bristol.de/backup-strategien-und-loesungen-aus-sicht-der-it-sicherheit/. [Zugriff am 18 August 2023].

[93] CyberDirekt GmbH, „Das Sicherheitsbackup - Was macht es so wertvoll?,“ [Online]. Verfügbar: https://www.cyberdirekt.de/das-backup-grundstein-der-it-sicherheit/. [Zugriff am 18 August 2023].

[94] Bank for International Settlements, „High-level principles for business continuity,“ [Online]. Verfügbar: https://www.bis.org/publ/joint17.htm. [Zugriff am 27 Juli 2023].

[95] „ISO/IEC DIS 27031:2023-04 - Entwurf,“ *Information technology — Cybersecurity — Information and communication technology readiness for business continuity*, Genf, International Organization for Standardization, 2023.

[96] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-4: Hilfsmittel,“ [Online]. Verfügbar: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/BSI-Standard-200-4_Hilfsmittel/BSI_Standard_200_4_Hilfsmittel_node.html. [Zugriff am 03 August 2023].

Bilderverzeichnis

Bild 1: Zeitstrahl BCM-Entstehung [1] 10
Bild 2: Umfrage zur Wirksamkeit von Notfallstrategien [13] 11
Bild 3: verschiedene Normen im zeitlichen Zusammenhang [14, p. 9] 12
Bild 4: Bsp. PDF-Version NFPA 1600 [75, p. 7] 47
Bild 5: Bsp. Online-Version NFPA 1600 [74] 48
Bild 6: Organigramm mit Personenanzahl der Mustermann GmbH 52
Bild 7: Netzplan der Mustermann GmbH 52
Bild 8: „Aufbau-BCMS“ im Vergleich zu „Standard-BCMS“ [30, p. 31] 54
Bild 9: Beispiel einer Ersteinschätzung eines Schadensereignisses in der IT [30, p. 79] 60
Bild 10: FOR-DEC Führungszyklus [78] 61
Bild 11: zeitkritische Produkte und Services der Mustermann GmbH 64
Bild 12: Beispiele für quantitative Leistungskennzahlen [30, p. 216] 83
Bild 13: Beispiele für qualitative Leistungskennzahlen [30, p. 217] 84
Bild 14: logische Zuordnung der BSI 100-4 Schritte zu BSI 200-4 [79] 87
Bild 15: Aufwandsvergleich zwischen ISMS-Vorgehensweisen [80] 89
Bild 16: Darstellung der geplanten VLANs der Mustermann GmbH 105
Bild 18: BSI 200-2 Schutzbedarfskategorie "normal" [84, p. 106] 151
Bild 19: BSI 200-2 Schutzbedarfskategorie "hoch" [84, pp. 106-107] 152
Bild 20: BSI 200-2 Schutzbedarfskategorie "sehr hoch" [84, p. 107] 152
Bild 21: Matrix zur Einstufung von Risiken [85, p. 27] 157

Tabellenverzeichnis

Tabelle 1: Übersicht Ergebnisse des Vergleichs 23
Tabelle 2: Darstellung der ermittelten Geschäftsprozesse der Mustermann GmbH 67
Tabelle 3: Bewertung des Schadenpotenzials „3rd Level-Anfragen lösen“ 68
Tabelle 4: Ressourcen: „3rd Level-Anfragen lösen" 70
Tabelle 5: Vergleich der gWAZ mit der wWAZ der IT-Ressourcen 72
Tabelle 6: Soll-Ist-Vergleich des maximalen Datenverlustes der Mustermann GmbH 73
Tabelle 7: Übungs- und Testplan Mustermann GmbH 82
Tabelle 8: Zeitplan der BCMS-Weiterentwicklung der Mustermann GmbH 86
Tabelle 9: Definition „Beeinträchtigung der Aufgabenerfüllung“ 96
Tabelle 10: Bewertung des Schadenpotenzials „Störungsbehebung“ 97
Tabelle 11: Vererbung des Schutzbedarfs: „Störungsbehebung“ 98
Tabelle 12: Zuordnung der verfügbarkeitsbeeinträchtigenden Gefährdungen zum Router 102
Tabelle 13: Bewertung einer Gefährdung des Routers 103
Tabelle 14: Risikobehandlung einer Gefährdung beim Router 103
Tabelle 15: Übersicht Ergebnisse des Vergleichs; Teil 1 135
Tabelle 16: Übersicht Ergebnisse des Vergleichs; Teil 2 136
Tabelle 17: Übersicht Ergebnisse des Vergleichs; Teil 3 137
Tabelle 18: Übersicht Ergebnisse des Vergleichs; Teil 4 138
Tabelle 19: Übersicht Ergebnisse des Vergleichs; Teil 5 139
Tabelle 20: Übersicht Ergebnisse des Vergleichs; Teil 6 140
Tabelle 21: Übersicht Ergebnisse des Vergleichs; groß 141
Tabelle 22: Definition der Schadenkategorien der Mustermann GmbH 145
Tabelle 23: Kategorisierung von Eintrittshäufigkeiten des BSI 200-3 [85, pp. 26-27] 156
Tabelle 24: Kategorisierung von Schadensauswirkungen [85, p. 27] 156
Tabelle 25: Definition von Risikokategorien [85, p. 28] 157

Anlagenverzeichnis und Anlagen

Anlage 1: Übersicht Ergebnisse des Vergleichs……135

Anlage 2: BCMS-Leitlinie der Mustermann GmbH……142

Anlage 3: Definition der Schadenskategorien……145

Anlage 4: IS-Leitlinie der Mustermann GmbH……148

Anlage 5: Definitionen für die Schutzbedarfskategorien vom BSI-Standard 200-2……...151

Anlage 6: IS-Richtlinie für IT-Systeme……153

Anlage 7: Risikoeinstufung BSI 200-3……..156

Anlage 8: IS-Richtlinie für Störungen und Ausfälle……158

Anlage 1: Übersicht Ergebnisse des Vergleichs:

Tabelle 15: Übersicht Ergebnisse des Vergleichs; Teil 1

Bezeichnung des Standards / Kriterien	BSI 200-4	NIST CSF
Prinziepien von ITSCM		
Vorfallprävention	nicht betrachtet	detailliert
Vorfallerkennung	detailiert	detailliert
Reaktion	detailiert	detailliert
Wiederherstellung	detailiert	kaum
Verbesserung	detailiert	angemessen
Elemente von ITSCM		
Mitarbeiter	vollständig - angmessen	vollständig – kaum
Einrichtungen	unvollständig – kaum	nicht betrachtet
Technologie - Hardware - Netzwerk - Software	unvollständig – kaum	vollständig - kaum
Daten	unvollständig – kaum	unvollständig – kaum
Prozesse	unvollständig - kaum	unvollständig - kaum
Lieferanten	unvollständig – kaum	unvollständig – kaum
Priorisierung	vorhanden	nicht betrachtet
Allgemein:		
Unternehmensgröße	jede	jede
Branche	jede	jede
Technologieunabhängig	ja	ja
Zertifizierung	nach ISO 22301:2019 möglich	nein
Umfang	234 Seiten + 576 Anforderungen	55 Seiten
Veröffentlichung	Entwurfsphase aktulle Version Community Draft 2: August 2022	16.04.2018
Konzipiert für	BCM	IS
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	konkret, teilweise Zwang	allgemein

Tabelle 16: Übersicht Ergebnisse des Vergleichs; Teil 2

Bezeichnung des Standards / Kriterien	NIST SP 800-53	NIST SP 800-34
Prinziepien von ITSCM		
Vorfallprävention	detailliert	detailliert
Vorfallerkennung	detailliert	nicht betrachtet
Reaktion	detailliert	nicht betrachtet
Wiederherstellung	detailliert	detailliert
Verbesserung	nicht betrachtet	angemessen
Elemente von ITSCM		
Mitarbeiter	vollständig – detailliert	vollständig – kaum
Einrichtungen	vollständig – detailliert	unvollständig – kaum
Technologie - Hardware - Netzwerk - Software	vollständig – detailliert	unvollständig – angemessen
Daten	unvollständdig - angemessen	unvollständig – kaum
Prozesse	vollständig - detailliert	unvollständig – kaum
Lieferanten	vollständig – detailliert	nicht betrachtet
Priorisierung	vorhanden	vorhanden
Allgemein:		
Unternehmensgröße	jede	jede
Branche	jede	jede
Technologieunabhängig	zum Großteil	ja
Zertifizierung	nein	nein
Umfang	492 Seiten	129 Seiten
Veröffentlichung	12.10.2020	Mai 10
Konzipiert für	IS	ISCP
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	konkret	allgemein
Preis	kostenlos	kostenlos

Tabelle 17: Übersicht Ergebnisse des Vergleichs; Teil 3

Bezeichnung des Standards / **Kriterien**	VdS 10000	ITIL
Prinziepien von ITSCM		
Vorfallprävention	angemessen	nicht betrachtet
Vorfallerkennung	angemessen	angemessen
Reaktion	angemessen	angemessen
Wiederherstellung	kaum	nicht betrachtet
Verbesserung	angemessen	angemessen
Elemente von ITSCM		
Mitarbeiter	vollständig – angemessen	vollständig – kaum
Einrichtungen	unvollständig - kaum	nicht betrachtet
Technologie - Hardware - Netzwerk - Software	vollständig – angemessen	nicht betrachtet
Daten	unvollständig - kaum	nicht betrachtet
Prozesse	vollständig - angemessen	vollständig - angemessen
Lieferanten	unvollständig – angemessen	unvollständig - kaum
Priorisierung	vorhanden	vorhanden
Allgemein:		
Unternehmensgröße	KMO	jede
Branche	jede	jede
Technologieunabhängig	ja	ja
Zertifizierung	durch VdS	einzelne Personen sind zertifizierbar
Umfang	43 Seiten	260 Seiten
Veröffentlichung	01.12.2018	Feburar 2019
Konzipiert für	ISMS	ITSM
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	konkret, teilweise Zwang	keine
Preis	83,18 €	85,00 €

Tabelle 18: Übersicht Ergebnisse des Vergleichs; Teil 4

Bezeichnung des Standards / **Kriterien**	FitSM	Good Practice Guidelines 2018
Prinziepien von ITSCM		
Vorfallprävention	angemessen	angemessen
Vorfallerkennung	kaum	nicht betrachtet
Reaktion	kaum	kaum
Wiederherstellung	nicht betrachtet	detailliert
Verbesserung	angemessen	detailliert
Elemente von ITSCM		
Mitarbeiter	nicht betrachtet	vollständig - detailliert
Einrichtungen	unvollständig - kaum	nicht betrachtet
Technologie - Hardware - Netzwerk - Software	unvollständig - kaum	nicht betrachtet
Daten	unvollständig - kaum	nicht betrachtet
Prozesse	vollständig – angemessen	vollständig – angemessen
Lieferanten	nicht betrachtet	nicht betrachtet
Priorisierung	vorhanden	vorhanden
Allgemein:		
Unternehmensgröße	jede	jede
Branche	jede	jede
Technologieunabhängig	ja	ja
Zertifizierung	nein	nein
Umfang	87 Seiten	108 Seiten
Veröffentlichung	14.06.2016, teilweise 17.08.2022 aktualisiert	08.11.2017
Konzipiert für	ITSM	BCM
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	allgemein	allgemein
Preis	kostenlos	30,00 £ ~ 35,00 €

Tabelle 19: Übersicht Ergebnisse des Vergleichs; Teil 5

Bezeichnung des Standards / **Kriterien**	COBIT	CISIS12
Prinziepien von ITSCM		
Vorfallprävention	detailliert	detailliert
Vorfallerkennung	detailliert	detailliert
Reaktion	detailliert	nicht betrachtet
Wiederherstellung	detailliert	kaum
Verbesserung	kaum	angemessen
Elemente von ITSCM		
Mitarbeiter	vollständig - detailliert	vollständig - detailliert
Einrichtungen	unvollständig - kaum	unvollständig – detailliert
Technologie - Hardware - Netzwerk - Software	vollständig - detailliert	unvollständig – detailliert
Daten	unvollständig - angemessen	unvollständig – kaum
Prozesse	vollständig - detailliert	vollständig – detailliert
Lieferanten	vollständig - detailliert	unvollständig – detailliert
Priorisierung	vorhanden	vorhanden
Allgemein:		
Unternehmensgröße	keine Angabe	KMO
Branche	keine Angabe	jede
Technologieunabhängig	ja	ja
Zertifizierung	nein	ja
Umfang	326 Seiten	1072 Seiten
Veröffentlichung	eng.:Dezember 2018 deut.: Dezember 2020	01.06.2021
Konzipiert für	Unternehmensstrategie	ISMS
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	zum Teil: allgemeine zum Teil: konkret	allgemein
Preis	kostenlos	150,00 € Behörden kostenlos

Tabelle 20: Übersicht Ergebnisse des Vergleichs; Teil 6

Bezeichnung des Standards / **Kriterien**	NFPA 1600
Prinziepien von ITSCM	
Vorfallprävention	kaum
Vorfallerkennung	nicht betrachtet
Reaktion	kaum
Wiederherstellung	detailliert
Verbesserung	detailliert
Elemente von ITSCM	
Mitarbeiter	vollständig - kaum
Einrichtungen	unvollständig – kaum
Technologie - Hardware - Netzwerk - Software	unvollständig – kaum
Daten	unvollständig – kaum
Prozesse	unvollständig – kaum
Lieferanten	unvollständig – kaum
Priorisierung	vorhanden
Allgemein:	
Unternehmensgröße	jede
Branche	jede
Technologieunabhängig	ja
Zertifizierung	möglich
Umfang	97 Seiten
Veröffentlichung	05.11.2018
Konzipiert für	BCM
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	allgemein
Preis	11,99$ pro Monat 84,00$ einmalig

Tabelle 21: Übersicht Ergebnisse des Vergleichs; groß

Bezeichnung des Standards / Kriterien	BSI 200-4	NIST CSF	NIST SP 800-53	NIST SP 800-34	VdS 10000	ITIL	FitSM	Good Practice Guidelines 2018	COBIT	CISIS12	NFPA 1600
Prinziepien von ITSCM											
Vorfallprävention	nicht betrachtet	detailliert	detailliert	detailliert	angemessen	nicht betrachtet	angemessen	angemessen	detailliert	detailliert	kaum
Vorfallerkennung	detailliert	detailliert	detailliert	nicht betrachtet	angemessen	angemessen	kaum	nicht betrachtet	detailliert	detailliert	nicht betrachtet
Reaktion	detailliert	detailliert	detailliert	nicht betrachtet	angemessen	angemessen	kaum	kaum	detailliert	nicht betrachtet	kaum
Wiederherstellung	detailliert	kaum	detailliert	detailliert	kaum	nicht betrachtet	nicht betrachtet	detailliert	detailliert	kaum	detailliert
Verbesserung	detailliert	angemessen	nicht betrachtet	angemessen	angemessen	angemessen	angemessen	detailliert	kaum	angemessen	detailliert
Elemente von ITSCM											
Mitarbeiter	vollständig - angmessen	vollständig – kaum	vollständig – detailliert	vollständig – kaum	vollständig – angemessen	vollständig – kaum	nicht betrachtet	vollständig - detailliert	vollständig - detailliert	vollständig - detailliert	vollständig - kaum
Einrichtungen	unvollständig – kaum	nicht betrachtet	vollständig – detailliert	unvollständig – kaum	unvollständig - kaum	nicht betrachtet	unvollständig - kaum	nicht betrachtet	unvollständig - kaum	unvollständig – detailliert	unvollständig – kaum
Technologie - Hardware - Netzwerk - Software	unvollständig – kaum	vollständig - kaum	vollständig – detailliert	unvollständig – angemessen	vollständig – angemessen	nicht betrachtet	unvollständig - kaum	nicht betrachtet	vollständig - detailliert	unvollständig – detailliert	unvollständig – kaum
Daten	unvollständig – kaum	unvollständig – kaum	unvollständig - angemessen	unvollständig – kaum	unvollständig - kaum	nicht betrachtet	unvollständig - kaum	nicht betrachtet	unvollständig - angemessen	unvollständig – kaum	unvollständig – kaum
Prozesse	unvollständig - kaum	unvollständig - kaum	vollständig - detailliert	unvollständig – kaum	vollständig - angemessen	vollständig - angemessen	vollständig – angemessen	vollständig – angemessen	vollständig - detailliert	vollständig – detailliert	unvollständig – kaum
Lieferanten	unvollständig – kaum	unvollständig – kaum	vollständig – detailliert	nicht betrachtet	unvollständig – angemessen	unvollständig - kaum	nicht betrachtet	nicht betrachtet	vollständig - detailliert	unvollständig – detailliert	unvollständig – kaum
Priorisierung	vorhanden	nicht betrachtet	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden
Allgemein:											
Unternehmensgröße	jede	jede	jede	jede	KMO	jede	jede	jede	keine Angabe	KMO	jede
Branche	jede	jede	jede	jede	jede	jede	jede	jede	keine Angabe	jede	jede
Technologieunabhängig	ja	ja	zum Großteil	ja	ja	einzelne Personen sind zertifizierbar	ja	ja	ja	ja	ja
Zertifizierung	nach ISO 22301:2019 möglich	nein	nein	nein	durch VdS		nein	nein	nein	ja	möglich
Umfang	234 Seiten + 576 Anforderungen	55 Seiten	492 Seiten	129 Seiten	43 Seiten	260 Seiten	87 Seiten	108 Seiten	326 Seiten	1072 Seiten	97 Seiten
Veröffentlichung	Entwurfsphase aktulle Version Community Draft 2: August 2022	16.04.2018	12.10.2020	Mai 10	01.12.2018	Feburar 2019	14.06.2016, teilweise 17.08.2022 aktualisiert	08.11.2017	eng.:Dezember 2018 deut.: Dezember 2020	01.06.2021	05.11.2018
Konzipiert für	BCM	IS	IS	ISCP	ISMS	ITSM	ITSM	BCM	Unternehmensstrategie	ISMS	BCM
konkrete Anforderungen/ bzw. Hinweise bzw. Vorschläge	konkret, teilweise Zwang	allgemein	konkret	allgemein	konkret, teilweise Zwang	keine	allgemein	allgemein	zum Teil: allgemeine zum Teil: konkret	allgemein	allgemein
Preis	kostenlos	kostenlos	kostenlos	kostenlos	83,18 €	85,00 €	kostenlos	30,00 £ ~ 35,00 €	kostenlos	150,00 € Behörden kostenlos	11,99$ pro Monat 84,00$ einmalig

Anlage 2: BCMS-Leitlinie der Mustermann GmbH

Business Continuity Management- Leitlinie der Mustermann GmbH

1. Einleitung
2. Definitionen Begriffe
3. Auswahl der Methode
4. Ziele
5. Geltungsbereich und Zeitraum
6. Aufbauorganisation
7. Verantwortung und Pflichten

1. Einleitung

Die Stärken eines Unternehmens zeigt sich in schwierigen Situationen. Dies haben wir in den letzten Jahren während der Corona-Krise gesehen. Wir hatten zwar auf Grund der Lieferprobleme auch zu kämpfen, haben aber die schwere Zeit gemeinsam überstanden. Dabei ist auch klargeworden, dass wir auf Ausnahmesituationen kaum vorbereitet sind. Hierbei muss nicht immer der Worst Case, wie eine globale Pandemie, eintreten, um uns bereits Probleme zu bereiten. Deshalb werden wir bei uns im Unternehmen ein Business Continuity Management System einführen. Dadurch werden wir in Zukunft besser auf Krisen reagieren können, um die wirtschaftliche Sicherheit des Unternehmens zu gewährleisten.

2. Definitionen Begriffe

Business Continuity Management System (BCMS) ist ein Konzept zur Umsetzung und Verwaltung der Aufrechterhaltung der Betriebsfähigkeit. Dadurch wird sichergestellt, dass in Notfällen geordnete Maßnahmen zur Beseitigung des Notfalles und zur Geschäftsfortführung getroffen werden. Zeitgleich mit der Feststellung eines Notfalls greift das BCMS.

Eine Störung ist ein geplantes oder ungeplantes Ereignis, das eine ungeplante, negative Abweichung von der erwarteten Lieferung von Produkten und Dienstleistungen, gemessen an den Zielen einer Organisation, verursacht.

Notfall ist ein plötzlicher, dringender, normalerweise unvorhergesehener Vorfall oder ein Ereignis, das sofortiges Handeln erfordert; häufig handelt es sich um

eine Störung oder einen Zustand, der zwar vorhergesehen wurde oder auf den man sich vorbereitet hat, der aber nicht genau vorhergesagt werden kann.

Krise ist ein instabiler Zustand, bei dem eine abrupte oder deutliche Veränderung droht, die dringende Aufmerksamkeit und Maßnahmen erfordert, um Leben, Werte, Eigentum oder die Umwelt zu schützen.

Katastrophe ist eine Situation, in der umfassende menschliche, materielle, wirtschaftliche oder ökologische Verluste eingetreten sind, welche die Fähigkeit der betroffenen Organisation, Gemeinschaft oder Gesellschaft überschreiten, sie mit den eigenen Ressourcen zu bewältigen und sich davon zu erholen.

Business Continuity Berater (BCB) ist für die Implementierung des BCMS zuständig.

3. Auswahl der Methode

Die Mustermann GmbH wird ein sogenanntes „Reaktiv-BCM“ einführen, das noch nicht vollständig ist, aber mit geringem Aufwand implementiert werden kann. Das „Reaktiv BCMS“ wird ausgewählt, da noch keine Erfahrungen in Bezug auf das BCMS vorhanden sind und damit ein leichter Einstieg zum Sammeln von Erfahrungen gegeben ist. Nach der erfolgreichen Implementierung, soll eine Erweiterung des BCMS stattfinden, so dass langfristig ein vollständiger Schutz gegeben ist.

4. Ziele

Ziel des BCMS ist die Absicherung unserer umsatzstärksten Geschäftsbereiche. Dadurch soll die Betriebsfähigkeit, für diese sichergestellt und insbesondere die Zufriedenheit der Bestandskunden gewährleistet werden.

5. Geltungsbereich und Zeitraum

Der Geltungsbereich für das BCMS begrenzt sich auf die Organisationseinheiten „Service“ und „Produktion“. Außerdem soll eine Absicherung der zeitkritischen Geschäftsprozesse für einen Zeitraum von 21 Tagen gewährleistet werden.

6. Aufbauorganisation

Nach Ausrufen eines Notfalles tritt unverzüglich der Krisenstab zusammen, der aus dem BCB als Leiter, dem verantwortlichen Mitarbeiter für die IT, einem Verwaltungsmitarbeiter als Protokollführer und der Geschäftsführung besteht. Je nach Bedarf kommen der Leiter der Produktion und ein Service-Mitarbeiter, als Experten für den Bereich, dazu. Der Krisenstab bleibt bis zur Beendigung des Notfalles in Kraft.

7. Verantwortung und Pflichten

Die Belegschaft hat die Pflicht, an den angebotenen Schulungen für Business Continuity teilzunehmen. Darüber hinaus müssen Störungen, Notfälle und Krisen unverzüglich an den Verantwortlichen oder dem BCB gemeldet werden. Die Realisierung der in den jeweiligen Bereichen erlassenen Sofortmaßnahmen hat zu erfolgen.

Der BCB ist Ansprechpartner für alle Fragen bezüglich des BCMS und bietet den Angestellten Sensibilisierungsmaßnahmen an. Des Weiteren ist er für die Implementierung des BCMS verantwortlich. In Notfallsituationen ist er weisungsbefugt und nur der Geschäftsführung zu Rechenschaft verpflichtet.

Die Geschäftsführung zeichnet sich für die Durchführung des Business Continuity verantwortlich und stellt angemessene Ressourcen dafür zur Verfügung.

Musterstadt, den 19.06.2023

Peter Mustermann

Anlage 3: Definition der Schadenskategorien

Tabelle 22: Definition der Schadenkategorien der Mustermann GmbH

Schadenskategorie	Definition der Kategorie für das jeweilige Szenario
1 (gering)	Beeinträchtigung der persönlichen Unversehrtheit: Eine Beeinträchtigung ist ausgeschlossen.
	Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb wird unwesentlich beeinträchtigt die Wiederaufarbeitung dauert weniger als 7 Tage.
	Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird gegen Gesetze oder Verträge mit geringen Strafen verstoßen.
	Negative Innen- und Außenwirkung: In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten.
	Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution unerheblich.
2 (mittel)	Beeinträchtigung der persönlichen Unversehrtheit: Eine geringe Verletzungswahrscheinlichkeit ist gegeben und beschränkt sich auf leichte Verletzungen.
	Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb ist eingeschränkt, die Wiederaufarbeitung dauert zwischen 7 und 14 Tage.
	Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird gegen Gesetze oder Verträge mit mittleren Strafen verstoßen.
	negative Innen- und Außenwirkung: Ein genereller. nicht

	nachhaltiger Imageschaden ist extern zu erwarten
	finanzielle Auswirkungen: Die finanziellen Auswirkungen sind erheblich.
3 (hoch)	Beeinträchtigung der persönlichen Unversehrtheit: Eine Verletzungswahrscheinlichkeit ist gegeben und beschränkt sich nicht auf leichte Verletzungen.
	Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb ist stark eingeschränkt, die Wiederaufarbeitung davon dauert mehr als 14 Tage.
	Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird gegen Gesetze oder Verträge mit hohen Strafen verstoßen.
	negative Innen- und Außenwirkung: Ein nachhaltiger Imageschaden ist in Einzelfällen, extern, zu erwarten
	finanzielle Auswirkungen: Die finanziellen Auswirkungen sind existenzbedrohend.

Anlage 4: IS-Leitlinie der Mustermann GmbH

Informationssicherheits-Leitlinie der Mustermann GmbH

1. Einleitung
2. Definitionen Begriffe
3. Ziele und Bedeutung der Informationssicherheit
4. Definition der Positionen und Verantwortlichkeiten
5. Konsequenzen bei Nichteinhaltung

1. Einleitung

Die Stärken eines Unternehmens zeigt sich in schwierigen Situationen. Dies haben wir in den letzten Jahren während der Corona-Krise gesehen. Wir hatten zwar auf Grund der Lieferprobleme auch zu kämpfen, haben aber die schwere Zeit gemeinsam überstanden. Dabei ist auch klargeworden, dass wir auf Ausnahmesituationen kaum vorbereitet sind. Hierbei muss nicht immer der Worst Case, wie eine globale Pandemie, eintreten, um uns bereits Probleme zu bereiten. Deshalb werden wir bei uns im Unternehmen im Rahmen der Informationssicherheit unsere Verfügbarkeit von IT-Systemen verbessern. Dadurch werden wir in Zukunft besser auf Krisen reagieren können, um die wirtschaftliche Sicherheit des Unternehmens zu gewährleisten.

2. Definition und Begriffe

Informationssicherheit (IS) stellt die Vertraulichkeit, Verfügbarkeit und Integrität von Daten und damit verbunden IT-Systemen im Unternehmen sicher.

Vertraulichkeit wird dann erreicht, wenn gewährleistet ist, dass nur Personen Zugang und Zugriff auf die Daten und IT-System haben, für die Sie, zur Erledigung Ihrer Aufgabe, berechtigt sind.

Verfügbarkeit ist gegeben, wenn innerhalb einer vorgegebenen Zeit auf die Daten bzw. IT-System zugegriffen werden kann bzw. eine Anfrage bearbeitet wird.

Integrität bedeutet, dass eine Manipulation von Daten oder IT-Systemen nicht möglich ist oder erkannt werden würde.

Informationssicherheitsmanagementsystem (ISMS) stellt durch einen geregelten

Ablauf die Aufrechterhaltung und Verbesserungen der IS sicher.

3. Ziele und Bedeutung der Informationssicherheit

Bei uns im Unternehmen soll durch das ISMS insbesondere die Ausfallrate und -dauer von IT-Systemen reduziert werden, da diese für einen geregelten Betrieb des Unternehmens unerlässlich sind. Deshalb sollen IS-Maßnahmen in jeden Bereich eingeführt und eingehalten werden.

4. Definition der Positionen und Verantwortlichkeiten

Topmanagement:

- Ziele: Erhalt der Betriebsfähigkeit der IT-Systeme
- Zuständigkeitsbereich: gesamtes Unternehmen
- Aufgaben: Übernahme der Gesamtverantwortung, Bereitstellung von Ressourcen, Benennung von benötigten Rollen, Integration des ISMS in die Unternehmensstruktur
- Berechtigungen: alle als Geschäftsführer
- Ressourcen: Budget wurde auf 15.000 € festgelegt
- Kontrollinstanz: keine
- Organisationseinheit: Geschäftsführung

Informationssicherheitsbeauftragter (ISB):

- Ziele: Absicherung der IT-Systeme gegen Ausfälle
- Zuständigkeitsbereich: gesamtes Unternehmen
- Aufgaben: Entwicklung von Zielen, Organisation und Überprüfung der ISMS-Einführung und Aktualisierung
- Berechtigungen: Weisungs- und Entscheidungsbefugnisse im Rahmen der IS
- Ressourcen: Budget wurde auf 13.000 € festgelegt
- Kontrollinstanz: Geschäftsführung
- Organisationseinheit: IT-Mitarbeiter, Stellvertreter: Entwicklungsleiter
- keine Funktionstrennung: Eine Funktionstrennung ist auf Grund der personellen Lage nicht möglich.

Informationssicherheitsteam (IST):

- Ziele: Unterstützung des ISB
- Zuständigkeitsbereich: gesamtes Unternehmen
- Aufgaben: Überwachung der Bedrohungslage, Analyse der Situation, Recherche von Maßnahmen, Bewertung der Maßnahmen
- Berechtigungen:
- Ressourcen: Budget wurde auf 1.000 € festgelegt

- Kontrollinstanz: keine, da Geschäftsführung Mitglied ist
- Organisationseinheit: Geschäftsführung, IT-Mitarbeiter (ISB, IT-Verantwortlicher), Herr Kurz (Mitarbeitervertretung), DSB (wurde an extern vergeben)

IT-Verantwortlicher:

- Ziele: Entwicklung von Maßnahmen
- Zuständigkeitsbereich: alle IT-Systeme des Unternehmens
- Aufgaben: Analyse der Situation, Recherche von Maßnahmen, Bewertung der Maßnahmen
- Berechtigungen: Weisungs- und Entscheidungsbefugnisse im Rahmen des IT
- Ressourcen: erhält Mittel vom ISB
- Kontrollinstanz: Geschäftsführung
- Organisationseinheit: IT-Mitarbeiter
- keine Funktionstrennung: Eine Funktionstrennung ist auf Grund der personellen Lage nicht möglich. Deshalb auch Geschäftsführung als Kontrollinstanz.

Administrator:

- Ziele: Umsetzung der Maßnahmen
- Zuständigkeitsbereich: alle IT-Systeme des Unternehmens
- Aufgaben: Ausarbeitung und Implementierung der Maßnahmen
- Berechtigungen: Adminberechtigungen und Zugang auf/ zu allen IT-Systemen
- Ressourcen: erhält Mittel vom IT-Verantwortlichen
- Kontrollinstanz: Geschäftsführung
- Organisationseinheit: IT-Mitarbeiter
- keine Funktionstrennung: Eine Funktionstrennung ist auf Grund der personellen Lage nicht möglich. Deshalb auch Geschäftsführung als Kontrollinstanz.

Auf Grund der geringen Anzahl an Vorgesetzten findet keine Unterscheidung zu normalen Beschäftigten statt.

Mitarbeiter und Externe:

- Ziele: Beitrag zur IS leisten
- Zuständigkeitsbereich: jeweiliger Arbeitsbereich
- Aufgaben: Einhaltung von Regelungen und Meldung von Störungen
- Berechtigungen:
- Ressourcen: Teilnahme an Schulungen für jeden Mitarbeiter
- Kontrollinstanz: Geschäftsführung
- Organisationseinheit: jeweiliger Arbeitsbereich

5. Konsequenzen bei Nichteinhaltung

Bei Nichteinhaltung der IS-Leitlinie erfolgt eine Verwarnung und die Pflicht zur Durchführung von Sensibilisierung Maßnahmen. Bei mehrfachen oder grob fahrlässigen Verstößen kann das Arbeitsverhältnis beendet werden.

Musterstadt, den 19.06.2023

Peter Mustermann

Anlage 5: Definitionen für die Schutzbedarfskategorien vom BSI-Standard 200-2

Schutzbedarfskategorie „normal“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Bild 17: BSI 200-2 Schutzbedarfskategorie "normal" [84, p. 106]

Schutzbedarfskategorie „hoch“	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Bild 18: BSI 200-2 Schutzbedarfskategorie "hoch" [84, pp. 106-107]

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Bild 19: BSI 200-2 Schutzbedarfskategorie "sehr hoch" [84, p. 107]

Anlage 6: IS-Richtlinie für IT-Systeme

IS-Richtlinie für IT-Systeme der Mustermann GmbH

1. Geltungsbereich und Verantwortlichkeiten
2. Ziele und Bedeutung Richtlinie
3. Vorgaben und Maßnahmen
    a. Allgemein
    b. Basisschutz
    c. kritische IT-System
4. Konsequenzen bei Nichteinhaltung

1. Geltungsbereich und Verantwortlichkeiten

Die Richtlinie regelt die Administration aller IT-Systeme der Mustermann GmbH und ist von der IT-Abteilung einzuhalten und umzusetzen.

2. Ziele und Bedeutung Richtlinie

Durch die Richtlinie wird eine einheitliche und sichere Konfiguration der IT-Systeme sichergestellt.

3. Vorgaben und Maßnahmen

a. Allgemein

Alle IT-Systeme müssen mit Seriennummer, Aufstellungsort, Einsatzzweck und Informationen über Garantien und Serviceverträge inventarisiert werden. Bei der Inbetriebnahme muss, anhand des Einsatzprozesses, die Kritikalität bestimmt werden. Mindestens der Basisschutz muss implementiert werden und eine Dokumentation der Konfiguration erfolgen. Bei der Aussonderung müssen wichtige Daten auf den Fileserver übertragen und anschließend alle Daten bei HDD siebenmal überschrieben werden. Bei SSD ist zweingend ein „PISD reset“ oder „SecureErase“ im BIOS/ UEFI durchzuführen. Alternativ kann auch die thermische Zerstörung erfolgen. Eine Aktualisierung der Inventarisierung und des Netzplans hat jeweils unverzüglich zu erfolgen.

b. Basisschutz

Jeder Angestellte erhält zunächst nur unsere Standardsoftware (Windows,

Office, Edge, Firefox, PDF24, Trellix). Jedes weitere Programm muss mit Begründung beantragt und vom Vorgesetzten genehmigt werden. Es ist sicherzustellen, dass nur von der Festplatte gebootet werden kann. Bei Trellix muss der Echtzeitschutz aktiviert und eine Überwachung der Schnittstellen stattfinden. Hier sind nur Eingabegeräte freigegeben.

Es muss eine Authentifizierung beim Systemstart durchgeführt werden. Im Betrieb findet diese erneut jeweils nach 30 Minuten Inaktivität statt. Eine Anmeldung über das Netzwerk muss durch ein aktuelles Verschlüsselungsprotokoll gesichert sein. Standardpasswörter müssen geändert werden und die Passwortvorgaben von mindestens zwölf Zeichen mit Zahlen, Sonderzeichen, Groß- und Kleinbuchstaben muss eingehalten werden. Eine zentrale Verwaltung der Kennungen muss über das Active Directory erfolgen.

Alle Berechtigungen von Usern und Anwendungen sind auf ein Minimum zu reduzieren.

Alle fehlgeschlagenen Anmeldeversuche, Fehler, IS relevante Ereignisse und Meldungen von Trellix müssen, auf dem jeweiligen System, protokolliert werden und für sechs Monate nachvollziehbar sein. Eine einheitliche Systemzeit wird durch die Verwendung eines einheitlichen NTP-Servers sichergestellt.

c. kritische IT-Systeme

Bei kritischen IT-Systemen müssen alle Gefahren ermittelt und an Hand von Eintrittswahrscheinlichkeit und Schaden priorisiert werden. Es muss ein Notbetriebsniveau festgelegt und dokumentiert werden. Zusätzlich muss dokumentiert werden, wer für das System verantwortlich ist, mit welchen Zugängen und Authentifizierungsmethoden eine Administration möglich ist, der Zweck des IT-Systems und warum, wer, wann Änderungen vorgenommen hat.

Änderungen müssen auf einem vom produktiven IT-System unabhängigen Testumgebung geprüft werden bzw. außerhalb der Betriebszeit durchgeführt werden. Es ist zwingendend darauf zu achten, dass das Produktivsystem jederzeit in einen funktionierenden Zustand zurückgesetzt werden kann.

Eine regelmäßige Sicherung der Konfiguration und wichtiger Daten muss erfolgen. Darüber hinaus muss das System auf Störungen, Ausfälle und hohe Auslastung überwacht werden. Die Notwendigkeit von Ersatzsystemen ist zu prüfen.

4. Konsequenzen bei Nichteinhaltung

Bei Verstößen gegen die Richtlinie, kann eine Verwarnung ausgesprochen werden. Bei mehrfachen bzw. grob fahrlässigen Missachtung kann eine Kündigung erfolgen.

Musterstadt, den 19.06.2023

Peter Mustermann

Anlage 7: Risikoeinstufung BSI 200-3

Tabelle 23: Kategorisierung von Eintrittshäufigkeiten des BSI 200-3 [85, pp. 26-27]

selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Tabelle 24: Kategorisierung von Schadensauswirkungen [85, p. 27]

vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

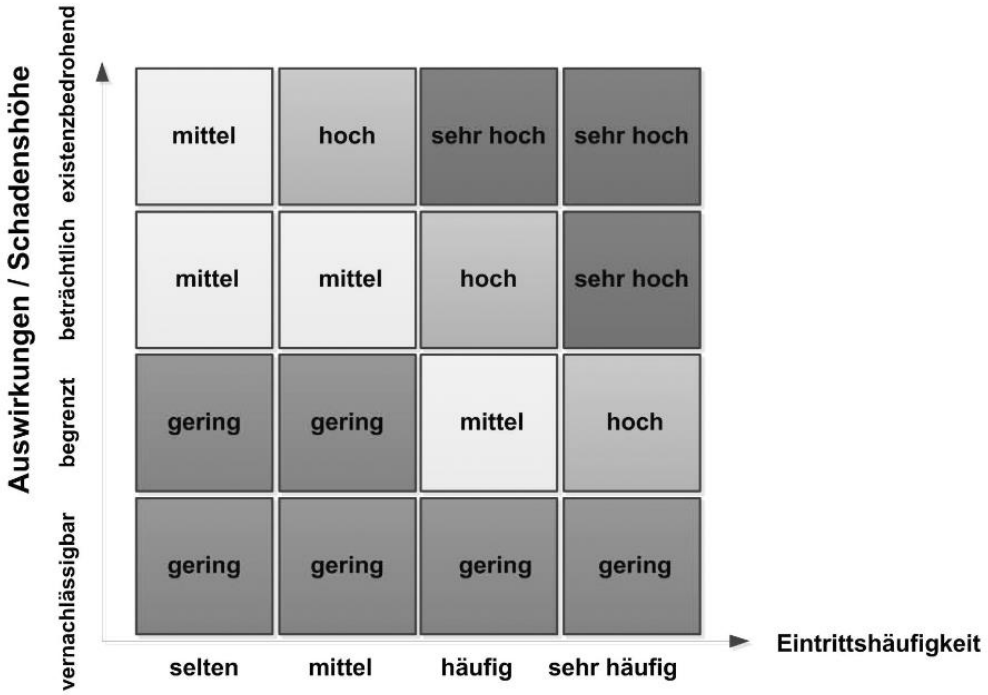

Bild 20: Matrix zur Einstufung von Risiken [85, p. 27]

Tabelle 25: Definition von Risikokategorien [85, p. 28]

gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
Sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Anlage 8: IS-Richtlinie für Störungen und Ausfälle

IS-Richtlinie für Störungen und Ausfälle der Mustermann GmbH

1. Geltungsbereich und Verantwortlichkeiten
2. Ziele und Bedeutung Richtlinie
3. Definition von Begrifflichkeiten
4. Vorgaben und Maßnahmen
    a. Meldungen
    b. Untersuchung des Vorfalls
    c. Interne und externe Kommunikation
5. Konsequenzen bei Nichteinhaltung

1. Geltungsbereich und Verantwortlichkeiten

Die Richtlinie regelt den Umgang mit Störungen und Ausfällen von IT-Systemen bei der Mustermann GmbH und ist von der gesamten Belegschaft einzuhalten.

2. Ziele und Bedeutung Richtlinie

Durch die Richtlinie werden Handlungsanweisungen zum Erkennen und zur Meldung von Störungen und Ausfällen definiert. Des Weiteren wird der Umgang mit Störungen und Ausfällen für das fachkundliche Personal und die Kommunikation innerhalb der Firma und mit Externen geregelt.

3. Definition von Begrifflichkeiten

Eine Störung ist ein geplantes oder ungeplantes Ereignis, das eine ungeplante, negative Abweichung von der erwarteten Lieferung von Produkten und Dienstleistungen, gemessen an den Zielen einer Organisation, verursacht.

Störungen sind dem IT-Mitarbeiter zu melden, wenn diese nicht durch den Neustart des IT-Systems behoben werden können oder regelmäßig auftreten.

Ausfall: Ein Ausfall eines IT-Systems bedeutet, dass das IT-System keinerlei Funktionalität mehr erbringt bzw. die Funktionalität in einer Art und Weise erbringt, die keine weitere Arbeit damit erlaubt. Ein Ausfall ist unverzüglich zu melden.

4. Vorgaben und Maßnahmen

Die folgenden Maßnahmen sind für alle Arbeitnehmer bindend.

a. Meldungen

Jede Störung und jeder Ausfall müssen den IT-Mitarbeiter unverzüglich gemeldet werden.

b. Untersuchung des Vorfalls

Der IT-Mitarbeiter ermittelt den Grund für die Störung bzw. den Ausfall. Dabei kann er vom Meldenden, Informationen und Kooperation fordern, die diese zu erbringen haben.

c. Interne und externe Kommunikation

Nach der Analyse der Störung bzw. des Ausfalles teilt der IT-Mitarbeiter die geschätzte Zeit bis zur Behebung, den Betroffenen mit. Falls bei einem Ausfall, eines zentralen IT-Systems, die geschätzte Zeit zur Behebung über einer Stunde liegt bzw. wenn es sofortige Außenwirkung entfaltet, wie Ausfall der telefonischen Erreichbarkeit, ist die Geschäftsführung zu informieren. Eine Kommunikation mit Externen darf nur nach Vorgabe der Geschäftsführung erfolgen.

5. Konsequenzen bei Nichteinhaltung

Bei Verstößen gegen die Richtlinie, kann eine Verwarnung ausgesprochen werden. Bei mehrfachen bzw. grob fahrlässigen Missachtung kann eine Kündigung erfolgen.

Musterstadt, den 19.06.2023

Peter Mustermann

Verzeichnis der Abkürzungen

BAO ..... besondere Aufbauorganisation
BCB ..... Business Continuity Beauftragter
BCI ..... Business Continuity Institute
BCM ..... Business Continuity Management
BCMS ..... Business Continuity Management System
BIA ..... Business Impact Analyse
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
CISIS12 ..... Compliance Informations-Sicherheitsmanagement System in 12 Schritten
COBIT ..... Control Objectives for Information and Related Technology
CSF ..... Framework for Improving Critical Infrastructure Cybersecurity
GFP ..... Geschäftsfortführungspläne
GPG2018 ..... Good Practice Guidelines Edition 2018
gWAZ ..... geforderte Wiederanlaufzeit
ICT ..... information and communications technology
IRBC ..... ICT Readiness for Business Continuity
IS. ..... Informationssicherheit
ISACA ..... Information Systems Audit and Control Association
ISB ..... Informationssicherheitsbeauftragter
ISCP ..... Information System Contingency Plan
ISMS ..... Informationssicherheitsmanagementsystem
ISO ..... International Organization for Standardization
IST ..... Informationssicherheitsteam
ITEMO ..... IT Education Management Organisation
ITIL ..... Information Technology Infrastructure Library
ITILv4 ..... Information Technology Infrastructure Library 4th Edition
ITSCM ..... IT service continuity management
ITSM ..... IT-Service-Management
KMO ..... kleine und mittler Organisationen
MTA ..... Maximal Tolerierbare Ausfallzeit
MTD ..... Maximal tolerierbarer Datenverlust
NFPA ..... 6.9 National Fire Protection Association
NIST ..... National Institute of Standards and Technology
NIST SP: 800-53r5 ..... Security and Privacy Controls for Information Systems and Organizations
NIST SP:800-34 ..... Contingency Planning Guide for Federal Information Systems
VdS ..... Verband der Sachversicherer
VdS 10000 ..... VdS-Richtlinien für die Informationsverarbeitung
WAP ..... Wiederanlaufplanung
wWAZ ..... wirkliche Wiederanlaufzeit

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Fassung entspricht der auf dem Medium gespeicherten Fassung.

xxx, 05. September 2023 Simon Lang

Ort, Datum (Unterschrift)

Thesen

Thema der Arbeit: Gegenüberstellung standardisierter Vorgehensweisen zur Implementierung eines Geschäftskontinuität-Managements mit Schwerpunkt auf die Informationstechnologie

Bearbeiter: Simon Lang

Thesen:

1. BCM und ITSCM tragen bei erfolgreicher Implementierung maßgeblich zur Überlebensfähigkeit von Unternehmen in Extremsituationen bei.
2. Die Implementierungsrate von BCM und ITSCM ist insbesondere bei KMOs aufgrund verschiedener Herausforderungen gering.
3. Es gibt nur einen speziell für ITSCM entwickelten Standard, der keine Implementierungshilfen bietet.
4. Verschiedene Normen, die für andere Themenbereiche entwickelt wurden, adressieren ITSCM teilweise und bieten Umsetzungshilfen.
5. Keines der untersuchten Dokumente bildet eine vollständige und detaillierte Realisierung von ITSCM ab.
6. BCM und ITSCM haben ein großes Synergiepotenzial mit anderen IT-Richtlinien und sollten mit diesen kombiniert werden, um einen umfassenderen Schutz zu erreichen.
7. Kleinst-Organisationen sollten sich auf die Hauptangriffsvektoren und Schutzmaßnahmen konzentrieren.
8. Insbesondere kleine Organisationen sollten sich an einem Standard orientieren, diesen aber weiter vereinfachen und an ihre Bedürfnisse anpassen.