DBA thesis

Erfolgsfaktoren für das Business Continuity Management bei fortschreitender Digitalisierung – Eine empirische Studie am Beispiel behördenerfahrener IT-Dienstleister in Deutschland

Neujahr, H.

___

Full bibliographic citation: Neujahr, H. 2024. Erfolgsfaktoren für das Business Continuity Management bei fortschreitender Digitalisierung – Eine empirische Studie am Beispiel behördenerfahrener IT-Dienstleister in Deutschland. DBA thesis Middlesex University / KMU Akademie & Management AG

Year: 2024

Publisher: Middlesex University Research Repository

Available online: https://repository.mdx.ac.uk/item/1xqx9q

___

KMU
Akademie & Management AG

DISSERTATION

Erfolgsfaktoren für das Business Continuity Management bei fortschreitender Digitalisierung – Eine empirische Studie am Beispiel behördenerfahrener IT-Dienstleister in Deutschland

NAME:	Holger Neujahr
MATRIKELNUMMER:	MUDR/0562
STUDIUM:	DBA
ADVISOR/IN:	Dr. Lars Bräutigam
ANZAHL DER WÖRTER:	61.635
EINGEREICHT AM:	15.09.2024

In partnership with Middlesex University London

EIDESSTATTLICHE ERKLÄRUNG

Hiermit erkläre ich an Eides statt, dass ich die vorliegende, an diese Erklärung angefügte Dissertation selbstständig und ohne jede unerlaubte Hilfe angefertigt habe, dass sie noch keiner anderen Stelle zur Prüfung vorgelegen hat und dass sie weder ganz noch im Auszug veröffentlicht worden ist. Die Stellen der Arbeit einschließlich Tabellen, Abbildungen etc., die anderen Werken und Quellen (auch Internetquellen) dem Wortlaut oder dem Sinn nach entnommen sind, **habe ich in jedem einzelnen Fall als Entlehnung mit exakter Quellenangabe kenntlich gemacht.** Hiermit erkläre ich, dass die übermittelte Datei ident mit der geprüften Datei und dem daraus resultierenden und übermittelten Plagiatsbericht ist und die Angabe der Wortanzahl diesem entspricht. **Mir ist bewusst, dass Plagiate gegen grundlegende Regeln des wissenschaftlichen Arbeitens verstoßen und nicht toleriert werden. Es ist mir bekannt, dass der Plagiatsbericht allein keine Garantie für die Eigenständigkeit der Arbeit darstellt und dass bei Vorliegen eines Plagiats Sanktionen verhängt werden**. Diese können neben einer Bearbeitungsgebühr je nach Schwere zur Exmatrikulation und zu Geldbußen durch die Middlesex University führen. Die Middlesex University führt das Plagiatsverfahren und entscheidet über die Sanktionen. **Dabei ist es unerheblich, ob ein Plagiat absichtlich oder unabsichtlich, wie beispielsweise durch mangelhaftes Zitieren, entstanden ist, es fällt in jedem Fall unter den Tatbestand der Täuschung**.

Sankt Augustin am 15.09.2024 ……

(Ort, Datum) Unterschrift

GESCHLECHTERSPEZIFISCHE FORMULIERUNGEN

Zur leichteren Lesbarkeit wird im folgenden Text auf eine geschlechtsspezifische Differenzierung, wie z.B. ExpertInnen verzichtet. Im vorliegenden Text wird durchgängig die männliche Form benutzt. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten, sondern schließen alle Formen gleichermaßen ein.

Inhaltsverzeichnis

I EINLEITUNGSTEIL

1 Ausgangslage

Wir befinden uns mit der Digitalisierung in der vierten industriellen Revolution (Schwab, 2016, S. 18-19). Damit sind einschneidende Veränderungen verbunden und es ist eine Beschleunigung in allen Bereichen zu erleben. Eine Umkehr der Digitalisierung ist unrealistisch und die gesamtgesellschaftlichen Konsequenzen sind derzeit nicht absehbar (Wittpahl, 2016, S. 5). Die Auswirkungen erfährt man nicht nur im individuellen Umgang mit der Technik, sondern auch Unternehmen, Organisationen und die staatliche Verwaltung stehen vor umfangreichen Herausforderungen. Nach Kotlarsky et al. sind mit der Komplexität und der Geschwindigkeit dieser digitalen Transformation auch Gefahren verbunden. Das Verhalten der Informationstechnik (IT) vorherzusagen, wird schwieriger und Unternehmen können von IT-Problemen immer stärker betroffen sein (2019, S. 95-96).

Ein Beispiel für die Abhängigkeit und die Gefahren bei der Nutzung von externen Cloud-Services zeigte sich im März 2021. Nach einem Großbrand in einem französischen Rechenzentrum des IT-Dienstleisters OVH waren in der Folge über drei Millionen Internetseiten nicht mehr abrufbar und es wurden Daten von Banken, Behörden und anderen Kunden vernichtet. Experten empfehlen den Kunden bzw. Unternehmen, auch für solche Situationen Strategien und Notfallpläne zu entwickeln (Kerkmann & Scheuer, 2021, S. 19). Bedeutend ist hier, dass ein eigentlich erwartbares regionales Schadensereignis weltweite Auswirkungen durch die Nichterreichbarkeit von Tausenden dort betriebenen Webseiten und IT-Services zur Folge hatte und auch Informationsdienste von Behörden betroffen waren.

Aufgrund von Nachteilen bei einer zu hohen Abhängigkeit von der IT fordern Newell und Marabelli (2015, S. 9) ein Gleichgewicht zwischen dieser IT-Abhängigkeit und dem Erhalt der Handlungsfähigkeit bei IT-Ausfällen. Zusätzlich müssen nach Wimelius et al. die wesentlichen IT-Systeme von Unternehmen für eine zielorientierte Nutzung der Digitalisierung regelmäßig erneuert werden. Hierin sehen die Autoren einen noch wenig erforschten Aspekt der Digitalisierung, der sowohl in der Theorie als auch in der Praxis zunehmend an Bedeutung gewinnt (2020, S. 215). Damit ergibt sich ein erster Teil der forschungsbegründenden Ausgangslage, der die Digitalisierung kritisch betrachtet und Handlungsnotwendigkeiten aufzeigt.

Die Digitalisierung hat auch Einfluss auf die öffentliche Verwaltung. Engel (2018, S. 25) spricht in diesem Zusammenhang von nachhaltigen Veränderungen und einem Transformationsprozess, der zugleich Chancen für eine weitreichende Neugestaltung von Prozessen der Verwaltung eröffnet.

Das gilt damit auch für staatliche Institutionen, die für die Sicherheit der Bundesrepublik Deutschland verantwortlich sind. Bei Nutzung dieser Weiterentwicklungschancen kann ein Ausfall der IT jedoch den gesamten Dienstbetrieb gefährden (Lasar, 2019, S. 106), sofern nicht mehr auf essenzielle Datenbestände oder relevante Applikationen zugegriffen werden kann. Während bei einem Unternehmen zunächst die Abwehr von wirtschaftlichen Schäden im Vordergrund steht, kann die unerwartete Einschränkung der Leistungserbringung bei staatlichen Einrichtungen weitreichende gesellschaftliche Schäden verursachen. Die öffentliche Verwaltung ist hierbei auf funktionierende IT-Systeme angewiesen, die von Unternehmen der IT-Industrie entwickelt und zunehmend auch für die Behörden betrieben werden.

Nach Beginn dieses Forschungsvorhabens ist die genannte Situation zu den Gefahren erstmals auch in Deutschland eingetreten und es wurde offiziell der „Erste digitale Katastrophenfall in Deutschland“ (BSI, 2022, S. 52) ausgerufen. Nach einem Ransomware-Angriff auf eine Landkreisverwaltung am 5. Juli 2021 konnten von der Verwaltung keine IT-gestützten Dienste mehr erbracht werden. Erst am 2. Februar 2022 wurde der Katastrophenfall aufgehoben und somit standen die Services für einen Zeitraum von 207 Tagen nicht zur Verfügung (BSI, 2022, S. 21).

Abbildung 1 – Erster digitaler Katastrophenfall in Deutschland (Quelle: BSI, 2022, S. 52)

Es ist davon auszugehen, dass eine Übertragung einer solchen Situation auf Sicherheitsbehörden, wie Polizei, Feuerwehr oder Bundeswehr, entsprechend drastische Auswirkungen haben kann. Auch der Ausfall von kritischen Infrastrukturen (KRITIS), wie

Energieversorgern, Krankenhäusern, dem öffentlichen Verkehrswesen und vergleichbar relevanten Einrichtungen der Landes- und Bundesbehörden, kann weitreichende Auswirkungen auf die allgemeine Sicherheit haben. Im geschilderten Fall waren die Auswirkungen noch regional und prozessual begrenzt. Die Situation verdeutlicht aber die Notwendigkeit einer resilienteren IT-Infrastruktur und zeigt die Dringlichkeit sowie die Aktualität der Thematik. Für ein Notfallmanagement gibt es nach Allweyer (2020, S. 211) die Praktiken des Business Continuity Managements (BCM) und für die IT das Service Continuity Management (ITSCM).

Mit dem vorliegenden Forschungsvorhaben wurde konkret das IT-Management mit Bezug zum Notfall- und Katastrophenfallmanagement unter besonderer Berücksichtigung der fortschreitenden Digitalisierung mit Blick auf die öffentliche Verwaltung untersucht. Die Ausgangssituation in den für diese Dissertation relevanten Themenfeldern stellt sich einleitend wie folgt dar.

1.1 Business Continuity Management (BCM)

Der deutsche Standard im IT-Notfallmanagement des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit der Bezeichnung „BSI-Standard 100-4, IT-Notfallmanagement Version 1.0“ (BSI, 2008, S. 1) wurde im November 2008 veröffentlicht. Im Januar 2021 wurde eine Neukonzeption herausgegeben, die in einer weiteren Version 2.0 im August 2022 überarbeitet erschienen ist (BSI, 2023, S. 11). Im Mai 2023 wurde unter dem Titel „BSI-Standard 200-4, Business Continuity Management“ daraus die aktuelle Version in Kraft gesetzt und hat damit den BSI-Standard 100-4 abgelöst (BSI, 2023, S. 11).

Um in einer Krise handlungsfähig zu bleiben und sich nicht von den Ereignissen der Krisen steuern zu lassen, können mit einem Business Continuity Management die zentralen Aufgaben kontrolliert abgearbeitet werden. Als einer der größten Vorteile des Business Continuity Managements wird die Minimierung von Ausfallzeiten gesehen (Mirkes und Özcan, 2020, S. 193). Die herausfordernde Ausgangslage ist hier, wie die Beispiele im vorherigen Kapitel gezeigt haben, dass ein Business Continuity Management offensichtlich noch nicht überall ausreichend etabliert ist.

1.2 Digitalisierung

Von verschiedenen Gefahren bei der Digitalisierung sprechen Proff et al. bereits im Vorwort der Veröffentlichung zur Digitalisierungsbeschleunigung. Noch vorhandene Probleme bei der Datensicherheit und hohe Unsicherheiten über die Möglichkeiten der Digitalisierung zeigen, dass hier aktuell Handlungsbedarf besteht (2021, S. V).

Als einen zentralen Punkt der Digitalisierung beschreibt Abolhassan die Cloud-Technologie. Der Autor bezeichnet die Cloud als Schlüsselfaktor für die Digitalisierung und als Basis, damit die Prozesse der Zukunft funktionieren können (2016, S. 149). Dem folgend werden in der weiteren Analyse des Business Continuity Managements die Aspekte der Cloud-Technologie als hervorgehobener Teil der Digitalisierung besonders mit untersucht.

Die Europäische Union (EU) veröffentlicht regelmäßig den ‚Digital Economy and Society Index' (DESI), der eine Kennzahl für die digitale Wirtschaft und Gesellschaft jedes Landes der EU ermittelt. In der Veröffentlichung aus dem Jahr 2022 liegt Deutschland zwar grundsätzlich insgesamt betrachtet im Mittelfeld auf Platz 13 von 28 Ländern (EU, 2022a, S. 19). Die Erhebung im Bereich E-Government bezüglich der Nutzung von behördlichen Services über das Internet zeigt für Deutschland allerdings mit Platz 25 von 28 (EU, 2022a, S. 67), dass hier die meisten europäischen Länder im Bereich der Bürgerservices bereits weitaus digitaler aufgestellt sind. Damit kann angenommen werden, dass es verstärkt zu weiteren Digitalisierungsprojekten in den deutschen Behörden kommen wird oder muss.

Die Behörden allein können allerdings diese Projekte nicht realisieren. Der Zusammenarbeit zwischen Staat und Wirtschaft kommt eine neue Bedeutung zu. Beide Bereiche sind aufeinander angewiesen und die digitalisierungsbezogene Produktentwicklung erfolgt in der Wirtschaft (Schmidt & van der Giet, 2018, S. 150). Daher liegt der Fokus dieser Arbeit in der Betrachtung des Business Continuity Managements aus Sicht der IT-Produktentwickler und IT-Dienstleister, die für Behörden bei der Digitalisierung die entsprechenden Leistungen erbringen. In Verbindung mit der Situation, dass mit der Digitalisierung auch Gefahren verbunden sind, ergibt sich diese von der Industrie abhängige Ausgangslage für die Digitalisierung in der Verwaltung, die entsprechend sicher erfolgen soll.

1.3 Relevanz für die öffentlichen Verwaltung

Wie bereits angeführt, sind von der Digitalisierung alle Bereiche betroffen. Damit ist diese auch für die öffentliche Verwaltung, die verantwortlichen Bereiche für die innere und äußere

Sicherheit und die kritische Infrastruktur in Deutschland erheblich relevant. Allerdings erreicht die Digitalisierung in Deutschlands Verwaltung noch nicht einmal durchgängig eine erste Stufe, so bilanzierten Klenk et al. im Jahr 2019 (S. 17). Die Autoren erläutern verschiedene Hemmnisse bei der Digitalisierung und bezeichnen es insgesamt als Politikproblem, dessen Bearbeitung stark verzögert erfolgt (2019, S. 19), womit bereits die Platzierungen des zitierten DESI-Index erklärbar werden. Explizit aus dem Bereich der Polizei werden mit der weiteren Digitalisierung auch Anreize für Kriminelle erwartet. Zudem wird damit gerechnet, dass sich dieser Trend weiter verstärken wird (Honekamp, 2019, S. 47). Hierdurch ergibt sich eine grundsätzlich problembehaftete Ausgangslage bei der weiteren Digitalisierung der öffentlichen Verwaltung. Basierend auf der Ausgangslage des Business Continuity Managements gemäß Kapitel I 1.1 und der Situation, Bedeutung und Notwendigkeit der Digitalisierung wurde die nachfolgende Problemstellung abgeleitet.

2 Problemstellung

Für einzelne Herausforderungen in der beschriebenen Ausgangslage existieren bereits Lösungsansätze durch Praktiken des Business Continuity Managements und des ITSCM, auf die im Folgenden näher eingegangen wird. Studien belegen allerdings, dass ein Notfallmanagement bisher nicht in allen Unternehmen zum etablierten Standard gehört. Lediglich ca. 43 % der Befragten einer Cybersicherheitsumfrage des Bundesamts für Sicherheit in der Informationstechnik haben angegeben, ein solches System zu betreiben, wie im jährlichen Lagebericht zur IT-Sicherheit veröffentlicht wurde (BSI, 2019, S. 50). Die Lageberichte der Folgejahre enthalten keine Umfrageergebnisse in dieser Form. Es muss aber davon ausgegangen werden, dass, wie die Beispiele in der Einleitung zeigen, hier weiterhin Nachholbedarf besteht.

Da sich das IT-Notfallmanagement in zahlreichen Bereichen noch im Aufbau befindet und die Veränderungen durch die Digitalisierung quantitativ wie qualitativ stark ansteigen, gilt es, den Managementaufwand für eine effiziente Notfallprävention nicht zu unterschätzen. Das Business Continuity Management betrachtet Schadensereignisse wie beispielsweise Erdbeben, Flutkatastrophen, Flugzeugabstürze oder Großbrände, deren Eintrittswahrscheinlichkeit zwar als gering eingeschätzt wird, deren Auswirkungen hingegen deutlich weitreichender sind als Vorfälle mit höherer Eintrittswahrscheinlichkeit. Hat sich die IT in den vergangenen Jahren rapide weiterentwickelt und ist die Abhängig davon gestiegen, während ein nur rudimentär vorhandenes Business Continuity Management nicht konsequent angepasst wurde, dann wird ein Katastrophenfall wie ein Großbrand oder eine Cyberattacke eklatante Auswirkungen haben.

2.1 Abhängigkeiten von der IT und drohender Kontrollverlust

Verschärfend kommt hinzu, dass nach einer 2022 durchgeführten Studie der Bitkom Research, bei der über 1000 Unternehmen Deutschlands befragt wurden, 45 % der Aussage zustimmten, dass Cyberangriffe ihre geschäftliche Existenz bedrohen. Ein Jahr zuvor, 2021, traf das auf nur 9 % der befragten Unternehmen zu (Bitkom, 2022a, S. 5). Hiermit wird die aktuell rapide steigende Bedeutung dieses Problems deutlich. In der Studie wurde unter der Überschrift „Kritische Infrastruktur rückt in den Fokus von Cyberangriffen“ zudem veröffentlicht, wie sich die Anzahl der Cyberattacken in den letzten zwölf Monaten entwickelt hat. Diese „Haben stark zugenommen“ (39 %) bzw. „Haben eher zugenommen“ (45 %), wie die Erhebung ergab

(Bitkom, 2022a, S. 6). Somit berichten aktuell 84 % der Unternehmen der KRITIS-Sektoren von zunehmenden Cyberattacken.

Ebenfalls problematisch ist, dass es bei bestimmten Aspekten der Digitalisierung aus technischen Gründen unmöglich ist oder sein wird, eine vollständige Absicherung durch Redundanzen im Rahmen der Notfallprävention zu schaffen. Die Rolle der IT ist als unbedenklich zu bewerten, solange sie nur unterstützend eingesetzt wird. Durch die bereits angesprochene Abhängigkeit steigen aber die damit verbundenen Gefahren und in der wissenschaftlichen Literatur wird die Digitalisierung diesbezüglich auch kritisch diskutiert. Faber (2019, S. 20) spricht von einem Kontrollverlust, der beispielsweise mit der weiteren Nutzung und Einführung von Cloud-Technologien einhergeht. Für einen sicheren Betrieb von Unternehmen, Behörden und staatlichen Organisationen ist bei einem Kontrollverlust über die IT allerdings von weitreichenden negativen Folgen auszugehen.

Eine besondere Herausforderung für das Notfallmanagement besteht darin, dass auch jene Technologien betrachtet werden müssen, die sich im digitalen Transformationsprozess in der Entwicklung befinden und noch nicht zum Einsatz kommen. Für diese neuen Entwicklungen ist eine frühzeitige Anpassung des ITSCM notwendig, um mit den zu erwartenden Veränderungen an der genutzten IT auch in IT-Notfällen sofort kompatibel zu sein. Inwieweit dies vor dem Hintergrund der fortschreitenden Digitalisierung zeitgerecht und technisch möglich ist, ist eine zentrale Fragestellung dieser Dissertation.

2.2 Zusammenfassende Problemstellung

Zusammenfassend zeigt sich das Problem, dass sich Unternehmen, Organisationen und Staaten im Rahmen der Digitalisierung zunehmend von der IT abhängig machen und es für IT-Katastrophen in einigen Bereichen noch keine resiliente Notfallprävention gibt oder geben kann. Die Digitalisierung ist unaufhaltbar und wird in immer schnelleren Zyklen neue Technologien, Prozesse und Veränderungen mit sich bringen. Deutschland hat hier insgesamt Nachholbedarf und insbesondere im Bereich der Digitalisierung von Behörden, die einerseits staatliche Services digital bereitstellen sollen und andererseits ebenfalls die gesamte digitale Transformation intern vollziehen müssen.

Das Business Continuity Management ist notwendig, um schnell auf bekannte Schadensgroßereignisse, wie Naturkatastrophen, die die IT-Infrastruktur zerstören, reagieren

zu können. Zudem entstehen mit der Digitalisierung neue Risiken, auf die ebenfalls zeitgerecht reagiert werden muss.

Zentrales Problem ist somit, dass das noch auf- bzw. auszubauende Business Continuity Management auf eine noch auf- bzw. auszubauende IT im Rahmen der Digitalisierung trifft. Dadurch gewinnt das Business Continuity Management zunehmend an Bedeutung. Dies gilt für Unternehmen allgemein, für Behörden und Organisationen der kritischen Infrastruktur, für Sicherheitsbehörden wie Polizei und Bundeswehr, aber auch alle Ämter auf Bundes-, Landes- oder kommunaler Ebene sind betroffen. Wie kann die weitere Digitalisierung derart sicher gestaltet werden, dass nicht durch bekannte und neue Risiken die allgemeine Sicherheit gefährdet wird, wenn der Staat seinen Aufgaben nicht mehr nachkommen kann? Mit dieser Problematik befasst sich die gesamte Arbeit, um Erfolgsfaktoren abzuleiten und nachvollziehbare Handlungsempfehlungen zu erstellen, die die Digitalisierung in Deutschland sicherer machen können.

3 Erkenntnisinteresse und Relevanz der Arbeit

Aus der dargestellten Problemstellung leitet sich die Relevanz der Arbeit bereits ab. Unternehmen und Behörden sollten das Ziel verfolgen, negative Auswirkungen und Schäden bei IT-Problemen so gering wie möglich zu halten. Für die Erarbeitung von Lösungen für diese Problematik werden im folgenden Kapitel die relevanten Themen erörtert und die konkreten Erkenntnisinteressen abgeleitet.

3.1 Themenfelder

Im Fokus stehen die übergeordneten Themenfelder Digitalisierung und Notfallmanagement. Für die gemeinsame Betrachtung werden die Bereiche IT-Management, ITSCM, Business Continuity Management und die Digitalisierung in Unternehmen und Behörden beleuchtet. In der nachfolgenden Abbildung 1 sind die Zuordnungen, die prinzipiellen Zusammenhänge und die Schnittstellen dieser relevanten Themenfelder visualisiert.

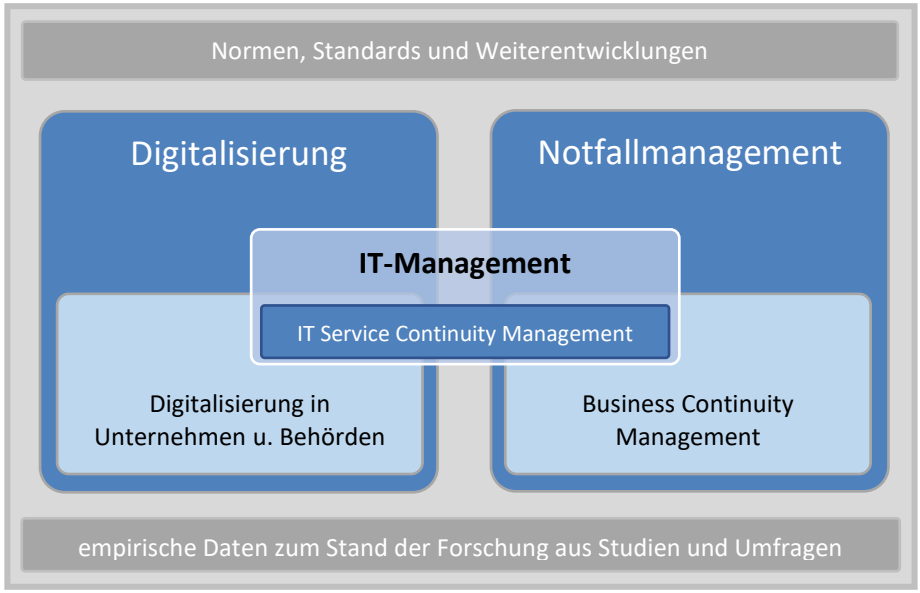


Abbildung 2 – Strukturierte Themenübersicht (Quelle: eigene Darstellung)

Die als unabhängig einzustufenden Bereiche Digitalisierung und Notfallmanagement sind in dieser Betrachtung über das IT-Management miteinander verbunden. Speziell das ITSCM bildet hier eine Schnittmenge zwischen der Digitalisierung in Unternehmen und dem Business Continuity Management. Ergänzend stehen Normen, Standards und die Weiterentwicklungen im Bereich der Digitalisierung und des Notfallmanagements im Fokus, um zukunftsorientierte und praktikable Empfehlungen zu erarbeiten. Inhaltlich sind diese Themen und weitere relevante Begriffe, beispielsweise IT-Sicherheit, in Kapitel II 2.1 (theoretische Ausführungen

zu den fachlichen Themenfeldern) ausführlich definiert und mit dem Stand der Forschung dargestellt, um eine einheitliche Basis für den empirischen Teil zu schaffen.

3.2 Forschungsrelevanz

Zur Wirkung der Digitalisierung auch im Bereich des öffentlichen Sektors gibt es bereits Forschungen, die größtenteils aus den USA oder China stammen, wobei die meisten die Effizienz und die Performanz analysieren. Zu den Auswirkungen der Digitalisierung in Verwaltungen und der Verknüpfung unterschiedlicher Wirkungsdimensionen wird eine intensivere Auseinandersetzung empfohlen (Fischer et al., 2021, S. 3).

Für die Forschung werden die theoretischen Zusammenhänge der Themenfelder in dieser Arbeit transparent, die das in Studien und Berichten dargestellte Sicherheitsniveau erklärbar machen. Es wird bewertet, welche Entwicklungen aufgrund der weiteren Digitalisierung Auswirkungen auf das Notfallmanagement haben werden. Mit besonderem Blick auf die IT-Dienstleister mit Behördenerfahrung können Rückschlüsse auf das Sicherheitsniveau in der öffentlichen Verwaltung im weiteren Transformationsprozess der Digitalisierung gezogen werden. Für weiterführende Forschungen im Bereich der Digitalisierung der öffentlichen Verwaltung bieten die Ergebnisse Anknüpfungspunkte zum Notfall- und Katastrophenfallmanagement im Allgemeinen und zum ITSCM im Speziellen.

Hinsichtlich der steten Erneuerung der zentralen IT im Rahmen der Digitalisierung wird in der Forschung noch Nachholbedarf konstatiert, da es hierzu erst wenige Untersuchungen gibt (Wimelius et al., 2020, S. 215). Für den Anteil des Business Continuity Managements und der Forschungen im Bereich des Notfallmanagements wird durch eine Berücksichtigung der Analyseergebnisse und Handlungsempfehlungen dieser Dissertation bewertbar, in welchen Bereichen mit der fortschreitenden Digitalisierung welche Vor- oder Nachteile im IT-Notfallmanagement zu erwarten sind. Zur Weiterentwicklung in der Digitalisierung zeigen die Ergebnisse aus dem theoretischen Teil die besonderen Herausforderungen in Bezug auf die IT-Sicherheit auf. Mit den Handlungsempfehlungen werden Lösungen angeboten, um die Weiterentwicklung der Digitalisierung auch theoretisch und aus Sicht der IT-Sicherheit für bestimmte Technologien zu unterstützen. Diese können andere Forscher nutzen, um bei Arbeiten, die nicht vorrangig auf die Sicherheit fokussiert sind, den Sicherheitsaspekt angemessen einzubeziehen.

3.3 Praxisrelevanz

Die dargestellte Digitalisierung ist für das IT-Management von Behörden und Unternehmen sowie ihre Kombination, insbesondere bei behördenerfahrenen IT-Dienstleistern, relevant. Diese Relevanz gliedert sich in die Hauptthemen Business Continuity Management und Digitalisierung. Für beide gilt, dass durch die steigende Abhängigkeit von der IT im Management abzuschätzen ist, welche Investitionen für die notwendige Sicherheit einzuplanen sind. Die Ergebnisse der Dissertation ermöglichen in der Praxis einen schnellen, geleiteten und wissenschaftlich fundierten Zugang zu diesen Herausforderungen der Digitalisierung. Die Empfehlungen zielen darauf ab, die Eintrittswahrscheinlichkeit von großen IT-Risiken für Unternehmen zu minimieren, indem die absehbaren Herausforderungen frühzeitig erkannt und berücksichtigt werden. Es wird diskutiert, wie sich die negativen Auswirkungen bei IT-Notfällen durch eine gute Organisation reduzieren lassen. Die Handlungsempfehlungen wirken nachhaltig, wenn sie bei Entscheidungen zur weiteren Digitalisierung als grundsätzliches Regelwerk berücksichtigt werden.

3.3.1 Betriebswirtschaftliche Relevanz aus Sicht des BCM

Investitionen in die Notfallprävention, die bei der Umsetzung von Digitalisierungsprojekten anfallen, sind so zu gestalten, dass auch die Voraussetzungen des Business Continuity Managements berücksichtigt werden. Nicht nur die Kosten der Präventionsmaßnahmen sind mit einzukalkulieren, sondern auch die etwaigen Aufwände bei der Notfallfallbewältigung nach Eintritt eines Schadensereignisses. Spörrer (2014, S. 2) sieht vor allem bei der Datenwiederherstellung ein hohes Einsparpotenzial und prognostiziert höhere Kosten bei längeren Ausfallzeiten. Der Autor spricht in diesem Zusammenhang von unnötig viel Zeit, die verloren geht und sich durch optimierende Maßnahmen einsparen ließe.

Neben der monetären Betrachtung ist von der Themenstellung auch das allgemeine betriebliche Risikomanagement betroffen. Ausdrücklich wird auf die Risiken eingegangen, deren Eintrittswahrscheinlichkeiten sehr gering sind und bei denen die betriebswirtschaftlichen Auswirkungen sehr hoch sein können. Königs (2017, S. 22) berücksichtigt in einer Risikomatrix beispielhaft eine Schadenshöhe von mehr als 10 Millionen Euro und bringt katastrophale Schäden in direkten Zusammenhang mit Unternehmensinsolvenzen. Sowohl die Eintrittswahrscheinlichkeit als auch die Schadenshöhe, insbesondere die Insolvenz von Unternehmen oder die Handlungsunfähigkeit staatlicher Organisationen, sollen durch Anwendung der zu erarbeitenden

Handlungsempfehlungen verringert werden. Betriebswirtschaftlich können auf diese Weise Unternehmensinsolvenzen durch unzureichende Aktivitäten bei der digitalen Transformation reduziert werden und die benötigten Investitionen werden kalkulierbarer.

Die Forschungsergebnisse lassen sich auch direkt nutzen, um das Business Continuity Management allgemein weiterzuentwickeln. Die später erarbeiteten Schwerpunkte und Empfehlungen aus dem empirischen Teil werden das in den letzten Jahren entstandene Defizit in diesem Bereich aus der Praxis aufzeigen, basierend auf den theoretischen Grundlagen. Auch die wissenschaftlichen Veröffentlichungen hierzu wurden berücksichtigt und diskutiert, um einen nachvollziehbaren Erkenntnisgewinn herauszuarbeiten, der das zukünftige Business Continuity Management in seiner Anwendung durch die BCM-Manager in den Unternehmen optimieren kann.

3.3.2 Digitalisierungsprojekte und -produkte

Mit einer Berücksichtigung der erarbeiteten Empfehlungen in Digitalisierungsprojekten kann vermieden werden, dass sich die aus der Praxis berichteten Fehler wiederholen. Ebenso lässt sich bereits bei der Entwicklung digitaler Produkte darauf achten, wo es im Bereich Business Continuity Management aktuell noch Schwierigkeiten gibt, um Lösungen hierfür direkt mit anbieten und integrieren zu können.

Dadurch entsteht ein Mehrwert, mit dem Digitalisierungsprojekte in Unternehmen und für den öffentlich Bereich effizienter gestaltet werden können, ohne neue Sicherheitsrisiken einzugehen.

4 Zielstellung der Dissertation

In diesem Kapitel wird das Hauptziel der Dissertation erläutert und die hierfür notwendigen Teilziele aus dem theoretischen, dem empirischen und dem Gestaltungsteil werden abgeleitet. Nachfolgend sind diese jeweils mit den erwarteten Ergebnissen dargestellt.

4.1 Haupt- und Teilzielstellungen

Hauptziel der Dissertation ist der Erkenntnisgewinn, mit welchen Maßnahmen die fortschreitende Digitalisierung derart sicher gestaltet werden kann, dass die steigende Abhängigkeit möglichst keine katastrophalen Auswirkungen haben wird. Im Fokus stehen behördenerfahrene IT-Dienstleister, von deren Dienstleistungsqualität es abhängig ist, ob die öffentliche Verwaltung bei IT-Notfällen handlungsfähig bleiben kann. Auf Basis der dargestellten Themenstruktur werden die Empfehlungen nach dem Business Continuity Management und dem ITSCM im Kontext der digitalen Transformation analysiert, um daraus gezielt Handlungsempfehlungen abzuleiten. Dazu werden Faktoren herausgearbeitet, die als Erfolgsfaktoren einen „langfristigen Erfolg maßgeblich beeinflussen“ (Baumgarth & Evanschitzky, 2009, S. 237) können. Diese Vorgehensweise ist geeignet, um Handlungsempfehlungen abzuleiten (Baumgarth & Evanschitzky, 2009, S. 253).

4.1.1 Hauptzielstellung

Für die zukunftsbezogenen Themen der kommenden Digitalisierung und des Zusammenspiels mit dem Business Continuity Management kann es noch kein fundiertes Vorwissen geben. In einer solchen Situation sind nach Döring Forschungsfragen zu erstellen (2023, S. 149). Die Formulierung von Forschungsfragen ist ein grundlegender Schritt und ein wesentlicher Aspekt in der Forschung allgemein (Alvesson und Sandberg, 2013, S. 1). Als Hauptzielstellung ist hier die Beantwortung der folgenden Hauptforschungsfrage zu sehen, die damit der Schließung der Forschungslücke dient. Die Forschungslücke wird auf Basis der theoretischen Grundlagen später in Kapitel II 1.2 explizit dargestellt.

Kongruent zum Titel der Dissertation lautet die Hauptforschungsfrage (HFF) wie folgt:

- HFF: Wie ist die Situation des Business Continuity Managements im Zeitalter der Digitalisierung und mit welchen Erfolgsfaktoren kann eine möglichst sichere Digitalisierung, auch in der öffentlichen Verwaltung, ermöglicht werden?

Um die Forschungsfrage zu beantworten, können Unterfragen dazu beitragen, die zu recherchierenden Informationen zu ermitteln (Karmasin und Ribing, 2017, S. 25). Zur Erarbeitung der Antworten wurden die folgenden drei Nebenforschungsfragen (NFF) jeweils mit gleichbleibendem Fokus der Zielgruppe aufgestellt:

- NFF1: Wie ist die Situation des Business Continuity Managements mit Blick auf die Digitalisierung?
- NFF2: Welche Aspekte der Digitalisierung sind hier kritisch?
- NFF3: Welche Lösungsmöglichkeiten gibt es hier in der Praxis?

Zur Erreichung des Hauptzieles durch Beantwortung der Haupt- und Nebenforschungsfragen ist das Erreichen mehrerer Teilziele aus dem Bereich der Theorie, der Empirie und des Gestaltungsteils notwendig, die in den nächsten Kapiteln beschrieben sind.

4.1.2 Theoriegeleitete Zielstellungen

Im theoretischen Teil der Dissertation sind die nachfolgenden Fragestellungen zu beantworten, um damit einen wissenschaftlichen Erkenntnisgewinn zu erzeugen und die Grundlagen für den empirischen Teil dieser Arbeit zu schaffen:

- Welche Facetten der Digitalisierung stehen in einem engen Zusammenhang mit der in der Problemstellung genannten Situation?
- Welche positiven oder negativen Auswirkungen sind mit der Einführung neuer Technologien in Bezug auf die IT-Notfallvorsorge grundsätzlich zu erwarten?

Ebenfalls theoriegeleitet gilt es, die Einflussfaktoren für ein effizientes IT-Notfallmanagement bei Behörden und behördennahen Unternehmen zu erkennen. Dieser Sachverhalt soll zusätzlich unabhängig von der digitalen Transformation betrachtet werden, um einen Zusammenhang zur erstgenannten Fragestellung ableiten zu können. Diese Zielstellung ergibt sich aus der Bearbeitung folgender Forschungsfragen:

- Welche neuen Herausforderungen entstehen für das IT-Notfallmanagement durch welche Aspekte der Digitalisierung?
- Welche Faktoren beeinflussen maßgeblich den Auf- und Ausbau des IT-Notfall-managements?

Mit den erwarteten Ergebnissen aus dem theoretischen Teil steht die Grundlage zur Verfügung, um den Erkenntnisgewinn über die Zusammenhänge der Themenfelder darzulegen. Gleichzeitig bilden die herausgearbeiteten Kernelemente der Digitalisierung den

fachlichen Fokus für den empiriegeleiteten Teil. Die Einflussfaktoren werden als wesentlicher Aspekt im Rahmen der später ausgewählten Erhebungsmethode diskutiert.

4.1.3 Empiriegeleitete Zielstellungen

Empirisch wurde untersucht, welche Zusammenhänge in der Praxis zu den im theoretischen Teil aufbereiteten Fragestellungen existieren. Insofern die im theoretischen Teil herausgearbeiteten Aspekte der Digitalisierung direkte Auswirkungen auf die bestimmenden Einflussfaktoren des IT-Notfallmanagements haben, sind diese zu bewerten. So hat beispielsweise eine Verlagerung großer Bereiche des eigenen IT-Betriebes in die Cloud einen erheblichen Einfluss auf die Wahl der organisatorischen und technischen Backup- und Recovery-Strategien. Mit welchen Möglichkeiten und in welcher Projektphase kann das IT-Management in der Praxis die Anforderungen an die IT-Sicherheit adäquat berücksichtigen? Die Fragestellung wird ausdrücklich um einen zielorientierten Teil ergänzt, der sich darauf bezieht, mit welchen Praktiken bereits positive Erfahrungen gemacht werden konnten. Damit lassen sich im späteren gestalterischen Teil Empfehlungen ableiten. Die Zielstellung ist somit die Bearbeitung der folgenden Fragestellungen:

- Wie und wann wird in der Praxis ein Business Continuity Management angewendet, um den neuen Herausforderungen der Digitalisierung gerecht zu werden?
- Welche Einflussfaktoren, Herausforderungen und Erfahrungen stehen hierzu in Unternehmen in welchem Zusammenhang?
- Welche bewährten Praktiken existieren bereits, um die IT-Sicherheit mit den Methoden eines Business Continuity Managements bei der weiteren Digitalisierung zu erhöhen?

Als ein Teilergebnis der empirischen Untersuchung werden praxisorientierte Vorgehensweisen erwartet, verglichen und bewertet. Es wird dargestellt, wann und in welcher Form das Notfallmanagement in der Praxis beim Ausbau der Digitalisierung Berücksichtigung erfährt. Hiermit wird gezielt das in der Ausgangslage dargestellte Problem mit empirischen Informationen aufgearbeitet.

Die Fragestellungen beziehen sich mittelbar auf die öffentliche Verwaltung und unmittelbar auf deren IT-Dienstleister. Damit wird erreicht, dass sich die Betrachtung nicht nur auf die theoretischen und technischen Aspekte konzentriert, sondern dass auch betriebswirtschaftliche Faktoren aus den Unternehmen mitberücksichtigt werden. Diese

lösungsorientierten Fragestellungen werden ergebnisoffen zum Ziel des Forschungsvorhabens hinführen und bilden den Übergang zum gestaltungsgeleiteten Teil.

4.1.4 Gestaltungsgeleitete Zielstellungen

Ziel ist die Herausarbeitung von Erfolgsfaktoren durch eine praxisorientierte Erhebung der Daten und die Erstellung eines praxisbezogenen Ergebnisses in Form von Handlungsempfehlungen. Diese Handlungsempfehlungen bieten Unternehmen der IT-Dienstleistungsbranche und Behörden die Möglichkeit, eine Notfallprävention, die technisch wie organisatorisch mit der fortschreitenden Digitalisierung vereinbar ist, effizient anzuwenden oder deren Einführung zu planen.

Es wird erwartet, dass zu einzelnen Komponenten der Digitalisierung, beispielsweise dem Cloud-Computing oder anderen Technologien, spezifische Empfehlungen erstellt werden können, die sich in der Praxis bereits bewährt haben oder die sich aus dem theoretischen Teil ableiten lassen. Außerdem soll auf die außergewöhnlichen Gefahren, beispielsweise auf die physische Zerstörung der Infrastruktur, auf den Kontrollverlust über die IT und auf Verschlüsselungstrojaner, kontextbezogen eingegangen werden, damit Unternehmen solche Risiken bei ihrem weiteren Ausbau der Digitalisierung ausreichend berücksichtigen. Aufgrund der weitreichenden Auswirkungen der Digitalisierung auf alle Bereiche der Wirtschaft und des Managements ist vorgesehen, die zu erstellenden Empfehlungen im Rahmen des Gestaltungsteils auf zielführende Themen der Beratung und des IT-Projektmanagements mit Fokus auf behördennahe IT-Dienstleister zu konzentrieren.

4.2 Erwartete neue Ergebnisse/Erkenntnisse

Die gemeinsame Betrachtung der in Kapitel I 3.1 dargestellten Themenfelder, beispielhaft fokussiert auf behördenerfahrene IT-Dienstleister in Deutschland, wurde noch nicht wissenschaftlich untersucht. Neu werden die Erkenntnisse sein, die aufzeigen, bei welchen Aspekten der Digitalisierung mit besonderen Auswirkungen auf das Business Continuity Management zu rechnen ist.

Die Untersuchung der Managementpraktiken im Bereich IT-relevanter Notfall- und Katastrophenfallvorsorge wird ebenfalls neue Ergebnisse generieren. Es wird überprüft, wie man sich in der Praxis systematisch auf die weiteren Digitalisierungsthemen einstellt. Bestehende Forschungsergebnisse zu Teilbereichen werden dahingehend berücksichtigt bzw.

weiterentwickelt, dass Rückschlüsse auf einen sicheren Umgang mit der Digitalisierung in der öffentlichen Verwaltung in Deutschland gezogen werden können.
Für die Wissenschaft werden diese Ergebnisse den Stand der Forschung zur Digitalisierung und zum Business Continuity Management allgemein und speziell für Behörden und behördennahe IT-Dienstleister ergänzen. Mit dem Schließen der Forschungslücke wird die weitere Entwicklung der Digitalisierung konkret mit den Anforderungen des Business Continuity Managements bewertet und eine optimierte Vorgehensweise für die Zielgruppe wird erstmals erarbeitet. Durch die Fokussierung auf behördenerfahrenen IT-Dienstleister grenzt sich die Dissertation von anderen Untersuchungen aus dem Bereich der IT-Sicherheit deutlich ab. Da die Themen Digitalisierung und des Business Continuity Managements nicht behördenspezifisch sind, bleibt die Übertragbarkeit auf andere Unternehmen und Organisationen grundsätzlich gegeben.

4.2.1 Erwartete neue Ergebnisse und Erkenntnisse der Dissertation insgesamt

Insgesamt wird das Zusammenspiel der Aktivitäten für eine weitere Digitalisierung und der Managementaktivitäten für ein notwendiges Business Continuity Management untersucht, um Zusammenhänge herauszuarbeiten, die mit diesem Fokus noch nicht erhoben wurden. Insbesondere die Betrachtung der behördenerfahrenen IT-Dienstleister ermöglicht eine Analyse des erhobenen Materials, um die dortigen Herausforderungen zu benennen und zu untersuchen. Die in diesem Zusammenhang dargestellten Ergebnisse mit Lösungsmöglichkeiten, analysiert auf Basis der theoretischen Grundlagen, stellen dann die neuen Erkenntnisse dar. Was sind die größten Herausforderungen aus Sicht der IT-Dienstleister, um insgesamt und mit Blick auf deutsche Behörden die Digitalisierung unter Berücksichtigung eines effektiven IT-Notfallmanagements erfolgreich umzusetzen? Die Antworten hierauf in Form von fundierten Empfehlungen für die Praxis und die Forschung sind insgesamt das Ergebnis der Dissertation.

4.2.2 Erwartete neue Ergebnisse und Erkenntnisse des theoretischen Teils

Im theoretischen Teil wird ein Überblick über die relevanten Studien und Veröffentlichungen geschaffen, um für die Zielgruppe vorhandene Grundlagen und Ergebnisse darzustellen. Der Vergleich und die Analyse der verschiedenen Erkenntnisse in der Theorie werden sowohl den Forschungsbedarf schärfen als auch die Empfehlungen anderer Forscher aufgreifen. Auf Basis der Erkenntnisse können dann neue Ergebnisse erarbeitet werden. Konkret geht es darum,

inwiefern die technischen Eigenschaften und Möglichkeiten der zu erwartenden Digitalisierungstechnologien bereits Vor- oder Nachteile mit Blick auf resiliente Infrastrukturen mit sich bringen. Die aus den Managementtheorien bekannten Vorgehensweisen, beispielsweise das klassische Risikomanagement, werden mit den Theorien der Digitalisierung und des Notfallmanagements reflektiert. Als Ergebnis des Theorieteils wird der aktuelle Sachstand zu den Themenfelder dargestellt und die dort aktuell schon vorhandenen Forschungsergebnisse werden, soweit schon möglich, auf die Kombination der Themenfelder abstrahiert.

Damit kristallisieren sich im Ergebnis die relevanten Themenfelder weiter heraus, die es zu untersuchen gilt. Welche Aspekte der Digitalisierung stehen hier im Vordergrund und sollen später im empirischen Teil konkret hinterfragt werden? Angewandt auf den Prozess der Digitalisierung auch im Bereich behördlicher IT und in Kombination mit dem Notfall-management stellt dieser theoretisch abgeleitete Untersuchungsumfang neue Erkenntnisse dar, die so noch nicht analysiert wurden.

4.2.3 Erwartete neue Ergebnisse und Erkenntnisse des empirischen Teils

Mit den Ergebnissen aus dem vorangegangenen Kapitel wurde der Rahmen des empirischen Teils bereits definiert. Es stellt sich nun die Frage, wie es in der Praxis bezüglich dieser Thematiken, Herausforderungen und Erfahrungen aussieht. Daher wird eruiert, welche Erfahrungen es gibt, die mit der Problemstellung in einem engen Zusammenhang stehen. Neu hierbei ist, dass nicht nur eine Einzelbetrachtung auf ein Themenfeld erfolgt. Es wird nicht die Digitalisierung singulär betrachtet und hinterfragt, sondern das Business Continuity Management wird stets miteinbezogen. Erfahrungen der Zielgruppe werden erfasst, die durch beide Bereiche beeinflusst sind, um hier neue Erkenntnisse zu erhalten. Die Ausarbeitung, z. B. im Sinne von Lösungsmöglichkeiten, werden als neue Ergebnisse gemäß dem nachfolgenden Kapitel ausgearbeitet.

Die Ergebnisse sollen in der Form erarbeitet werden, dass Erfahrungen aus der Praxis erhoben und im Anschluss kategorisiert sowie bewertet werden. Basierend auf der Theorie werden bestimmte Situationen, Meinungen und Erfahrungen hinterfragt: Werden die in den Theorien geforderten und empfohlenen Vorgehensweisen auch in der Praxis umgesetzt? Wie wird das Business Continuity Management tatsächlich in der Praxis angewandt? Welche positiven Erfahrungen und Empfehlungen existieren hier und können weiter aufbereitet werden? Sind Gründe erkennbar, durch die sich die Situationen aus Kapitel 1 (Ausgangslage) und Kapitel 2

(Problemstellung) erklären lassen? Das sind die wesentlichen erwarteten neuen Ergebnisse und Erkenntnisse des empirischen Teils, die sich teilweise in Modellen darstellen lassen. In jedem Fall werden sie in Form kategorisierter Segmente der relevanten Aspekte abgebildet.

4.2.4 Erwartete neue Ergebnisse und Erkenntnisse des Gestaltungsteils

Nicht neu wären Empfehlungen, dass bei der weiteren Digitalisierung auch Aspekte der IT-Sicherheit und des Business Continuity Managements zu betrachten sind. So hat Pohlmann die These formuliert „Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung“ und im Rahmen einer weiteren These fordert er, dass mehr Verantwortung hierfür direkt durch die IT-Hersteller übernommen werden muss (Pohlmann, 2018, S. 210). Die neuen Ergebnisse im Gestaltungsteil sollen diese Forderungen konkretisieren und die aus der Praxis bekannten Defizite benennen sowie Verbesserungsmöglichkeiten vorschlagen. Diese werden als Handlungsempfehlungen formuliert. Neue Erkenntnisse sind zudem die Ausarbeitungen zu Managementaktivitäten, Mitarbeiterintegration oder einer zeitgerechte Projekteinbindung, auf die sich die Empfehlungen fokussiert haben. Damit können explizite Handlungs-anleitungen als Erfolgsfaktoren herausgestellt werden. Hier wird erwartet, dass die relevantesten und größten Herausforderungen für eine sichere Digitalisierung mit dem Fokus auf behördennahe IT in Form von Empfehlungen, Mindmaps und Anleitungen lösungsorientiert gestaltet werden können.
Aufgrund der weitreichenden Auswirkungen der Digitalisierung auf alle Bereiche der Wirtschaft und des Managements ist vorgesehen, die Arbeit, wie im nachfolgenden Unterkapitel beschrieben, abzugrenzen.

4.3 Inhaltliche Abgrenzung

Die Themengebiete Digitalisierung, Management und Sicherheit sind so umfassend, dass zur Fokussierung dieser Dissertation eine praxisorientierte Schwerpunktbildung notwendig ist. Allgemeingültige Empfehlungen sind in diesem Zusammenhang nicht zielführend bzw. stellen keine Forschungslücke dar, da es bereits Best Practices für das IT-Management gibt, die in Kapitel II 2.1. detaillierter dargestellt sind. In Ableitung der Problemstellung stehen lediglich die IT-Notfallprozesse aus Sicht des IT-Managements im Fokus der Untersuchungen.
Als weitere Abgrenzung wird nicht die Digitalisierung in allen Facetten betrachtet, sondern es geht um die für die unternehmenskritischen Prozesse bei Behörden bzw. behördennahen

IT-Dienstleistern relevanten Anteile. Bereiche der Digitalisierung, die nach aktuellen Erkenntnissen keine Auswirkungen auf das Notfall- und Katastrophenfallmanagement bzw. auf den Betrieb der öffentlichen Verwaltung haben, werden ausgeschlossen. ‚Smart Home' ist beispielsweise kein Untersuchungsobjekt. Hierzu wurden die Schwerpunkte und Empfehlungen aus der Theorie berücksichtigt, so dass beispielsweise das Cloud-Computing hervorgehoben mitbetrachtet wird. Dadurch kann eine Schärfung auf die Kernelemente der IT erfolgen, die für Behörden und Unternehmen aktuell von hoher Bedeutung sind und deren zuverlässiger Betrieb existenzsichernd ist. Für diese Anteile sind nicht alle Unternehmensprozesse relevant. Die Betrachtungen konzentrieren sich auf das Business Continuity Management und die ITSCM-Prozesse. Zusammenfassend wird eine Eingrenzung auf bestimmte Anteile der Digitalisierung und dort auf die Betrachtung der Notfallprozesse vorgenommen.

Eine weitere Eingrenzung erfolgt auf die unternehmenskritischen Applikationen und Daten. Applikationen, deren Ausfälle zwar ggf. teuer und problematisch, aber nicht existenzgefährdend sind, werden nicht berücksichtigt. Beispielsweise sei hier die Zerstörung eines elektronischen Arbeitszeiterfassungssystems genannt, womit zahlreiche innerbetriebliche und juristische Probleme verbunden sein können, wodurch aber der Fortbestand des Unternehmens grundsätzlich nicht gefährdet ist. Hassel und Cedergren (2019, S. 1504) sprechen von kritischen Funktionen, die es als Ziel von Business Continuity Management seitens der Organisation abzusichern gilt. Übertragen auf Behörden könnte der Verlust aller digitalen Ermittlungs- oder Vorgangsakten gravierende Auswirkungen haben und direkt die allgemeine Sicherheit gefährden. Teilweise erfolgte diese Abgrenzung explorativ durch offene Fragestellungen in den Interviews, um die in der Praxis relevanten Themen vorrangig zu untersuchen. Aspekte, die bereits aus der Theorie von hoher Bedeutung sind, wurden hinterfragt, allerdings sollten die sich wiederholenden Punkte aus der Praxis im Schwerpunkt aufgenommen werden. Dies gilt sowohl für die Digitalisierungsthemen als auch für die Best Practices des Business Continuity Managements und insbesondere für die aufgezeigten Defizite. In Theorie und Praxis nicht genannte Aspekte werden abgegrenzt.

Eine weitere Abgrenzung ergibt sich daraus, dass die öffentliche Verwaltung nicht vorrangig gewinnorientiert agiert (Schaefer & Gornas, 2018, S. 53-54). Daher wird die Wirtschaftlichkeit der Handlungsempfehlungen nicht primär beurteilt. Mit der Datenerhebung aus der Praxis wird in diesem Kontext der Aspekt ‚Aufwand und Nutzen' erfragt, wobei die dort erarbeiteten

Ergebnisse mit Erkenntnissen aus der Theorie diskutiert werden und damit zum Gesamtergebnis beitragen.

Die Beschränkung auf die wesentlichen Geschäftsprozesse, die Applikationen und die relevanten Aspekte der Digitalisierung bei Behörden bzw. behördennahen IT-Dienstleistern stellt, neben der Konzentration auf die IT-Notfallprozesse, die zielorientierte Abgrenzung dar.

5 Aufbau der Dissertation

Die Dissertation ist in die folgenden Teile und Hauptkapitel untergliedert:

Teile und Hauptkapitel	Fachlicher Inhalt
I Einleitungsteil •1 Ausgangslage •2 Problemstellung •3 Erkenntnisinteresse und Relevanz •4 Zielstellung	Situationsdarstellung zum Business Continuity Management und der Digitalisierung in Deutschland mit Ereignissen aus dem Bereich von IT-Notfällen/-katastrophen.
II Theoretischer Teil •1 Stand der Forschung und Forschungslücke •2 Theoretische Ausführungen •3 Konklusion theoretischer Teil	Darstellung Business Continuity Management und Digitalisierung auf Basis wissenschaftlicher Veröffentlichungen. Herleitung der Forschungslücke.
III Empirischer Teil •1 Forschungsdesign •2 Ergebnisse •3 Diskussion, Interpretation, Konklusion	Auswahl, Begründung und Dokumentation der empirischen Methode Experteninterviews. Darlegung und Diskussion der Ergebnisse.
IV Gestaltungsteil •1 Empfehlungen Forschung •2 Empfehlungen Praxis •3 Zusammenfassung und Konklusion	Auf Basis der vorherigen Kapitel erstellte Empfehlungen, wie die Digitalisierung aus Sicht des Business Continuity Managements sicherer gestaltet werden kann.
V Schlussteil •1 Zusammenfassung und Fazit •2 Ergebnisse und Erkenntnisse •3 Ausblick •4 Verzeichnisse	Zusammenfassende Darstellung der Dissertation mit ihren Ergebnissen und einem Ausblick, wie sich die Digitalisierung entwickeln kann, um die dokumentierten Probleme zu vermeiden.
Anlagen •Expertenliste, Protokolle, Codebuch, ...	Übersicht Experten, Interviewleitfaden, Gesprächsprotokolle, …

Abbildung 3 – Grobstruktur Aufbau der Dissertation (Quelle: eigene Darstellung)

Nachfolgend werden die Kapitel der ersten und zweiten Ebene in ihrer Reihenfolge genannt und beschrieben. Damit ergibt sich neben dem strukturellen auch ein inhaltlicher Überblick über die gesamte Arbeit.

Teile und Hauptkapitel	Kurze Inhaltsbeschreibung
I Einleitungsteil	
1 Ausgangslage	Die fortschreitende Digitalisierung im Kontext von großen IT-Ausfällen/IT-Notfällen wird dargestellt. Das für solche Situationen vorgesehene Business Continuity Management wird betrachtet und die Relevanz der Arbeit, auch für die öffentliche Verwaltungen, wird erläutert.
2 Problemstellung	Der Fakt, welche schwerwiegende Folgen die Situation aus der Ausgangslage haben kann, wird hier dargestellt. Inhaltlich zusammenfassend sind es folgende problematischen Fragestellungen: Macht man sich zu sehr von der IT abhängig? Verliert man die Kontrolle, wenn die IT nicht mehr zur Verfügung steht? Können zukünftig die staatlichen Sicherheitsorganisationen noch ihrem Auftrag nachkommen, wenn die IT ausfällt? Wo stehen wir hier bei den notwendigen IT-Management-Standards?
3 Erkenntnisinteresse und Relevanz der Arbeit	Wie sieht die in der Theorie dargestellte Situation zum Business Continuity Management fokussiert auf behördenerfahrene IT-Dienstleister aus und wie verhält es sich damit im Rahmen der weiteren Digitalisierung? Es wird die Relevanz sowohl für die Forschung als auch für die Praxis dargestellt. Es wird das Interesse beschrieben, dass sich mit neuen Erkenntnissen das IT-Management optimieren lässt, um die weitere Digitalisierung ausreichend resilient zu gestalten. Für die Forschung ist von Bedeutung, dass hier noch nicht untersuchte Konstellationen betrachtet werden und hierzu die Einflussfaktoren herausgearbeitet werden.
4 Zielstellung der Dissertation	In diesem Kapitel wird die Zielstellung dargestellt, wonach der aktuelle Stand des Business Continuity Managements im Kontext behördenerfahrener IT-Dienstleister erforscht werden soll. Dazu werden von der Problemstellung ausgehend die Teilziele der unterschiedlichen Kapitel der Dissertation betrachtet, um für das Hauptziel anschließend nachvollziehbare Handlungsempfehlungen für die Praxis und Wissenschaft abzuleiten.

5 Aufbau der Dissertation	Struktureller und inhaltlicher Überblick über die Dissertation.
II Theoretischer Teil	
1 Stand der Forschung	Die einschlägigen Studien und Veröffentlichungen zu den Themenfelder werden in diesem Kapitel aufgezeigt. Der Bezug zu dieser Arbeit wird erläutert und die Inhalte werden als Grundlage für die weitere Forschung genutzt. In Unterkapitel 1.2 wird die Forschungslücke aufgezeigt, die die Betrachtung der Digitalisierung im Zusammenspiel mit dem Management und der Sicherheit im behördennahen Kontext fokussiert. Anschließend werden die theoriegeleiteten Fragestellungen dargelegt.
2 Theoretische Ausführungen	Basierend auf dem Stand der Forschung werden die theoretischen Grundlagen mit ihrer Relevanz zu diesem Forschungsprojekt ausgeführt. Wie und wo ist beispielsweise ein Business Continuity Management im IT-Management nach der Theorie zu berücksichtigen? Welche Notfalloptionen und Herausforderungen bringen die neuen Digitalisierungs-technologien mit sich?
3 Konklusion theoretischer Teil	Hier wird der theoretische Teil zusammengefasst und die theoriegeleiteten Fragestellungen werden beantwortet. Es wird zu dem zur Schließung der Forschungslücke benötigten empirischen Teil dieser Arbeit übergeleitet.
III Empirischer Teil	
1 Forschungsdesign	Die geplanten Untersuchungen und Rahmenbedingungen werden mit ihren Einzelschritten beschrieben. Es erfolgt die Abwägung von verschiedenen Erhebungsmethoden, wie Fragebögen, Umfragen oder Interviews. Die ausgewählte Methode der Experteninterviews wird begründet und die dazu passenden qualitativen Auswertungsmethoden werden erläutert. Die konkrete Operationalisierung wird vorgestellt und das gesamte Vorgehen und der Ablauf der Datenerhebung und der Auswertung sind hier beschrieben.
2 Ergebnisse	Das erhobene Material in Form von transkribierten Interviews wurde qualitativ inhaltlich ausgewertet. Sowohl ein deduktiver als auch ein induktiver Ansatz kamen zur Anwendung. Mit Auszügen aus den Gesprächs-dokumentationen werden die Ergebnisse dargelegt, die jeweils zusammengefasst und graphisch aufbereitet wurden.

3 Diskussion, Interpretation, Konklusion	Unter Berücksichtigung der theoretischen Grundlagen werden die Ergebnisse aus den Interviews mit den Experten diskutiert und interpretiert. Wie sieht es in der Praxis aktuell tatsächlich aus bezüglich der Berücksichtigung von BCM-Anforderungen im Rahmen der Digitalisierung bei Behörden bzw. behördennahen IT-Dienstleistern? Die zentralen Erkenntnisse werden dargestellt und die Fragestellungen dieses Teils beantwortet, um damit zum Gestaltungsteil überzuleiten.
IV Gestaltungsteil	
1 Handlungsempfehlungen Lösungsansätze Forschung	Die interpretierten Ergebnisse der beiden ersten Teile werden in Form von drei Handlungsempfehlungen für die Forschung gestaltet. Welche Empfehlungen können für die Forschung, sowohl methodisch als auch inhaltlich, für weitere wissenschaftliche Arbeiten im Bereich Digitalisierung, IT-Management und Business Continuity Management gegeben werden?
2 Handlungsempfehlungen Lösungsansätze Praxis	Für die Praxis wurden sechs Handlungsempfehlungen erstellt, die nach Analyse der Ergebnisse für die wesentlichen Herausforderungen nachvollziehbare Lösungsansätze darstellen können.
3 Zusammenfassung und Konklusion	Hier werden die gestalterischen Fragestellungen beantwortet und die erarbeiteten Teile zusammengefasst. Es wird erläutert, wie die gestaltungsgeleitete Zielstellung erreicht werden konnte. Welche in der Theorie bereits diskutierten Aspekte der Digitalisierung unter Berücksichtigung der notwendigen Notfallpräventionen wirken sich bereits wie in der Praxis aus? Die darauf aufbauenden Empfehlungen werden hier zusammengefasst in einem Überblick dargestellt.
V Schlussteil	
1 Zusammenfassung und Fazit	In einer Gesamtsicht vom Beginn dieser Forschungsarbeit bis zur Finalisierung der Ergebnisse werden die Arbeit und die fachlichen Ergebnisse zusammengefasst. In das Fazit fließen auch die verschiedenen krisenhaften Situationen und weltpolitischen Ereignisse der Jahre 2020 (Coronapandemie), 2021 (Hochwasserkatastrophe im Ahrtal), 2022 (Ukrainekrieg) in Ihrem Kontext zur Digitalisierung und zum Business Continuity Management ein.

2 Ergebnisse und Erkenntnisse	Die zentralen Ergebnisse und Erkenntnisse für Forschung und Praxis werden abschließend dargestellt. Welche Maßnahmen müssen aus Sicht des Business Continuity Managements im Rahmen der weiteren Digitalisierung berücksichtig werden, um für Unternehmen, Staat und Gesellschaft keine neuen Gefahren zu riskieren, sondern das allgemeine Sicherheitsniveau eher zu steigern? Explizit sind hiermit die IT-Systeme staatlicher Sicherheitsbehörden und kritischer Infrastruktur fokussiert.	
3 Ausblick	Sowohl für die Praxis als auch für die Forschung wird ein Ausblick gegeben. Insbesondere für den Praxisanteil werden die begründeten Prognosen der Experten aus dem empirischen Teil abschließend dargestellt. Für die Forschung werden Hinweise für zielführende weitere Studien gegeben, die quantitativ hier nicht erfolgen konnten. Aufbauend auf den Ergebnissen dieser Arbeit können damit weitere offene Fragen für die zukünftige Digitalisierung im Zusammenwirken mit einem Business Continuity Management beantwortet werden.	
4 Verzeichnisse	Das Literaturverzeichnis, Abbildungsverzeichnis, Tabellen-verzeichnis und das Abkürzungsverzeichnis bilden das Kapitel V 4 des Schlussteils.	
Anlagen		
I. bis VIII.	I. II. III. IV. V. VI. VII. VIII.	Übersicht Experten und durchgeführter Interviews Interviewleitfaden Interviewprotokolle DSGVO-Text der Einverständniserklärung MAXQDA-Codebuch (Codierleitfaden) Analysedatei (codierte Segmente) Codierungsstatistik Tabellarische Darstellung der Expertenaussagen

Tabelle 1 – Detaildarstellung zum Aufbau der Dissertation (Quelle: eigene Darstellung)

II THEORETISCHER TEIL

1 Stand der Forschung

Im theoretischen Teil wird zunächst der Stand der Forschung dargestellt und erläutert, wie die Ermittlung dieses Forschungsstandes erfolgt ist. Auf Basis dieser Informationen und der im vorherigen Teil I dargestellten Problemstellung wird die Forschungslücke aufgezeigt. In Kapitel II 2 folgen zu den relevanten Themenfeldern, beispielsweise Business Continuity Management, IT-Sicherheit und Digitalisierung, die Definitionen der verwendeten Begriffe und es wird ein Einblick in vorhandene Forschungsergebnisse gegeben, um ein fundiertes Verständnis für das gesamte Projekt zu schaffen. Kapitel II 3 fasst den theoretischen Teil zusammen und leitet mit den Fragestellungen für die Empirie zu Teil III über.
Das folgende Kapitel II 1 beschreibt das Vorgehen bei der Literaturrecherche und stellt das erste Ergebnis auf der Grundlage von Studien und Untersuchungen zu den beiden Themenfeldern Digitalisierung und Business Continuity Management dar. Hierfür wurden Studien aus dem Bereich der Digitalisierung und mit einem Fokus auf die öffentliche Verwaltung recherchiert. Zusammen mit den Ergebnissen aus Analysen zur Unternehmenssicherheit und zum Business Continuity Management konnten damit die wesentlichen Aspekte der IT-Sicherheit und Handlungsfelder aus der Problemstellung beginnend aufbereitet werden.

1.1 Grundlagen zur Ermittlung des Forschungstandes

1.1.1 Recherchevorgehen

Die anfängliche Literaturrecherche ist von hoher Bedeutung, um festzustellen, zu welchen Bereichen aus der Problemstellung bereits erklärende Erkenntnisse vorliegen. Sie ist ebenfalls zur Identifizierung der Forschungslücke hilfreich, die dann bearbeitet werden kann (Kaiser, 2020, S. 95). Um nach geeigneter Literatur suchen zu können, sind nach Döring (2023, S. 162) Suchbegriffe zusammenzustellen. Zudem empfiehlt die Autorin, diese Begriffe auch in das Englische zu übersetzen, damit der internationale Forschungsstand erfasst werden kann. Für diese Arbeit wurden mit den Stichworten ‚Digitalisierung' und ‚Notfallmanagement' maßgebliche Themenblöcke ermittelt, die in einem engen fachlichen Zusammenhang zu den

Forschungsfragen, zur Problemstellung und zum Titel der Dissertation stehen. Als internationale Bezeichnungen wurden die Begriffe ‚Digitalization' und der schon im Deutschen gebräuchliche Begriff ‚Business Continuity Management' genutzt.

Die amerikanische Schreibweise des Wortes ‚Digitalization' mit ‚z' anstelle der britischen Schreibweise ‚Digitalisation' mit ‚s' ist für die weitere Betrachtung hier nicht relevant. Zur Vermeidung von Verwechslungen mit dem deutschen Begriff wird im weiteren Verlauf einheitlich die amerikanische Schreibweise genutzt. Die Unterscheidung der internationalen Begriffe ‚Digitalization' und ‚Digitization' besteht im Wesentlichen darin, so erläutert Gobble (2018, S. 56) nach einer Literaturrecherche, dass mit ‚Digitization' die Umwandlung von analoger in digitale Information gemeint ist. Unter ‚Digitalization' wiederum wird die neue Nutzung digitaler Technologien verstanden. Im Deutschen ist beides mit dem Begriff der ‚Digitalisierung' synonym (Schumacher et al., 2016, S. 3).

Die Ergebnisse der Recherchen und die Begriffe selbst werden in Kapitel II 2.1 ausführlich dargestellt. Zusätzlich wurde gezielt nach Studien zur Digitalisierung mit den Stichwörtern ‚Verwaltung', ‚Behörden' und ‚Government' bzw. ‚E-Government' gesucht, um den Forschungsstand mit Behördenbezug national und international in diesem Umfeld erfassen zu können. Als E-Government wird die „elektronische Abwicklung von Verwaltungs- und Demokratieprozessen" (Wirtz und Daiser, 2018, S. 981) bezeichnet.

Eine Schwierigkeit bestand darin, dass die Suche nach ‚Digitalisierung' eine große Anzahl von Treffern liefert, wogegen eine gezielte Recherche nach Notfallmanagement in deutschen Behörden unter Berücksichtigung der Digitalisierung wiederum keine Ergebnisse erbrachte. Es wurde dann, Kollmann et al. (2016, S. 29) folgend, nach verwandten Themengebieten gesucht, um die Erkenntnisse anschließend auf das eigene wissenschaftliche Projekt übertragen zu können.

Für wissenschaftliche Arbeiten empfiehlt Kornmeier (2021, S. 79-81) vor allem die Nutzung von Fachzeitschriften, weist aber darauf hin, dass es erhebliche Qualitätsunterschiede gibt. Um vorrangig wissenschaftliche Veröffentlichungen möglichst hoher Qualität zu berücksichtigen, wurde das Zeitschriftenrating des Verbandes der Hochschullehrer für Betriebswirtschaft e. V. (VHB) berücksichtigt. Die Zeitschriften werden dort von A+ über A, B und C bis D absteigend nach ihrer wissenschaftlichen Bedeutung bewertet.

Zusätzlich waren Veröffentlichungen des Bundesamtes für Informationssicherheit (BSI), der Vereinten Nationen (UN) und des Bitkom Branchenverbandes e. V. weitere relevante Eingangskanäle mit den dort dokumentierten Studienergebnissen. Wenn diese nicht in

wissenschaftlichen Zeitschriften veröffentlicht waren, erfolgte hierzu eine Prüfung der Angaben zu Forschungsmethoden, Auftraggebern und Veröffentlichungsmodalitäten, um keine einseitig beeinflussten Ergebnisse zu berücksichtigen.

Die Recherche mittels Google Scholar ermöglicht zusätzlich eine quantitative Abschätzung über die vorhandene wissenschaftliche Literatur vorzunehmen. Dabei wurde deutlich, dass insbesondere für die Digitalisierung auch aktuell zahlreiche Veröffentlichungen erscheinen. Google Scholar verweist mit Stand Mai 2023 zum deutschen Suchbegriff ‚Digitalisierung' auf ca. 69 500 Ergebnisse, die Veröffentlichungen ab dem Jahr 2020 berücksichtigen. Für die Kombination der Themenbereiche Notfallmanagement und Digitalisierung und zu wissenschaftlich fundierten empirischen Untersuchungen im Bereich des Business Continuity Managements gibt es aktuell vergleichsweise deutlich weniger Fundstellen. Eine Recherche unter den genannten Rahmenbedingungen zeigt zum Begriff ‚Notfallmanagement' lediglich 1010 Ergebnisse und für ‚Business Continuity Management' 4440 Ergebnisse, die jedoch den Digitalisierungskontext nicht im Fokus mitbetrachten. Für den singulären Begriff ‚Notfallmanagement' wurden zudem zahlreiche Veröffentlichungen aus dem medizinischen Bereich gefunden, die es herauszufiltern galt. Bei Nutzung beider Suchbegriffe ‚Digitalisierung' und ‚Notfallmanagement' in einer Abfrage wurden für das Jahr 2022 insgesamt 92 Treffer angezeigt und für die Kombination mit dem Schlüsselbegriff ‚Business Continuity Management' statt ‚Notfallmanagement' ergaben sich 71 Fundstellen.

Erstmalig wurde diese Analyse in Vorbereitung der empirischen Datenerhebung bereits im Mai 2021 durchgeführt. Im Mai 2023 erfolgte eine erneute Erhebung, um einen möglichst aktuellen Sachstand zu dokumentieren. Eine Übersicht über die quantitativen Ergebnisse der Google-Scholar-Suche am 29.05.2023 ist in der nachfolgenden Tabelle dargestellt:

Google Scholar Anzahl ungefährer Ergebnisse (Stand: 29.05.2023)			
Suchbegriff	ungefähre Anzahl Ergebnisse für den Zeitraum:		
	2020–2023	2021	2022
Digitalisierung	69.500	25.300	24.600
Notfallmanagement	1.010	285	286
Digitalisierung Notfallmanagement	283	76	92
Digitalisierung IT-Notfallmanagement	22	3	8
‚Business Continuity Management'	4.440	1.300	1.320
Digitalization	276.000	98.100	64.900
Digitalisierung ‚Business Continuity Management'	172	42	71
Digitalization ‚Business Continuity Management'	822	297	271

Tabelle 2 – Quantitative Übersicht der Google-Scholar-Ergebnisse (Quelle: eigene Darstellung)

Aus der Anzahl der Treffer ist erkennbar, dass insbesondere für den Bereich Digitalisierung aktuell zahlreiche wissenschaftliche Veröffentlichungen erscheinen und auch der Bereich Business Continuity Management bzw. IT-Notfallmanagement bereits untersucht wird. Allerdings sind wenige Veröffentlichungen zu finden, die beide Thematiken beinhalten. Keine Ergebnisse erhält man bei einer Suche nach Studien, die zusätzlich mit Blick auf deutsche Behörden das Business Continuity Management im Zeitalter der Digitalisierung analysieren. Nach dieser quantitativen Betrachtung erfolgt die qualitative Herleitung der Forschungslücke später in Kapitel II 1.2.

Neben der Suche mit Suchbegriffen wurden auch regelmäßig erscheinende Veröffentlichungen gesichtet, um relevante Studien zu erkennen, die diese expliziten Begriffe nicht im Titel oder Text enthalten. Die nachfolgenden Zeitschriften wurden hierzu bei der Recherche regelmäßig geprüft. Die aktuelle Bewertung nach dem VHB mit Stand 2023 sowie die International Standard Serial Number (ISSN) sind in Klammern mit angegeben: European Journal of Information Systems (A, ISSN 0960-085X), Information Systems Journal (A, ISSN 1350-1917), Information System Research (A+, ISSN 1047-7047), Journal of Information Technology (A, ISSN 0268-3962) und The Journal of Strategic Information Systems (A,

ISSN 0963-8687). Im Verlauf des Studiums wurden diese Quellen kontinuierlich gesichtet, erweitert und wiederholt hinsichtlich neuer Erkenntnisse ausgewertet. Dadurch konnten aktuelle Ergebnisse aus anderen Forschungsvorhaben auch im Verlauf der empirischen Untersuchung noch in die Analyse einfließen. Zusammenfassend ergibt sich zum Recherchevorgehen, dass zitierfähige Beiträge aus Quellen der nachfolgend dargestellten Ebenen recherchiert wurden.

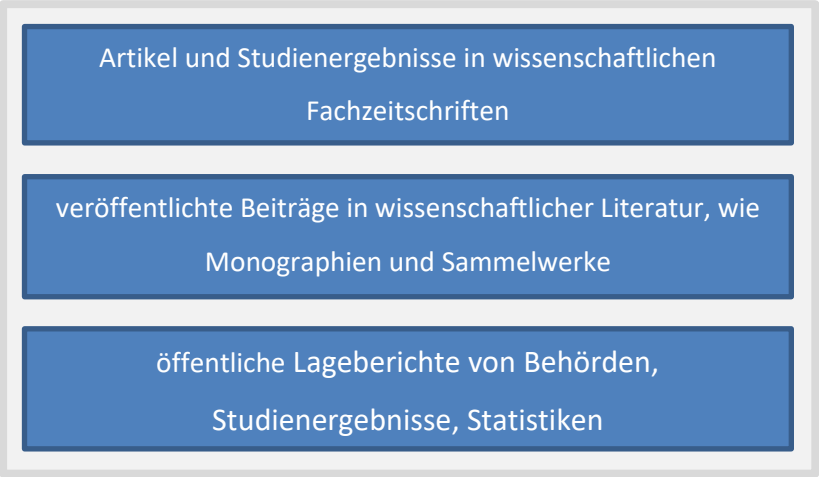


Abbildung 4 – Recherchevorgehen, Ebenen der Quellen (Quelle: eigene Darstellung)

Die Ebenen stellen keine Reihenfolge dar, sondern symbolisieren, dass neben der einschlägigen wissenschaftlichen Literatur auch Publikationen vom BSI, vom Bitkom Verband, von der EU und der UN im Rahmen der Analyse herangezogen wurden. Damit wurden möglichst aktuelle Bezüge verwendet, die einen Einblick in die IT im öffentlichen Bereich geben und in dieser Form nicht in klassischer wissenschaftlicher Literatur erschienen sind.
Zur Formulierung von Empfehlungen für behördennahe IT-Dienstleister in Deutschland wurden Studienergebnisse recherchiert, die national orientiert die Digitalisierung und das Business Continuity Management fokussiert haben. Allerdings ist die Gesamtthematik auch international relevant, wie aus Tabelle 2 mit den quantitativen Suchergebnissen zu ersehen ist. Somit wurde auch die internationale Forschung berücksichtig, wie im nächsten Kapitel dargelegt, um diese Erkenntnisse für Deutschlands IT nutzbar zu machen.

1.1.2 Einbezug Internationalität/internationale Forschung

Die Digitalisierung vollzieht sich global und über alle nationalen Grenzen hinweg. Internationale Konzerne wie „Amazon, Google, IBM und Microsoft“ zählt Faber (2019, S. 17) als Marktführer im Bereich der Cloud-Technologien auf, wobei er diesen Teil der Digitalisierung sowohl gegenwärtig als auch zukünftig als herausgehobenen Treiber einstuft

(Faber, 2019, S. 20). Obwohl vorrangig Auswirkungen auf nationale Behörden beleuchtet werden, stehen Technologien der Digitalisierung zur Diskussion, die weltweit Anwendung finden. Eine Transfermöglichkeit der Ergebnisse in das internationale Umfeld ist hiermit gegeben. Forschungen aus dem internationalen Bereich, wie die später noch genannte BCM-Studie von Sawalha und die Analysen von Kappelmann et al., sind in die Darstellung des Forschungsstandes eingeflossen. Ebenso wurde ein Bericht mit Empfehlungen der Vereinten Nationen berücksichtigt, der nicht national auf Deutschland begrenzt ist. Der bereits in der Ausgangslage genannte DESI-Index betrachtet neben Deutschland auch die weiteren Länder Europas. Ebenfalls für das später noch näher erläuterte europäische GAIA-X-Projekt wurden Veröffentlichungen aus dem Bereich der internationalen Forschung konsultiert.

Aus Fachzeitschriften wurden Beiträge unter anderem von Kotlarsky et al. (Neuseeland), Sawalha (Jordanien), Newell und Marabelli (Großbritannien), Wilemius et al. (Schweden), Zhang et al. (China) und Baldwin (USA) sowie von weiteren internationalen Autoren berücksichtigt. Damit wurde sichergestellt, dass eine möglichst global gültige und über Deutschland hinaus authentische Sachdarstellung zu den Problemfeldern herausgearbeitet werden kann.

1.1.3 Beschreibung des Standes der Forschung

Zur Ableitung der Forschungslücke wurden Studien und Analysen ausgewertet, die sich in die nachfolgenden zwei Themengebiete gruppieren lassen: wissenschaftliche Untersuchungen zur Digitalisierung und zur Thematik Unternehmenssicherheit mit Notfallmanagement.

Die für die Forschungsfragen relevanten Informationen werden herausgestellt und bilden damit eine erste dokumentierte Grundlage, die zum geschilderten Phänomen in der Problemstellung aus Kapitel I 2 beitragen. Es werden nachfolgend mehrere Veröffentlichungen zitiert, die bereits konkret die Thematik betreffen und zum Teil durch Studien oder wissenschaftliche Umfragen die Ausgangslage und die Problemstellung in der Theorie erklärbar machen können. Für die Erstellung des Forschungsdesigns und die Erarbeitung von Forschungsfragen, insbesondere für den empirischen Teil, konnte der Forschungsstand bis März 2022 berücksichtigt werden. Im Rahmen der Auswertung und der Analyse der empirisch erhobenen Daten wurden weitere und neuere Quellen berücksichtig, um ein möglichst aktuelles Ergebnis zu erarbeiten.

Die nächsten beiden Kapitel stellen für die Bereiche der Digitalisierung in der öffentlichen Verwaltung und den Anteil der Unternehmenssicherheit aus Sicht der IT den auf die

Aufgabenstellung fokussierten Stand der Forschung dar, bevor über die Darstellung der Forschungslücke in Kapitel II 2 alle weiteren Themenfelder ausführlicher betrachtet werden.

1.1.4 Studien zur Digitalisierung mit Fokus auf die öffentliche Verwaltung

Für den Sachstand zur Digitalisierung in Behörden wurde die Untersuchung „Digitalisierung der Bürgerämter in Deutschland“ aus dem Jahr 2019 von Schwab et al. berücksichtigt. Die Autoren schreiben zusammenfassend, dass es im Bereich der digitalen Informationsbereitstellung zwar deutliche Fortschritte gibt, in den Bereichen Kommunikation und Transaktionen von Verwaltungsvorgängen dennoch Lücken und Defizite bestehen (S. 66). Es existiere ein Modernisierungsrückstand und der Erhalt des aktuellen Leistungsniveaus der öffentlichen Verwaltung könne massive Probleme bereiten, wenn die Optimierung der Digitalisierung hier nicht gelinge (Weiß, 2019, S. 83).

Im Vorwort der internationalen E-Government-Umfrage der UN empfiehlt Zhenmin (2020, S. 7) ausdrücklich die Zusammenarbeit zwischen Regierungen und dem privaten Sektor im Zusammenhang mit der digitalen Transformation. In dem Bericht werden mit der zunehmenden Digitalisierung im Bereich des E-Governments auch unzureichende Kapazitäten mit Blick auf die Sicherheit oder den Datenschutz genannt (UN, 2020, S. 146). Beide Aspekte bestärken die Notwendigkeit der Forschung in diesem Bereich. Neben der Fokussierung auf die öffentliche Verwaltung ist hieraus abgeleitet zudem die Wirtschaft direkt zu betrachten. Windoffer (2018, S. 370) nennt neben Partnerschaften im öffentlichen Bereich explizit auch Partnerschaften mit der Privatwirtschaft und nennt Cloud-Anbieter beispielhaft für ein Outsourcing an externe Dienstleister. Die Beweggründe einer großen staatlichen Organisation für eine enge Partnerschaft mit der Industrie im Bereich der IT erläuterte Theis bereits 2012 mit Bezug auf die Modernisierung der Bundeswehr. Der Autor nennt verschiedene Gründe, beispielsweise eine Entlastung des eigenen Personals und die jährliche Festlegung der limitierten Finanzmittel im öffentlichen Haushalt. Das bedingt die zukünftige Nutzung von IT-Standardlösungen in der öffentlichen Verwaltung und eine enge Kooperation mit der Wirtschaft (S. 186).

Aus diesem Sachverhalt heraus wurde für den Überblick zur Digitalisierung auch die Metastudie vom Institut der deutschen Wirtschaft Köln berücksichtigt, die den Mittelstand betrachtet. Insbesondere die Ergebnisse und Aspekte der kritischen Auseinandersetzung mit der IT-Sicherheit im Rahmen der digitalen Transformation wurden analysiert. Die Autoren fassen in den Handlungsempfehlungen zusammen, dass die IT-Sicherheit sowie die

Datensicherheit und der Datenschutz die Plätze 1 bzw. 2 beim Unterstützungsbedarf von Unternehmen im Digitalisierungsprozess einnehmen (Demary et al., 2016, S. 53). Für die mittelständischen behördennahen IT-Dienstleister zeigt sich somit bereits aus der Theorie, dass die Herausforderungen eines sicheren IT-Betriebes aktuell von hoher Bedeutung sind. Da auch mittelständische Unternehmen im empirischen Teil berücksichtigt werden, ist das ein Aspekt, der im weiteren Verlauf diskutiert und untersucht wird, um herauszufinden, wie sich diese Situation in der Praxis darstellt.

Für einen weiteren Überblick zum aktuellen Stand der Digitalisierung in Unternehmen der Industriebranchen dient eine Studie aus der Zeitschrift für Arbeitswissenschaft, wobei vorrangig der erste Anteil der Forschung hier von Relevanz ist. Härtwig und Sapronova (2020, S. 62) widmen sich dem aktuellen Digitalisierungsstand in Deutschland in verschiedenen Branchen der Industrie. Untersucht wurde die Nutzung von ausgewählten Technologien durch die Mitarbeiter der Unternehmen. Die Autoren kommen zu dem Ergebnis, dass es sich um eine beginnende Digitalisierung handelt, die hauptsächlich durch die Nutzung von Informations- und Kommunikationssystemen (IKT-Systeme) gekennzeichnet ist (2020, S. 58). Die für eine Untersuchung im Bereich Business Continuity Management relevanten Applikationen der Unternehmenssoftware, die sogenannten Enterprise-Ressource-Planning-Systeme (ERP-Systeme), werden von deutlich weniger Mitarbeitern genutzt (Härtwig & Sapronova 2020, S. 65).

Hoberg et al. haben die digitale Transformation konkret mit Umfragen und anhand von Fallbeispielen in Branchen untersucht. Ein Ergebnis war, dass nur ein knappes Drittel der Unternehmen eine klare Transformationsstrategie besitzt (2018, S. 71). Mit Blick auf die vorliegende Forschungsarbeit ist es von besonderer Bedeutung, wenn ein Business Continuity Management auf eine noch nicht geplante oder bekannte Veränderung im Unternehmen reagieren soll, da hierfür zukunftsorientierte Abschätzungen vorgenommen werden müssen.

Zusammenfassend zeigen die Studien, dass die öffentliche Verwaltung in Deutschland aktuell noch einen erheblichen Entwicklungsbedarf bei der Digitalisierung hat. Vad spricht in einem Interview über die Gefahren der Digitalisierung und nennt einen politischen Kontrollverlust, der entsteht, wenn die Datensicherheit und die geschützte Kommunikation nicht mehr bestehen. Im gleichen Interview bewertet er, dass Deutschland und Europa die digitale Revolution ‚*verschlafen*' haben und sieht die Gefahr, dass Europa lediglich zu einem Anhängsel der technologischen Giganten USA und China wird. Hier müsse die Politik Anreize schaffen

und es bestehe die Notwendigkeit von sowohl öffentlichen als auch privatwirtschaftlichen Investitionen (Pickl, 2019, S. 258-259).

Ein wiederkehrender Begriff im Rahmen der Digitalisierung ist die digitale Souveränität. Lambach und Oppermann stellen hierzu sieben unterschiedliche Deutungen vor. In diesem Zusammenhang wird auch von einer Resilienz Deutschlands im Cyberspace als einem wesentlichen Bestandteil der digitalen Souveränität gesprochen (2022, S. 8). Dadurch wird die Relevanz der digitalen Souveränität für das Business Continuity Management deutlich und ist in der weiteren Ausarbeitung und Analyse sowie bei der Erstellung von Empfehlungen zu berücksichtigen.

Bei den öffentlichen Verwaltungen in Deutschland ist auch der strukturelle Aufbau zu beachten. Die Verantwortungen in Deutschland liegen nicht nur föderal bei den Gemeinden und Bundesländern, sondern es sind hier auch die Ressorts des Bundes von Relevanz. In der nachfolgenden Abbildung sind die Aufgaben der sogenannten „Kernverwaltung des Bundes“ (Schmidt & van der Giet, 2018, S. 139) dargestellt:

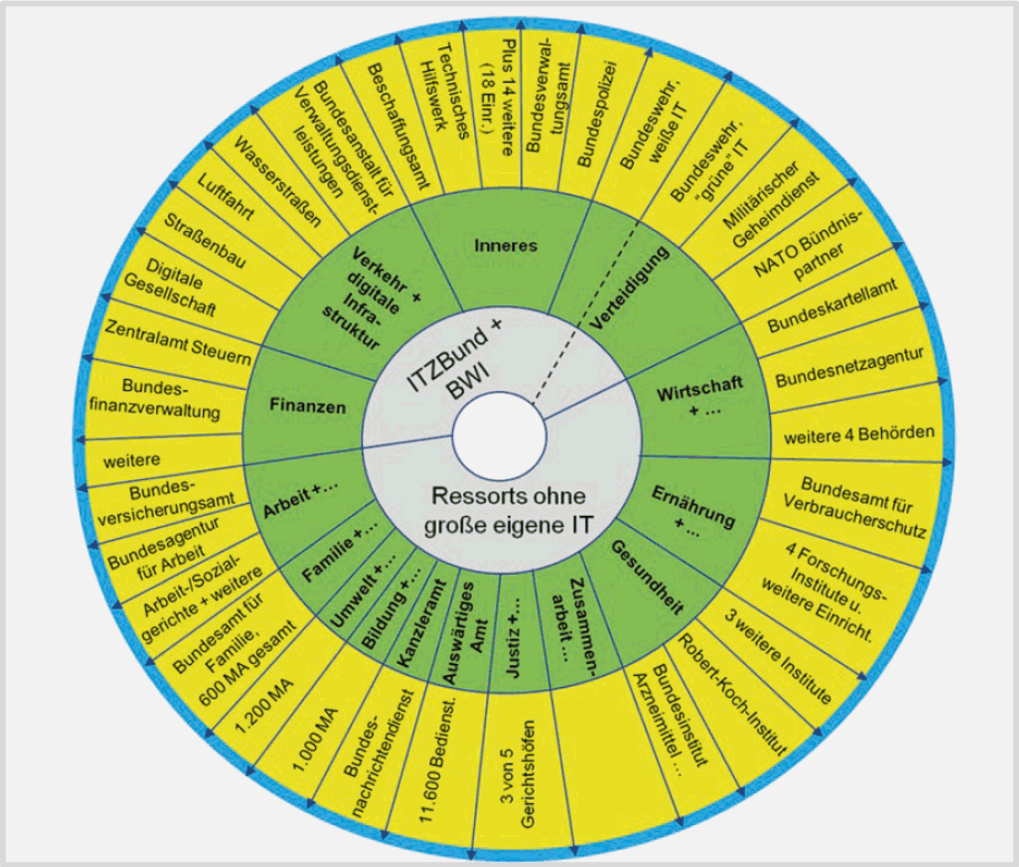


Abbildung 5 – Übersicht der Aufgaben der Kernverwaltung des Bundes (Quelle: Schmidt & van der Giet, 2018, S. 139)

Im äußeren gelben Kreis sind die verschiedenen Kernaufgaben genannt, für die eine entsprechende IT-Unterstützung notwendig ist. Dort sind fachliche Aufgaben, z. B.

Straßenbau, organisatorische Elemente, wie das Robert-Koch-Institut, aber auch Mitarbeiteranzahlen (MA) angeführt. Die Zuordnung zum jeweiligen Ministerium ist im grünen Kreis dargestellt. Die Ministerien sind alle einem Bereich im mittleren Kreis zugeordnet. Dieser graue Bereich ist für die Digitalisierung insofern relevant, als hier ersichtlich ist, ob für die jeweils eigene IT dieser Behörde bereits eine Zuständigkeit beim Informationstechnikzentrum Bund (ITZBUND) zuzüglich der BWI GmbH gesehen wird. Von den 15 Ressorts sind dort noch elf dem Bereich „ohne große eigene IT“ zugeordnet und damit insbesondere von externen IT-Dienstleistern abhängig, wenn sie IT-Services nutzen oder anbieten.

Das E-Government wird auch regelmäßig in der bereits genannten DESI-Studie der EU betrachtet. Es wird zwar nicht direkt über den Digitalisierungsstand in Verwaltungen berichtet, jedoch lassen die nachfolgend genannten Untersuchungsteile Rückschlüsse auf den Digitalisierungsstand dort zu. Für Abbildung 6 wurden folgende Indikatoren erhoben: prozentuale E-Government-Nutzer bezogen auf alle Internetnutzer des Landes, Bewertung der Verfügbarkeit von elektronisch vorbefüllten Formularen, digitale Bürgerservices und digitale Services für Unternehmen, die von den Behörden bereitgestellt werden (EU, 2022a, S. 66). Der fünfte Indikator bezieht sich auf ‚Open Data‘ und darauf, wie diesbezüglich der Entwicklungsstand und die Förderung durch die Politik aktuell einzustufen sind (EU, 2022a, S. 69-70).

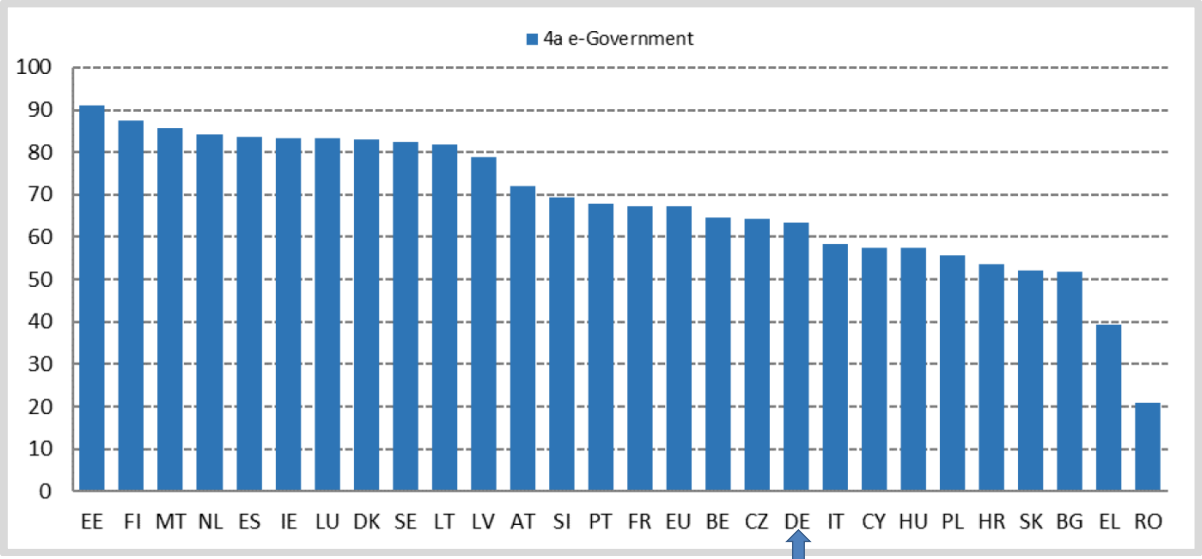


Abbildung 6 – Digital Economy and Society Index (DESI) 2022, Digital public services (Quelle: EU, 2022a, S. 66)

Danach liegt Deutschland im Bereich E-Government mit Platz 19 von 27 noch unterhalb des EU-Durchschnitts, was den in diesem Kapitel bereits genannten Nachholbedarf und die noch vorhandenen Defizite im Bereich der Digitalisierung bestätigt. In diesem Zusammenhang

spricht Schmid (2019, S. 8) von vielen und noch ungeklärten konzeptionellen Fragestellungen und einem fehlenden Grundverständnis. Hier ist ein entsprechendes Fundament erforderlich, um Fehlentwicklungen verhindern zu können.

Pérez-Morote et al. (2020, S. 13) haben herausgefunden, dass staatliche Investitionen in ein E-Government zwar die Verbreitung der Nutzung digitaler Services durch die Bevölkerung fördern, dennoch sind sie aber ausdrücklich nur dann effizient, wenn alle Bürger, auch weniger gebildete oder weniger wohlhabende, von diesen IT-Services profitieren. Hiermit soll verdeutlicht werden, dass Digitalisierungsprojekte nicht per se erfolgreich sind, sondern dafür müssen diverse Anforderungen berücksichtigt werden.

Vom Bundesministerium für Wirtschaft und Energie (BMWi) wurde ein Gutachten des Wissenschaftlichen Beirates mit dem Titel „Digitalisierung in Deutschland – Lehren aus der Corona-Krise“ veröffentlicht, in dem berichtet wird, dass sich die „Strukturen und Prozesse der öffentlichen Verwaltung […] als wesentliche Hemmnisse für eine effektive Digitalisierung erwiesen“ haben (BMWi, 2021, S. 20). Entgegen modernen Abläufen wird auf eine noch gängige Praxis verwiesen, die auf „Aktenlaufplänen, sequenzieller Bearbeitung und strikt hierarchisch geordneten Arbeitsverhältnissen“ (BMWi, 2021, S. 22) basiert. In den Empfehlungen nennt der Wissenschaftliche Beirat unter anderem ausdrücklich die Integration neuartiger Managementansätze, um neue Technologien schneller einsetzen zu können (BMWi, 2021, S. 22).

Damit dies insgesamt bei der Digitalisierung in Deutschland aus Sicht eines Business Continuity Managements erfolgen kann, wurde diese Empfehlung hier aufgenommen. Im nachfolgenden Kapitel wird ein weiterer dazu notwendig Teil betrachtet. Dieser befasst sich mit der Sicherheit eines Unternehmens bzw. einer Organisation aus Sicht der IT.

1.1.5 Unternehmenssicherheit aus Sicht der IT

Der zweite einleitende Schwerpunkt dieser Recherche betrifft das Themenfeld Business Continuity Management bzw. IT-Notfallmanagement. Dazu werden die wissenschaftlichen Erkenntnisse im Bereich der Unternehmenssicherheit mit Bezug zur IT ermittelt. Vorab kann bereits gesagt werden, dass IT-Risiken von zahlreichen Unternehmen erheblich unterschätzt und im Ernstfall nicht vollständig beherrscht werden (Urbach & Ahlemann, 2019, S. 86).

Der Branchenverband Bitkom hat in einem Studienbericht 2020 veröffentlicht, dass nach einer Befragung von mehr als 1000 Unternehmen mit Stand 2019 lediglich 48 % über ein Notfallmanagement verfügten, um etwa bei Cyberattacken Ad-hoc-Maßnahmen ergreifen zu

können (Bitkom, 2020, S. 38). In der aktualisierten Veröffentlichung wurde für 2021 hier ein Anstieg auf 51 % dokumentiert (Bitkom, 2021, S. 2), womit aber lediglich eine leichte Verbesserung zu verzeichnen ist.

Ein vergleichbares Ergebnis wurde vom BSI 2019 veröffentlicht, wonach im Jahr 2018 bei 43 % der befragten Unternehmen ein Notfallmanagement etabliert war, um bei einem Cyber-Vorfall schnell handlungsfähig zu sein. Hierzu hatten 1039 Institutionen an einer öffentlichen Onlineumfrage der Allianz für Cyber-Sicherheit teilgenommen (BSI, 2019, S. 49-50). Zur Einordnung dieser Ergebnisse ist von Bedeutung, dass Cyberattacken neben anderen Risiken, wie physischen Angriffen oder Naturkatastrophen, nur ein Auslöser von IT-Notfällen größten Ausmaßes sein können. Im Jahresbericht 2022 für die IT-Sicherheit in Deutschland gibt das BSI an, dass sich die zuvor bereits angespannte Lage weiter zuspitze und aktuell die Bedrohung im Cyberraum so hoch wie noch nie sei (BSI, 2022, S. 11). Aus den Meldungszahlen von Juni 2021 bis Mai 2022 ist bei den KRITIS-Sektoren ersichtlich, dass besonders im Bereich der Managementsysteme für Informationssicherheit (ISMS) ein Anstieg der Mängelmeldungen dokumentiert ist (BSI, 2022, S. 69-70). Das zeigt, dass der Handlungsbedarf in den letzten Jahren drastisch gestiegen ist und auch für die Sicherheit in Deutschland kritische und relevante Bereiche betroffen sind.

Neben diesen auf Deutschland bezogenen Veröffentlichungen unter anderem des BSI wurden auch weitere internationale wissenschaftliche Studien recherchiert, die das Business Continuity Management untersucht haben. So hat Sawalha im Jahr 2020 eine für die Thematik treffende Untersuchung zur Etablierung des BCM in Jordanien veröffentlicht. Demnach besteht bei zahlreichen Unternehmen Unsicherheit, wie ein Business Continuity Management implementiert werden soll (S. 83). Zudem ist bei 23 % der Unternehmen noch kein Business Continuity Management etabliert, weder durch interne Mitarbeiter noch durch externe Dienstleister (S. 86). In der Diskussion und im Vergleich mit anderen Ländern erläutert er für die regionalen Ergebnisse, dass sich jordanische Unternehmen der Bedeutung des Business Continuity Managements relativ bewusst sind, indem 77 % der untersuchten Unternehmen ein Business Continuity Management praktizieren. Es gibt aber auch große Unterschiede in anderen Ländern (S. 88-89). Einzelaussagen dieser Studie, wie die Situation, dass eine ISO-Zertifizierung der Initiator für die Einführung eines BCM-Systems ist (S. 83), wurden hier für die empirische Untersuchung in Deutschland transferiert und werden später analysiert.

In einer weiteren Untersuchung wurden Manager interviewt, die für die IT-Sicherheit und das Business Continuity Management verantwortlich sind. Aufschlussreich war, dass diese

Personen sich nach Übertragung der Verantwortlichkeiten auf andere Bereiche nicht mehr um die IT-Sicherheit gekümmert haben. Für diese Situation und im Bereich der Anwendung von Standards für das Business Continuity Management und die IT-Sicherheit sieht die Autorin noch Forschungsbedarf (Järveläinen, 2012, S. 343).

Roselieb veröffentlichte 2022 mehrere Beiträge mit Fallbeispielen zum Business Continuity Management. Der Autor sieht eine steigende Bedeutung mit den Erfahrungen aus der Coronapandemie und mit dem kommenden BSI-Standard 200-4 (S. 10-11). Diese nicht explizit auf die Digitalisierung oder die IT-Services bezogenen Fallbeispiele und Krisenmanagementerfahrungen aus der Praxis zeigen an vielen Stellen die Relevanz der IT. So berichtet Gleißner bei der Betrachtung der „Robustheit und Resilienz von Staaten und Unternehmen“, dass die Digitalisierung durch die Coronapandemie zugenommen hat und sich eine steigende Abhängigkeit von der IT allgemein und konkret vom Internet abzeichnet (2022, S. 253). Hiermit wird erneut die Aktualität der gesamten Thematik bestätigt.

Kappelmann et al. haben 2017 bei IT-Managern von 276 internationalen Unternehmen eine Umfrage zu unterschiedlichen IT-Themen durchgeführt. Auf einer Top-Ten-Liste zu den relevantesten Themen aus Sicht der Unternehmen belegte die digitale Transformation Platz 2 und die IT-Sicherheit Platz 3. Die Kategorie Business Continuity erreichte mit 14,1 % den letzten Platz. Gleichzeitig wurde die IT-Sicherheit für IT-Manager als die besorgniserregendste Thematik genannt (Kappelmann et al., 2018, S. 3). Die Autoren diskutieren dieses Teilgebiet unter dem Begriff ‚Cybersecurity Practices‘ auch vor dem Hintergrund kritisch, dass nur 60 % der Unternehmen einen ‚Chief Information Security Officer‘ (CISO) haben (2018, S. 12).

Auch der Bereich von Sicherheitsrisiken beim Vergleich von Cloud-Services gegenüber selbst betriebener IT, sogenannte ‚On-Premises‘-Lösungen, wurden bereits untersucht. Zhang et al. beschreiben einleitend, dass Cloud-Services auch die Verwaltungen in einem immer schnelleren Tempo verändern werden (2020, S. 848). Als erste Implikation wurde herausgefunden, dass für Kunden, die besonders empfindlich auf Datenverluste durch Cyberattacken reagieren würden, ein Wechsel in die Cloud anstelle von On-Premises-Lösungen die bessere Wahl sein kann (2020, S. 862). Auch Bartsch und Frey beschreiben zum Cloud-Computing, dass dort grundsätzlich eine bessere Sicherheitsarchitektur vorhanden ist (2017, S. 108). Hier muss aus der Perspektive eines Business Continuity Managements kritisch hinterfragt werden, ob ein solcher Wechsel in die Cloud ggf. neue Risiken birgt. Hamidian und Kraijp sprechen hier sogar von einem Sicherheits-Paradoxon (2013, S. 18) bei der Nutzung von vertraulichen Daten in Cloud-Umgebungen.

Zusammenfassend zeigen diese beiden Kapitel, dass es einerseits bei der Digitalisierung in Deutschland und in deutschen Behörden noch Nachholbedarf gibt und dass andererseits der Bereich IT-Sicherheit und insbesondere das Business Continuity Management noch nicht überall ausreichend berücksichtigt werden. Es kann darüber hinaus neue Gefahren geben. Wissenschaftliche Veröffentlichungen, die genau diesen Fokus aufweisen und dabei besonders die deutschen Behörden in den Blick nehmen, konnten nicht recherchiert werden. Damit wird die nachfolgende Forschungslücke aufgezeigt.

1.2 Forschungslücke

Wenn bestimmte Dimensionen eines Gegenstandes noch nicht untersucht wurden, kann man von einer Forschungslücke sprechen und diese zum Anlass nehmen, eine eigene Studie durchzuführen (Döring, 2023, S. 149). Das Schließen dieser Lücke begründet den Forschungsbedarf. Sawalha (2020, S. 83) hat herausgefunden, dass bei zahlreichen Unternehmen noch eine Unsicherheit vorhanden ist, wie ein Business Continuity Management eingeführt werden kann. Als einen noch wenig erforschten Aspekt im Rahmen der Digitalisierung sehen Wimelius et al. (2020, S. 215) die Situation der regelmäßig zu erneuernden IT-Systeme.
Die Anfälligkeit für Störungen steigt mit der Komplexität von Systemen und von daher müssen IT-Systeme durch Resilienz entsprechend widerstandsfähig gemacht werden, so beschreiben Hippmann et al. (2018, S. 15) Forschungsziele im Rahmen der Digitalisierung. Einen Appell an die Wissenschaft richten Hiermaier und Scharte (2018, S. 309) mit dem Hinweis auf eine Vielzahl offener Fragen im Bereich der „Resilienz komplexer technischer Systeme“. Aus dieser fachlichen Sicht, dem genannten Forschungsziel und vor allem aus der Problemstellung ergibt sich das nachfolgend dargelegte Spannungsfeld mit der zu schließenden Forschungslücke.
Die erläuterten Studien und Analysen haben gezeigt, dass zu den Themengebieten Digitalisierung und Unternehmenssicherheit aus Sicht der IT wissenschaftliche Erkenntnisse existieren. Zur Herleitung der Lücke wird die Unternehmenssicherheit aus Sicht der IT hier in die Bereiche Digitalisierung, Management und Sicherheit aufgeteilt, womit drei Themenfelder existieren, die gemeinsam betrachtet werden sollen. Jeweils in der Kombination von zwei dieser drei Themen (Digitalisierung, Management, Sicherheit) liegen Forschungsergebnisse vor. Für Sicherheit und Management sind es Untersuchungen im Bereich des Notfallmanagements. Allerdings wirkt sich hierbei zunehmend die Digitalisierung wesentlich auf die Sicherheit aus und diese ist von den Entscheidungen des Managements abhängig. Auch

die Digitalisierung mit ihren Auswirkungen auf das Management ist kein unerforschtes Gebiet. Diese Beziehungen werden aktiv analysiert, wenn Veröffentlichungen aus dem Bereich IT-Management die neuen Technologien betrachten. Bei diesen Veröffentlichungen mangelt es aber an tiefgreifender Forschung, falls die neuen Möglichkeiten der Digitalisierung durch einen IT-Notfall unerwartet nicht mehr zur Verfügung stehen. Dann ist auch direkt die allgemeine Sicherheit durch Defizite in der IT-Sicherheit gefährdet.

Als dritte Betrachtung ist die Digitalisierung in Kombination mit der Sicherheit zu nennen. In der Literatur sind hierzu zwar kritische Diskussionen zur IT-Sicherheit in Bezug auf die unterschiedlichen Aspekte der Digitalisierung vorhanden, jedoch fehlen dort Untersuchungen zu geeigneten Managementpraktiken, um genau diese Herausforderungen effizient bewältigen zu können.

Daraus resultierend bildet das IT-Management im Spannungsfeld von Digitalisierung und Sicherheit den wesentlichen Teil der Forschungslücke. Zur abschließenden Definition ist die Untersuchungsgruppe der behördenerfahrenen IT-Dienstleister in Deutschland als weitere Dimension anzuführen. Im digitalen Zeitalter unterstützen ihre Services die Arbeitsfähigkeit der öffentlichen Verwaltung zunehmend oder ermöglichen diese teilweise erst. Die dadurch steigende Abhängigkeit der Behörden von diesen Dienstleistern ist somit ein weiterer Teil der Forschungslücke. Vorhandene Forschungen berücksichtigen Unternehmen unterschiedlicher Branchen oder betrachten die Entwicklungen im öffentlichen Sektor, es fehlt aber an einer fokussierten Erhebung bei genau den hier tätigen IT-Dienstleistern in der Schnittstelle, die im Weiteren als behördennahe IT-Dienstleister bezeichnet werden.

Wie in Unterkapitel I 4.2 abgegrenzt, konzentriert sich dieses Forschungsvorhaben auf die von der öffentlichen Verwaltung genutzte IT und die soeben definierten behördennahen IT-Dienstleister. Hier existieren keine bekannten wissenschaftlichen Forschungsergebnisse. Unter Berücksichtigung des in Kapitel I 1 zitierten Kontrollverlustes und der daraus direkt ableitbaren weitreichenden Auswirkungen auf die nationale öffentliche Sicherheit offenbart sich die Notwendigkeit, diese Forschungslücke zu schließen. Dazu muss die Situation an der nachfolgend dargestellten Position fokussiert untersucht werden:

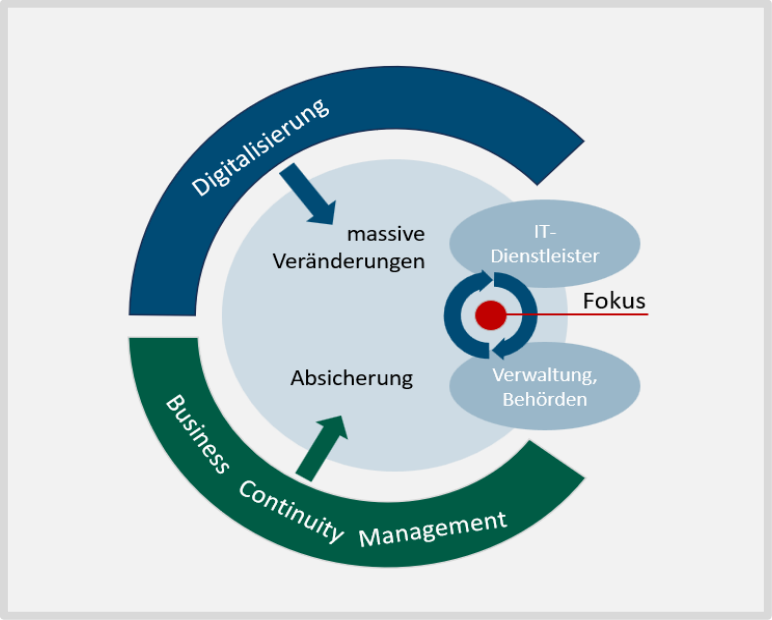


Abbildung 7 – Forschungslücke, Fokus der Untersuchungen (Quelle: eigene Darstellung)

Die Abbildung verdeutlicht, dass sich die Digitalisierung mit gravierenden Veränderungen auswirken wird. Diese sind durch die Methoden eines Business Continuity Managements abzusichern, auf die ebenfalls massive Veränderungen durch den Anpassungsbedarf zukommen werden. Von beiden Aspekten betroffen sind dabei sowohl die Verwaltungen und Behörden als auch die IT-Dienstleister und die IT-Produktentwickler, die maßgeblich die Digitalisierung umsetzen. Namensgebend für diese Arbeit kann damit die Forschungslücke derart geschlossen werden, dass mit der Analyse des Business Continuity Managements im Zeitalter der Digitalisierung Handlungsempfehlungen für behördennahe IT-Dienstleister erarbeitet werden. Zur weiteren Vorbereitung dafür sind in den nachfolgenden Kapiteln die theoretischen Fragen und Grundlagen ausgearbeitet.

1.3 Theoriegeleitete Fragestellungen

Aus den bisherigen Kapiteln heraus können bereits folgende Fragestellungen direkt abgeleitet werden:

- Welche Facetten der Digitalisierung stehen in einem engen Zusammenhang mit der in der Problemstellung genannten Situation?
- Welche positiven oder negativen Auswirkungen sind mit der Einführung neuer Technologien in Bezug auf die IT-Notfallvorsorge grundsätzlich zu erwarten?
- Welche neuen Herausforderungen entstehen für das IT-Notfallmanagement durch welche Aspekte der Digitalisierung?
- Welche Faktoren beeinflussen maßgeblich den Auf- und Ausbau des IT-Notfall-managements?

Weiterhin stellt sich die Frage, ob sich die öffentliche Verwaltung bei der Digitalisierung durch signifikante Besonderheiten kennzeichnet. Es ist zu hinterfragen, welche bei den Behörden zu erwartenden weiteren Digitalisierungsschritte zu einem der zitierten Kontrollverluste führen können. Gibt es für große Handlungsfelder der Digitalisierung, wie das Cloud-Computing, bereits wegweisende Projekte und wie stellt sich deren Situation in der Theorie dar? Schwierig aus der Theorie zu beantworten ist voraussichtlich die Fragestellung, ob mit der Digitalisierung automatisch ein erhöhtes Sicherheitsniveau verbunden ist oder ob zukünftig die allgemeine Sicherheit eher gefährdet ist. Die aus der Theorie nicht abschließend beantwortbaren Fragen werden später um Erkenntnisse aus dem empirischen Teil ergänzt. Zusammenfassend sind hier die Fragen nach diesen Sachständen, Faktoren und deren Gewichtung zu beantworten, um den theoretischen Stand bestmöglich abzubilden. Dazu werden in den nachfolgenden Kapiteln die theoretischen Grundlagen ausführlich herausgearbeitet und für eine Lösung der Problemstellung fokussiert analysiert. Zum Ende von Teil II werden die hier aufgestellten Fragen konkret beantwortet.

2 Theoretische Ausführungen

Mit den Erkenntnissen der Analysen und Studien aus Kapitel II 1.1.4 und Kapitel II 1.1.5 folgen hier die dazugehörigen theoretischen Ausführungen zu allen relevanten Themenfeldern. Neben den genannten Journalen wurden auch wissenschaftliche Monografien konsultiert, aus denen die Begriffsdefinitionen und Bedeutungen für dieses Forschungsobjekt entnommen sind. Bei abweichenden Festlegungen in der Literatur werden diese hier kritisch diskutiert und die Begriffsdefinition wird für die weitere Verwendung festgelegt.

2.1 Fachliche Themenfelder

Im Einleitungsteil wurden in Kapitel I 3.1 bereits alle Themenfelder aufgelistet und deren grundsätzliche Zusammenhänge genannt. Diese Begriffe und Themenkomplexe sind in den nachfolgenden Unterkapiteln einzeln mit Definitionen, Sachstand und Besonderheiten im Kontext des Forschungsprojektes erläutert.

2.1.1 Digitalisierung

Der Begriff ‚Digitalisierung' wird nach Bengler und Schmauder derzeit in zwei Bedeutungen verwendet. Einerseits bezeichnet er die technische Umwandlung von analogen in digitale Daten und andererseits werden die auf dieser technischen Basis entstandenen und zukünftigen Effekte auf die gesamte Gesellschaft inkl. Unternehmen als ‚Digitalisierung' bezeichnet (2016, S. 75). Dieser Begriff beschreibt auch alle Auswirkungen und Folgen, die die Verfügbarkeit von digitalen Informationen auslösen (Schumacher et al., 2016, S. 3).

Nach Ansicht von Zöller wird darüber hinaus von der digitalen Revolution gesprochen, die implizit mit dem Begriff der Digitalisierung gemeint ist. Als Prozessbeschreibung hat der Begriff jedoch nach Auffassung des Autors noch wenig Aussagekraft (2019, S. 6). Auch weitere Autoren, wie Hess et al. (2016, S. 124), stellen die Komplexität dieser digitalen Transformationen heraus, indem zahlreiche oder sogar alle Bereiche eines Unternehmens davon betroffen sind. Zudem ist nach Krcmar (2018, S. 10) dieser Prozess für Unternehmen unausweichlich und dieser Autor empfiehlt, die Möglichkeiten zur Weiterentwicklung zu untersuchen, statt an bestehenden Geschäftsmodellen festzuhalten.

In einer Metastudie wurden 23 zum Teil deutlich differierende Definitionen des Begriffes ‚digital transformation' untersucht. Als Ergebnis wurde eine Begriffserklärung entworfen,

wonach darunter ein Verbesserungsprozess zu verstehen ist, der sich durch signifikante Veränderungen verschiedener technologischer Komponenten kennzeichnet (Vial, 2019, S. 121). Auch im Bereich der öffentlichen Verwaltung gehören zu einer digitalen Transformation kulturelle und organisatorische Veränderungen, womit auch die Förderung von digitalen Kompetenzen bei den Mitarbeitern und den Führungskräften gemeint ist (Mergel, 2019, S. 165).

Eine Auflistung und Erläuterung aller Bestandteile der Digitalisierung ist an dieser Stelle nicht möglich, da sich dieser Transformationsprozess auf nahezu alle Lebensbereiche auswirkt. Im Weiteren werden somit nur jene Aspekte der Digitalisierung näher beleuchtet, die einen mittelbaren Einfluss auf behördennahe IT-Dienstleister und Behörden haben und in einem direkten Zusammenhang mit dem Notfallmanagement stehen. Beispielsweise ist hier das Cloud-Computing relevant, das in der Literatur aus Sicht der Sicherheit auch kritisch diskutiert wird. Faber (2019, S. 20) beschreibt neben den vielen Chancen und positiven Effekten des Cloud-Computings auch mehrere Risiken und spricht von dem in der Problemstellung genannten Kontrollverlust, der mit der Cloud-Technologie verbunden ist.

Bezüglich der Sicherheit resümiert Weber (2017, S. 33), dass bei Betrachtung der Chancen und Risiken die IT-Sicherheit eine Grundbedingung bei der Digitalisierung ist. Von Lucke (2018, S. 29) beschreibt zur Digitalisierung den Einsatz von IT im öffentlichen Sektor und wie die Internettechnologien zu nachhaltigen Veränderungen führen. Er verdeutlicht die immer stärker werdende Vernetzung der Behörden mit Bürgern und Unternehmen im Gegensatz zu traditionellen Systemen der EDV. Hieraus lässt sich schließen, dass zukünftige IT-Ausfälle zunehmend direkte Auswirkungen auf die Bürger haben werden.

Bezüglich der beispiellosen Geschwindigkeit bei Veränderungen in der IT spricht Schaudel von einer der wichtigsten Auswirkungen der Digitalisierung. Bei Aktualisierungen in der IT, die vor Jahren noch z. B. quartalsweise erfolgten, können heute sogar tägliche Updates als langsam angesehen werden (2018, S. 128). Herauszufinden, ob und wie mit diesen verkürzten Intervallen der Innovationszyklen der digitalen Transformation noch alle Resilienz- bzw. Sicherheitsanforderungen erfüllbar sind, ist ein Element dieses Forschungsvorhabens.

Der Stand der Forschung zur Digitalisierung kann im Rahmen dieses wissenschaftlichen Vorhabens aufgrund der Agilität der Thematik und des Umfanges der Digitalisierung nur im Ansatz diskutiert werden und wird sich weiter auf den Bereich Business Continuity Management fokussieren. Die dargestellten Definitionen bilden die wissenschaftliche Grundlage zur Digitalisierung, um die Forschungsstände der weiteren Themenfelder im

Kontext der Digitalisierung darstellen zu können. In den anschließenden Unterkapiteln werden die genannten Fakten zu diesem Stand der Digitalisierung reflektiert.

Für eine zusammenfassende Übersicht über die zahlreichen diskutierten Komponenten der Digitalisierung dient die nachfolgende Abbildung. Es zeigte sich bereits, dass die dort genannten Begriffe, wie Veränderungen, Komplexität, Vernetzungen, Cloud etc., bei den zitierten Definitionen zur Digitalisierung von anderen Autoren ebenfalls genannt wurden. Zusätzlich veranschaulicht hier der mittlere Ring die wirtschaftlichen Phänomene, die als Erklärungsansatz für das digitale Zeitalter identifiziert wurden (Resch, 2020, S. 157). Zentriert dargestellt sind verschiedene Technologien, von denen diejenigen, die für Behörden bzw. behördennahe IT-Dienstleister von Relevanz sind, später auch aus Sicht des Business Continuity Managements betrachtet werden.

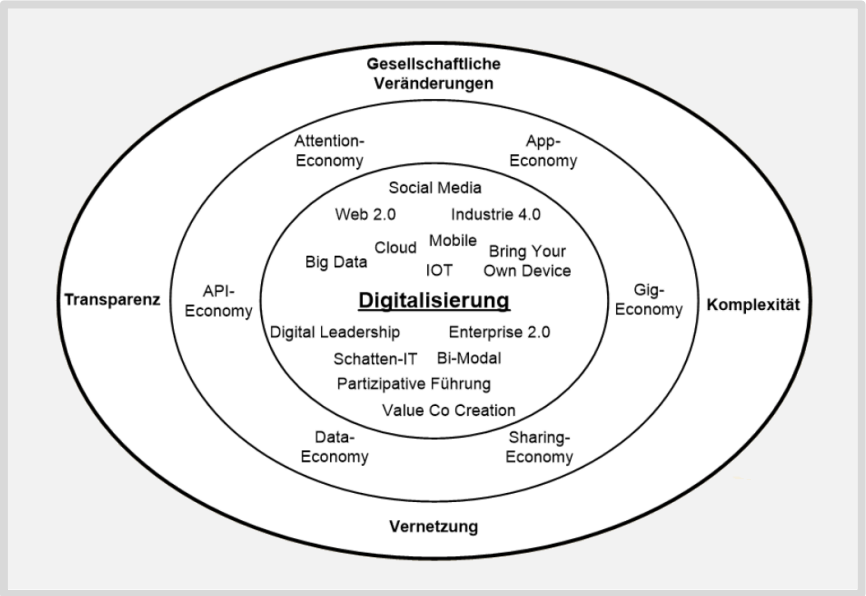


Abbildung 8 – Übersicht über Digitalisierungsthemen (Quelle: Resch, 2020, S. 154)

Kritisch ist anzumerken, dass der mittlere Kreis der Abbildung keine abschließende Auflistung der Technologien und Managementprozesse sein kann. So lassen sich in der Literatur auch weitere Bestandteile finden, die unter dem Begriff ‚Digitalisierung' in diesem Zusammenhang zu verstehen sind. Als hier nicht genannte Aspekte sieht Specht unter den zehn wichtigsten Technologietrends der Digitalisierung zusätzlich Virtual und Augmented Reality, den 3-D-Druck, die Künstliche Intelligenz (KI), Blockchain, Robotik sowie die Nano- und Biotechnologie (2021, S. 175).

Grundsätzlich damit übereinstimmend erläutern Hofmann und Staiger (2020, S. 91) die nachfolgenden Schlagworte, die als Bestandteile der Digitalisierung gelten. Für den Anteil der Beschaffung werden sie als die relevantesten Treiber der Industrie 4.0 genannt (2020, S. 86).

Diese Punkte wären demnach in der oben angegebenen Abbildung unter dem entsprechenden Digitalisierungspunkt Industrie 4.0 zusätzlich aufzunehmen: „Blockchain und Smart Contracts“, „Enterprise 3D Printing“, „Ubiquitos Computing und RFID-Technologie“, „Internet der Dinge und Dienste (IoTS) und Cloud-Computing“, „Big Data und Analytics-Dienste“, „Maschine-zu-Maschine-Kommunikation“, „Robotics, Automatisierung und selbstfahrende Fahrzeuge“ sowie „Virtual and Augmented Reality (Mensch-Maschine-Interaktion)“ (Hofmann & Staiger, 2020, S. 86-90). Damit wird der umfassende Bereich dieses Themenfeldes deutlich und es wird einsehbar, dass nicht alle Komponenten im Rahmen der Zielstellung tiefer untersucht werden können.

Weitere Darlegungen zur Digitalisierung wurden bereits in den vorangegangenen Kapiteln vorgenommen, so dass hiermit der relevante Bereich festgelegt ist, und die wesentlichen Komponenten wurden genannt. Zur Reflexion der Problemstellung ist die Frage von grundlegender Bedeutung, inwiefern Behörden auf diese Technologien zukünftig zwingend angewiesen sind oder ob bei IT-Störungen vorübergehend darauf verzichtet werden kann. Die Abhängigkeit von der IT steigt nach Gadatsch und Mangiapane (2017, S. 15) und das Management steht vor schwierigen Aufgaben, da die Komplexität und die Zusammenhänge insbesondere aus Sicht der IT-Sicherheit nicht immer transparent sind. Zum Begriff ‚Management‘ werden im Weiteren das IT-Management und das IT-Notfallmanagement detaillierter dargestellt.

2.1.2 IT-Management und IT-Notfallmanagement

IT-Management

Als IT-Management in einem Unternehmen wird das Management bezeichnet, das vorrangig für die Belange der IT des Unternehmens zuständig ist. Resch hat hierzu folgende Ziele der IT genannt, deren Unterstützung als Aufgabe des IT-Managements zu sehen ist. Die IT soll demnach mit möglichst niedrigen Kosten einen Wertbeitrag für das Unternehmen leisten und dabei die Sicherheit beachten (2020, S. 160-161).

Die Auswirkungen der Digitalisierung auf das IT-Management sind umfangreich. So wurde von Urbach und Ahlemann (2016, S. 64-65) das IT-Management-Paradigma „Innovate-Design-Transform“ vorgeschlagen, um den derzeitigen Fokus der IT-Abteilungen auf Entwicklung und Betrieb gegenüber einer innovativeren Vorgehensweise mit Kulturwandel abzugrenzen. Dieser Aspekt ist von hoher Relevanz für diese Forschungsarbeit, da auch neue Vorgehensweisen aus der Praxis ermittelt und untersucht werden sollen. Nach Urbach

(2018, S. 124) haben die IT-Abteilungen einen technikorientierten Fokus und weniger Kenntnisse im geschäftlichen Umfeld. Zukünftig, so prognostiziert Ahlemann (2018, S. 126), wird die strategische Relevanz dieser Abteilungen steigen. Die klassischen IT-Abteilungen werden kleiner und stattdessen werden IT-Professionals direkter in den geschäftlich orientierten Abteilungen des Unternehmens tätig sein. Damit sind wesentliche Veränderungen im und für das IT-Management zu erwarten. Es wird daher als Teil der empirischen Untersuchung mit betrachtet. Janottas These „Nahezu jedes Unternehmen ist heute ein Informationstechnologieunternehmen“ (2019, S. 257) verdeutlicht den hohen Stellenwert der IT und damit des IT-Managements für Unternehmen.

Im vorhergehenden Unterkapitel wurde beschrieben, dass IT-Veränderungen immer schneller und häufiger erfolgen. Dadurch ist auch das IT-Management gefordert, schneller zu agieren. Ebenfalls analog zur Digitalisierung ist das IT-Management eine ausgesprochen agile Thematik, die an Bedeutung gewinnen wird. Schwer und Hitz diskutieren hierzu im Zusammenhang mit der Digitalisierung, inwiefern die klassischen hierarchischen Organisationsformen weiterhin gebraucht werden. Als Ergebnis sehen sie die Notwendigkeit einer neuen holokratischen Unternehmensstruktur (2018, S. 20). Dadurch können sich auch die Verantwortlichkeiten im Business Continuity Management ändern.

Bereits vor über 13 Jahren diskutierte Keuper das IT-Management aus strategischer Sicht und bestätigte dabei die These, dass das IT-Management selbst auch Wettbewerbsvorteile generieren kann. Er wies aber bereits auf die Notwendigkeit der Verflechtung mit anderen Teilen des Unternehmens hin und sah die Möglichkeit, dass die Initiierung für solche Vorteile aus dem IT-Management selbst entstehen kann (2010, S. 25-26). Ebenso kommen Eul et al. zu dem Ergebnis, dass durch ein angemessenes IT-Management der Einsatz der IT wertsteigernd sein kann. Die Titelgebung des Beitrages „Strategisches IT-Management – Vom Kostenfaktor zum Werttreiber“ (2010, S. 69) zeigt deutlich, wie sich das IT-Management bereits damals gewandelt hat.

In einer Ausarbeitung zu einem modernen IT-Management mit Blick auf kleine und mittlere Unternehmen (KMU) stellen Mangiapane und Büchler (2015, S. 1) fest, dass dort ein „unternehmensweites IT-Management […] nur in Ausnahmefällen zum Einsatz“ kommt. Als Gründe sehen sie unter anderem eine fehlende Sensibilisierung in der Leitungsebene und dass es keine passenden IT-Managementmodelle gibt. In ihrer Zusammenfassung wird empfohlen, mit einer schrittweisen Vorgehensweise unter Einbindung der Geschäftsleitung zu beginnen

(2015, S. 169-170). Die vorgeschlagenen Methoden haben sich auch im Bereich einer öffentlichen Verwaltung bewährt (Mangiapane & Büchler, 2015, S. 170).

In aktuelleren Veröffentlichungen wird das IT-Management auch anhand der Digitalisierung reflektiert. Tiemeyer (2020, S. 18) sieht hier die Notwendigkeit, dass sich sowohl die Geschäftsführung als auch das IT-Management neu positionieren müssen, damit es zu keiner Überforderung kommt und Digitalisierungsprojekte erfolgreich umgesetzt werden können.

Damit wurde insgesamt dargestellt, dass das IT-Management ein bedeutender und sich verändernder Bereich ist, um die Digitalisierung weiter zu steuern. In der nachfolgenden Abbildung sind die Kernprozesse des IT-Managements für einen plakativen Überblick aufgeführt:

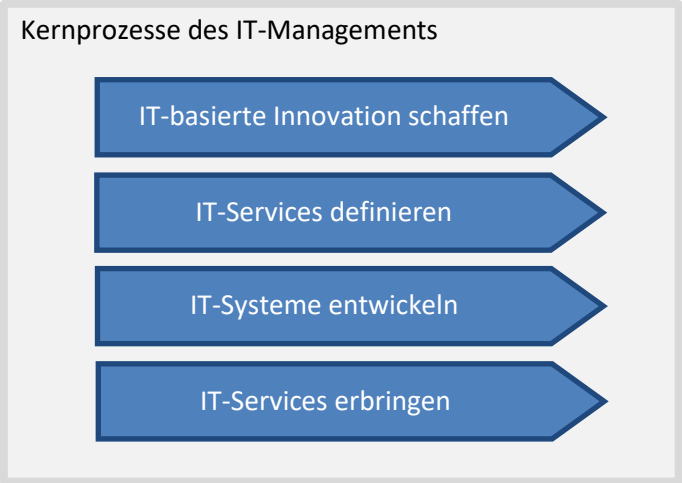


Abbildung 9 – Kernprozesse des IT-Managements nach Allweyer (Quelle: eigene Darstellung, angelehnt an Allweyer, 2020, S. 38)

Beginnend mit der Innovation über die Servicedefinition und die Systementwicklung bis zur Serviceerbringung sind damit alle wesentlichen Bestandteile genannt, die auch im Rahmen der Umsetzung von Digitalisierungsprojekten notwendig sind. Neben diesen Kernprozessen gehören auch Führungsprozesse zum Aufgabenfeld des IT-Managements, unter anderem die IT-Strategie und die IT-Governance, mit der alle IT-bezogenen Aktivitäten geplant, gesteuert und überwacht werden (Allweyer, 2020, S. 41). Als einen unterstützenden Prozess definiert der Autor das IT-Sicherheitsmanagement, in dem auch das Notfallmanagement angesiedelt ist (Allweyer, 2020, S. 210).

Mit Bezug auf die Einführung neuer Technologien wird das IT-Management als entscheidender Faktor erachtet, um die wirtschaftlichen Herausforderungen zu lösen (Pilorget und Schell, 2018, S. 6). Analog zu Digitalisierung wird damit die steigende Bedeutung des IT-Managements immer klarer. Die im Anschluss an den empirischen Teil zu erarbeitenden Empfehlungen müssen mit den Standards des IT-Managements harmonieren, um in der Praxis

akzeptiert zu werden. Wie aus dem Zitat von Allweyer ersichtlich wird, ist das IT-Notfallmanagement als unterstützender Teil des IT-Managements einzustufen.

IT-Notfallmanagement

Unter IT-Notfallmanagement werden allgemein nicht nur die Aktivitäten nach Eintritt eines Notfalls, sondern auch die Vorbereitung auf Notfallszenarien im Sinne einer Prävention verstanden. Im Fokus stehen die Kernprozesse in Unternehmen oder Behörden, die nur möglichst kurz ausfallen sollen (Osterhage, 2017, S. 217). Wenn diese Notfälle ursächlich in enger Verbindung mit der IT stehen, spricht man von IT-Notfällen. Die Abgrenzung zu normalen IT-Störungen stellen Kersten und Klett (2017, S. 16) so dar, dass die Schadensauswirkung entscheidend ist und ein IT-Notfall mindestens gravierende Auswirkungen auf die betroffene Organisation haben muss. Auch Störungen mit höchstmöglichen katastrophalen Auswirkungen werden als Notfälle bezeichnet. Die Autoren setzen das Notfallmanagement mit dem Begriff ‚Business Continuity Management' gleich (2017, S. 135). Dieser Festlegung wird hier nicht gefolgt, da unterschiedliche Auslegungen in der Literatur existieren, wie die explizite Abgrenzung zum Business Continuity Management noch zeigen wird.

IT-Notfälle sind eingetretene, in Art, Umfang und Zeitpunkt grundsätzlich unvorhersehbare Ereignisse, für deren Bewältigung besondere Maßnahmen zu ergreifen sind. Hierfür ist insgesamt das IT-Notfallmanagement zuständig, um die bestmöglichen Vorbereitungen zu treffen und um Schäden zu minimieren. Nach Allweyer (2020, S. 211) gehört eine möglichst schnelle Wiederherstellung des Betriebes zu den Aufgaben des Notfallmanagements, das, wie auch dieser Autor sagt, synonym als ‚Business Continuity Management' (BCM) bezeichnet wird. Kersten und Klett wiederum differenzieren an einer anderen Stelle deutlicher, dass es einerseits IT-Notfälle geben kann, die die Geschäftsfortführung nicht unmittelbar gefährden. Andererseits können Notfälle auftreten, die die Existenz des Unternehmens bedrohen, aber nicht ursächlich ein IT-Notfall sind (Kersten & Klett, 2017, S. 37). Diese differenziertere Begriffsbestimmung wird in der weiteren Arbeit genutzt und zur genauen Abgrenzung wird das Business Continuity Management noch separat erläutert.

Bemerkenswert im Zusammenhang mit dem Begriff ‚Notfallmanagement' ist, dass der bis zum Jahr 2023 gültige Standard des BSI die Bezeichnung „BSI 100-4 Notfallmanagement" trägt. Der seit dem Jahr 2023 verfügbare Standard heißt nun offiziell „BSI 200-4 Business Continuity Management". Der Begriff ‚Notfallmanagement' wird auch noch im aktuellen Standard erläutert und es wird insbesondere für „global agierende Institutionen" empfohlen,

stattdessen den Begriff ‚Business Continuity Management' zu nutzen, da dieser international geläufig ist. Es kann für deutsche Behörden aber auch weiterhin sinnvoll sein, die Bezeichnung ‚Notfallmanagement' zu verwenden. Die Begriffe sind grundsätzlich je Institution individuell anpassbar (BSI, 2023, S. 67).

Zusammenfassend sind damit im Kontext dieser Arbeit unter IT-Management die Managementaktivitäten zu verstehen, die neben dem vorhandenen IT-Betrieb auch maßgeblich die Digitalisierung in Unternehmen und Behörden umsetzen. Das Notfallmanagement kann grundsätzlich auch für Notfälle zuständig sein, die nicht direkt die Geschäftsfortführung eines Unternehmens oder einer Behörde bedrohen. Als für Deutschland empfohlene neue Bezeichnung und explizit für Schadensereignisse, die den Weiterbetrieb oder den Fortbestand des Unternehmens oder der Behörde bedrohen, wird der Begriff ‚Business Continuity Management' verwendet.

2.1.3 Business Continuity Management (BCM)

Wie bereits dem Titel dieser Arbeit zu entnehmen, ist das Business Continuity Management expliziter Untersuchungsgegenstand. Zur tatsächlichen Etablierung in Unternehmen wurden in Kapitel II 1.1.5 bereits verschiedene Veröffentlichungen dahingehend ausgewertet. Vorab war festzustellen, dass nach der Studie von Sawalha (2020, S. 83) zahlreichen Unternehmen nicht bekannt ist, wie ein Business Continuity Management effektiv zu implementieren ist, obwohl die Bedeutung für die Geschäftskontinuität offensichtlich ist. Ein diesbezüglicher Motivationsfaktor scheint die mögliche Erreichung einer ISO-Zertifizierung durch den Aufbau eines BCM-Systems zu sein, wie der Autor in der Studie resümiert. Inwiefern die dort auf Jordanien bezogenen Ergebnisse auf deutsche Unternehmen und Behörden übertragbar sind, wird ein Ergebnis der empirischen Untersuchung sein. Kritisch beschreibt Mandl (2021, S. 554) die Komplexität des Business Continuity Managements und sieht damit verbundene Defizite in der Darstellungsmöglichkeit von Zusammenhängen. Diese Ansicht wird im späteren Diskussionsteil zusammen mit den Beobachtungen aus der Praxiserhebung reflektiert, um anschießend geeignete Lösungsvorschläge und Vorgehensweise zu erläutern.

Es folgen Definitionen und Auslegungen zum Begriff ‚Business Continuity Management', damit eine einheitliche Basis geschaffen wird, um das Themenfeld untersuchen zu können.

2.1.3.1 Definitionen und Begriffsbestimmung

Gadatsch und Mangiapane (2017, S. 39) verstehen unter Business Continuity Management eine Managementmethode, die auch unter Krisenbedingungen die „Fortführung der Geschäftstätigkeit“ absichern soll. Sie weisen auf einen Irrglauben hin, dass in deutschsprachigen Ländern eine zu enge Bindung an die IT und die Informatik gesehen wird. Nach Ansicht der Autoren ist das IT-Notfallmanagement allerdings nur ein Teil des Business Continuity Managements. Kritisch wird hier angemerkt, dass andere Wissenschaftler es explizit als synonym bezeichnen und auch die jüngst erfolgte Umbenennung des BSI-Standards von IT-Notfallmanagement in Business Continuity Management eine klare Abgrenzung erschwert. Ebenfalls definieren Brauner und Fiedrich (2018, S. 212) Business Continuity ohne Hinweise auf die IT. So bezeichnen sie es als Fähigkeit eines Unternehmens, sowohl strategisch als auch taktisch auf Betriebsstörungen vorbereitet zu sein. Es geht um die Aufrechterhaltung des Betriebes und die Weiterführung oder Wiederherstellung der kritischen Geschäftsprozesse (Brauner und Fiedrich, 2018, S. 212).

Nach Königs (2017, S. 308) wird der Geschäftskontinuität, bezeichnet als ‚Business Continuity‘, eine hohe und überlebenswichtige Bedeutung für Unternehmen zugemessen. Da die Geschäftsprozesse in zahlreichen Unternehmen stark von den IT-Systemen abhängig sind, empfiehlt der Autor die Verbindung der IT-Notfallplanung mit dem Business Continuity Management. Zudem sollte es in der strategischen Zielsetzung der Unternehmen mitberücksichtigt werden (Königs, 2017, S. 308). In Verbindung mit Katastrophen hat Moşteanu (2020, S. 175) das Business Continuity Management analysiert und empfiehlt allen Unternehmen, neben einer Abteilung für das Risikomanagement auch eine spezialisierte Abteilung für das Katastrophenfallmanagement vorzusehen. In einer anderen Untersuchung zu einer Business-Continuity-Abteilung fokussiert sich diese auf die kritischen Applikationen und Daten und soll, zusammen mit der IT-Sicherheit, für möglichst minimale Ausfälle sorgen (Njenga & Brown, 2012, S. 596).

Suresh et al. (2020, S. 131) erläutern, wie verschiedene Praktiken und Konzepte aus der Vergangenheit nun unter dem Begriff ‚Business Continuity Management‘ versammelt werden. Als besondere Eigenschaft nennen sie die geringe Eintrittswahrscheinlichkeit der Situationen, hohe Auswirkungen und dass Führungskräfte in solchen Fällen nur eine äußerst kurze Reaktionszeit haben. In einer Entwicklungsanalyse des Business Continuity Managements berichtet Herbane (2010, S. 995), dass es sich in der Praxis in den Unternehmen mit der

Einführung neuer IT verändert hat. Aber auch nach Katastrophen, wie den Terroranschlägen vom 11. September 2001, gab es Veränderungen. Dieses Ereignis erläutert der Autor als relevanten Punkt, der die Notwendigkeit und die Präsenz eines Business Continuity Managements in zahlreichen Sektoren und öffentlichen Einrichtungen gezeigt hat.

Internationale Veröffentlichungen verwenden den Ausdruck ‚Business Continuity' oft zusammen mit dem Begriff ‚Disaster Recovery'. Zur Entstehung stellen unter anderem Baldwin (2019, S. 103), Elliot et al. (2010, S. 1) und Herbane (2010, S. 979) eine direkte Verbindung zu diesem Begriff her. Baldwin (2019, S. 103) berichtet, wie in den 1980er Jahren erstmals Risiken betrachtet wurden, die sich mit dem Ausfall von IT und den damit verbundenen unternehmerischen Auswirkungen beschäftigen. Er führt die Entstehung konkret auf neue Aufgaben in den damaligen Rechenzentren zur Erstellung von Backups sowie auf das Bestreben, Datenbestände sicher aufzubewahren und wiederherzustellen, zurück. Der Schutz und die Wiederherstellung der kritischen IT-Services machen den Anteil der Business Continuity aus, der als ‚IT Disaster Recovery' bezeichnet wird (Watters, 2014, S. 57).

Hiermit wird deutlich, dass auch international die Definition und die Bedeutung des Begriffes ‚Business Continuity Management' eng mit der IT verbunden sind.

Heute wird vorgeschlagen, dass das Business Continuity Management nicht nur aus Werterhaltungssicht betrachtet werden sollte, sondern dass es auch als wertsteigernd für Unternehmen anzusehen ist (Niemimaa et al., 2019, S. 210). Über die eigentliche Wiederherstellung ausgefallener Systeme hinaus sieht auch Baldwin (2019, S. 109) die Verhinderung von Störungen als spezifische und dauerhaft wertsteigernde Fähigkeit des Business Continuity Managements. Hiermit wird die steigende Bedeutung des Business Continuity Managements von einer eher reaktiven Ausrichtung auf eine proaktiv wertsteigernde Funktion deutlich.

National hat das BSI die Bezeichnung ‚Business Continuity Management' als Nachfolge-bezeichnung für das Notfallmanagement gewählt. Abbildung 10 zeigt den vom BSI dargestellten Wirkungsrahmen in Bezug auf Störungen, Notfällen und Krisen:

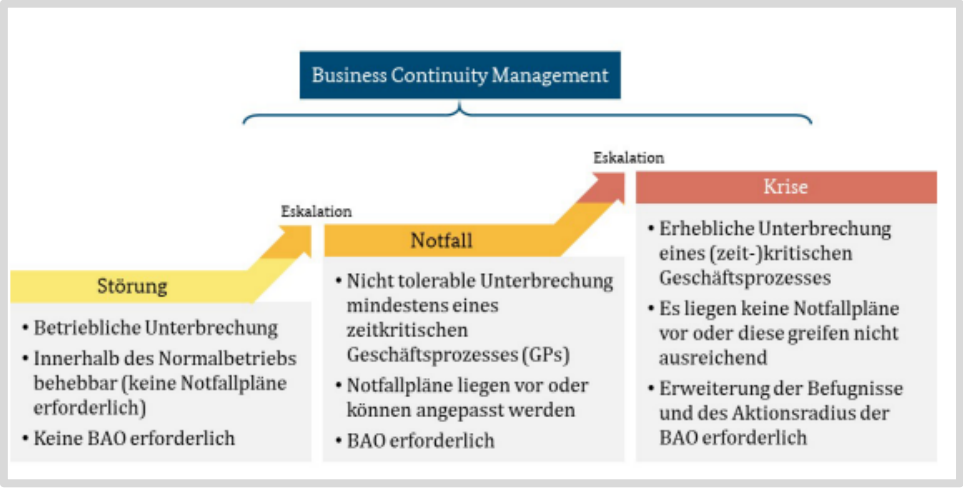


Abbildung 10 – BSI 200-4: Business Continuity Management (Quelle: BSI, 2023, S. 20)

Aus der Zuordnung das BSI ist ersichtlich, dass für das Business Continuity Management bereits erste Störungen relevant sein können. Zentral und umfänglich liegen die Bereiche der Notfälle bis hin zu Krisen im Fokus. Die Klammer des Business Continuity Managements erstreckt sich von der Eskalation von Störungen über die Notfallbearbeitung bis hin zur Krisenbewältigung. Als ‚BAO' werden hier besondere Aufbauorganisationen bezeichnet: Personal und organisatorische Strukturen, die im Routinebetrieb und bei einfachen Störungen noch nicht benötigt werden oder vorhanden sind, werden im Notfall erforderlich. Hervorzuheben ist, wie aus der Abbildung ersichtlich, dass für Situationen, für die es keine Notfallpläne gibt oder in denen die vorliegenden Pläne nicht funktionieren, das Business Continuity Management die Vorbereitungen treffen soll bzw. dafür zuständig ist. Das BSI spricht hier von existenzbedrohenden Beeinträchtigungen nach Eintritt entsprechender Schadensereignisse. Vor diesen Beeinträchtigungen können Organisationen sich mit einem angemessenen Business Continuity Management schützen (BSI, 2023, S. 14).

Zur Definition wird, angelehnt an Păunescu und Argatu (2020, S. 501), im Weiteren unter dem Begriff ‚Business Continuity Management' ein für die Resilienz von Organisationen vorgesehenes Framework verstanden, mit dem die Widerstandsfähigkeit gegenüber potenziellen Bedrohungen erhöht werden kann. Damit soll die Wiederaufnahme oder Fortführung des Betriebes, auch unter ungünstigsten Bedingungen, ermöglicht werden. Ferner wird darauf hingewiesen, dass zahlreiche Veröffentlichungen bezüglich der Definition auf die ISO-Norm 22301 verweisen, die im Kapitel II 2.1.5 noch erläutert wird.

Nach dieser Festlegung, den Begriffsursprüngen und Entwicklungen werden nachfolgend die wesentlichen Elemente eines Business Continuity Managements vorgestellt.

2.1.3.2 Elemente des Business Continuity Managements

BCM-Lifecycle

Sowohl im BSI-Standard 200-4 (BSI, 2023, S. 40) als auch in der Literatur sind Hinweise auf die Good Practice Guidelines (GPG) des britischen Business Continuity Institutes (BCI) zu finden. Baumann und Rössing (2018, S. 168) erläutern die sechs Phasen, die in zahlreichen Unternehmen Anwendung finden und auch Mirkes und Özcan (2020, S. 194) berichten von diesen Kernelementen, die sich durchgesetzt haben. Hier muss kritisch angemerkt werden, dass es in der Literatur verschiedene Darstellungen, Interpretationen und Übersetzungen dieses Lebenszyklus gibt. Beispielsweise wurde in der soeben zitierten Quelle das ‚Program Management' als ‚Projektmanagement' übersetzt und entspricht damit nicht mehr der Originalaussage, da Projekte zeitlich befristete Aktivitäten sind. Zur Vermeidung weiterer Interpretationsdifferenzen wird hier die Originaldarstellung vom BCI aus dem Jahr 2013 erläutert:

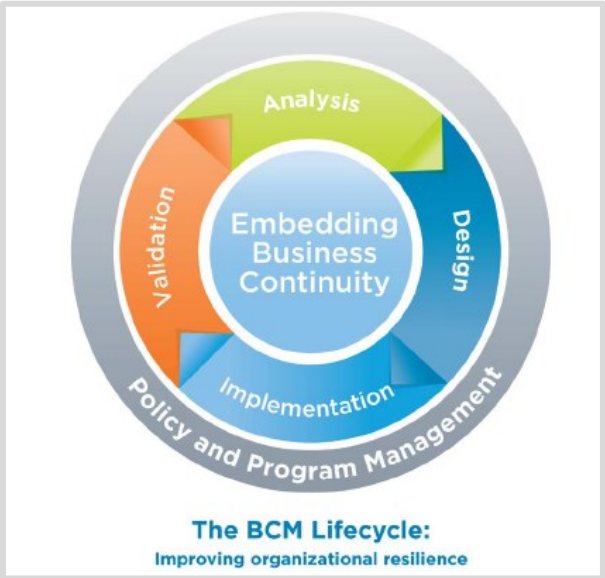


Abbildung 11 – Der BCM-Lifecycle (Quelle: BCI, 2013, S. 17)

Die Grafik zeigt, dass eine BCM-Politik bzw. -Richtlinie und das Programm-Management eine alle Phasen übergreifende Managementaufgabe ist, um ein Business Continuity Management zu implementieren bzw. in Unternehmen und Organisationen einzubetten. Es wird auch deutlich, dass nach der Analyse, der Entwicklung und der Implementierung der Lösungen stets eine Überprüfung erfolgen soll, wonach wieder in die Analysephase übergegangen wird. Das Business Continuity Management ist damit als ein nicht endender Prozess zu verstehen, der durch diese Eigenschaft mit den fortwährenden Veränderungen durch die Digitalisierung harmoniert.

Business-Impact-Analyse (BIA)

Ein Teil der Analysephase ist die Business-Impact-Analyse und diese kann aus Sicht Faertes (2015, S. 1402) als eines der zentralen Elemente eines Business Continuity Management Systems (BCMS) angesehen werden. Hier geht es darum, die etwaigen Auswirkungen auf Kernprozesse der Organisation zu identifizieren und zu bewerten.

Die ISO-Norm 22301 (DIN EN ISO 22301, 2020, S. 24) fordert ebenfalls die Business-Impact-Analyse im dortigem Kapitel 8.2.2. und legt fest, dass die folgenden Analyseschritte durchgeführt werden müssen: Die Organisationen haben die maximal tolerierbaren Ausfallzeiten zu ermitteln, die Betriebstätigkeiten mit hoher Priorität festzulegen und die benötigten Ressourcen und Schnittstellen zu betrachten. Königs (2017, S. 323) erläutert die Business-Impact-Analyse auch unter dem Begriff ‚Geschäfts-Impact-Analyse' und nennt als ersten Schritt die Ermittlung kritischer Geschäftsfunktionen. Die Betrachtung der Abhängigkeiten, der Auswirkungen und der maximalen Ausfallzeiten sind weitere Ziele, die genannt werden (Königs, 2017, S. 324). Zudem müssen ein Notbetrieb und eine minimale Verfügbarkeit bzw. Produktivität festgelegt werden.

Osterhage (2016, S. 13) bezeichnet die Business-Impact-Analyse als „Rückgrat des Notfallmanagements" und damit wird eine Basis für einen sicheren IT-Betrieb geschaffen. Mit dem Hinweis auf die in fast allen Bereichen vorhandenen IT-Prozesse und deren Verknüpfungen sind alle Geschäftsprozesse zu erfassen (Osterhage, 2016, S. 14).

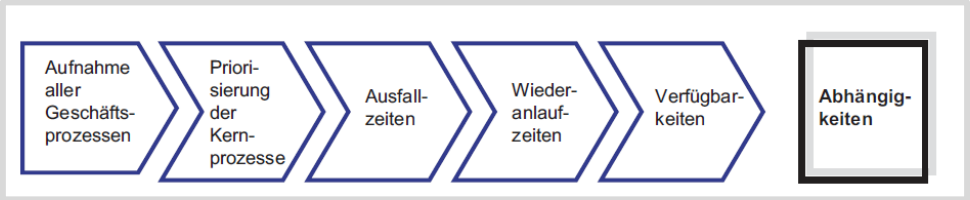


Abbildung 12 – „Schrittfolge bei der BIA" (Quelle: Osterhage, 2016, S. 14)

Aus Abbildung 12 wird ersichtlich, dass die Aktivitäten aufeinander aufbauen. Erst wenn alle Geschäftsprozesse im Rahmen der Business-Impact-Analyse erfasst sind, können auch die Kernprozesse priorisiert werden. Sobald ermittelt ist, wie lange Services tolerierbar ausfallen dürfen, wie lange ein Wiederanlauf dauern darf und welche Verfügbarkeiten grundsätzlich vorzusehen sind, können die Abhängigkeiten betrachtet werden. Bemerkenswert ist, dass der Autor bei der Bewertung der Prozesse neben den finanziellen, logistischen oder Image-schädlichen Auswirkungen auch explizit das „Leib und Leben der Mitarbeiter" als relevanten Bewertungspunkt nennt (Osterhage, 2016, S. 14). Damit wird die hohe Bedeutung der Thematik transparent und es wird nachvollziehbar, weshalb im Business Continuity

Management stets auch katastrophale Schadensgroßereignisse im Schwerpunkt zu betrachten sind.

Im Rahmen der Business-Impact-Analyse soll nach Vorgaben des BSI-Standards 200-4 von einem „Totalausfall des Geschäftsprozesses (Worst Case)“ ausgegangen werden, unabhängig davon, wie oder warum der Service ausgefallen ist (BSI, 2023, S. 158). Die Abschätzung des möglichen Schadens, der durch eine Betriebsunterbrechung aufgrund des Ausfalls kritischer Systeme und IT-Applikationen entsteht, gehört ebenfalls zur Business-Impact-Analyse (Mónica et al., 2020, S. 4).

Zusammengefasst zeigt sich damit ein in der Literatur einheitliches Verständnis der Bedeutung und der Inhalte einer Business-Impact-Analyse als Teil des Business Continuity Managements.

PDCA-Zyklus

Im Zusammenhang mit dem Business Continuity Management erläutert Spörrer (2014, S. 59-61) das Modell ‚Plan-Do-Check-Act‘ (PDCA). Damit existiere ein theoretischer Kreislauf an wiederkehrenden Managementaktivitäten, der angewandt werden kann. Dieser Zyklus ist in der ISO-Norm 22301, die später erläutert wird, ebenfalls so benannt und beschrieben (DIN EN ISO 22301, 2020, S. 7). Auch das BSI weist im Business Continuity Management Standard 200-4 auf diesen Zyklus hin und sieht einen steigenden Reifegrad des Managementsystem mit jedem Durchlauf (BSI, 2023, S. 25). Diese Methode ist nicht spezifisch für das Business Continuity Management. Die Planung und die Implementierung sowie die Überwachung und die stetige Verbesserung zeichnen jedes Managementsystem aus und damit ist es auch für die Aufrechterhaltung der Geschäftsprozesse notwendig (Cornish, 2011, S. 123).

Die Strukturen für Serviceverbesserungen im IT-Servicemanagement wurden durch den PDCA-Ablauf inspiriert und dieser Zyklus ist hier ein bedeutendes Merkmal (Verlaine, 2017, S. 267). In zahlreichen Veröffentlichungen wird auf die Entstehung der Methode des PDCA-Zyklus auf Basis des Deming-Kreises, nach Dr. W. Edwards Deming, hingewiesen (Supriadi & Pheng, 2018, S. 48; Verlaine, 2017, S. 267; Moen und Norman, 2009, S. 1). Damit ist ein Ursprung dieser Methode genannt. Die weitere Analyse bezieht sich auf Auslegungen in der Literatur, die sich auf die Anwendung im Rahmen des Business Continuity Managements fokussieren.

Mit der Anwendung dieser Methode lässt sich für das Business Continuity Management in Unternehmen oder Organisationen ein vollständiger Blueprint erstellen, der vom Beschließen der Richtlinien über das tägliche Besprechen der Ergebnisse bis zu einer kontinuierlichen Verbesserung reicht (Hersyah & Derisma, 2018, S. 393). Auch für allgemeine Problemlösungen

kann der PDCA-Zyklus bereits Anwendung finden (Foth, 2016, S. 13-14). Foth nennt diese Methode als einen Erfolgsfaktor für schlanke IT-Organisationen (S. 15-16) und empfiehlt sie als Hilfsmittel für eine nachhaltige Organisationsentwicklung (S. 115). Für die bereits erwähnte ISO-Norm 22301 wurde mit der ISO 22313:2020 eine Anleitung zur Verwendung der Norm 22301 veröffentlicht. Dort ist die nachfolgende Abbildung eines PDCA-Zyklus enthalten, der auf die Prozesse eines Business Continuity Management Systems angewandt werden kann:

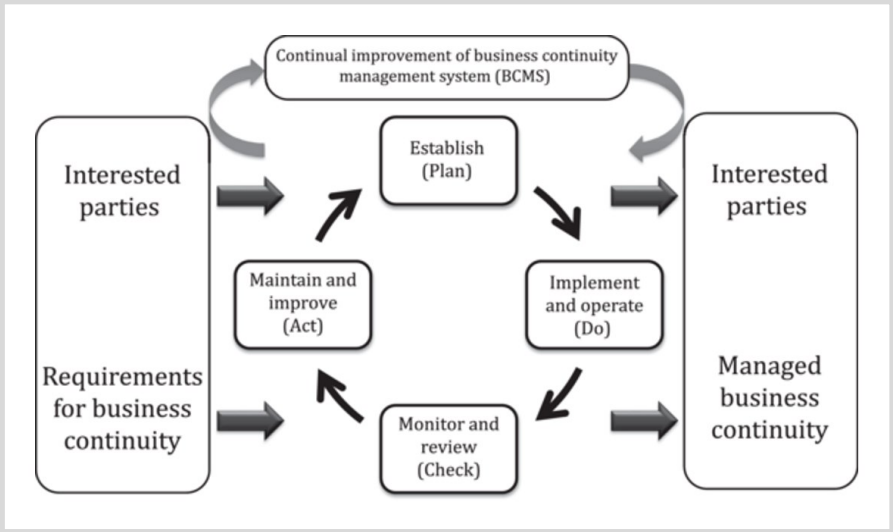


Abbildung 13 – „PDCA cycle applied to BCMS processes" (Quelle: ISO 22313, 2020)

Hier ist der Kreislauf dargestellt, dessen Iterationen zu einer kontinuierlichen Verbesserung des Business Continuity Management Systems führen können. Die beteiligten Bereiche („Interested parties") liefern mit ihren Anforderungen an das Business Continuity einen Beitrag für das System. Gleichzeit erhalten sie als Ergebnis eine gemanagte Business Continuity.

Zusammenfassend lässt sich auf Basis der Bezüge feststellen, dass diese Methode für Managementsysteme allgemein und explizit auch für das Business Continuity Management als geeignet angesehen und empfohlen wird. Ob und wie es in der Praxis auch Anwendung findet, wird im empirischen Teil eruiert.

Damit wurden sowohl der Begriff ‚Business Continuity Management' als auch wesentliche Elemente aus Sicht der Theorie dargestellt. Wiederkehrend ist in der Literatur in diesem Zusammenhang zusätzlich der Begriff des IT Service Continuity Managements (ITSCM) zu finden, der im Folgenden erläutert wird.

2.1.4 IT Service Continuity Management (ITSCM)

Das soeben erläuterte Business Continuity Management hat allgemein die gesamte Geschäftsfortführung im Fokus. Das ITSCM grenzt sich dahingehend ab, dass es sich auf die Fortführung der betriebenen oder genutzten IT-Services konzentriert. Es ist als technischer Anteil des Business Continuity Managements zu sehen (Wan und Chan, 2008, S. 21). Nach Kersten und Klett entspricht die Bezeichnung ‚IT Service Continuity Management' aus dem ITIL-Standard („Information Technology Infrastructure Library") dem deutschen Begriff ‚IT-Notfallmanagement' (2017, S. 133). Müller (2018, S. 154) sieht das ITSCM als unterstützend für das Business Continuity Management an, indem mit seiner Hilfe die IT innerhalb von vereinbarten Zeiten wieder verfügbar gemacht wird. Der Autor erläutert vier Phasen des Lebenszyklusmodells: Initiierung, Anforderungen und Strategieentwicklung, Implementierung sowie kontinuierlichen Betrieb (Müller, 2018, S. 154-155). Für die zweite Phase wird unter anderem die bereits vorgestellte Business-Impact-Analyse genutzt und im kontinuierlichen Betrieb sind regelmäßige Reviews, Schulungen, Sensibilisierungen und Übungen vorgesehen (Müller, 2018, S. 155). Grundsätzlich deckungsgleich bezeichnet Spilker (2022, S. 145) die folgenden Phasen als zu durchlaufende Schritte, um ein ITSCM zu etablieren: Initiierung, Anforderungsanalyse und Strategie, Implementierung sowie laufenden Betrieb.

Abbildung 14 – Phasen bzw. Schritte des ITSCM (Quelle: eigene Darstellung, angelehnt an Müller, 2018, S. 154; Spilker, 2022, S. 145)

In Abbildung 14 sind die wesentlichen vier Elemente dargestellt, nach denen ein ITSCM in der Theorie erfolgen soll. Wird nun die fortschreitende Digitalisierung berücksichtigt, die mit neuen einzuführenden Technologien jeweils eine dazu passende Analyse erfordert, müssen die Schritte ab der Anforderungsanalyse erneut durchlaufen werden. Erst nach einer ggf.

wieder notwendigen Phase der Implementierung soll aus Sicht des ITSCM der Betrieb erfolgen. Ebenfalls können sich aus der Betriebsphase durch Updates oder durch Erkenntnisse aus Tests und Übungen Situationen ergeben, die einen erneuten Durchlauf ab der Anforderungsanalyse und ggf. eine Überarbeitung der Strategie notwendig machen.

Parallel zur Abgrenzung bei der Definition des Begriffes ‚IT-Notfall' gibt es auch beim ITSCM eine klare Unterscheidung zu Störungen (Incidents) im IT-System. Krishna Kaiser (2018, S. 95) beschreibt das ITSCM als Prozess, der für Katastrophen epischen Ausmaßes und lang andauernde IT-Ausfälle anzuwenden ist. Er erläutert die ebenfalls aus dem ITIL-Standard abgeleitete Definition einer Störung (Incident). Diese besagt, dass jede Unterbrechung eines Services bereits ein Incident ist (Krishna Kaiser, 2018, S. 166). Obgleich es sich in beiden Fällen um unerwartete Ausfälle des IT-Systems handelt, ist diese Unterscheidung für das Notfallmanagement wesentlich. Hier bestehen deutliche Unterschiede hinsichtlich der Eintrittswahrscheinlichkeiten und der Auswirkungen. Leimeister (2012, S. 75) spricht von Risiken durch unvorhersehbare Katastrophenfälle, zu denen „Hackerangriffe, Feuer, Stromausfälle und Naturkatastrophen" zählen, für die das ITSCM zuständig ist.

Ein ITSCM ist, wie bereits erwähnt, auch im ITIL-Standard und zudem in COBIT („Control Objectives for Information and related Technology") berücksichtigt. COBIT wird, neben ITIL, im Kapitel zu den Best Practices noch erläutert. Nachrowi et al. analysieren diese Standards im IT-Management und bringen die Fachbegriffe ‚IT Continuity Management' und ‚Service Continuity Management' nach ITIL mit dem aus dem COBIT-Framework stammenden Begriff ‚Maintain Business Resilience' zusammen (2020, S. 767). Mit der Bezeichnung ‚Resilienz' und der expliziten Unterscheidung gegenüber normalen Störungen gemäß ITIL und nach COBIT wird verdeutlicht, dass eine Abgrenzung zur normalen Bearbeitung von IT-Störungen vorzunehmen ist.

In der neuen Version ITIL v4, veröffentlicht 2019, ist statt des Begriffs ‚ITSCM' nun dieser Anteil unter dem Bereich ‚Service-Management-Praktiken' als ‚Service-Continuity-Management' bezeichnet zu finden (Johanning, 2020, S. 71-72). Der im Jahr 2023 veröffentliche BSI-Standard 200-4 nutzt und erläutert allerdings weiterhin den Begriff ‚ITSCM' (BSI, 2023, S. 35). Deshalb wird diese Bezeichnung auch hier im weiteren Verlauf genutzt und stellt eine Differenzierung des Begriffs ‚Business Continuity Management' dar, sobald explizit Betriebskomponenten der IT oder die so bezeichneten Standards angesprochen werden. Die weitere Entwicklung dieser Begrifflichkeiten in der Zukunft ist sicher interessant, aber von einer Untersuchung oder Erarbeitung von Prognosen wird an dieser Stelle abgesehen. Als

wesentliche Festlegung für den empirischen Teil werden die derzeit gebräuchlichen Bezeichnungen in ihrer aktuellen Auslegung, wie erläutert, verwendet.

Zusammenfassend kann das ITSCM als technischer Anteil des Business Continuity Managements verstanden werden, der nach Festlegungen in Standards wie ITIL den Grundprinzipien der Initiierung, der Analyse, des Designs, der Implementierung und der regelmäßigen Kontrolle folgt. Das Ziel ist hier analog zum Business Continuity Management die Aufrechterhaltung des Betriebes auch in Ausnahmesituation bzw. eine zeitgerechte Wiederherstellung der kritischen IT-Services.

2.1.5 Relevante Normen, Gesetze und Best Practices

Normierende Vorgaben, Gesetze und bereits wissenschaftlich betrachtete Best Practices sind für diese Forschungsarbeit von besonderem Interesse. Einerseits bilden sie eine allgemeingültige Grundlage und ermöglichen eine Vergleichbarkeit, andererseits steht im Fokus der Dissertation die Frage, inwiefern derartige Vorgaben im Zuge der Digitalisierung in der Praxis noch berücksichtigt werden. Für die Erstellung von Empfehlungen bietet es sich an, herauszufinden, welche Best Practices nach aktuellem Stand in der Praxis angewandt werden und welche mit Blick auf die rapide Digitalisierung noch geeignet sind. Kritisch merkt Petrenko (2021, S. 139) in diesem Kontext an, dass Normen und Standards keine Verpflichtungen darstellen. Der Autor weist darauf hin, dass diese nicht aus wissenschaftlicher Forschung entstanden sind und dass das Entwickeln eigener Standards mit Kompatibilitätsproblemen verbunden sein kann. Vor diesem Hintergrund werden die nachfolgenden Standards ausführlich vorgestellt, um die später entwickelten Empfehlungen darauf zu referenzieren.

<u>Normen</u>

Von der International Standardization Organization (ISO) wurde im Jahr 2012 die Norm 22301 mit dem Titel „Business Continuity Management System“ herausgegeben. Die aktuelle Version von November 2019 trägt als Europäische Norm (EN) das Kürzel: EN ISO 22301, die deutsche Fassung wird dort als DIN EN ISO 22301:2020-06 bezeichnet (DIN EN ISO 22301, 2020, S. 5), wobei 2020-06 hier für Juni 2020 steht (DIN EN ISO 22301, 2020, S. 1).

Die Norm enthält Begriffsdefinitionen und legt die Anforderungen an ein Business Continuity Management System (BCMS) fest. Der Aufbau und der Betrieb eines BCMS ist dabei nicht optional, sondern eine zwingende Voraussetzung. Die gesamte Verantwortung hierzu sieht die Norm bei der Geschäftsführung bzw. der Leitung des jeweiligen Unternehmens (DIN EN ISO 22301, 2020, S. 18).

Spörrer erläutert die Norm und kommt zu dem Schluss, dass diese erstmals die Möglichkeit bietet, Business Continuity Management Systeme grundsätzlich, aber auch international zu vergleichen (2018, S. 130). Seine Ausführungen zu Kapitel 1 der Norm widmen sich dem Anwendungsbereich. Als Zielgruppe wird jegliche Art von Organisation definiert, die ein Business Continuity Management System aufbauen und betreiben möchte (Spörrer, 2018, S. 96). Im Kontext des IT-Notfallmanagements und des ITSCM besitzt die ISO-Norm 22301 eine hohe Relevanz. Ihr Inhalt und ihre Umsetzung werden in der gesamten Arbeit mit betrachtet. Osterhage hebt bei den Merkmalen der ISO-Norm 22301 hervor, dass die Leitungsebene einer Organisation nicht nur eingebunden werden muss, sondern Business Continuity Management auch aktiv voranzutreiben hat und dass hierfür Ressourcen bereitzustellen sind (2016, S. 8).

Bereits in der Einleitung der ISO-Norm wird die Zielrichtung deutlich, dass es hier um ein System geht, bei dem einerseits die Aufrechterhaltung des Betriebes im Fokus steht und andrerseits wird auch das Überstehen der Organisation bei Störungen angesprochen (DIN EN ISO 22301, 2020, S. 6). Neben dieser Norm existieren zahlreiche weitere Normen und Standards, die hier von Relevanz sind. Passend zum Business Continuity Management wurde unter der Bezeichnung „BCM-Standards“ im Jahr 2023 vom BSI die nachfolgende Übersicht veröffentlicht:

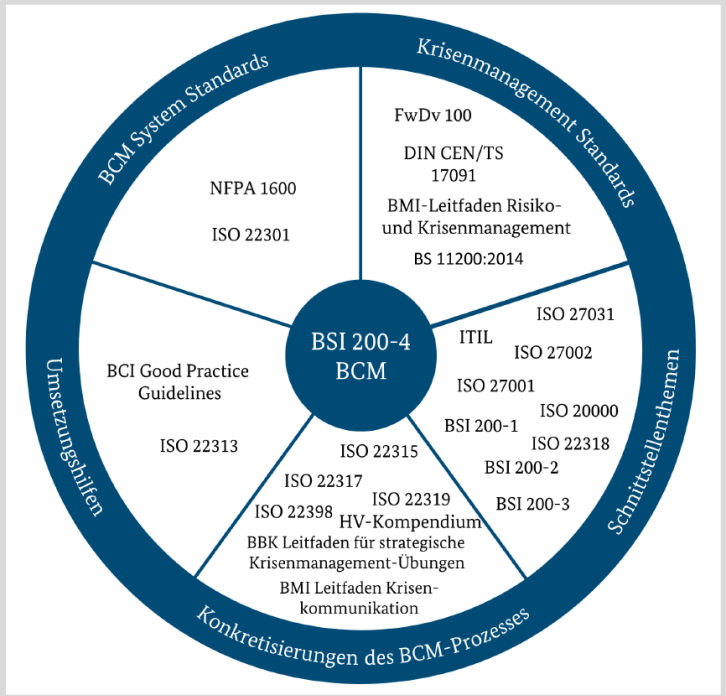


Abbildung 15 – „Übersicht über BCM-Standards sowie korrespondierende Sicherheitsthemen“ (Quelle: BSI, 2023, S. 39)

Grundsätzlich alle hier abgebildeten und im äußeren Kreis kategorisierten Begriffe werden nachfolgend angesprochen, bewertet oder erläutert. Auf eine tiefere Analyse der NFPA 1600 („Standard on Continuity, Emergency, and Crisis Management“ der National Fire Protection Association, USA) wird hier aufgrund der vorrangig nationalen Ausrichtung verzichtet. Auch auf die allgemeinen Krisenmanagementstandards ohne direkten IT-Bezug (rechts oben in Abbildung 15 dargestellt) wird nicht eingegangen. Zur Erläuterung dieser Standards ist zunächst für alle Begriffe in der nachfolgenden Tabelle die Langbezeichnung aufgeführt, anhand derer bereits auf den Inhalt geschlossen werden kann:

Kürzel	Titel bzw. Langbezeichnung
ISO 20000	Informationstechnik – Service Management
ISO 22301	Sicherheit und Resilienz – Business Continuity Management System
ISO 22313	Sicherheit und Resilienz – Business Continuity Management System – Anleitung zur Verwendung von ISO 22301
ISO 22315	Sicherheit und Schutz des Gemeinwesens – Massenevakuierung – Leitfaden für die Planung
ISO 22317	Sicherheit und Resilienz – Business Continuity Management System – Leitfaden für die Business Impact Analyse
ISO 22318	Sicherheit und Resilienz – Business Continuity Management System – Leitfaden für das Supply Chain Continuity Management
ISO 22319	Sicherheit und Resilienz – Resilienz der Gesellschaft – Leitfaden für die Planung der Einbindung spontaner freiwilliger Helfer
ISO 22398	Sicherheit und Schutz des Gemeinwesens – Leitfaden für das Üben und Erproben
ISO 27001	Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen
ISO 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen
ISO 27031	Informationstechnik – Cybersicherheit – Informations- und Kommunikationstechnologische Bereitschaft für Geschäftskontinuität
BSI 200-1	Managementsysteme für Informationssicherheit (ISMS)
BSI 200-2	IT-Grundschutz-Methodik
BSI 200-3	Risikomanagement
BSI 200-4	Business Continuity Management
ITIL	Information Technology Infrastructure Library
BCI GPG	Business Continuity Institutes (United Kingdom), Good Practice Guidelines
HV Kompendium	Hochverfügbarkeitskompendium
BKK Leitfaden	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Leitfaden für strategische Krisenmanagement-Übungen
BMI Leitfaden	Bundesministerium des Inneren und für Heimat Leitfaden Krisenkommunikation

Tabelle 3 – Auszug BCM-Standards gemäß BSI (Quelle: eigene Darstellung)

Die bereits genannte ISO-Norm 22301 ist hier als einzige ISO-Norm gemäß Abbildung 15 der Kategorie ‚Systemstandard' zugeordnet. Die weiteren Normen sind den Sektoren ‚Hilfen', ‚Konkretisierungen' oder ‚Schnittstellenthemen' subsumiert. Die konkrete Untersuchung zum

Business Continuity Management fokussiert damit die ISO 22301 als zentrales Vorgabedokument. National und im Zentrum der Abbildung dargestellt ist der BSI-Standard 200-4. Alle weiteren Normen und Standards sind eher thematisch unterstützend zu sehen und werden daher hier nicht im Detail vorgestellt. Da die Möglichkeit besteht, dass sich Unternehmen und Organisationen nach einer ISO-Norm zertifizieren lassen können, wurde die aktuelle und weltweite Verbreitung der erteilten Zertifikate nach ISO 22301 ermittelt und diese stellt sich wie folgt dar.

Roselieb geht davon aus, dass eine Zertifizierung nach der ISO-Norm 22301 im weltweiten Vergleich zur ISO 9001 (Qualitätsmanagement) noch als Ausnahme anzusehen ist, und stellt erhebliche länderspezifische Unterschiede fest. Nach seiner Analyse war im Jahr 2020 Großbritannien führend mit 336 Zertifikaten und Deutschland stand dem, wie der Autor es formuliert, mit „gerade einmal 33“ Zertifikaten gegenüber (Roselieb, 2022, S. 73). Die Anzahl der erteilten Zertifikate wird von der ISO im Internet unter der Adresse *https://www.iso.org/the-iso-survey.html* veröffentlicht. Die im Juni 2023 verfügbaren Zahlen mit Stand der erteilten Zertifikate bis zum 31.12.2021 sind in der nachfolgenden Tabelle abgebildet, wobei eine Filterung auf die relevanten Anteile, z. B. öffentliche Verwaltung, erfolgt ist. Ebenfalls wurden nicht alle der 106 im Bericht genannten Länder aufgeführt. Hierzu wurde eine Reihenfolge der ersten 20 Länder mit den meisten Zertifizierungen gebildet. Von den im Bericht genannten 39 Sektoren wurden nur die ausgewählt, bei denen eine direkte Assoziierung mit der öffentlichen Verwaltung oder der öffentlichen Sicherheit nachvollziehbar ist. Andere Bereiche, beispielsweise Schiffsbau, metallverarbeitendes Gewerbe oder Hotels/Gastronomie, wurden für die Übersichtlichkeit ausgeblendet. Deren Anzahl ist in den Gesamtsummen enthalten.

ISO 22301 Zertifizierungen Stand: 31.12.2021			Sektoren (Auswahl)							
	Land	Sum	Electricity supply	Gas supply	Water supply	Transport, storage and communication	Information technology	Public administration	Sector, unknown	Sector, other
1	United Kingdom	**446**	1			57	19	3	240	126
2	India	**178**	3			52	32		67	24
3	Korea (Republic of)	**173**	3			10	3	5	55	97
4	Turkey	**150**				6	110		20	14
5	China	**134**							131	3
6	Singapore	**125**			1	15	13		19	77
7	United Arab Emir.	**111**	1			11	10	17	49	23
8	Greece	**95**				3	20		14	58
9	Thailand	**82**	10	1	1	17		2	3	48
10	Japan	**73**				8	10		5	50
11	Italy	**69**					2		66	1
12	USA	**57**				7	14		19	17
13	Spain	**52**			1	25	10	2	7	7
14	Netherlands	**50**				2	1		35	12
15	Germany	**49**				5	8		33	3
16	Saudi Arabia	**49**		2		7	4	1	17	18
17	Philippines	**44**	3		1	3	10		15	12
18	Poland	**42**	2	2	1	6	6	1	15	9
19	Nigeria	**41**				3	5	1		32
20	Serbia	**38**				3	8		18	9

Tabelle 4 – ISO 22301 Zertifizierungen (Quelle: eigene Darstellung auf Basis der ISO Survey 2021 unter https://www.iso.org/the-iso-survey.html [abgerufen am 06.07.2023])

Da für Deutschland bei insgesamt 49 Zertifizierungen eine Sektorenzuordnung für 33 nicht veröffentlicht ist, ist eine Auswertung dieser Zuordnungen nicht vollständig möglich. Allerdings zeigt sich, auch im Vergleich zu den anderen Ländern, dass Deutschland im Bereich öffentliche Verwaltung („Public Administration“) noch keine Einträge vorweisen konnte. Damit wird auf Basis der Anzahl der ISO-Norm-22301-Zertifizierungen insgesamt bestätigt, dass das genormte Business Continuity Management in Deutschland noch nicht nachweisbar verbreitet ist. Andere, auch kleinere Länder wie Griechenland oder Singapur sind hier quantitativ in der Gesamtsumme deutlich weiter. Auch im Bereich der öffentlichen

Verwaltung gibt es Länder, die bereits Nachweise erbracht haben. Der herausragende Zertifizierungsstand von Großbritannien ist hier nicht Bestandteil der Untersuchung.

Als Zwischenfazit ist festzuhalten, dass die ISO 22301 für ein Business Continuity Management System eine anerkannte und empfohlene Orientierung ist. Eine Zertifizierung danach findet aber in Deutschland eher selten statt. Die Anzahl der Zertifikate hat sich in Deutschland vom Jahr 2020 mit 33 zum Jahr 2021 mit 49 um lediglich 16 erhöht. Wie sich die Situation hierzu in der Praxis darstellt, wird im empirischen Teil hinterfragt.

Die ISO-Norm 27001 behandelt die Themen der IT-Sicherheit. Damit kommt ihr im Rahmen der Themenblöcke dieser Arbeit ebenfalls eine relevante Rolle zu. Mit Bezug zu steigenden Risiken durch verstärkte Vernetzung misst Disterer einem Information Security Management System (ISMS), wie es die ISO-Norm 27001 vorsieht, eine hohe Bedeutung bei (2013, S. 98). Für vergleichbare nationale Zertifizierungen in Deutschland erläutert Disterer die Beziehungen der ISO-Norm 27001 zum IT-Grundschutz gemäß dem BSI. Seit 2006 ist diese Zertifizierung nach BSI-IT-Grundschutz konform zum internationalen Standard ISO 27001 (2013, S. 97). Kersten et al. bestätigen das und sehen eine vielfach über den Standard der ISO 27001 hinausgehende Zertifizierung, wenn eine Organisation sich nach dem BSI zum IT-Grundschutz zertifizieren lässt (2017, S. 8).

Auf die anderen in Tabelle 3 genannten Normen wird kontextbezogen in weiteren Kapiteln eingegangen. Eine ausführlichere Erläuterung aller Hintergründe und Verbreitungszahlen sämtlicher unterstützender Normen sind für die Beantwortung der Forschungsfragen nicht notwendig und würde den Rahmen dieser Arbeit übersteigen. Nach der Vorstellung der Normen werden nun weitere relevante Standards erläutert.

<u>BSI 100-4 und BSI 200-4</u>

Eine ganzheitliche Sicht auf die Thematik Business Continuity ist im BSI-Standard 100-4 zu finden (Kersten et al., 2013, S. 259). Dieser Standard wurde bereits in der Ausgangslage genannt und in Kapitel I 2.1.2 diskutiert. Der Standard unter der Bezeichnung „Notfall-management“ wurde im Jahr 2008 veröffentlicht (BSI, 2008, S. 1). Enthalten ist eine Methodik, mit der ein behördenweites und auch unternehmensweites Notfallmanagement aufgebaut und aufrechterhalten werden kann (Spörrer, 2018, S. 35). Merschbacher beschreibt es als systematischen Weg, der mit dem Standard BSI 100-4 aufgezeigt wird, um die Geschäftskontinuität sicherstellen zu können. Er spricht von der Absicherung der Existenz von Behörden auch bei größeren Schadensereignissen (2018, S. 509). Im Januar 2021 wurde ein erster Community Draft (CD) des BSI-Standards 200-4 veröffentlicht, der auf Basis des

vorherigen Standards BSI 100-4 neu konzipiert wurde. Der neue Standard soll als Anleitung dienen, wenn eine Organisation die Anforderungen der ISO-Norm 22301:2019 umsetzen möchte (BSI, 2023, S. 11). Nach einer weiteren Version des Community Drafts im August 2022 wurde die finale Version 1.0 im Mai 2023 fertiggestellt und im Juni 2023 veröffentlicht (BSI, 2023, S. 11).

Von hoher Bedeutung für diese Forschungsarbeit ist, dass bereits zu Beginn der Erstellung des Exposés der neue Standard unter der Bezeichnung „Business Continuity Management" bekannt und im Entwurf vom BSI verfügbar war. Während der empirischen Phase stellte sich heraus, dass dieser kommende Standard bereits bei den Experten der Branche bekannt ist. Die dann im Jahr 2023 veröffentlichte Version enthält nur wenige Veränderungen, beispielsweise die Anpassung an eine geschlechtergerechte Formulierung. Damit sind die in den Jahren 2022 und 2023 durchgeführten Gespräche und erarbeiteten Analysen, die sich auf diesen Standard beziehen, weiterhin uneingeschränkt verwertbar. Es wurde insgesamt auch nicht ausschließlich auf den BSI-Standard fokussiert, sondern das Business Continuity Management wurde im Rahmen der Digitalisierung im fachlichen Sinne untersucht. Der nun hinsichtlich des Titels gleichlautende Standard des BSI bleibt ein relevantes Bezugsdokument, da es auch in der Praxis eine entsprechende Bedeutung hat.

Der Inhalt des BSI-Standards 200-4 ist wie folgt gegliedert:

Kapitel	Titel
1	Einleitung
2	Was ist Business Continuity Management (BCM)?
3	Initiierung des BCMS durch die Institutionsleitung
4	Konzeption und Planung des BCMS
5	Aufbau und Befähigung der BAO
6	BIA-Vorfilter
7	Business-Impact-Analyse
8	Soll-Ist-Vergleich
9	BCM-Risikoanalyse
10	Business-Continuity-Strategien und -Lösungen
11	Geschäftsfortführungsplanung
12	Wiederanlauf- und Wiederherstellungsplanung
13	Üben und Testen
14	Leistungsüberprüfung und Berichterstattung
15	Aufrechterhaltung und Verbesserung

Tabelle 5 – BSI 200-4 BCM, Kapitelstruktur (Quelle: eigene Darstellung nach BSI, 2023, S. 5-9)

Aus dieser Kapitelstruktur ist der ganzheitliche Ansatz des Standards erkennbar. Nach der Definition und Initiierung zu Beginn sind bereits erläuterte Themen wie die Business-Impact-Analyse (BIA) vorgesehen. Die Notwendigkeit einer besonderen Aufbauorganisation (BAO) wurde schon in Kapitel II 2.1.3.1 angesprochen. Ebenfalls der Bereich Strategieentwicklung und die Durchführung von Tests und Übungen wurden in den vorherigen Kapiteln aus anderen Perspektiven beleuchtet und zeigen sich hier konkret in den dortigen Kapiteln 10 und 13.
Aus der Bezeichnung des Kapitels 15 des Standards („Aufrechterhaltung und Verbesserung“) wird ersichtlich, dass die hier in Kapitel II 2.1.3 bereits genannten Prozesswiederholungen durch die notwendige Aufrechterhaltung und Verbesserungen des Systems abzubilden sind. Weitere wissenschaftliche Analysen und Bewertungen dieses jüngst veröffentlichten Standards waren zum Zeitpunkt der Erstellung dieser Arbeit noch nicht verfügbar. Diese Situation wird später im Forschungsausblick zur Diskussion gestellt.
International mehrfach zitiert wird das britische Business Continuity Institute (BCI) mit den veröffentlichten Leitlinien unter dem Titel „Good Practice Guidelines“ (GPG). Auf den Ursprung im Jahr 2002 und die Zielsetzung wird auch aus dem BSI-Standard 200-4 heraus verwiesen (BSI, 2023, S. 40).

<u>BCI GPG</u>

Die Edition 2018 dieser GPG wurde online unter der Internetadresse *https://www.thebci.org/* vom BCI zur Verfügung gestellt. Es sind sowohl kostenpflichtige als auch kostenfreie Versionen dort erhältlich. Wie bereits beim BCM-Lifecycle in Kapitel II 2.1.3.1 dargestellt, bilden die nachfolgenden Überschriften den Inhalt dieser Leitlinie ab. Diese sind nach ‚Professional Practices‘ (PP) benannt (BCI, 2018, S. 6):

PP1 Policy und Programme Management
PP2 Embedding
PP3 Analysis
PP4 Design
PP5 Implementation
PP6 Validation

Spörrer (2018, S. 35) erläutert die GPG des BCI und bezeichnet diese als einen Quasi-Standard und als eine sinnvolle Umsetzungshilfe. Petrenko (2021, S. 328) hat verschiedene Unternehmensberatungen im Bereich Continuity Management analysiert und beschreibt die GPG als einen wichtigen Ansatz. Er fasst diese Leitlinien so zusammen, dass damit Standards bereitgestellt werden, und weist darauf hin, dass hierfür bewährte Verfahren aus der Praxis

von den Mitgliedern des BCI entwickelt wurden, um damit die Umsetzung eines Business Continuity Managements zu unterstützen. Der Autor Ee sprach bereits 2014 von Problemen, die aus einer Vielzahl von Standards entstehen. In solchen Fällen sei es unmöglich zu wissen, welcher Standard der beste für das jeweilige Unternehmen ist (2014, S. 103). Neben den ISO-Normen 22301 und 22313 wurde die GPG dort als Best Practice genannt (Ee, 2014, S. 104).
Damit sind die relevanten Normen aufgeführt und sowohl der nationale Standard als auch internationale Leitlinien wurden vorgestellt. Im Folgenden wurde recherchiert, ob und wie in den Best Practices des IT-Managements das Business Continuity Managements berücksichtig ist.

Best Practices

Nach Limaj und Bernroider (2022, S. 7) gibt es im IT-Servicemanagement einige beliebte Frameworks, wie die „Information Technology Infrastructure Library“ (ITIL), die „Control Objectives for Information and Related Technology“ (COBIT) und das „The Open Group Architecture Framework“ (TOGAF).
Die ITIL ist in der unternehmerischen Praxis für die Umsetzung von serviceorientierten IT-Managementprozessen nach Hochstein et al. (2004, S. 382) ein „De-facto-Standard“. Dieser vom Unternehmen AXELOS gepflegte Standard wird in der Praxis bereits häufig für den IT-Betrieb eingesetzt (BSI, 2023, S. 40-41). Ebenfalls wird darin erläutert, wie Institutionen damit die digitale Transformation gestalten können (BSI, 2023, S. 40). Bis 2019 war die Version 3 (v3) der ITIL relevant, die 2007 erschienen ist und mit der Standardprozesse für das IT-Servicemanagement definiert wurden. Im Jahr 2019 wurde die aktuelle Version 4 (v4) veröffentlicht, die nicht mehr Prozesse festlegt, sondern Praktiken empfiehlt. Für die erläuterte Agilität der Digitalisierung ist die Anpassbarkeit dieser Prozesse bzw. Praktiken zu beachten. Verlaine et al. (2016, S. 331) belegen, dass ITIL v3 nicht zu agilen Methoden passt. Damit wird das problematische Spannungsfeld zwischen Digitalisierung und Business Continuity Management im IT-Management verdeutlicht, wenn eine rapide voranschreitende Digitalisierung auf weniger agile Standards im IT-Management trifft. Ob ITIL in der 2019 veröffentlichten Version 4 mit Blick auf das Notfallmanagement effizientere Praktiken vorsieht bzw. wie sich ITIL in diesem Zusammenhang in der Praxis etabliert, wird im empirischen Teil hinterfragt. Grundsätzlich soll die aktuelle Version agile Werte, Praktiken und Methoden betonen (Limaj und Bernroider, 2022, S. 7). Moeller (2008, S. 221) misst dem ITIL Continuity Management eine außergewöhnlich hohe Bedeutung insofern zu, da mit der Anwendung von ITIL die Verbindung von Geschäftsfunktionen und IT-Prozessen hergestellt wird. Katastrophale

Ausfälle bei den IT-Services haben Auswirkungen auf alle Geschäftsebenen und ITIL sieht hier vor, dass für das Management und die IT entsprechende Continuity-Management-Prozesse entwickelt werden.

COBIT lässt sich als „Rahmenwerk für die IT-Governance“ (Allweyer, 2020, S. 84) bezeichnen. Schwerpunkt von COBIT ist die Erreichung der Unternehmensziele durch die optimale Ausrichtung der IT-Nutzung (Ridley et al., 2004, S. 1). Allweyer (2020, S. 90) bewertet es als nützliches Modell, kritisiert allerdings den hohen Aufwand, der die Nutzung in einem Unternehmen erschwert. Resch (2020, S. 268) erläutert ITIL und differenziert gegenüber COBIT die in ITIL deutlicher vorhandene Einbeziehung des Kunden. Bei der Betrachtung von IT-Dienstleistern ist dieser Aspekt der Kundenbeziehung von hoher Bedeutung, da auch die deutschen Behörden als Kunden dieser Dienstleister anzusehen sind.

Das TOGAF ist eine Methode, um neue Geschäftsprozessarchitekturen und die dazugehörige IT aufzubauen (Sofyana und Putera, 2019, S. 1). Business Continuity ist eines der Prinzipien von TOGAF, womit die Überlebensfähigkeit eines Unternehmens gesichert werden kann. Danach muss es möglich sein, dass die Geschäftsfunktion auch z. B. nach Naturkatastrophen mit alternativen Mechanismen der Informationsbereitstellung fortgeführt werden kann (Zadeh et al., 2012, S. 4274). Damit wäre sichergestellt, dass ein Business Continuity Management, wenn es beginnend beim Aufbau der Geschäftsprozesse nach TOGAF berücksichtigt wird, grundsätzlich bereits adressiert ist. Als Herausforderung gilt allerdings weiterhin, dass durch die fortschreitende Digitalisierung und die Aufrechterhaltung des Betriebes regelmäßige Anpassungen notwendig bleiben.

<u>Gegenüberstellung TOGAF, ITIL und COBIT</u>

Johanning (2020, S. 74) sieht ITIL und COBIT sich ergänzend und empfiehlt sie als Werkzeugkasten zu verstehen, aus dem jeweils geeignete Teile entnommen werden können. Dem Vorschlag folgend wurde die nachfolgende Gegenüberstellung generiert und um TOGAF ergänzt. Die im Kontext dieser Arbeit besonders relevanten Bausteine dieser Standards wurde verortet. Außerdem wurde die exakte Bezeichnung übernommen und zum jeweiligen Rahmenwerk nachfolgend aufgelistet. Zusätzlich werden die aktuelle sowie die vorherige Version mit dem Erscheinungsjahr genannt.

Bezeichnung	TOGAF	ITIL	COBIT
aktuelle Version (Erscheinungsjahr)	10th Edition (2022) 9.2th Edition (2018)	V4 (2019) V3 (2007)	COBIT 2019 (2018) COBIT 5 (2012)
Behandlung der BCM-Aspekte	Architecture Principles Business Principles Principle 4: **Business Continuity**	Service management practices: **Service continuity management**	Deliver, Service and Support (DSS), DSS04: **Managed continuity**
Fokus	Aufbau von IT- & Geschäftsprozess-architekturen	IT-Service-Management	Rahmenwerk IT-Governance

Tabelle 6 – Gegenüberstellung TOGAF, ITIL und COBIT (Quelle: eigene Darstellung)

Die Stärken der verschiedenen Ansätze lassen sich aus den zitierten Quellen und nach der Tabelle wie folgt zusammenfassen: TOGAF wird als etablierte Methode angesehen, mit der sich der Aufbau von IT- und Geschäftsprozessarchitekturen unterstützen lässt und das Vorgehen dabei den in TOGAF definierten Prinzipien folgt. Als Standard im IT-Management kann ITIL angesehen werden. ITIL definiert Praktiken für das IT-Servicemanagement und gilt, wie auf S. 70 bereits zitiert, als weit verbreitet und etabliert. Die Stärke von COBIT wird in der Unterstützung zur Einhaltung der IT-Governance gesehen, wodurch hier die Steuerung und die Einhaltung von Regeln und Vorgaben im Fokus stehen.

Damit sind die theoretischen Grundlagen zu diesen relevanten Rahmenwerken einleitend genannt. Im später folgenden Diskussions- und Gestaltungsteil wird auf sie referenziert. Welche Empfehlungen zur Vorgehensweise nach TOGAF, COBIT oder ITIL als Best Practices für das Continuity Management erstellt werden können, wird nach der Analyse und der Berücksichtigung des empirischen Teils diskutiert.

<u>Gesetze</u>

Bei den gesetzlichen Vorgaben in Deutschland sind beginnend das IT-Sicherheitsgesetz (IT-SiG) und das Bundesdatenschutzgesetz (BDSG) zu nennen. Kipker und Scholz (2021, S. 42) erläutern die aktuellen Entwicklungen im IT-SiG, wonach schon der Geltungsbereich, für welche Unternehmen sich Pflichten aus dem Gesetz ergeben, unklar ist. Aus dem BDSG ist § 64 zu nennen, der die „Anforderungen an die Sicherheit der Datenverarbeitung“ regelt. Dort heißt es im ersten Absatz, dass „ein dem Risiko angemessenes Schutzniveau zu gewährleisten ist“. Im zweiten Absatz werden explizit physische und technische Zwischenfälle angeführt, bei denen die Verfügbarkeit von personenbezogenen Daten „rasch“ wiederhergestellt werden

soll (§ 64 BDSG Absatz 2 Satz 2.). Die zitierte Wortwahl im BDSG zeigt auch hier, wie von Kipker und Scholz bereits zum IT-Sicherheitsgesetz analysiert, dass mit Unklarheiten aufgrund der ungenauen Formulierungen zu rechnen ist.

Im Zusammenhang mit dem IT-SiG erläutert Voigt das BSI-Gesetz (BSIG), durch das dort definierte Unternehmen verpflichtet werden, hohe IT-Sicherheitsstandards einzuhalten (2022, S. 107). Der Autor erläutert anhand der gesetzlichen Grundlagen nach § 2 Absatz 10 des BSIG, welche Unternehmen als Betreiber sogenannte kritischer Infrastrukturen (KRITIS) einzustufen sind (Voigt, 2022, S. 110-111). Als exemplarische Stichworte seien hier der Energiesektor, die Gesundheitsversorgung und das Transportwesen genannt. Zusätzlich muss bei deren Ausfall ein erheblicher Versorgungsengpass oder eine Gefahr der öffentlichen Sicherheit eintreten.

Auf europäischer Ebene verweist der Autor auf die Netz- und Informationssicherheits-Richtlinie (NIS-Richtlinie) und gibt den Hinweis auf die erwartete NIS-2-Richtlinie. Ziel der neuen Richtlinie ist eine weitere „Verbesserung der Resilienz und Reaktion auf Sicherheitsvorfälle öffentlicher und privater Einrichtungen auf dem Gebiet der Cybersicherheit“ (Voigt, 2022, S. 108-109).

Heuermann (2018, S. 132) diskutiert die von Bund und Ländern erlassenen E-Government-Gesetze und erkennt darin eine Verbesserung, beispielsweise im Bereich der persönlichen Identifizierung von Bürgern. Es werden aber noch Herausforderungen bei der Akzeptanz gesehen (Adelskamp, 2018, S. 73). Interessant ist, dass Heuermann (2018, S. 133) dabei in seiner Bewertung die Situation der IT-Dienstleister kritisch hinterfragt und am Beispiel von Polizei und Justiz thematisiert, dass selbst länderintern unterschiedliche IT-Dienstleister agieren.

Für das Business Continuity Management ist eine Vielzahl weiterer branchenspezifischer Gesetze in Deutschland relevant, die hier nicht im Einzelnen zu analysieren sind. Roselieb (2022, S. 15-16) referenziert unter anderem auf das Arbeitsschutzgesetz (ArbSchG), das GmbH-Gesetz (GmbHG), das Aktiengesetz (AktG) und das Kreditwesengesetz (KWG), die hiermit zumindest namentlich aufgezählt sind. Erwähnenswert für die digitale Transformation der öffentlichen Verwaltung in Deutschland ist das aus dem Jahr 2017 stammende Onlinezugangsgesetz (OZG). Nach Mergel (2019, S. 162) ist damit das Reformvorhaben zur Umstellung auf digitale Verwaltungsleistungen angestoßen worden. Von übergeordneter Bedeutung ist zudem die Richtlinie 2022/2555 der EU. Am 14. Dezember 2022 wurde diese NIS-2-Richtlinie mit „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau“

erlassen (EU, 2022b, S. 1). Als Grundstein für Netz- und Informationssicherheit (NIS) in der EU bezeichnen Bendiek und Stürzer (2022, S. 3) bereits die erste Richtlinie aus dem Jahr 2016. Inhaltlich sind hier verpflichtende Mindeststandards festgelegt, die Anbieter digitaler Dienste einzuhalten haben. Mit der neuen Richtlinie NIS-2 werden „massive Ausweitungen bei IT-Sicherheitspflichten“ erwartet (Vogel & Ziegler, 2023, S. 17).

Zusammenfassend lässt sich zu diesem Kapitel feststellen, dass verschiedene Vorgaben, Gesetze, Praktiken und Regelungen existieren, deren Anwendbarkeit und Flexibilität insbesondere aufgrund der Veränderungen durch die Digitalisierung hier untersucht werden. Dadurch werden Formulierungen von vertretbaren und realistischen Handlungs-empfehlungen für das IT-Management ermöglicht. Die sich dafür ergebenden empiriegeleiteten Fragestellungen werden in Kapitel II 3 nach der Zusammenfassung aufgestellt.

2.1.6 Die Begriffe Sicherheit, IT-Sicherheit und individuelles Sicherheitsempfinden

Der Begriff ‚Sicherheit‘ prägt das gesamte Forschungsvorhaben. In der Ausgangslage und der Problemstellung wurden sicherheitsrelevante Aspekte der Digitalisierung aufgezeigt und ein Business Continuity Management soll eine Betriebskontinuität absichern. Es werden in diesem Kapitel die Begriffe Sicherheit, IT-Sicherheit und Informationssicherheit erläutert. Im Vorgriff auf den empirischen Teil wird auch die Erfassbarkeit des persönlichen Sicherheitsempfindens von Personen kritisch betrachtet.

<u>Sicherheit</u>

Das Wort ‚Sicherheit‘ kann sprachlich auf die Formulierung ‚ohne Sorge‘ zurückgeführt werden. Hierbei ist stets zu konkretisieren, um was oder vor was sich jemand nicht sorgen muss (Frevel, 2016, S. 3,). Daraus folgt, dass der Begriff nicht isoliert, sondern oft in Kombinationen genutzt wird, beispielsweise bei IT-Sicherheit oder öffentliche Sicherheit. Der Begriff ‚Sicherheit‘ wird von Frevel wie folgt strukturiert dargestellt:

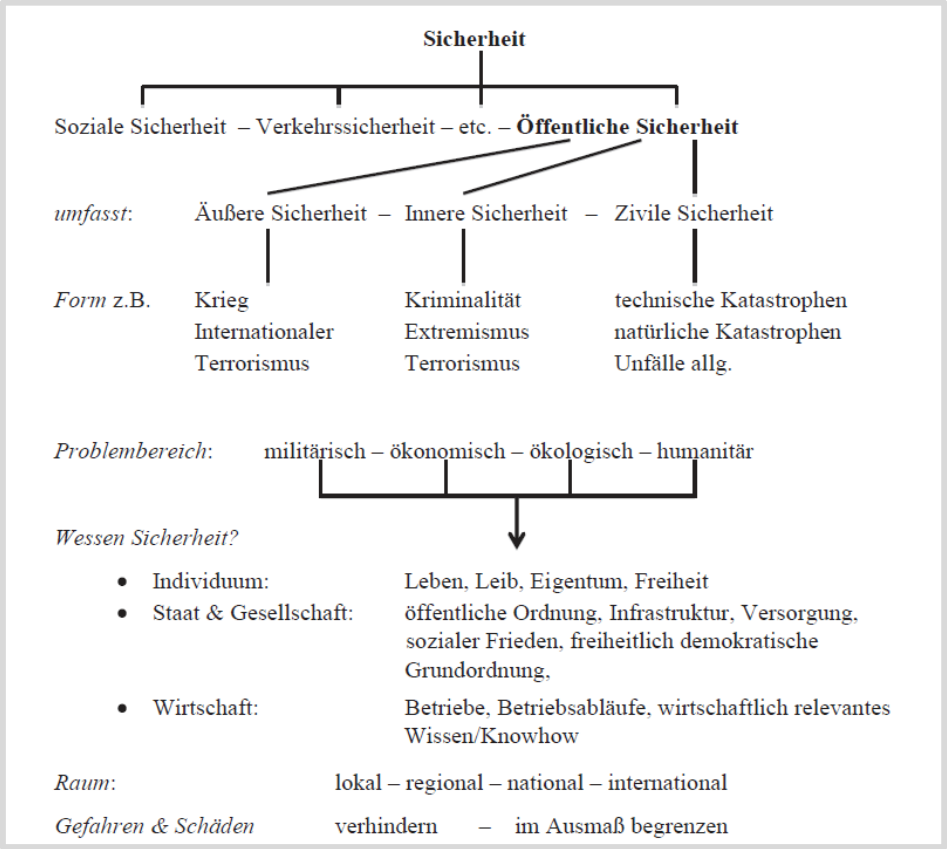


Abbildung 16 – Sicherheitsbegriff (Quelle: Frevel, 2016, S. 8)

Für den Kontext dieser Arbeit passend wird hier für den Anteil der öffentlichen Sicherheit die Unterteilung in äußere, innere und zivile Sicherheit vorgenommen. Beispielhaft werden bekannte Formen aufgelistet. Davon explizit im Fokus des Business Continuity Managements läge das gemeinsame Auftreten von technischen Katastrophen und natürlichen Katastrophen. Ebenfalls der Bezugspunkt „Wessen Sicherheit?“ ist hier in allen Punkten relevant. In der Ausgangslage gab es Auswirkungen auf Individuen in Form von Bürgern, gleichzeitig waren auch Staat und Gesellschaft sowie Unternehmen von den Sicherheitsproblemen betroffen. Bereits zum Business Continuity Management wurde ausgeführt, dass es nicht nur auf die Verhinderung von Gefahren ausgerichtet ist, sondern auch das Ausmaß von Schadensereignissen begrenzen soll, wie es ebenfalls in der Abbildung zur Definition von Sicherheit dargestellt ist.

Einen engen Zusammenhang des Begriffs mit Risiken und Gefahren konstatiert Müller (2015, S. 131-132) und bezeichnet Sicherheit als einen Risikobereich oberhalb eines Schwellwertes, wobei der Bereich darunter als Gefahr bezeichnet wird. In einer knapp gehaltenen Definition kann ‚Sicherheit‘ als „Abwesenheit von Gefahren“ (Witt, 2006, S. 1) charakterisiert werden. Die Menschen streben nach Sicherheit. Eine hundertprozentige Sicherheit kann es allerdings nicht geben. Es lassen sich nie sämtliche Bedrohungen ausschließen, die die menschliche

Sicherheit gefährden (Frevel, 2016, S. 33). Damit sind grundlegende Deutungen des Begriffes ‚Sicherheit' genannt und insbesondere mit Blick auf die Digitalisierung wird im Folgenden der Begriff ‚IT-Sicherheit' näher bestimmt.

IT-Sicherheit

Eckert (2023, S. 3) definiert die IT-Sicherheit über ihre Schutzaufgabe für Unternehmen. Es soll damit verhindert werden, dass durch den Verlust von Daten oder eine Störung der vom Unternehmen angebotenen Dienste wirtschaftliche Schäden entstehen. Interessanterweise weist auch diese Autorin direkt im nächsten Satz darauf hin, dass eine vollständige Vermeidung solcher Situationen nicht möglich ist und dass Schadensbegrenzungen sowie eine frühzeitige Erkennung ebenfalls Teil der IT-Sicherheit sind.

Eine besondere Bedeutung sieht Weber bei der IT-Sicherheit für die Digitalisierung und bewertet Erstere als Grundbedingung, damit die Digitalisierung gelingen kann (2017, S. 27). Aus Sicht der Digitalisierung weist er für die IT-Sicherheit auch auf Chancen hin, insofern damit IT-Sicherheitsprobleme erkannt werden können und die IT-Sicherheit sowie der Datenschutz berücksichtigt werden (Weber, 2017, S. 28). Ebenfalls bewertet Pohlmann (2018, S. 215) aus Sicht der Digitalisierung die IT-Sicherheit mit der Kapitelüberschrift „Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung" als entsprechend relevant. Es werden dort sechs Herausforderungen erläutert und in der Zusammenfassung sieht er zeitnahen Handlungsbedarf, um für eine angemessene IT-Sicherheit in der Gesellschaft zu sorgen (Pohlmann, 2018, S. 211). Als „Kernthema schlechthin" bezeichnet Neugebauer (2018, S. 5) die Sicherheit bei der Digitalisierung, so dass die IT-Systeme „immer und ausnahmslos im Interesse der Menschen funktionieren" sollen. Damit zusammenhängend sieht er in diesem Bereich einen hohen Forschungsbedarf (2018, S. 6). Darüber hinaus lässt sich die IT-Sicherheit auch als eine Enabling-Technologie bezeichnen, die neue Anwendungen und Dienstleistungen ermöglicht. Sogar eine Erhöhung der öffentlichen Sicherheit kann mit der Anwendung der Möglichkeiten der IT-Sicherheit erzielt werden (Eckert, 2023, S. 3).

Aus Sicht der IT-Sicherheit sehen Fallenbeck und Eckert (2017, S. 166) für die Digitalisierung die Notwendigkeit von neuen Sicherheitstechnologien. Das wurde konkret an den Themenfeldern Industrie 4.0 und Cloud-Computing untersucht und zeigt damit die stete Dynamik im Bereich der IT-Sicherheit. Hier besteht parallel zur Digitalisierung ebenfalls ein Weiterentwicklungsbedarf.

Zum Begriff ‚IT-Sicherheit' assoziiert Frevel einen Zusammenhang zur Abhängigkeit von der IT und erachtet dies als Gefahr. Als Schutz der IT-Systeme vor Angriffen sowohl auf die Software

als auch auf die Hardware mit äußerer Gewalt definiert der Autor den Begriff ‚IT-Sicherheit' (2016, S. 5). Als Übersetzung der Bezeichnung ‚IT Security' bezeichnet Porath die IT-Sicherheit ebenfalls prägnant als „Schutz von Computersystemen, Netzwerken, Programmen oder Daten vor Diebstahl, Manipulation oder Zerstörung" (2020, S. 163).

Hellmann (2023, S. 3) erläutert, dass IT-Sicherheit neben Begriffen wie Cybersecurity, Informationssicherheit oder Computersicherheit auch unter dem Begriff ‚Datensicherheit' gesehen werden kann. IT-Sicherheit konkret bezieht sich dabei eher auf die technischen Aspekte, wobei der Schutz der Informationssysteme im Vordergrund steht. Dieser bezieht sich darauf, die Hardware, die Software und jegliche Art von vertraulichen Daten zu schützen. Ebenfalls auf die Vielzahl von synonym genutzten Begriffen weist Harich (2021, S. 31) hin und stuft dabei den Bereich der dort englisch bezeichneten IT-Security als Untermenge der Informationssicherheit ein. Hierzu passend führt Mierowski (2021, S. 4) aus, dass sich IT-Sicherheit auf digital gespeicherte Daten bezieht. Wenn dagegen analoge Informationen einbezogen werden, so erläutert der Autor mit Verweis auf den BSI-Grundschutz, wird der Begriff ‚Informationssicherheit' genutzt. Bei einer Ausweitung der IT-Sicherheit auf sämtliche über das Internet verbundene Systeme inklusive ihrer „Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen" kann man es unter dem Begriff ‚Cybersicherheit' definieren (Pohlmann, 2019, S. 2).

Als Zwischenfazit ist zu den Begriffen der Sicherheit und der IT-Sicherheit festzustellen, dass es zwar in Nuancen verschiedene Auslegungen gibt, insgesamt aber ein gemeinsames Verständnis vorliegt. Insbesondere hinsichtlich der Relevanz der IT-Sicherheit für die Digitalisierung und der zukünftig steigenden Bedeutung von sicheren IT-Systemen konnten keine gegenteiligen Erkenntnisse oder Meinungen recherchiert werden. Damit kann die IT-Sicherheit als größte Herausforderung bei der Digitalisierung angesehen werden. Aufgrund der Parallelen des Begriffes ‚Sicherheit' mit den Definitionen des Business Continuity Managements sollte ebenfalls ein hoher Stellenwert des Business Continuity Managements in Unternehmen und Behörden erwartbar sein.

Individuelles Sicherheitsempfinden

Der Begriff ‚Sicherheit' wurde soeben hergeleitet und im Kontext reflektiert. Für den empirischen Teil war eine Erhebung von Praxiserfahrungen vorgesehen, bei der Experten aus der Branche interviewt wurden. Es stellte sich die Frage, wie und ob sich diese Sicherheit objektiv ermitteln und diskutieren lässt. Im Bereich der Kriminalistik wird von einem

subjektiven Sicherheitsgefühl des Einzelnen gesprochen. Untersuchungen haben ergeben, dass dieses Sicherheitsgefühl in keinem Zusammenhang mit der objektiven Gefährdungslage steht (Schewe, 2006, S. 323). So stellt auch Renn (2014, S. 49) zusammenfassend fest, dass eine große Diskrepanz zwischen der intuitiven Risikowahrnehmung und dem errechneten Risiko existiert. Sicherheitsrisiken werden in unserer Gesellschaft oft nicht korrekt gedeutet (Renn, 2014, S. 63).

Es war demnach schwierig, durch die Befragungen von Individuen zur Sicherheitseinschätzung objektive Ergebnisse zu erhalten, die in der Analyse verwendet werden können. Zur Qualitätssteigerung wurde in den geplanten Interviews einleitend eine persönliche Selbsteinschätzung zum eigenen Sicherheitsempfinden erfragt, um die Ergebnisse auf dieser Basis gewichten zu können. Im fachlichen Teil der Interviews wurde dann nicht direkt das persönliche Sicherheitsgefühl erfragt, sondern es wurde um eine Einschätzung zur Sicherheitsentwicklung in Deutschland gebeten. Damit wurden die soeben geschilderten Problematiken der Sozialforschung berücksichtigt.

2.1.7 Das GAIA-X-Projekt aus Sicht des Business Continuity Managements

Die Schlagworte Sicherheit, Souveränität, Cloud-Computing, Cloud-Anbieter und die IT der öffentlichen Verwaltung wurden in der Ausgangslage, der Problematik und der Darlegung der theoretischen Grundlagen bereits an verschiedenen Stellen genannt. Das GAIA-X-Projekt ist in diesem Zusammenhang aufgrund seiner konkreten Zielrichtung zu nennen. GAIA-X ist eine Initiative für Datensouveränität (Pohle & Thiel, 2020, S. 10), Datenaustausch und die Speicherung und Behandlung von Datenbeständen in Cloud-Plattformen (Otto, 2022, S. 9). Tardieu (2022, S. 41) erläutert, wie das Projekt 2019 aus einer Zusammenarbeit der Wirtschaftsministerien von Frankreich und Deutschland mit dem Ziel initiiert wurde, dass Unternehmen nicht die Kontrolle über ihre Daten verlieren sollen, sobald diese bei Nicht-EU-Cloud-Anbietern gespeichert sind. Nach der Gründung durch elf Unternehmen aus Deutschland und elf Unternehmen aus Frankreich (Draheim et al., 2021, S. 186) verfügte das Projekt 2022 bereits über 300 Unternehmen als Mitglieder aus 20 Ländern (Tardieu, 2022, S. 41). Ziel von GAIA-X ist es, mit einem Verbundsystem von Cloud-Anbietern ein Dateninfrastruktur-Ökosystem in Europa zu schaffen, um damit digitale Souveränität in Europa sicherzustellen (Bernhard & Steininger, 2021, S. 66).

Nach einer beauftragten Expertenbefragung trifft der Branchenverband Bitkom in einer im Jahr 2022 veröffentlichten Studie zu Rechenzentren in Deutschland folgend Aussage: „GAIA-X

erhöht die digitale Souveränität und führt zu einer sicheren und vertrauensvollen Dateninfrastruktur in Europa“ (Bitkom, 2022b, S. 35). In einer ebenfalls im Jahr 2022 veröffentlichten Studie kommen Lundborg et al. (2022, S. 38) allerdings zu dem Ergebnis, dass zu den Auswirkungen auf den Cloud-Markt durch GAIA-X derzeit noch keine Aussagen getroffen werden können. Zusätzlich weisen die Autoren darauf hin, dass insbesondere aus der öffentlichen Verwaltung die Nachfrage nach Cloud-Services mit dem Projekt steigen könnte. Kritisch fassen auch Lang und Kneuper (2022, S. 781) zusammen, dass aktuell durch mangelnde Transparenz eine Bewertung z. B. aus Sicht des Datenschutzes sehr schwierig sei. Erst in Zukunft könne sich dies ändern, da sich GAIA-X noch im Aufbau befindet.

Zusammenfassend kann das Projekt aus Sicht des Business Continuity Managements im Zeitalter der Digitalisierung ein bedeutender Baustein sein, um IT-Services auch deutscher Behörden zukünftig sicher und souverän zu betreiben. Auf Basis der theoretischen Ausführungen zur Digitalisierung sind mehrere Implikationen aus dem empirischen Teil dieser Arbeit erwartbar, die dann mit den Lösungsansätzen von GAIA-X zu diskutierten sind. Nach aktuellem Stand können es aber lediglich Prognosen sein, da, wie soeben dargelegt, GAIA-X noch als ein Zukunftsprojekt zu bezeichnen ist, dessen praktischer Nutzen sich erst bewähren muss. Ein hierzu empfohlener Forschungsbedarf ist im Ausblick dieser Arbeit nach der Berücksichtigung der aus der Praxis gewonnenen Erkenntnisse formuliert.

3 Konklusion Theoretischer Teil

In der Zusammenfassung der Rechercheergebnisse des theoretischen Teils werden zuerst die Grundlagen aus der wissenschaftlichen Literatur und aus den relevanten Studienergebnissen fokussiert auf die Forschungsfragen betrachtet. Die zur Beantwortung der Forschungsfragen insgesamt notwendigen empiriegeleiteten Fragestellungen für die spätere Erhebung werden am Ende dieses Kapitels abgeleitet.

3.1 Konklusion und Beantwortung der theoriegeleiteten Fragestellung

Zunächst werden die betrachteten Themenfelder bewertet, um anschließend damit konkret die Forschungsfragen zu beantworten. Die Aussagen basieren auf den recherchierten theoretischen Ergebnissen, wodurch der Stand der Forschung dargestellt wird. Darüber hinaus werden Defizite aufgezeigt, um die bereits erläuterte Forschungslücke weiter zu schärfen.

3.1.1 Zusammenfassung Theorie

In Kapitel II 1.1 wurden die Grundlagen zur Ermittlung des Forschungsstandes dargestellt. Bei der Recherche war auffällig, dass der Bereich Digitalisierung durch zahlreiche Fundstellen in wissenschaftlichen Zeitschriften und Datenbanken viele und aktuelle Informationsquellen bietet. Für die Thematik Business Continuity Management gibt es im Vergleich deutlich weniger Forschungsergebnisse, die hier berücksichtigt werden konnten. Zum Bereich der IT in Deutschland und speziell im öffentlichen Sektor existieren zwar Studienergebnisse, die allerdings nicht auf das Business Continuity Management fokussieren. Als Ergebnis kann hier festgehalten werden, dass die allgemein bekannte Situation bezüglich eines Nachholbedarfes bei der Digitalisierung in Deutschland und im Bereich des E-Governments durch die Forschungsliteratur bestätigt wird.

Die Internationalität dieser Arbeit konnte aus mehreren Perspektiven bestätigt werden: Die Digitalisierung ist ein globales Thema und das Business Continuity Management ist hinsichtlich seiner Entstehung und Fortentwicklung sowie bei den Prognosen nicht nur für Deutschland eine Herausforderung. Rein nationale Lösungen sind in diesem Kontext derzeit nicht erkennbar. Deutschland sucht im Rahmen des GAIA-X-Projektes einen EU-weiten Ansatz und ist zur Nutzung von aktuellen Digitalisierungstechnologien auf Services und Produkte internationaler Anbieter angewiesen.

Die Recherchen im Bereich der Unternehmenssicherheit zeigten analog zur Digitalisierung einen weiteren Handlungsbedarf im Bereich des Business Continuity Managements. Es wurde bereits die herausgehobene Bedeutung der IT-Sicherheit für eine erfolgreiche und sichere Digitalisierung deutlich.

Kapitel II 1.2 skizziert die Forschungslücke, die sich wie folgt zusammenfassen lässt und damit kongruent zur Hauptforschungsfrage formuliert ist:

- Wie ist die Situation des Business Continuity Managements im Zeitalter der Digitalisierung und mit welchen Erfolgsfaktoren kann eine möglichst sichere Digitalisierung, auch in der öffentlichen Verwaltung, ermöglicht werden?

Da es international große Unterschiede im Entwicklungsstand von digitalen Verwaltungen gibt, wie unter anderem die zitierten DESI-Ergebnisse belegen, erfolgen die weitere Analyse und Erhebung von Erfahrungen aus der Praxis bezogen auf Deutschland. In Kapitel II 1.3 sind die theoriegeleiteten Fragestellungen formuliert, die im nachfolgenden Kapitel beantwortet werden.

Kapitel II 2 beinhaltet zu allen relevanten Themenfeldern die theoretische Aufarbeitung der Rechercheergebnisse im Kontext der Forschungsfragen. Die herausragende Bedeutung der weiteren Digitalisierung für die Gesellschaft, die Unternehmen und auch die staatlichen Institutionen wurde belegt. Allein aus der technologischen Sicht besteht die Digitalisierung aus einer Vielzahl an Facetten. Hier in der Zusammenfassung wird auf die besondere Bedeutung des Cloud-Computings hingewiesen, das technologisch, rechtlich und mit Blick auf die IT-Sicherheit diskutiert wird. Aber auch die weiteren Aspekte und Technologien sollen in der Analyse mit den zu erhebenden empirischen Daten und den auszuarbeitenden Ergebnissen bewertet werden.

Die Begriffe IT-Management, IT-Notfallmanagement und Business Continuity Management wurden erläutert und stecken den wesentlichen Rahmen aus Sicht des Managements ab, um Digitalisierungsprojekte sicher, effizient und effektiv gestalten zu können. Hervorgehoben werden die Business-Impact-Analyse und der PDCA-Zyklus, die hier aus verschiedenen Perspektiven relevant und bewährt sind. Normierende Vorgaben wie die ISO-Norm 22301 und der BSI-Standard 200-4 sind vorhanden und aktuell. Auch bei den gesetzlichen Vorgaben sind aus Sicht der Theorie bereits viele Grundlagen geschaffen worden. Zu den Best Practices wird zusammengefasst, dass hier unterschiedlich argumentiert wird, inwiefern ITIL, COBIT oder TOGAF aus Sicht des Business Continuity Managements zielführend eigesetzt werden kann. Es wurden zwar keine grundsätzlich problembehafteten Aussage in diesem Zusammenhang

ermittelt, allerdings gab es auch keine eindeutigen Hinweise, nach denen hier priorisiert vorgegangen werden sollte. Damit bleibt es weiterhin eine explorative Teilaufgabe für die empirische Untersuchung, diesbezüglich valide Erkenntnisse zu ermitteln.

Zu den wesentlichen Begriffen ‚Sicherheit' und ‚IT-Sicherheit' gibt es in der Literatur keine grundsätzlich unterschiedlichen Ansichten. Dass es keine hundertprozentige Sicherheit geben kann, wurde bestätigt und gleichzeitig wurde die IT-Sicherheit als relevantester Aspekt herausgestellt. Sogar die Funktion als ‚Enabler' für die Digitalisierung wurde der IT-Sicherheit zugesprochen.

Mit der Ausarbeitung des theoretischen Teils und durch die Berücksichtigung von Hinweisen aus der Literatur zum GAIA-X-Projekt wurden der Hintergrund und der Sachstand zu GAIA-X ermittelt. Offensichtlich wird noch an mehreren Herausforderungen gearbeitet, die aktuell als wesentlicher Handlungsbedarf für eine sichere Digitalisierung mit Blick auf das Business Continuity Management gesehen werden. Es wurde festgestellt, dass das Projekt noch am Anfang steht (Lundborg et al., 2022, S. 38). Deshalb waren für die durchzuführende empirische Untersuchung noch keine praxisbezogenen Erkenntnisse zu erwarten. GAIA-X ist dennoch in der Gesamtbewertung und bei der Erstellung von Empfehlungen grundsätzlich mit zu betrachten.

Nach dieser Zusammenfassung und Berücksichtigung der genannten Aspekte der theoretischen Ausführungen werden die theoriegeleiteten Fragestellungen im folgenden Kapitel beantwortet.

3.1.2 Beantwortung der theoriegeleiteten Fragestellung

Die eingangs in der Zielstellung genannten Fragen lassen sich nun wie folgt beantworten.

- Welche Facetten der Digitalisierung stehen in einem engen Zusammenhang mit der in der Problemstellung genannten Situation?

Die weitere Digitalisierung ist unaufhaltsam und muss in immer schnelleren Innovationszyklen umgesetzt werden. Das birgt mit Bezug zur Problemstellung grundsätzlich die Gefahr, dass die benötigten Sicherheitsvorkehrungen nicht zeitgerecht oder ausreichend berücksichtigt werden können. Als weitere Facette wurde explizit die IT-Sicherheit in der Theorie als eine Grundvoraussetzung für die Digitalisierung genannt. Technologisch wurde das Cloud-Computing als ein besonderer Aspekt der Digitalisierung herausgestellt, der in mehreren Punkten für die Problemstellung relevant ist. Der infrastrukturelle Betrieb dieser IT und deren

Absicherung im Sinne der IT-Sicherheit wird an die Cloud-Provider ausgelagert. In diesem Zusammenhang ist die Datensouveränität bereits eine Herausforderung, die weiter zunimmt. Einleitend weisen viele Quellen darauf hin, dass mit der Digitalisierung weniger die technischen Weiterentwicklungen im Fokus stehen, sondern dass diese als Transformationsprozess insgesamt zu verstehen ist, der in einem hohen Maße die Abläufe, Geschäftsmodelle und Services von Unternehmen und Behörden ganzheitlich verändern wird. Es sind es diese Veränderungen der Dienstleistungen, die notwendigen schnellen Umsetzungen, die Fragestellung nach dem geeigneten infrastrukturellen Betrieb mit ausreichender IT-Sicherheit sowie die steigende Abhängigkeit von der IT, die in einem engen Zusammenhang mit der Problemstellung stehen. Als Facette der Digitalisierung zählt hierzu auch ein drohender Kontrollverlust oder eine länger andauernde Serviceunterbrechung bei Ausfall der IT, wovon bereits die Darstellungen in der Ausgangslage und der Problemstellung geprägt waren. Für die weitere Ausarbeitung sind diese Aspekte im Schwerpunkt im Rahmen der empirischen Phasen weiter zu untersuchen und dafür ist es vorgesehen, die Beantwortung dieser Frage auch anhand der Erkenntnisse aus der Praxis zu verifizieren. Mit der nächsten Frage werden die Schwierigkeiten und die positiven Effekte aufgezeigt, die auf Basis der Theorie zu erwarten sind.

- Welche positiven oder negativen Auswirkungen sind mit der Einführung neuer Technologien in Bezug auf die IT-Notfallvorsorge grundsätzlich zu erwarten?

Positiv für das Business Continuity Management, welches eine IT-Notfallvorsorge vorsieht, ist herauszustellen, dass bei Einhaltung der IT-Sicherheit auch Chancen hinsichtlich der Digitalisierung gesehen werden, um etwaigen Nachholbedarf aus den letzten Jahren zu berücksichtigen. Am Beispiel des bereits genannten Cloud-Computings können moderne Datensicherungskonzepte genutzt werden, wie sie von den Cloud-Anbietern konzipiert, gepflegt und weiterentwickelt werden. Als Paradoxon hierzu ist der damit verbundene Kontrollverlust oder der Verlust der Souveränität zu sehen, wenn Organisationen sich in diese Abhängigkeiten begeben. Ebenfalls negativ ist die steigende Komplexität einzustufen, wenn die zukünftigen Prozesse noch mehr automatisiert, vernetzt und untereinander integriert ablaufen werden. Für die Beherrschbarkeit und die Etablierung von Rückfallpositionen, wenn diese automatisierte IT-Unterstützung ausfällt, werden dann deutlich umfangreichere Arbeiten notwendig. Nach dieser grundsätzlichen Betrachtung werden mit der nächsten Fragestellung einzelne Herausforderungen konkretisierter beantwortet.

- Welche neuen Herausforderungen entstehen für das IT-Notfallmanagement durch welche Aspekte der Digitalisierung?

Aus Projektsicht muss sich durch die angezeigte Geschwindigkeit der Digitalisierung das IT-Notfallmanagement ebenfalls entsprechend agil positionieren. Bei vollautomatisierten Prozessabläufen in der digitalen Welt sind analog auch die IT-Notfallmechanismen möglichst vollautomatisiert zu gestalten, um hier kompatibel zu bleiben. Lösungen aus dem IT-Notfallmanagement, die vormals noch durch manuelle Aktivitäten geprägt waren – beispielsweise Neuinstallationen von Servern und Zurückladen von Backups –, passen vom Ansatz her nicht mehr zu vollständig automatisierten Prozessabläufen. Outsourcing und die Nutzung weiterer, neuerer Services von externen Dienstleistern stellen das IT-Notfallmanagement vor eine weitere Herausforderung, hier die Notfallprozesse im eigenen Unternehmen im Zusammenwirken mit den externen Komponenten zu synchronisieren.

Durch die weitreichende Vernetzung muss das IT-Notfallmanagement zunehmend die Abhängigkeiten, Datenflüsse und Kommunikationsbeziehungen berücksichtigen und absichern, um bei Ausfällen schnellstmöglich wieder funktionierende Systeme zur Verfügung stellen zu können. Es müssen neue Ausfall- und Angriffsszenarien bewertet werden, die vor der weiteren Digitalisierung in dieser Form noch nicht existierten.

Zusammenfassend muss sich das Business Continuity Management eines Unternehmens oder einer Behörde ganzheitlich den mit der Digitalisierung erwartbaren Veränderungen stellen. Prozessual, technologisch und organisatorisch muss es sich im gleichen Tempo wie die Digitalisierung weiterentwickeln, damit die Eintrittswahrscheinlichkeit und die Schadenshöhe von IT-Katastrophen nicht mit jedem weiteren Schritt in Richtung Digitalisierung zunehmen.

Neben der Betrachtung der Digitalisierung wurde das Business Continuity Management auch in der Theorie untersucht. Durch die Beantwortung der folgenden Frage werden die Anknüpfungspunkte herausgearbeitet, bei denen Handlungsempfehlungen zielorientiert und effektiv eingebracht werden können.

- Welche Faktoren beeinflussen maßgeblich den Auf- und Ausbau des IT-Notfall-managements?

Nach der Theorie ist bekannt, dass große IT-Ausfälle existenzbedrohende Auswirkungen für Unternehmen haben können oder die Dienstleistungserbringung von Behörden dadurch gänzlich eingeschränkt werden kann. Grundlegende Regelungen, Gesetze und Standards berücksichtigen dies und sind damit schon heute ein Faktor, der den Auf- und Ausbau des Business Continuity Managements forciert. Die übergreifende Zuständigkeit und die

Verantwortung werden jeweils auf höchster Ebene, etwa der Geschäftsführung, der Amtsleitung oder einer vergleichbaren Positionen, gesehen.

Aus technologischer Sicht existiert der Einflussfaktor, ob neue IT-Systeme bereits in ihrem Standard bezüglich der Ausfallsicherheit, der Redundanz und des Schutzes der Daten die Ansprüche der IT-Sicherheit erfüllen. Andrerseits können damit auch neue Gefahren entstehen, die Business-Continuity-Management-Maßnahmen erfordern, die in den vorher noch analogen Bereichen nicht notwendig waren. Ein weiterer Faktor ist das Vertrauen in die Dienstleister und die Übertragung der Verantwortung auf externe Bereiche, wenn prozess- oder systembedingt der Betrieb und der Schutz der IT nicht mehr in der eigenen Organisation sichergestellt werden können.

Organisatorische Anpassungen aus Sicht der Digitalisierung als Transformationsprojekt werden in allen Bereichen erwartet, so dass auch bei dieser Situation davon auszugehen ist, dass ein IT-Notfallmanagement agil und flexibel auszuprägen ist. Die finanziellen Ressourcen sind, wie bei der weiteren Transformation der behördlichen IT zu Standardlösungen bereits angemerkt, grundsätzlich ein limitierender Faktor, der den Umfang der möglichen Maßnahmen bestimmt. Abschließend sei hierzu das Verständnis für die Digitalisierung allgemein und speziell für die IT-Sicherheit genannt. Bei einer weiteren proaktiven Ausrichtung der Digitalisierung auf Automatisierung der Prozesse ist in einem ausreichenden Maße auf die adäquate Absicherung zu achten.

Damit sind wesentlichen Einflussfaktoren aus der Theorie genannt, die mit den Erfahrungen aus der Praxis in der Analyse reflektiert und bewertet werden.

3.1.3 Zusammenfassung

Zusammenfassend zeigt sich, dass in der Theorie sowohl die hohe Bedeutung der Digitalisierung als auch die Aspekte der IT-Sicherheit in diesem Zusammenhang bekannt sind und diskutiert werden. Weitgehend einheitlich ist auch das Verständnis über das Business Continuity Management und die hohe Priorität, die einem koordinierten Vorgehen hiernach im weiteren Auf- und Ausbau der IT-Systeme zukommt. Vorgehensweisen, normierende Vorgaben und gesetzliche Anforderungen sind vorhanden und Best Practices sind dokumentiert. Damit stehen die Voraussetzungen zur Verfügung, um eine weitere Digitalisierung mit den Mitteln des IT-Managements ausreichend sicher gestalten zu können. Aufschlussreich wird es nun sein, wie diese theoretischen Grundlagen in der Praxis zur

Anwendung kommen. Dafür sind zusätzlich die nachfolgenden Fragestellungen zu beantworten.

3.2 Empiriegeleitete Fragestellungen

Zur Konkretisierung der Fragestellungen aus den Zielstellungen in Kapitel I 4 werden die ermittelten Ergebnisse der theoretischen Ausführungen berücksichtigt. Die erste Erhebung hat gezeigt, dass gesetzliche Vorgaben teilweise ungenau und statische Praktiken im Zeitalter der Digitalisierung nur noch bedingt anwendbar sind. Die Berücksichtigung von Standards, Normen und Richtlinien kann einen hohen Aufwand mit sich bringen und die Verantwortung insgesamt ist in Unternehmen und Behörden hierarchisch auf Leitungsebene zu verorten. Für praktische Empfehlungen sind die zu klärenden Fragestellungen, wie ein Business Continuity Management im Rahmen der digitalen Transformation effektiv angewendet werden kann, um folgende praxisrelevante Punkte zu ergänzen:

- Wie und wann wird in der Praxis ein Business Continuity Management angewendet, um den neuen Herausforderungen der Digitalisierung gerecht zu werden?

Bei der empirischen Erforschung der Best Practices und beim Umgang des IT-Managements mit der Digitalisierung in Bezug auf das Notfallmanagement sollen die Antworten auf folgende zusätzliche Fragen unterstützen:

- Welche Einflussfaktoren, Herausforderungen und Erfahrungen stehen hierzu in Unternehmen in welchem Zusammenhang?
- Existieren bereits bewährte Praktiken, um die IT-Sicherheit mit den Methoden eines Business Continuity Managements bei der weiteren Digitalisierung zu erhöhen?

Zur Erhebung der benötigten Daten wird im nächsten Teil III die Methode ermittelt, das gesamte Forschungsdesign skizziert und es werden der Ablauf sowie die Durchführung erläutert. Anschließend werden die Ergebnisse dargestellt, analysiert und diskutiert. Im übernächsten Teil IV, dem Gestaltungsteil, werden basierend auf den empirischen Resultaten und unter Berücksichtigung der Theorie die Handlungsempfehlungen abgeleitet.

III EMPIRISCHER TEIL

1 Forschungsdesign

Kapitel III 1 beschreibt und begründet die Auswahl der Forschungsmethode, die Anwendung im Detail und die Art der Analyse, bevor in Kapitel III 2 die damit ermittelten Ergebnisse dargestellt werden. Ebenso beinhaltet dieser Teil III die Interpretation und Diskussion der Ergebnisse sowie die Darlegung der Validität.

Die in Teil II herausgearbeiteten Ergebnisse sollen nun mit der Realität in Zusammenhang gebracht werden. Nach Eisend und Kuß (2021, S. 20) erfolgt dies mit Methoden der Empirie, die in einem engen Zusammenhang mit der Theorie steht. Die Autoren sehen es als die wesentliche Funktion der Empirie an, dass Theorien mittels Erfahrungen geprüft werden. Für den Bereich von anwendungsorientierten Fragestellungen haben sie den folgenden schematischen Ablauf veröffentlicht, an dem sich dieses Forschungsdesign orientiert:

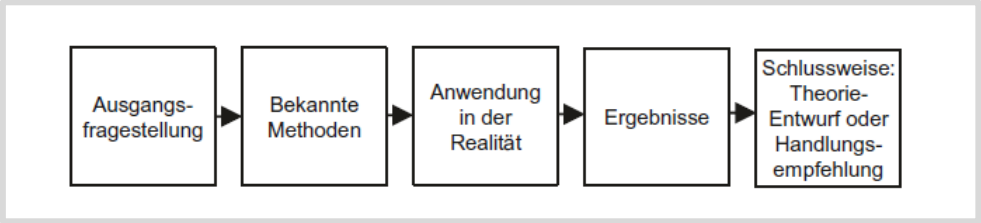


Abbildung 17 – Schema empirische Untersuchung (Quelle: Eisend und Kuß, 2021, S. 17)

Die Fragestellungen wurden bereits formuliert und bekannte Methoden zum Business Continuity Management in der Theorie diskutiert. Dem abgebildeten Ablauf folgend wird in Teil III nun die tatsächliche Situation in der Praxis herausgearbeitet, um mit den Ergebnissen fundierte Handlungsempfehlungen zu erstellen.

Flick (2022a, S. 264) resümiert zu Forschungsdesigns, dass diese das Mittel sind, um die Forschungsziele zu erreichen, und er nennt Faktoren, die das Design beeinflussen. Dabei führt er unter anderem die Fragestellung, das Darstellungsziel, die Ressourcen, der theoretische Rahmen, die Methoden und die Zielsetzung an. Unter Beachtung dieser Festlegungen wurde das Forschungsdesign, das im weiteren Verlauf erläutert wird, erstellt.

1.1 Untersuchungen

Bevor in Kapitel III 1.2 die konkrete Methodenauswahl dargelegt wird, werden die für die Untersuchungen relevanten Besonderheiten und Rahmenbedingungen genannt. Für die

empirische Forschung muss das Forschungsdesign geeignet und begründet sein und die Methoden müssen passend sein (Hug & Poscheschnik, 2020, S. 34). Dazu wurden die Gegebenheiten aus der Ausgangslage und der Theorie analysiert, um die Rahmenbedingungen für die zu beschreibende Untersuchung aufzuzeigen.

1.1.1 Beschreibung und Rahmenbedingungen

In den empiriegeleiteten Fragestellungen wurde deutlich, dass sich die Untersuchung auf Erfahrungen aus der Praxis konzentrieren muss, die das Zusammenspiel von Digitalisierung und Business Continuity Management fokussieren. Zudem sollen Lücken identifiziert werden und es ist beabsichtigt, auch die allgemeinen Planungen für eine weitere Digitalisierung zu betrachten. Das sind beides Situationen, für die eine einfache Erhebung vorhandener Fakten aus der Vergangenheit nicht möglich ist. Eine erste Rahmenbedingung ist somit, dass keine vorhandenen Daten erhoben oder abgefragt werden können, sondern dass die zur Beantwortung notwendigen Erkenntnisse aus der Kombination mehrerer Managementerfahrungen und Prognosen für die Praxis herausgearbeitet werden müssen. Die hierfür möglichen Methoden werden in Kapitel III 1.2.1 betrachtet und ausgewählt.

Eine weitere Rahmenbedingung ist, dass ggf. nicht alle Informationsquellen zu allen vorgesehenen Themenblöcken der Digitalisierung vergleichbar viel Erfahrung vorweisen können. Die Digitalisierung ist wie in der Theorie beschrieben umfangreich und komplex. Für die Erhebung muss eine Abstraktionsebene zur Digitalisierung geschaffen werden, damit verwertbare Praxiserfahrungen aus unterschiedlichen Quellen in die Analyse einfließen können. Diese Ebene muss durch dafür geeignete und generalisierte Fragestellungen erreicht werden.

Es wurde festgestellt, dass ein Business Continuity Management in Unternehmen und Behörden teilweise nicht praktiziert wird oder nicht vorhanden ist. Von daher war bei der Auswahl der Interviewpartner zu identifizieren, ob von diesen überhaupt relevante Informationen erhoben werden können. Dies wurde bei der Akquise dahingehend berücksichtigt, dass Informanten aus Unternehmen angefragt wurden, die hierzu über fundierte Kenntnisse verfügen und gleichzeitig Einblicke in mehrere Unternehmen und Behörden zu diesen Themenkomplex haben.

Als weitere Rahmenbedingung ist zu nennen, dass der Autor dieses Dokumentes über langjährige Erfahrung im Bereich Business Continuity Management und auch im Bereich behördennaher IT-Dienstleister verfügt. Da aus Sicht der verfügbaren Ressourcen für dieses

Projekt keine externe Vergabe der Datenerhebung vorgesehen war, musste der Umstand einer etwaigen Beeinflussung durch den Autor berücksichtigt werden. Häder (2019, S. 234-235) weist hier auf eine Fehlerquelle hin, wenn sogenannte latente Merkmale eines Interviewleiters, zu denen unter anderem der soziale Status, der Bildungsstatus und die Erwartungen zählen, die Ergebnisse beeinflussen können. Der Umgang mit dieser Rahmenbedingung ist im übernächsten Kapitel III 1.1.3 ‚Bias und deren Vermeidung' beschrieben.

1.1.2 Untersuchungseinheiten und Schritte

Die Untersuchung gliedert sich in folgende Teiluntersuchungen und Arbeitsschritte, die separat abzuschließen waren und jeweils Einfluss auf die Folgeuntersuchungen haben. Der ursprünglich geplante und dann durchgeführte Ablauf ist in Unterkapitel III 1.4 im Rahmen der konkreten Operationalisierung visualisiert und erläutert.

Als erste Untersuchungseinheit waren die theoretischen Grundlagen mit den Erkenntnissen aus den Studien und Marktanalysen zum Stand der Forschung zu analysieren. Damit wurde anschließend die Fokusgruppe weiter eingegrenzt und die Fragestellungen wurden darauf aufbauend entworfen. Die geplante Diskussion zum Umgang mit der Digitalisierung aus Sicht des Business Continuity Managements in den Unternehmen und Behörden war nach verschiedenen technischen Aspekten der Digitalisierung aufzuteilen. Bei einer zu pauschalisierten Betrachtung wären keine konkretisierten Handlungsempfehlungen ableitbar gewesen.

Im nächsten Schritt musste die geeignete Erhebungsmethode ausgewählt werden, die im Kapitel zur Methodenauswahl noch hergeleitet wird. Vor Beginn der Datenerhebung waren die rechtlichen Rahmenbedingungen nach den Datenschutzgesetzen zu prüfen und vor der Durchführung waren notwendige Einverständniserklärungen einzuholen. Nach Erstellung eines ersten Fragebogens mit einem Leitfaden musste validiert werden, ob hiermit eine zielführende Diskussion geleitet werden kann. Dazu waren die Fragestellungen anhand des Erkenntnisgewinns aus abgehaltenen Probeinterviews zu optimieren.

Eine wesentliche Untersuchungseinheit war danach die Durchführung der Experteninterviews, für die in einem ersten Schritt die Akquise erfolgen musste. Nach der Durchführung wurde die Transkription vorgenommen und als Untersuchungseinheit ist hier zu nennen, dass dabei bereits qualitativ geprüft wurde, ob die Themengebiete entsprechend abgedeckt wurden. Es wurde fortlaufend untersucht, ob weitere Interviews notwendig waren

oder ob bereits eine Sättigung vorlag. In einem weiteren Schritt wurden die verschriftlichten Dokumente den Interviewteilnehmern zur Verfügung gestellt und nach deren Freigabe flossen sie in die Analyse ein. In einem nächsten Schritt wurden die Transkripte mittels qualitativer Inhaltsanalyse ausgewertet und die Erkenntnisse und Ergebnisse dokumentiert. Die Methodenauswahl und die exakte Durchführung sind als Schwerpunkte in den weiteren Kapiteln noch erläutert.

Als letzte Untersuchungseinheit des empirischen Teils ist die nachvollziehbare Aufbereitung und Darstellung der Ergebnisse und Erkenntnisse in Bezug auf die Forschungsfragen zu nennen. Mit der dann folgenden Analyse wurde die Erkenntnisse im Gestaltungsteil mit den Grundlagen aus der Theorie zu objektiv nachvollziehbaren Handlungsempfehlungen aufbereitet.

Damit sind die grundlegenden Untersuchungseinheiten und die einzelnen aufeinander aufbauenden Schritte genannt. Sie prägen in dieser Struktur die weiteren Kapitel und sind dort mit den inhaltlichen Ergebnissen dargestellt.

1.1.3 Bias und deren Vermeidung

Nach Maindok (2003, S. 22) gilt es, eine Beeinflussung der befragten Personen zu vermeiden, und die Meinungen des Interviewleiters sowie dessen Einstellung zur Thematik sollen nicht erkennbar sein. In diesem Forschungsvorhaben wurden die Interviews durch den Dissertanten, der über mehrjährige Erfahrung im Bereich Business Continuity Management und hinsichtlich der Digitalisierung im öffentlichen Sektor verfügt, selbst geleitet. Grundsätzlich bestand damit die Gefahr eines Bias, der zu verzerrten Ergebnissen führen kann. Zur Vermeidung dieser Gefahr fanden vor der Interviewdurchführung keine Kennenlern- oder Fachgespräche statt. Es nahmen keine Arbeitskollegen an der Datenerhebung teil, die ggf. bereits die Meinungen und Sichtweisen des Forschungsleiters kannten und unbewusst reflektiert hätten. Auch Gläser und Laudel (2010, S. 118) warnen hier deutlich vor einem Bias, den es zu vermeiden gilt.

Die konkrete Akquise und die Auswahl der Experten sind in Kapitel III 1.3.3 detaillierter beschrieben. Die Teilnehmer wurden vor der Interviewdurchführung bereits darauf hingewiesen, dass vorab lediglich die Forschungsthematik vorgestellt wird. Es wurde in allen Fällen vereinbart, sich erst nach Durchführung des Interviews näher im Gespräch kennenzulernen und fachlich auszutauschen. Dadurch konnte vermieden werden, dass der

Interviewleiter die angesprochenen Themenfelder insgesamt und die geäußerten Erfahrungen und Empfehlungen der Experten beeinflusst.

Ein weiterer relevanter Punkt war, dass nicht schon durch die Fragestellungen eine Beeinflussung erfolgt. Bei Suggestivfragen, in deren Formulierung bereits gewünschte Antworten ersichtlich wären, würden Befragte unter Umständen keine ehrliche Antwort geben (Hussy et al., 2013, S. 229). Der erstellte Leitfaden für die Interviewdurchführung wird im Kapitel III 1.3.2 detailliert vorgestellt. Nach diesem Leitfaden wurde konsequent vorgegangen und kontextbezogene Rückfragen waren bereits vorab im Leitfaden definiert, so dass nicht unstrukturiert die persönlichen Interessen des Interviewleiters im Rahmen der Erhebung angesprochen oder diskutiert wurden. Im Gesprächsverlauf ergaben sich Situationen, in denen ein Experte durchaus die Sichtweisen und Meinungen des Forschungsleiters hören wollte. Es wurde dann zur Wahrung eines unbeeinflussten Interviews auf ein mögliches Gespräch im Nachgang verwiesen.

Zusammenfassend wurden somit nur Experten interviewt, die die persönlichen Sichtweisen des Forschungsleiters zu den Themen nicht kannten und vorab nicht beeinflusst wurden. Während des Interviews wurden keine Erfahrungen des Forschungsleiters mit den Experten geteilt, so dass die Datenerhebung nicht verzerrt wurde. Die weiteren Kapitel zur Akquise, zur Erarbeitung des Leitfadens und zur Vorbereitung der Interviewführung dokumentieren ergänzend die Berücksichtigung dieser Gefahr eines Bias und die in diesem Kontext erfolgte optimierte Vorbereitung zur Sicherstellung einer unvoreingenommenen Datenerhebung.

1.2 Methodisches Vorgehen und Methodenauswahl

Der Forschungsgegenstand bestimmt die Erhebungsmethode. Die Begründung der Methodenwahl und eine passende sowie korrekte Erhebung der Daten sind unabdingbar, um für die Forschung verwertbares Analysematerial zu erhalten (Przyborski & Wohlrab-Sahr, 2021, S. 106). Dem folgend wird die Wahl der Erhebungs- und der Analysemethode auf Basis der Themenstellung nachfolgend erläutert.

1.2.1 Erhebungsmethode

Grundsätzlich wird zwischen quantitativen und qualitativen Erhebungsmethoden unterschieden. Schumann (2018, S. 167) erläutert das Ziel der quantitativen Forschung mit einer möglichst exakten Wiedergabe der Realität und sieht bei der qualitativen empirischen

Sozialforschung den Menschen im Vordergrund. Sowohl bei der Analyse des Managements als Bestanteil des Business Continuity Managements als auch bei der Erstellung von Handlungsempfehlungen steht der Mensch mit seinem fachlich orientierten Handeln im Mittelpunkt der Betrachtung. Dies spricht bereits nicht für einen quantitativen Ansatz. Ebenfalls mit einer zielorientierten Betrachtung differenziert Wichmann (2019, S. 43) die qualitative und die quantitative Forschung treffend. Die Autorin sieht bei der quantitativen Forschung eine Verallgemeinerung, Vergleichbarkeit und Wiederholbarkeit der Ergebnisse im Fokus. Qualitativ wiederum werden deutlich andere Ziele verfolgt. Hier geht es um die Schaffung eines Verständnisses für Einzelfällen und eine Verallgemeinerung ist damit explizit nicht vorgesehen. Stattdessen stehen das Sinnverstehen und die Erarbeitung der Übertragbarkeit der Ergebnisse auf andere Kontexte im Vordergrund.

Diesen Ausführungen folgend ist hier ein qualitativer Ansatz indiziert, da mit einer Verallgemeinerung von quantitativ erhobenen Daten zur den Sachständen Digitalisierung und Business Continuity Management noch kein Mehrwert generiert werden kann. Ein Verstehen der Situation und die Übertragung auf weitere zukünftige Digitalisierungsschritte ist notwendig, um Lösungen für die Problemstellung zu finden. In diesem Forschungsvorhaben wurde das IT-Management bei speziellen Aspekten der Digitalisierung mit Fokus auf das Business Continuity Management betrachtet. Die Problemstellung und die genannten Studien weisen auf Defizite in der Praxis hin und sehen auf diesem Gebiet Handlungsbedarf. Wenn nach Begründungen für ein bestimmtes menschliches Verhalten gesucht wird und dafür z. B. ein Bezug auf Erlebnisinhalte erfolgt, sind das Anzeichen für eine qualitative Forschung (Kirchmair, 2022, S. 3-4).

In dieser Arbeit wurden Erfahrungen von Experten ermittelt, weshalb aus Managementsicht bestimmte Entscheidungen getroffen werden oder wurden. Wergen (2019, S. 121) erläutert und differenziert ebenfalls zur quantitativen Forschung dahingehend, dass mit einer qualitativen Forschungsmethode auch individuelle Erfahrungen betrachtet werden können. Die Autorin nennt zudem die Möglichkeit der Beschreibung von subjektiven Interpretationen, womit sich im Kontext dieser Arbeit Erklärungen für die in der Problemstellung dargestellte Situation ergeben können (Wergen, 2019, S. 121).

Mit diesen Erkenntnissen wurde die Entscheidung für einen qualitativen Ansatz getroffen. Als Nächstes wurde die konkrete Erhebungsmethode herausgearbeitet, mir der die Datenerhebung passend für die Problemstellung erfolgen kann.

Es war zu erwarten, dass für die Beantwortung der empirischen Fragestellungen die Antwortmöglichkeiten offengehalten werden müssen, da grundsätzlich alle Einflussfaktoren und Hintergrundinformation zur Themenstellung erfragt werden sollten. Hierfür sehen Reinders und Ditton (2011, S. 50) beispielsweise die Durchführung von Interviews vor, um den befragten Personen möglichst wenig Vorgaben zu machen und viel Antwortraum zu bieten. Häder (2019, S. 201-202) bezeichnet diese Methode als mündliche Befragung, stuft sie als universell einsetzbar ein und hebt hervor, dass durch den sozialen Kontakt während eines Interviews die Chance auf verlässliche und gültige Informationen besteht.

Zur Digitalisierung und zum Business Continuity Management liegen, wie im theoretischen Teil dargestellt, Erkenntnisse vor. Hierzu sollen von verschiedenen Personen die jeweiligen Sichtweisen erhoben und verglichen werden, wozu sich die Durchführung mit leitfadengestützten Interviews anbietet (Hussy et al., 2013, S. 227). Das Themenfeld ist durch verschiedene sensible Aspekte gekennzeichnet, da auch Bereiche der IT-Sicherheit und des Datenschutzes sowie Datensicherungskonzepte oder präventive Vorkehrungsmaßnahmen gegen Angriffe diskutiert werden. Dieser Punkt ist ein Kennzeichen, das nach Bogner und Menz (2009, S. 8) auch in Abgrenzung zu anderen Erhebungsmethoden deutlich für Experten-interviews spricht. Die Autoren verweisen auf „tabuisierte Themenfelder“, die in Gesprächen mit Experten diskutiert werden können. In diesem Forschungsvorhaben werden sich solche Situationen bei Fragen nach Backup-Konzepten und -Intervallen ergeben, insbesondere dann, wenn eigentlich notwendige Backup-Strategien oder Sicherheitsvorkehrungen nicht vorhanden sind. Gläser und Laudel (2010, S. 11) definieren Experten als Personen, die über ein besonderes Wissen oder besondere Informationen verfügen. Passend dazu verdeutlicht die nachfolgende Definition die besondere Eignung von Experten für den hier beschriebenen Forschungszweck:

> *„Experten lassen sich als Personen verstehen, die sich – ausgehend von einem spezifischen Praxis- oder Erfahrungswissen, das sich auf einen klar begrenzbaren Problemkreis bezieht – die Möglichkeit geschaffen haben, mit ihren Deutungen das konkrete Handlungsfeld sinnhaft und handlungsleitend für Andere zu strukturieren.“*
> (Bogner et al., 2014, S. 13)

Zusammenfassend wurde damit eine qualitative Forschungsmethode und -analyse ausgewählt, deren Datenerhebung mittels Experteninterviews erfolgen soll.

Ein nach Döring (2023, S. 355-356) erläutertes halbstrukturiertes Interview mit einem Interviewleitfaden lässt offene Antworten zu, wobei die Themenfelder und Fragen strukturiert

aus einem Katalog vorgegeben werden. Dazu wurden die Interviews mit einem Leitfaden vorbereitet und organisiert, wobei Quantität und Granularität der Fragen zu Beginn der Erhebung noch nicht abschließend festgelegt waren. In dieser Arbeit geht es um die Informationen, die als Einflussparameter für das IT-Notfallmanagement aufgrund der Digitalisierung zu betrachten sind. Mit entsprechend offenen Antworten wurde gerechnet, da beispielsweise erfragt wurde, ob bereits Zusammenhänge im Unternehmen erkennbar sind und wie der derzeitige Stand der Digitalisierung ist. Die unternehmerische Abhängigkeit wurde im Interviewverlauf herausgearbeitet und konkreter wurden Themen besprochen, die Erfahrungen zu bereits vorhandenen IT-Notfallpräventionen zum Inhalt hatten. Damit konnte eine valide Datengrundlage durch halbstrukturierte, leitfadengestützte Experteninterviews erhoben werden. Die Daten wurden anschließend durch die im nächsten Kapitel erläuterten Analyse- und Auswertungsmethoden bearbeitet, damit eine nachvollziehbare Grundlage für die Konzeption von Handlungsempfehlungen vorhanden war.

1.2.2 Analyse- / Auswertungsmethode

Die Ergebnisse der Interviews lagen nach der obligatorischen Transkription in textlicher Form als Gesprächsprotokolle vor. Die wissenschaftlich fundierte Auswertung der Protokolle ist ein wesentlicher Bestandteil des Forschungsvorhabens. Um die Forschungsfragen beantworten zu können, wurden die Texte mittels qualitativer Inhaltsanalyse ausgewertet. Nach Döring (2023, S. 533) kann mit dieser Methode schrittweise der Bedeutungsgehalt zum Forschungsproblem herausgearbeitet werden. Hierzu sind Kategorien und Codes verbal zu beschreiben. Mayring stellt einen Ablauf vor, der ausgehend vom Analysegegenstand einen zeilenweisen Materialdurchgang vorsieht, mehrstufig die Kategorien induktiv definiert und diese wiederholend einer Revision unterzieht. Anschließend werden auf Grundlage eines endgültigen Materialdurchgangs die Ergebnisse interpretiert und ausgewertet (2023, S. 99).
Es erfolgte sowohl eine deduktive als auch eine induktive Kategorienbildung, wie auch Döring (2023, S. 533) es bei der qualitativen Inhaltsanalyse als Möglichkeit anführt. Deduktiv bedeutet hier, passend zur Erläuterung von Schneijderbergs et al. (2022, S. 120) zu dieser Analysemethode, dass aus der Theorie abgeleitete Kategorien am erhobenen Material codiert werden. Deduktiv wurden insbesondere die aus der Theorie erwarteten Handlungsfelder zur Digitalisierung codiert. Es wurde daher geprüft und markiert, welche Aspekte von den Experten genannt wurden, die bereits aus der theoretischen Analyse erwartbar waren, beispielsweise ‚Automatisierung von Geschäftsprozessen' oder ‚Cloud-Computing'.

Anschließend erfolgte eine weitere Analyse mittels induktiver Kategoriebildung. Bei dieser Methode sind die Kategorien nicht vorgegeben, sondern entstehen im Rahmen der Materialanalyse (Schneijderberg et al., 2022, S. 84). Diese Kategorien ergaben sich aus den Antworten und Auskünften der Interviewpartner zu erlebten Situationen. Es wurden ebenfalls die Empfehlungen zur Kategoriebildung genutzt. Insbesondere wenn mehrere Experten noch nicht erfasste Themen übereinstimmend angesprochen hatten, wurde hieraus eine Kategorie erzeugt und das Material auch aller anderen Experten hierzu analysiert und codiert. Das so entstandene Codebuch ist als Anlage IV. beigefügt. Für die Resultate aus den Experteninterviews mit Not- und Katastrophenfallmanagern bzw. IT-Managern war es von besonderem Interesse, welche Kategorien sich mit Blick auf die Sicherheit und die fortschreitende Digitalisierung ergeben. Es wurde erwartet, dass die dann erstmals kodierten Kategorien bei weiteren Interviewpartnern ebenfalls gefunden werden. Hierbei wurde dann auch deren Häufigkeit betrachtet. Die qualitative Inhaltsanalyse mit induktiver Kategorienbildung liefert ein dazu geeignetes Set an Kategorien als Ergebnis (Mayring, 2023, S. 100).

Wie aus den Fragestellungen ersichtlich, sollen Zusammenhänge der verschiedenen Themen der Digitalisierung und des Notfallmanagements herausgearbeitet werden. Kuckartz (2018, S. 118-120) stellt Auswertungsformen vor, in denen sowohl die Zusammenhänge zwischen den Hauptkategorien als auch zwischen den Unterkategorien einer Hauptkategorie zu untersuchen sind. Der Autor empfiehlt hier zu prüfen, welche Erwähnungen in welchen Zusammenhängen vorkommen, wie diese formuliert sind und ob sich Muster erkennen lassen (2018, S. 118-120). Diese Methoden wurden nach der genannten Kategorienbildung angewendet und in der Ergebnisdarstellung abgebildet.

Für einen Überblick sollten die Ergebnisse auch graphisch dargestellt werden. Hierzu empfiehlt Kuckartz (2018, S. 120), aufgrund der Anzahl der Untersuchungsobjekte vorab die Sinnhaftigkeit zu prüfen. Er nennt Concept-Maps, die ein geeignetes Mittel sein können, um Zusammenhänge zu visualisieren. Neben der Eignung zur Ergebnispräsentation sind derartige Maps auch ein Hilfsmittel bei der Analyse und der Textarbeit (Kuckartz & Rädiker, 2022, S. 228). Daran angelehnt wurden für den Ergebnissteil neben der deskriptiven Ausarbeitung entsprechende Abbildungen erstellt. Als ein häufig eingesetztes Computerprogramm für die Inhaltsanalyse nennt Mayring (2022, S. 111) MAXQDA, mit dem bereits viele Kategorisierungsfunktionen möglich sind. Dieses Tool wurde zur Analyse und Auswertung der Interviewprotokolle eingesetzt und das Vorgehen ist in Kapitel III 1.3.5 zur

Operationalisierung im Detail beschrieben. Die bei diesem methodischen Vorgehen relevanten Gütekriterien zur Sicherstellung der Qualität der Ergebnisse sind später in Kapitel III 3.2 erläutert und die Prüfung ist ebenfalls dokumentiert.
Damit sind Wahl der passenden Methoden und das methodische Vorgehen erläutert. Die konkrete Umsetzung ist im folgenden Kapitel beschrieben.

1.3 Operationalisierung

In diesem Kapitel wird die Operationalisierung dargelegt. Hierbei wird unter anderem erläutert, wie im konkreten Projekt die Datenerhebung mit der soeben erläuterten Methode erfolgt ist. Die Reihenfolge der Fragen und deren Formulierungen werden im Detail beschrieben, wie es nach Stier (1999, S. 30) zur Operationalisierung gehört. Der Autor fasst die Operationalisierung als zweistufigen Prozess auf, in dem zuerst die Indikatoren bestimmt und folgend auch umgesetzt werden. Alle Schritte bei der Konstruktion des Interviewleitfadens zu dokumentieren, erachten auch Gläser und Laudel (2010, S. 115) als einen wesentlichen Grundsatz bei der Betrachtung der methodologischen Prinzipien für Leitfadeninterviews.
Zur Berücksichtigung der theoretischen Erkenntnisse in diesem empirischen Teil wurde ein Interviewleitfaden erstellt, der die aus der Theorie abgeleiteten Fragestellungen enthält. Unter anderem sollte darüber gesprochen werden, welche nächsten Schritte die Experten aus der Praxis im Bereich der weiteren Digitalisierung in Deutschland sehen. Es wurde hinterfragt, wie sie diese bewerten und wo sie Gefahren ausmachen. Dabei wurde eruiert, wann und mit welchem Stellenwert ein Business Continuity Management berücksichtigt wird. Die im Rahmen dieser Dissertation vervollständigten Merkmale der Digitalisierung auf Basis der theoretischen Erkenntnisse wurden einzeln als Fragepunkte vorbereitet. Die konkreten Interviewfragen, die Expertenauswahl, das Transkribieren und Codieren des Materials sowie die Sättigungsanalyse sind in den nachfolgenden Unterkapiteln beschrieben.

1.3.1 Umsetzung der Forschungsfragen in Interviewfragen

In Kapitel I 4.1.1 wurde die Hauptzielstellung dargelegt, die durch die Beantwortung der Haupt- und Nebenforschungsfragen erreicht werden kann. Die Umsetzung in Interviewfragen erfolgte durch Aufteilung der Forschungsfragen auf mehrere Fragenstellungen, die sich an eine erfahrene Person richten. Diese soll darauf mit Hintergrundwissen, Zusammenhängen,

Fakten und einem Ausblick mit Empfehlungen antworten können. Dazu wurde zuerst ein grober Leitfaden erstellt, der, wie Leitner und Wroblewski (2002, S. 250) es empfehlen, damit sowohl den Expertenkreis weiter festlegt als auch die Informationen aus Vorgängerstudien und den theoretischen Annahmen aufgreift. Für einen strukturierten Verlauf der Interviews ist die hier erarbeitete Hauptforschungsfrage (HFF) zu umfangreich und damit ungeeignet, so dass für die Ausarbeitung der Interviewfragen (IF) die Nebenforschungsfragen (NFF) zugrunde gelegt wurden.

Es wurden insgesamt 18 übergeordnete Interviewfragen erstellt, die sich teilweise noch in spezifische Subfragen untergliedern. Grundsätzlich lassen sich drei Fragearten unterscheiden: einleitende Fragen, Leitfadenfragen und Ad-hoc-Fragen (Hussy et al., 2013, S. 225-226).

Beginnend wurde – noch ohne expliziten Bezug zu den Forschungsfragen – der zur Teilnahme an den Interviews begründende Expertenstatus als einleitende Frage gestellt. Die persönlichen Erfahrungen im Bereich IT-Management mit Fokus Business Continuity Management wurden mit Schwerpunkt der Erfahrungszeit erfragt und es wurde eine Aussage zu Erfahrungen in den Bereichen behördlicher IT, IT-Dienstleistungen und des dortigen Business Continuity Managements erbeten. Zur Einordnung der später folgenden Aussagen wurde zudem das persönliche Sicherheitsempfinden eruiert. Diese Einstiegsfragen beendeten den ersten Teil des Interviews und es folgte der Teil zum Business Continuity Management.

Aus der ersten Nebenforschungsfrage abgeleitet wurde die allgemeine Situation in den Bereichen Business Continuity Management, IT-Notfallmanagement und IT-Sicherheit erfragt. An die konkrete Frage zur Bedeutung aus Sicht des Experten schlossen sich die Detailfragen an, ob die Thematik aus Sicht des Experten ausreichend Berücksichtigung findet. Als weitere Ergänzungsfrage hierzu wurde um eine Aufwand/Nutzen-Bewertung gebeten und erfragt, wie es sich bei IT-Projekten verhält, ob das Business Continuity Management hier eher als Projektbremse oder Projekt-Enabler wahrgenommen wird. Separat wurden die Teilnehmer dann hinsichtlich sowohl positiver als auch negativer Erfahrungen in dem Bereich interviewt, bevor der erste fachliche Block beendet wurde. Insbesondere die letzte Frage leitet sich neben der ersten Forschungsfrage auch aus der dritten Forschungsfrage ab, in der praxisorientierte Lösungsmöglichkeiten herausgearbeitet werden sollen.

Der nächste Block behandelte die Digitalisierung insgesamt und als erste Frage wurde offen nach Aspekten der Digitalisierung gefragt, die aus Sicht der Experten aktuell und zukünftig von besonderer Bedeutung sein werden. Damit wurde die zweite Nebenforschungsfrage direkt angesprochen und als Subfragen waren hier die aus der Theorie bereits herausgearbeiteten

Themenfelder der Digitalisierung vorbereitet. Trotz der grundsätzlichen Offenheit wurden zur Lenkung des Gesprächs im Sinne des Forschungsinteresses, wie Helfferich (2022, S. 876) die Anwendung eines Leitfadens beschreibt, einige Aspekte der Digitalisierung explizit angesprochen. In jedem Fall wurden die Teilnehmer nach Einordnung des Cloud-Computings gefragt, das, wie bereits im Einleitungsteil Kapitel I 1.2 zitiert, als eine Schlüsseltechnologie für die Digitalisierung angesehen wird. Mit einer weiteren Nachfrage wurde um eine Einschätzung gebeten, ob konkret Sicherheitsbehörden ihre IT-Infrastruktur hierzu an externe Anbieter auslagern können oder sollten. Eine weitere Interviewfrage war mit dem Ziel vorbereitet, genau diese genannten Aspekte dann vor dem Hintergrund des Business Continuity Managements zu reflektieren.

Im nächsten Fragenblock wurden Normen und Standards hinterfragt. Ebenfalls ergebnisoffen wurde beginnend lediglich erfragt, was aus Sicht des Experten hier zu nennen sei. Falls dies von den Experten noch nicht genannt wurde, waren Fragen nach Erfahrungen im Bereich der Vorgehensmodelle ITIL und COBIT, des BSI-Grundschutzes, des BSI-Notfallmanagements nach BSI 100-4 und 200-4 sowie der ISO-Normen vorbereitet. In Teil II wurde bereits die Motivation für Zertifizierungen nach der ISO-Norm 22301 oder nach anderen ISO-Normen angesprochen; dies wurde in einer separaten Interviewfrage vorbereitet. Abgeschlossen wurde der Fragenblock mit den Interviewfragen zu gesetzlichen Regelungen in diesem Bereich. Bereits dieser Block leitet sich aus der dritten Nebenforschungsfrage ab, da diese Vorgaben, Normen und Standards dahingehend betrachtet wurden, ob sie im Kontext des Business Continuity Managements und der Digitalisierung als zielführend einzustufen sind.

Zur Abrundung des Interviews wurde mit der direkt aus Forschungsfrage drei abgeleiteten Interviewfrage nach Empfehlungen gefragt, die die Experten vor dem Hintergrund der eigenen Ausführungen und Erfahrungen geben würden. Abschließend wurde ein begründeter Ausblick dazu erbeten, wie sich die weitere Digitalisierung insbesondere im behördlichen Umfeld auf das allgemeine Sicherheitsniveau auswirken wird oder könnte.

Aus der nachfolgenden Abbildung sind die soeben genannten Ableitungen und das Prinzip ersichtlich, wonach sich die Interviewfragen auf die Forschungsfragen beziehen. Aus jeder Nebenforschungsfrage wurde ein Themenkomplex abgeleitet, der auch jeweils durch eine explizite Interviewfrage repräsentiert ist. Dies ist in der Abbildung mit dem blauen Pfeil dargestellt. Ergänzende Fragen zur jeweiligen Forschungsfrage sind mit den grauen Pfeilen gekennzeichnet und indirekte sowie unterstützende Verbindungen von Fragestellungen im Interview zu anderen Forschungsfragen werden mit den gestrichelten Pfeilen verdeutlicht.

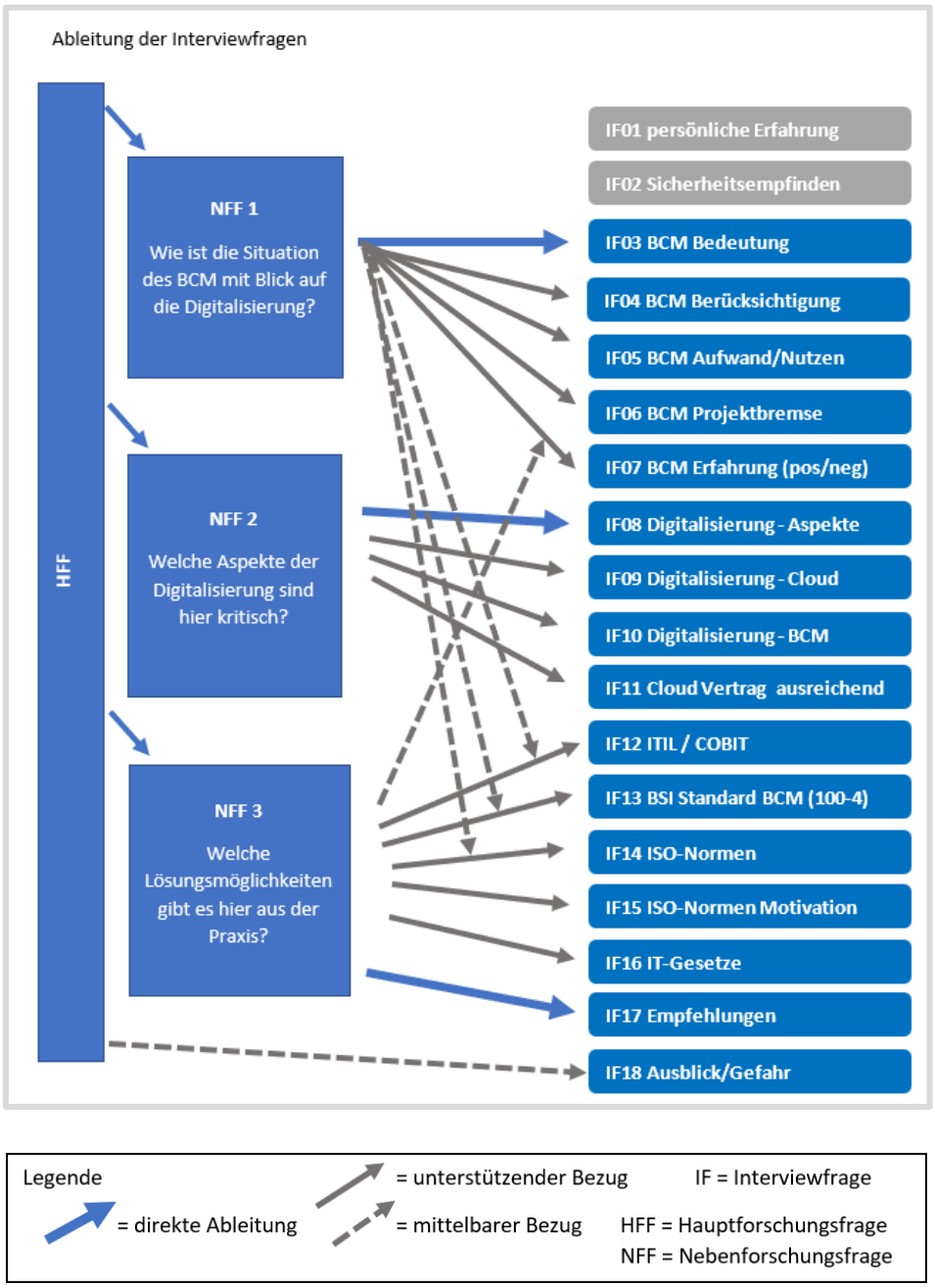


Abbildung 18 – Ableitung der Interviewfragen (Quelle: eigene Darstellung)

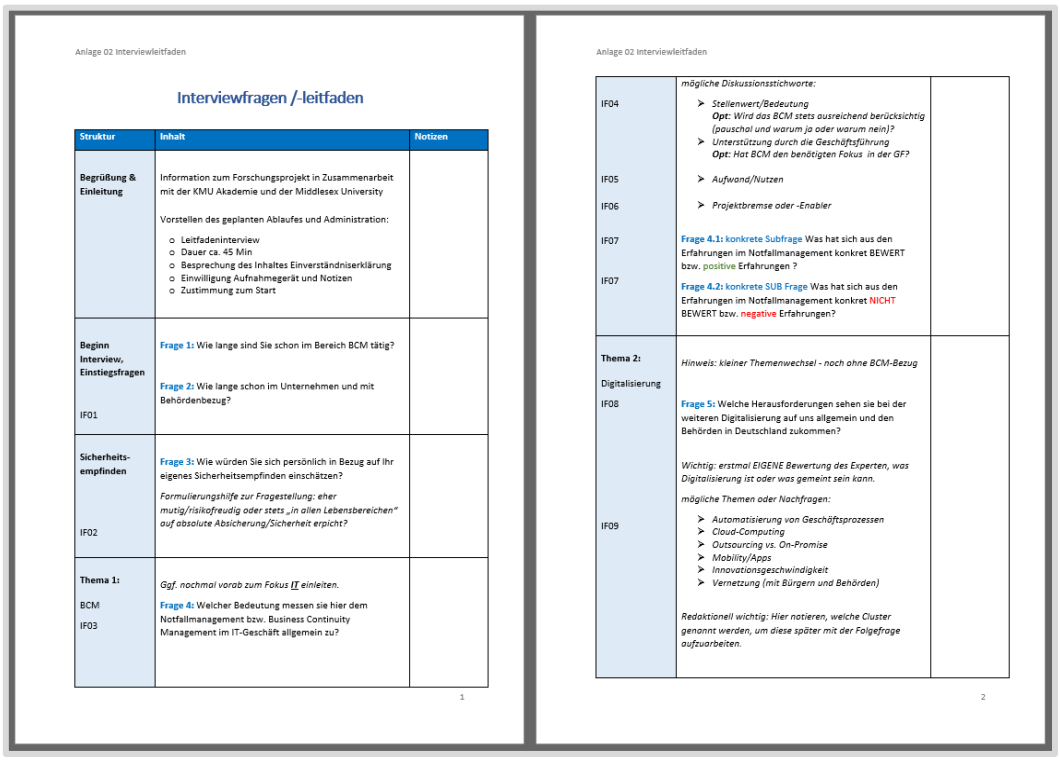
Das gesamte Experteninterview ist damit konsequent auf die Themenfelder der Forschungsfragen fokussiert und damit mittelbar aus der Theorie abgeleitet. Neben dieser Ableitung der Interviewfragen werden der Interviewleitfaden und dessen Operationalisierung im folgenden Kapitel beschrieben.

1.3.2 Interviewleitfaden

Der Interviewleitfaden ist von zentraler Bedeutung, um von den Forschungsfragen zu einem Erkenntnisgewinn gelangen zu können. Anfangs und insbesondere nach den ersten Interviews hat sich der Leitfaden dynamisch weiterentwickelt, wie es auch Reinders (2011, S. 94) im

Grundsatz beschreibt. Leitner und Wroblewski (2002, S. 250) sprechen hierzu von einer laufenden Überarbeitung aufgrund von Neubewertungen der Themenbereiche. Erwartungsgemäß ergab sich auch im vorliegenden Projekt diese Notwendigkeit. Allerdings werden diese Anpassungen aufgrund der verfügbaren Kapazitäten in diesem Dokument im weiteren Verlauf nicht in allen Einzelheiten dargestellt und in Anlage II. ist der Leitfaden beigefügt, der sich nach mehreren Evolutionsschritten für die Interviews bewährt hat. Strukturell gliedert sich der Leitfaden in die auch nach Misoch (2019, S. 68) vorgesehenen vier Bereiche, so dass zunächst ein Informationsblock für den Einstieg vorgesehen ist. Nach den Einstiegsfragen beginnt der Hauptteil mit den Fachthemen, bevor am Ende ein Abschlussblock vorgesehen ist.

Dieser Interviewleitfaden stand zur Interviewführung ausgedruckt zur Verfügung und hier konnten Notizen erfasst werden, um bei bestimmten Themengebieten nachzufragen, ohne den Experten zu unterbrechen. Zusätzlich wurden bemerkenswerte Aussagen und Aspekte handschriftlich notiert, um hier beim zusammenfassenden Teil am Ende des Interviews erneut Rückfragen stellen zu können. Der im vorherigen Kapitel dargestellten chronologischen Reihenfolge der Interviewfragen (IF) folgend, wurde der Leitfaden aufgebaut und um redaktionelle Hinweise ergänzt. Administrativ gibt es zusätzlich einen Einleitungsblock zur Begrüßung und zur Klärung der Rahmenbedingungen. Am Ende war ein Block für die Verabschiedung und die Besprechung etwaiger noch offener Fragen vorgesehen. Auf der nachfolgenden Abbildung sind das Layout, eine unterstützende Farbgebung und die Notizmöglichkeit ersichtlich. Auf die fachlichen und methodischen Inhalte dieses Leitfadens wird im weiteren Text ausführlich eingegangen.



Anlage 02 Interviewleitfaden

Interviewfragen /-leitfaden

Struktur	Inhalt	Notizen
Begrüßung & Einleitung	Information zum Forschungsprojekt in Zusammenarbeit mit der KMU Akademie und der Middlesex University Vorstellen des geplanten Ablaufes und Administration: ○ Leitfadeninterview ○ Dauer ca. 45 Min ○ Besprechung des Inhaltes Einverständniserklärung ○ Einwilligung Aufnahmegerät und Notizen ○ Zustimmung zum Start	
Beginn Interview, Einstiegsfragen IF01	**Frage 1:** Wie lange sind Sie schon im Bereich BCM tätig? **Frage 2:** Wie lange schon im Unternehmen und mit Behördenbezug?	
Sicherheits-empfinden IF02	**Frage 3:** Wie würden Sie sich persönlich in Bezug auf Ihr eigenes Sicherheitsempfinden einschätzen? *Formulierungshilfe zur Fragestellung: eher mutig/risikofreudig oder stets „in allen Lebensbereichen" auf absolute Absicherung/Sicherheit erpicht?*	
Thema 1: BCM IF03	*Ggf. nochmal vorab zum Fokus IT einleiten.* **Frage 4:** Welcher Bedeutung messen sie hier dem Notfallmanagement bzw. Business Continuity Management im IT-Geschäft allgemein zu?	

1

Anlage 02 Interviewleitfaden

IF04 IF05 IF06 IF07 IF07	*mögliche Diskussionsstichworte:* ➢ *Stellenwert/Bedeutung* ***Opt:** Wird das BCM stets ausreichend berücksichtig (pauschal und warum ja oder warum nein)?* ➢ *Unterstützung durch die Geschäftsführung* ***Opt:** Hat BCM den benötigten Fokus in der GF?* ➢ *Aufwand/Nutzen* ➢ *Projektbremse oder -Enabler* **Frage 4.1: konkrete Subfrage** Was hat sich aus den Erfahrungen im Notfallmanagement konkret BEWERT bzw. positive Erfahrungen ? **Frage 4.2: konkrete SUB Frage** Was hat sich aus den Erfahrungen im Notfallmanagement konkret NICHT BEWERT bzw. negative Erfahrungen?	
Thema 2: Digitalisierung IF08 IF09	*Hinweis: kleiner Themenwechsel - noch ohne BCM-Bezug* **Frage 5:** Welche Herausforderungen sehen sie bei der weiteren Digitalisierung auf uns allgemein und den Behörden in Deutschland zukommen? *Wichtig: erstmal EIGENE Bewertung des Experten, was Digitalisierung ist oder was gemeint sein kann.* *mögliche Themen oder Nachfragen:* ➢ *Automatisierung von Geschäftsprozessen* ➢ *Cloud-Computing* ➢ *Outsourcing vs. On-Promise* ➢ *Mobility/Apps* ➢ *Innovationsgeschwindigkeit* ➢ *Vernetzung (mit Bürgern und Behörden)* *Redaktionell wichtig: Hier notieren, welche Cluster genannt werden, um diese später mit der Folgefrage aufzuarbeiten.*	

2

Abbildung 19 – Symbolbild zwei von vier Seiten des Interviewleitfadens (Quelle: Anlage II., eigene Darstellung)

Im einleitenden Begrüßungsblock wurde das Forschungsvorhaben vorgestellt und das geplante Interview als Teil der empirischen Datenerhebung erläutert. Die voraussichtliche Dauer, die vorab übermittelte Einverständniserklärung und die Einwilligung zur elektronischen Aufnahme des Gesprächs wurden besprochen und nach abschließender Prüfung der Technik wurde das Interview begonnen.

Die ersten drei Einstiegsfragen bezogen sich auf den beruflichen Hintergrund, die Erfahrungszeit, den Behördenbezug und das persönliche Sicherheitsempfinden. Der Bereich Business Continuity Management wurde mit einer offenen Fragestellung eröffnet, die nach der allgemeinen Bedeutung aus Sicht des Experten fragte. Es waren optionale Nachfragen vorformuliert, die je nach Verlauf des Interviews gezielt gestellt wurden, wenn zu diesen Stichworten noch keine Beiträge erfolgt waren. Für den Bereich der Bedeutung des Business Continuity Managements wurde dann konkret thematisiert, ob es aus Sicht des Experten ausreichend Anwendung findet. Es wurde nachgefragt, wie der Experte die Bedeutung, das Verständnis und den Stellenwert auf Ebene der Geschäfts- oder Amtsleitungen einstuft. Eine Abschätzung zum Bereich Aufwand/Nutzen-Vergleich wurde angesprochen und es wurde um eine Bewertung gebeten, ob das Business Continuity Management grundsätzlich eher als IT-Projektverhinderer oder -verzögerer gesehen wird. Als Subfragen zum Ende des ersten Themenblocks waren im Leitfaden noch die offenen Fragen nach positiven oder negativen Erfahrungen vorgesehen, wonach dann zum zweiten Themenblock übergeleitet wurde.

Der Interviewblock zur Digitalisierung wurde im Leitfaden derart vorbereitet, dass die allgemeine Frage zur Digitalisierung zunächst noch ohne konkreten Bezug zum Notfallmanagement beantwortet werden kann. Dadurch konnten Antworten für die zweite Nebenforschungsfrage gefunden werden, um zielorientiert die wesentlichen Herausforderungen der Digitalisierung aus der Praxis zu ermitteln. Im Fragebogen wurde hierzu ein Hinweis für den Interviewleiter notiert. Um in jedem Fall die aus der Theorie abgeleiteten Aspekte der Digitalisierung zu berücksichtigen, waren Stichworte für Unterfragen vorbereitet, zu denen gezielt nachgefragt wurde. Aufgrund der dynamischen und unvorhersehbaren Gesprächsverläufe wurde insgesamt im Interviewverlauf wiederholend geprüft, ob diese Aspekte bereits angesprochen wurden. Damit konnten die Erfahrungen und Meinungen zu Themengebieten wie Cloud-Computing, Automatisierung von Geschäftsprozessen und IT-Outsourcing in allen Interviews angesprochen werden, auch wenn diese nicht schon aktiv vom Befragten genannt wurden. Wie bereits im ersten Themenblock erfolgte auch hier das Notieren von wesentlichen Aussagen in Stichworten im Leitfaden, um im dritten Block jeweils die Themen zusammen zu betrachten.

Eingeleitet wurde der dritte Block durch die Frage, ob die vom Experten bereits dargestellte Situation des Business Continuity Managements gemeinsam mit den zuletzt genannten Aspekten der Digitalisierung betrachtet werden kann. Insbesondere mit einem Blick auf die Zukunft wurden damit Aussagen generiert, die mit der dritten Nebenforschungsfrage und der Hauptforschungsfrage in einem engen Zusammenhang stehen. Anschließend wurde zu Modellen und Standards übergeleitet, um auch diesen praxisorientierten Anteil ausreichend zu berücksichtigen. Erneut erfolgte eine offene Fragestellung nach Vorgehensmodellen, Standards, Normen, Gesetzen und sonstigen Vorgaben, die aus Sicht der Experten relevant sind. Im Fragebogen waren die erwarteten Themen notiert, auf die die Experten noch angesprochen werden sollten, wenn diese nicht bereits genannt wurden. Damit wurden auch die aus der Theorie relevanten Grundlagen thematisiert, die sich ggf. in der Praxis nicht bewähren oder durchsetzen, und die Experten konnten dazu ausgeführt, weshalb dies in der Praxis so ist.

Zum Ende der Interviews war ein zusammenfassender Block vorbereitet, in dem auch explizit nach Empfehlungen für das Business Continuity Management gefragt wurde, die für den Forschungszweck entsprechend relevant sind, aber noch nicht erwähnt wurden. Die Einschätzung, ob wir uns zukünftig aufgrund der Digitalisierung auf eine allgemein sicherere oder unsicherere Welt zubewegen, wurde als letzte Frage gestellt. Die obligatorische

Nachfrage, ob es noch weitere Punkte gibt, die der Teilnehmer nennen möchte, beendete den fachlichen Anteil des Interviews.

Im Leitfaden waren für den Abschluss des Interviews noch die Danksagung für die Zusammenarbeit und der Hinweis, dass nach Beendigung der Audioaufnahme der weitere Ablauf besprochen wird, vorgesehen. Dort wurden die als Nächstes beabsichtigte Verschriftlichung und die Anonymisierung des Interviews erläutert und es wurde darauf hingewiesen, dass der Experte die erstellte Datei vor jeglicher Verwendung oder Analyse erhält, prüfen kann und auch weiterhin jederzeit seine abgegebene Einwilligung widerrufen kann.

Um den Fragenkatalog vor der Durchführung zu optimieren und verständlich zu gestalten, sind Probeinterviews von hoher Bedeutung (Mayer, 2013, S. 45). Auch zur eigenen Schulung in der Interviewdurchführung erfolgten Pretests mit einer ersten Version des Leitfadens. Hussy et al. (2013, S. 226) beschreiben diese Phase als Pilotphase, an die sich die eigentliche Hauptphase der Interviews anschließt. Zur Überprüfung der Leitfäden und zur Abschätzung der Dauer der Interviews werden Probeinterviews vorgesehen (Döring, 2023, S. 367). Dies ist hier ebenfalls erfolgt, so dass damit Interviews von zirka 45 bis 60 Minuten Dauer vorbereitet wurden. Als Pretests wurden Interviews mit Probanden geführt und die Transkription sowie die Codierung wurden mit dem erhobenen Material getestet, um im Ergebnis den ersten Leitfaden weiter auszuarbeiten. Direkt nach der Erhebung der ersten Interviews können erste Auswertungen erfolgen und es kann dabei geprüft werden, ob neue, bislang noch nicht berücksichtigte Aspekte in Folgeinterviews aufzunehmen sind (Reinders & Ditton, 2011, S. 50). Dem folgend wurde der Leitfaden bis zu der in Anlage II. beigefügten Version angepasst, verfeinert und erweitert.

Insgesamt erfüllte dieser so entstandene Leitfaden damit die Aufgabe, die aus der Theorie und der Forschungsfrage abgeleiteten Thematiken strukturiert im Rahmen von empirischen qualitativen Experteninterviews zu behandeln. Das Vorgehen, um für die Durchführung geeignete Experten zu finden, anzusprechen und Interviews zu vereinbaren, ist im nächsten Kapitel beschrieben.

1.3.3 Expertenauswahl und Akquise

In diesem Kapitel ist beschrieben, wie die Auswahl der Experten erfolgt ist, wie die Anzahl der benötigten Interviews im Vorfeld abgeschätzt wurde und wie sich diese im weiteren Verlauf entwickelt hat. Es wird dargelegt, wie die Zusammensetzung der Gruppe geplant war, und

ebenfalls ist die praktizierte Methode zur Akquise erläutert, um auskunftsfähige und bereitwillige Teilnehmer zu erreichen. Grundsätzlich war eine Gruppe von Experten vorgesehen und im Vordergrund stand das jeweilige Expertenwissen, das in den vergangenen Jahren aufgebaut wurde, unabhängig davon, in welcher Firma und Position die Personen aktuell tätig sind. Die Auswahl der Teilnehmer an den Experteninterviews ist davon abhängig, welches Ziel mit der Untersuchung verfolgt wird (Gläser & Laudel, 2010, S. 40). Aus der Hauptzielstellung ergibt sich, dass die Managementaktivitäten im Bereich des Business Continuity Managements unter dem Einfluss der Digitalisierung zu analysieren sind. Damit bilden IT-Manager wie z. B. BC-Manager, IT-Notfallmanager, Katastrophenfallmanager, aber auch Beauftragte für die Digitalisierung in Unternehmen die Fokusgruppe. Eine Involvierung von IT-Fachkräften wurde als nicht zielführend oder ausreichend bewertet, da ggf. der notwendige Ausblick für zukünftig zu lösende Probleme hier nicht ausreichend ausgeprägt sein könnte. Es wurden, je nach Unternehmensgröße, verantwortliche Direktoren, deren Geschäftsfeld vorrangig die hier behandelten Themenbereiche betrifft, und möglichst Vertreter der Geschäftsführung interviewt.

Leitner und Wroblewski (2002, S. 249) empfehlen, dass anfangs nur eine erste und vorläufige Auswahl getroffen wird, da sich im Verlauf des Projektes noch Hinweise auf weitere mögliche und geeignete Interviewpartner ergeben können. Auch Bogner und Menz (2009, S. 75) berichten davon, dass sich aus den ersten Interviews noch Informationen ergeben, die bei der Suche nach weiteren Experten hilfreich sind. Dem folgend wurde mit der Interviewdurchführung unmittelbar begonnen, noch bevor eine größere Anzahl an möglichen Interviewpartnern angesprochen wurde. Dass die weitere Datenerhebung durch unmittelbare Erstauswertung der schon durchgeführten Interviews noch gesteuert werden kann, ist ein typisches Zeichen von qualitativen Studien und wird als zirkuläres Vorgehen bezeichnet (Döring, 2023, S. 26).

Die Auswahl der Experten erfolgte anhand folgender Kriterien: Die Teilnehmer sollten grundsätzlich in einem IT-Dienstleistungsunternehmen tätig sein. Falls entwickelte Produkte in der öffentlichen Verwaltung genutzt werden, sollten Produktanbieter aus der IT-Branche die Fokusgruppe ergänzen. Die Experten mussten Erfahrungen im Business Continuity Management haben und sollten die Themen praxisorientiert aus dem aktuellen oder früheren Unternehmen reflektieren können. Idealerweise sollten die Teilnehmer als verantwortliche Manager, IT-Notfallmanager oder BC-Manager tätig sein, die mit Vorgängen der digitalen Transformation für das eigene Unternehmen oder für öffentliche Auftraggeber erfahren sind.

Zwingende Voraussetzung war, dass die Dienstleistung unmittelbar oder das Produkt mittelbar von der öffentlichen Verwaltung genutzt wird. Es waren IT-Manager als Experten gesucht, die grundsätzlich bereits mit dem Business Continuity Management im Sinne des BSI-Notfallmanagements vertraut waren. Hier musste eine mehrjährige Erfahrungszeit vorhanden sein. Ebenfalls im Bereich des IT-Projektmanagements, der IT-Entwicklung und zu Digitalisierungstechnologien waren Projekterfahrungen notwendig, die die Experten mit Bezug zu Behörden, zur öffentlichen Verwaltung oder zu vergleichbaren Auftraggebern gesammelt haben.

So wurde sichergestellt, dass bei der Interpretation der Ergebnisse die geplanten Ziele der Arbeit erreicht werden können. Es wurden folgende Kanäle genutzt, um mögliche Kandidaten anzusprechen:

- Besuch von Fachmessen
- Internetrecherche und gezielte Kontaktaufnahme (E-Mail, Telefon)
- Anschreiben von Unternehmen auf Basis von Ausstellerlisten
- Ansprechen von Vertretern aus der Community, z. B. vom BSI
- Nutzung von Weiterempfehlungen durch erste Interviewpartner

In der konkreten Umsetzung geschah die Akquise wie folgt. Auf der jährlich stattfindenden Fachausstellung des Vereines ‚Anwenderforum für Fernmelde- und Computertechnik, Elektronik und Automatisierung' (AFCEA Bonn e. V.) im World Conference Center Bonn (WCCB) mit 200 Ausstellern und 35 Industrievorträgen wurden im Mai 2022 passende Unternehmen angesprochen. Diese Ausstellung des ursprünglich aus dem Bereich der Verteidigung entstandenen Vereins wird zunehmend von weiteren Vertretern aus dem Bereich der inneren und der öffentlichen Sicherheit besucht. IT-Beratungsfirmen, Hersteller und Großkonzerne stellen dort aus. Eine Ausstellerübersicht ist im Internet unter der Adresse *https://www.afcea.de/fachausstellung.html* (abgerufen 25.02.2023) einsehbar. Hier konnten mehrere Unternehmen angefragt werden, die im Rahmen der genannten Expertenauswahl und des ausgestellten Portfolios der Zielgruppe entsprechen.

IT-Unternehmen, die nicht nur auf den Bereich der Streitkräfte ausgerichtet waren, sondern bereits Produkte oder IT-Dienstleistungen in weiteren Behörden erbringen, wurden hier gezielt angesprochen. Im persönlichen Gespräch konnte das Forschungsprojekt grob dargestellt werden und durch den anschließenden Austausch der Kontaktdaten erfolgte in den darauffolgenden Tagen und Wochen die Vermittlung an entsprechende BCM-Experten.

Weitere Experten konnten durch gezieltes Anschreiben von Kontakten aus dem Ausstellerverzeichnis dieser genannten Fachausstellung gewonnen werden. Anzumerken ist, dass einige Unternehmen für die speziellen Thematiken des Business Continuity Managements auf externe Firmen verwiesen haben, deren Dienstleistungen sie selbst im Behördenkontext nutzen und empfehlen. Den Empfehlungen folgend, wurden die Kontakte direkt angesprochen, deren Leistungsspektrum und Referenzen nach einer Internetrecherche passend erschienen.

Die bereits genannte Methode zur Expertengewinnung auf Basis von Weiterempfehlungen nach den ersten Interviews wurde im weiteren Verlauf ebenfalls genutzt. Sowohl schon nach den Probeinterviews als auch im Rahmen der ersten Interviews der Hauptphase wiesen die Experten auf Bekannte anderer Bereiche hin, die hierzu angesprochen werden könnten. Auch diese Empfehlungen wurden aufgenommen und es ergaben sich interessante Interviewpartner, die im Fokus des Forschungsthemas kompetent ihre Erfahrungen teilen konnten.

Gezielt kontaktiert wurden auch Personen, die an Quellen, die im Teil I bereits zitiert wurden, mitgewirkt haben. Auch hier gab es Zusagen, so dass damit weitere Experten für Interviews gefunden wurden. Parallel zur Interviewakquise, -vorbereitung und -durchführung wurde kontinuierlich geprüft, ob Experten aus allen vorgesehenen Bereichen, die im übernächsten Absatz genannt werden, vertreten waren. Abschließend wurden weitere Firmen aus Branchen explizit angesprochen, damit sich das anvisierte Gesamtbild der Experten aus den relevanten Bereichen und Unternehmensgrößen ergeben hat.

Damit erfolgte die Expertenauswahl anhand der vorgesehenen Kriterien. Es mussten Erfahrung in den Bereichen des Business Continuity Managements und der Digitalisierung vorhanden sein und gleichzeitig musste der Bereich IT-Projektmanagement in der öffentlichen Verwaltung profund reflektiert werden können. Die Expertenakquise erfolgte zusammenfassend durch das gezielte Anschreiben von möglichen Unternehmen mit entsprechenden Kompetenzen und Experten, die Nutzung von Fachausstellungen, und die Kontaktaufnahme zu Personen, die empfohlen oder in einschlägigen Veröffentlichungen genannt wurden.

Qualitativ wurde zu Beginn des Forschungsprojektes definiert, dass es vorgesehen ist, Vertreter aus den Bereichen kleiner, mittlerer und großer behördenerfahrener IT-Dienstleister und -Anbieter zu interviewen. Dabei sollten sowohl klassische IT-Dienstleistungen beim bzw. für den Kunden als auch Service- und Produktanbieter einbezogen werden. Auf Basis der

theoretischen Erkenntnisse sollten Systemhäuser, Cloud-Spezialisten und Anbieter aus dem Bereich der Unternehmenssoftware berücksichtigt werden. Bei drei Unternehmensgrößen, zwei Arten der Leistungserbringung und drei Spezifikationen war geplant, quantitativ mindestens 18 Experten zu interviewen. Im Verlauf der Akquise und der Durchführung der Interviews ergab sich die Situation, dass mehrere Experten gewonnen werden konnten, die jeweils über Erfahrungen in mehr als einem der eben genannten Bereiche verfügen. Gleichzeitig war die Trennung nach klassischer IT-Dienstleistung beim Kunden und Produktanbietern nicht so trennscharf, dass eine Aufteilung ausreichend zielführend gewesen wäre. Auch die Produktanbieter verfügten über ein großes Angebot an IT-Dienstleistungen, so dass Erfahrungen aus ursprünglich unterschiedlichen Bereichen mehrfach jeweils von einem Experten bedient werden konnten. Zusätzlich verwiesen angeschriebene Kontakte auf Fremdfirmen und andere Beratungshäuser, bei denen sie selbst die entsprechende Unterstützung einkaufen. Darüber konnten Experten für die Interviews gewonnen werden, die sich durch branchenübergreifende Erfahrung auszeichnen, aber damit nicht mehr in die ursprüngliche Berechnung der Expertenauswahl passten. Ebenso berichteten die Experten nicht nur von ihren Erfahrungen aus dem aktuellen Beschäftigungsverhältnis, sondern erklärten auch BCM-Situationen früherer Stationen bei anderen Arbeitgebern. Damit erwies sich das ursprüngliche Kriterium der Firmengröße nicht mehr als ‚hartes' Auswahlkriterium.

Bereits im Vorfeld zu dieser Arbeit wurde davon ausgegangen, dass sich vor oder während der Interviewphase neue Erkenntnisse ergeben würden und die Berechnung anzupassen sein könnte. Auch nach Beginn der Interviewphase sollte die Möglichkeit bestehen, weitere oder andere Experten zu akquirieren. Gläser und Laudel (2010, S. 118) empfehlen dieses Vorgehen, wenn sich beispielsweise erst im Rahmen von Interviews Hinweise zu Experten ergeben, die zusätzlich berücksichtigt werden könnten. Mehrere Experteninterviews wurden exakt nach diesem Vorgehen arrangiert, bei denen sich die Eignung und die Auskunftsfähigkeit qualitativ als außerordentlich hoch gezeigt haben. Somit konnten die Erfahrungen von Experten aus allen vorgesehenen Bereichen in die Analyse einfließen.

Zur Wahrung der Anonymität wird der Expertenkreis hier nur grob dargestellt. Wie vorgesehen sind Experten aus den unterschiedlichen Unternehmensgrößen berücksichtigt. Eine separate Auflistung der anonymisierten Interviewpartner ist in Anlage I. beigefügt.

Sechs der Interviewpartner waren aktuell in Unternehmen tätig, die mit einem Jahresumsatz von teilweise deutlich über 100 Millionen Euro (bzw. US-Dollar) zu den großen Konzernen zählen, die sowohl in den Bereichen Digitalisierung und IT-Sicherheit beratend, aber auch als

Produktanbieter auf dem Markt vertreten sind. Weitere Experten kamen aus dem Bereich des Mittelstandes und sind sowohl mit Softwarelösungen als auch im Bereich Consulting für Cloud- und Sicherheitslösungen oder konkrete BCM-Lösungen tätig. Vier Experten lassen sich in ihrer aktuellen Tätigkeit den Klein- und Kleinstunternehmen zuordnen, die jedoch ebenfalls alle für den behördlichen Sektor in diesem Kontext tätig sind oder waren.

Damit wurde erreicht, dass sowohl hinsichtlich der Größe der Unternehmen als auch in Bezug auf die Ausrichtung als Produktanbieter oder Beratungsunternehmen jeweils mehrere Experten teilnahmen. Der wesentliche Inhalt aller Interviews und das Auswahlkriterium der Experten war in allen Fällen der vorhandene Bezug zum Business Continuity Management vor dem Hintergrund der Digitalisierung. Die qualitative Analyse der Interviews nach neuen Erkenntnissen wurde stetig durchgeführt, bis die später noch erläuterte Sättigung eintrat. Als Aspekt der Datenerhebung nennen Krüger und Riemeier (2014, S. 134) die Sättigung, die das Ende der Datenaufnahme bei der qualitativen Sozialforschung begründen kann, sobald keine neuen Erkenntnisse mehr hinzukommen. Die Anzahl der 14 durchgeführten Interviews hat sich als Ergebnis der Sättigungsanalyse, die in Kapitel III 1.3.7 dokumentiert ist, ergeben. Quantitativ entspricht diese Anzahl der durchgeführten Interviews auch dem von Döring (2023, S. 369) genannten Umfang von üblicherweise 10 bis 20 zu involvierenden Personen bei Leitfadeninterviews.

1.3.4 Halbautomatische Transkription

Die Interviews standen nach der Durchführung als Audiodatei auf dem lokalen Computer zur Verfügung. Für die Verschriftlichung, als ‚Transkription' bezeichnet, sind zunächst Regeln zu erstellen, wie dieser Schritt zu erfolgen hat (Kuckartz & Rädiker, 2022, S. 197). In Anlehnung an die Vorschläge von Kuckartz und Rädiker (2022, S. 200-201) wurde ein einfaches Regelsystem gewählt, indem wörtlich transkribiert wurde. Die Sprecherwechsel wurden durch Absätze kenntlich gemacht, unbedeutende Lautäußerungen wurden nicht transkribiert und es erfolgte eine leichte Glättung in das Schriftdeutsch. Sprechpausen und die Modulation der Stimme müssen nur erfasst werden, wenn diese auch Teil der Analyse sein sollen (Döring, 2023, S. 576). Unter Berücksichtigung des Forschungsproblems war das hier nicht notwendig.

Als halbautomatisch wird in diesem Kontext das Vorgehen bezeichnet, dass zunächst eine automatische Transkriptionssoftware genutzt wurde. Kuckartz und Rädiker (2020, S. 2) nennen hier unter anderem die Software f4x, mit der zwar eine automatische Transkription

erstellt werden kann, deren manuelle Nachbereitung aber dennoch unbedingt notwendig bleibt. Die Nutzung des Tools f4x lieferte dabei Ergebnisse, die in zahlreichen Abschnitten bereits exakt dem gesprochenen Wort entsprachen. Zur Sicherstellung, dass keine Transkriptionsfehler vorhanden sind, wurde anschließend das Dokument mehrfach manuell geprüft und überarbeitet. Diese Nachbearbeitung erfolgte im Tool MAXQDA durch Abhören der Audiodatei und Korrigieren der Texte. In MAXQDA lassen sich hierfür die Audio- und die Transkriptionsdateien miteinander verbinden, so dass die manuelle Überarbeitung einfach durchgeführt werden konnte. Danach standen sowohl die Interviews in Textform als auch die Tonaufnahmen während der Analyse zur Verfügung.

Dadurch wurde die im nachfolgenden Kapitel genannte Codierung dahingehend erleichtert, dass etwaige Betonungen oder ironische Bemerkungen mittels des Audiosignals verifiziert werden konnten. Die Ergebnisse dieser Vorgehensweise der halbautomatischen Transkription stehen in Anlage III. als vollständige Gesprächsprotokolle zur Verfügung.

1.3.5 Codierung in MAXQDA

Codierung bedeutet, dass für Passagen im Text eine Zuordnung zu Themenfeldern, die im Weiteren als ‚Kategorien' bezeichnet werden, erfolgt. Dabei ist die inhaltliche Bedeutung von Relevanz und Textpassagen können auch mehreren Codes zugeordnet werden (Misoch, 2019, S. 124). Wie in Kapitel III 1.2.2 bereits beschrieben, wurde eine deduktive und induktive Codierung zur Kategoriebildung und -zuordnung angewandt. Angelehnt an die Vorgehensweise von problemzentrierten Interviews kann dies als ‚induktiv-deduktives Wechselspiel' bezeichnet werden, wobei das vorhandene Vorwissen aus der Theorie in die Interviews eingebracht wird (Misoch, 2019, S. 71-72). Rädiker und Kuckartz erläutern das Prinzip, dass aus dem Leitfaden bereits die Kategorien abgeleitet und dabei diese stets an den Forschungsfragen reflektiert werden (2019, S. 99). Auf dieser Basis erfolgte die erste deduktive Codierung nach der Struktur des Leitfadens und den inhaltlichen Hauptthemen:

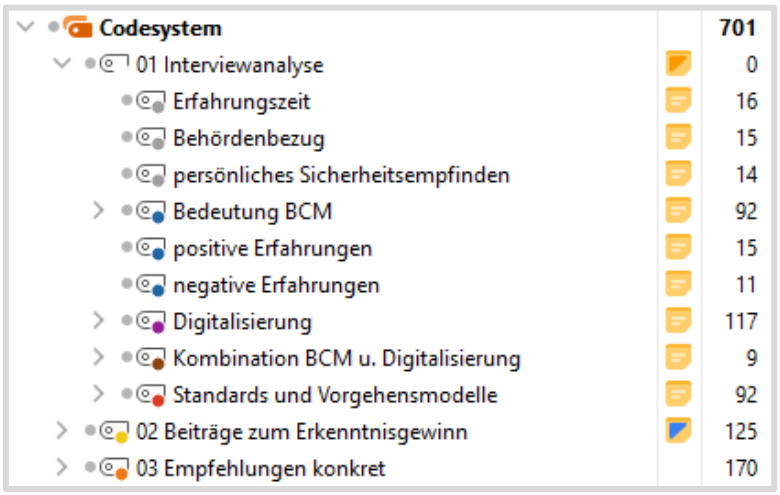


Abbildung 20 – MAXQDA-Codesystem erste Ebenen, deduktiv (Quelle: eigene Darstellung)

Die Abbildung zeigt die Codes, die am Leitfaden orientierten erstellt wurden, und die Anzahl der mit Stand März 2023 bereits zugeordneten Textpassagen. Wesentlich ist, dass auch für die weiteren Ebenen eine deduktive Analyse erfolgte, so dass sich beispielsweise unterhalb der Digitalisierung weitere vorab festgelegte Kategorien befinden. In diesem Kapitel zur Erläuterung des Forschungsdesigns wird lediglich das Prinzip anhand von Fallbeispielen dargestellt. Beispielhaft wurde mit ‚Bedeutung BCM' eine Hauptkategorie erstellt, die sich direkt aus den Forschungsfragen ableiten ließ. Dieses Vorgehen entspricht dem nach Früh (2017, S. 67) vorgesehenen Entwickeln des Messinstrumentes, bei dem beginnend aus den Forschungsfragen heraus durch einen deduktiven Analyseschritt entsprechende Hauptkategorien abgeleitet werden. Die weiteren Codierungen und Analyseergebnisse folgen in Kapitel III 2 und sind in der Anlage V. (Codebuch) und Anlage VI. (codierte Segmente) vollständig abgebildet.

Weiterhin deduktiv codiert wurden im Bereich der Digitalisierung dann Thematiken wie Cloud-Computing, Outsourcing oder Big-Data. Aus dem Bereich des Business Continuity Managements wurde unter anderem die Sicht der Geschäftsführung mit dieser Methode erfasst. Ebenfalls im Bereich der Standards und der Vorgehensmodelle waren Aussagen erwartbar, so dass Themenfelder wie die BSI-Standards oder die ISO-Normen vorab als Codes hinterlegt und dann in den Interviewtexten entsprechend markiert wurden.

Nach der Codierung wurden in MAXQDA sogenannte Sets angelegt, in denen ausgewählte Codes zu Interviews selektiert werden können. Beispielhaft abgebildet ist das Set ‚01 Interviewrahmen', mit dessen Hilfe die Interviewanalyse zeitsparend erfolgen konnte:

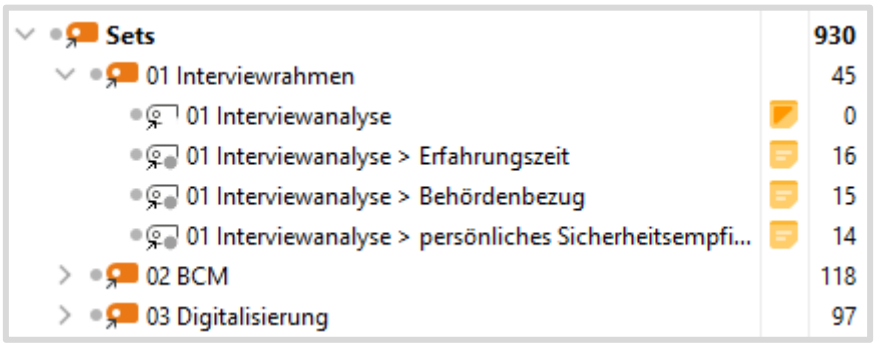


Abbildung 21 – MAXQDA-Setsystem erste Ebene (Quelle: eigene Darstellung)

Als vorhandene Kategorien dienten dabei die Gegenstände der Interviewfragen. Es erfolgte eine einfache Prüfung, ob diese Fragen behandelt wurden. Die Aussagen der Experten konnten auf diese Weise schnell codiert und dann einfach analysiert werden. Es gab hier erwartete Ergebnisse bei den Antworten, beispielsweise die Erfahrungszeit in Jahren. Diese wurden entsprechend im Tool markiert und anschließend qualitativ analysiert. Äquivalent dazu erfolgte die Strukturierung zu den beiden Hauptthematiken der Forschungsfragen: Business Continuity Management (oben abgebildet als Set ‚02 BCM') und ‚03 Digitalisierung'. Hier wurden die fachlichen Inhalte eingangs ebenfalls mit dem deduktiven Ansatz codiert und untersucht. Die Besonderheit besteht darin, dass durch die grundsätzlich halboffenen Fragestellungen deduktiv die Themen, Aspekte, Probleme oder Empfehlungen aus dem theoretischen Teil dieser Arbeit gesucht werden mussten. Diese lagen nicht unmittelbar als Antwort auf eine Frage vor. Es wurden die Aspekte der Digitalisierung als zu codierende Inhalte erwartet und die Zuordnung basiert damit auf den aus den theoretischen Grundlagen erarbeiteten Kategorien. Im nächsten Schritt erfolgte die induktive Codierung.

Als typisch für qualitative Forschung bezeichnen Rädiker und Kuckartz das Vorgehen, die Bildung der Kategorien erst am vorhandenen Datenmaterial vorzunehmen (2019, S. 102). Dies ergab sich insbesondere bei Fragestellungen der Art ‚Warum denken Sie, dass das so ist …' oder ‚Welche Empfehlungen würden Sie geben für …'. Diese Fragen wurden ergebnisoffen gestellt und ohne eine vorgegebene Auswahl an Kategorien wurden für die Antworten neue Codes angelegt. Mayring folgend wurde als Bezeichnung der Kategorie ein Begriff nahe am selektierten Text gewählt und regelmäßig die Gesamtlogik des Kategoriesystems überprüft (2023, S. 99-100). Demzufolge wurde bei der Neuaufnahme von Codes jeweils das bereits analysierte Material einer erneuten Prüfung unterzogen, um sicherzustellen, dass Aspekte zu diesem Punkt von allen Experten zusammenfassend betrachtet und ausgewertet werden können.

Die Ergebnisse der Codierung sind im Ergebniskapitel III 2.1.2 aufgelistet und vollständig in Anlage VI. nach dem Codebuch als Anlage ‚Codierte Segmente' beigefügt. Damit entstand ein Codesystem in MAXQDA, das anfangs 52 Codes beinhaltete, die anschließend in Gruppen als Sets zusammengefasst wurden. Darüber wurde eine weitere Gruppierung als oberste Hierarchieebene angelegt, um den Inhalt strukturiert analysieren zu können. Die Sets dienten einerseits der Unterteilung zur Interviewanalyse, andererseits konnte damit geprüft werden, ob die Interviewpartner der Zielgruppe entsprechen und ob alle Themen des Leitfadens behandelt wurden. Es wurde geprüft, dass es keine vorgesehenen Fragen gab, die lediglich von wenigen oder keinem Experten betrachtet wurden. Textpassagen, die sich direkt den Fragestellungen aus den Forschungsfragen zuordnen ließen, wurden unter dem Stichwort ‚Beiträge zum Erkenntnisgewinn' zusätzlich klassifiziert. Abschließend wurden konkrete Empfehlungen zur gesamten Thematik des Forschungsprojektes entsprechend markiert.

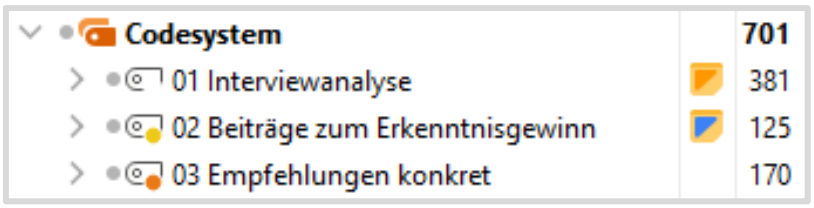


Abbildung 22 – MAXQDA-Codesystem, erste Strukturebene (Quelle: eigene Darstellung)

Mit Analysestand März 2023 waren bereits 170 Empfehlungen in den Interviews codiert, so dass die weitere qualitative Analyse auf diese codierten Segmente angewandt werden konnte und hier im Ergebnisteil beschrieben ist. Damit ist das grundsätzliche Prinzip der Codierung in MAXQDA im Rahmen dieses Forschungsdesigns dargelegt.

1.3.6 Prüfung durch die Experten

Nach der in Kapitel III 1.3.4 beschriebenen Verschriftlichung der Interviews wurden die Transkripte als Word-Dokument dem jeweiligen Experten zur Verfügung gestellt. Mit dieser Methode kann sichergestellt werden, dass in den Dokumenten die Erfahrungswirklichkeit abgebildet ist, und es lassen sich Missverständnisse ausräumen (Döring, 2023, S. 576). Bereits mit der Einverständniserklärung zur Teilnahme an den Experteninterviews war mit allen Teilnehmern vereinbart, dass sie das Protokoll zur Durchsicht erhalten und Aussagen löschen und korrigieren dürfen, bevor diese weiterverwendet werden. Das wurde mit der genannten Vorgehensweise zur Prüfung der transkribierten Interviews durch die Teilnehmer erfüllt. Im Ergebnis bestand allerdings kein Veränderungsbedarf an den Protokollen nach der Prüfung

durch die Teilnehmer. Als Antworten auf die Übermittlung gab es aufschlussreiche Kommentare und es wurde das Interesse am weiteren Verlauf des Projektes geäußert.

1.3.7 Sättigungsanalyse

In diesem Kapitel ist das grundsätzliche Prinzip zur durchgeführten Überprüfung, ob noch weitere Interviews zu arrangieren waren, beschrieben. Unter der theoretischen Sättigung ist nach Döring (2023, S. 26) die Situation zu verstehen, dass keine neuen Erkenntnisse mehr generiert werden; hierzu erfolgt eine vorläufige Datenauswertung und die Datenerhebung wird ansonsten fortgesetzt. Ob mit weiteren Interviews ein zusätzlicher Erkenntnisgewinn zu erwarten ist, wurde fortlaufend anhand einer Redundanz der vorliegenden Antworten und Ergebnisse geprüft. Damit wurde verifiziert, ob bereits die theoretische Sättigung insgesamt eingetreten ist. Die Datenerhebung wurde beendet, als weitere Untersuchungen keinen Erkenntniszuwachs versprachen, wie Eisend und Kuß (2021, S. 148) es an einem Beispiel zur theoretischen Sättigung erklären.

Die Analyse der Sättigung bezieht sich auf die Fachfragen ab IF03, da die ersten Fragen an die interviewte Person zum persönlichen Hintergrund und zum Sicherheitsempfinden stets neue Erkenntnisse erbringen und für eine Sättigungsanalyse nicht relevant sind.

Die Fragen im Bereich der Bedeutung und der Berücksichtigung des Business Continuity Managements ließen bereits verschiedene Antwortmöglichen zu. Allerdings waren diese im erwarteten Antwortspektrum ebenfalls noch eingeschränkt. Die Antworten der Art, dass es eine geringe oder hohe Bedeutung hat oder dass es viel oder wenig Berücksichtigung findet, können für eine Sättigungsanalyse ebenfalls nicht genutzt werden. Erst die begründenden Aussagen dazu wurden untersucht. Auch die Fragen nach dem Aufwand/Nutzen und der Bewertung von Business Continuity Management als Projekthemmnis ließen nur wenig Antwortmöglichkeiten zu, wie teilweise ‚Ja' oder ‚Nein', so dass hier eine Sättigungsanalyse aus fachlicher Sicht ebenfalls nicht anzuwenden ist. Hier wurden ebenfalls die erfolgten Begründungen zu dieser Situation qualitativ analysiert, um Wiederholungen zu erkennen und eine bereits eingetretene Sättigung abschätzen zu können.

Insbesondere aus dem induktiven Anteil der Codierung wurde ersichtlich, ab wann sich keine neuen Kategorien aus dem Datenmaterial mehr ableiten ließen, wann keine neuen Empfehlungen ausgesprochen wurden oder keine neuen Zusammenhänge genannt wurden, die zur Beantwortung der Forschungsfragen relevant sind. Neben diesen grundsätzlichen

Prinzipien ist die durchgeführte Sättigungsanalyse mit dem erhobenen Datenmaterial im Ergebniskapitel III 2.2.5 erläutert.

1.4 Vorgehen und Ablauf

In diesem Kapitel ist das Vorgehen mit allen operativen Schritten beschrieben, wie das soeben erläuterte Forschungsdesign umgesetzt wurde. Die folgenden drei Kapitel sind chronologisch verfasst, so dass erkennbar ist, wie von der Theorie ausgehend die empirische Phase aufgebaut und durchgeführt wurde. Hierzu ist zuerst die operative Schrittfolge visualisiert und erläutert. Der Ablauf der Experteninterviews wird dokumentiert und im letzten Unterkapitel sind die durchgeführte Codierung und die Analyse beschrieben. Im darauffolgenden Kapitel III 2 sind die konkreten Ergebnisse dokumentiert.

1.4.1 Operative Schrittfolge

Die Vorgehensweise im empirischen Teil ist in der folgenden Abbildung 23 dargestellt. Nach vorläufig abschließender Ausarbeitung der theoretischen Grundlagen waren die Themen festgelegt und ein erster Fragenkatalog wurde entworfen. Gleichzeitig wurden die Kriterien für die Expertenauswahl verfeinert, so dass die Akquise geeigneter Interviewpartner über die bereits beschriebenen Wege erfolgen konnte. Mithilfe von Probanden wurde der Leitfaden getestet und die Ergebnisse des Tests wurden validiert. Als Konsequenz wurden die Details der Interviewführung, der Eröffnungsdialog und die Reihenfolge sowie die Formulierung der Fragestellungen optimiert. Im Anschluss wurde die erste Version des Leitfadens finalisiert und die Interviewphase mit den Experten begann. In dieser Phase waren weitere Anpassungen am Leitfaden und hinsichtlich der Auswahlkriterien für Experten möglich und wurden umgesetzt. Baur und Blasius sehen dieses Vorgehen als integralen Bestandteil des qualitativen Forschungsprozesses, vor allem dann, wenn neue Inhalte, Themen oder Aspekte erforscht werden (2022, S. 13). Dieser iterative Prozess ist in der Abbildung an den zwei nach oben gerichteten Pfeilen erkennbar. Es besteht aus der Interviewphase heraus sowohl die Möglichkeit, den Leitfaden anzupassen als auch weitere Experten für die Teilnahme an den Interviews zu werben. In allen Fällen wurden die Protokolle, die zunächst lediglich als Audiodatei vorlagen, transkribiert, um eine Codierung und eine Analyse vornehmen zu können.

Diese Schritte wiederholten sich, bis keine neuen Erkenntnisse mehr zu erwarten waren und von einer theoretischen Sättigung auszugehen war. Aufgrund der wiederholt durchgeführten Einzel- und Gesamtanalyse aller Protokolle stand zu diesem Zeitpunkt bereits ein Analyseergebnis in MAXQDA zur Verfügung. Dieses Ergebnis wurde abschließend so aufbereitet, dass es als Grundlage für den gestalterischen Teil zur Anwendung kommen konnte.

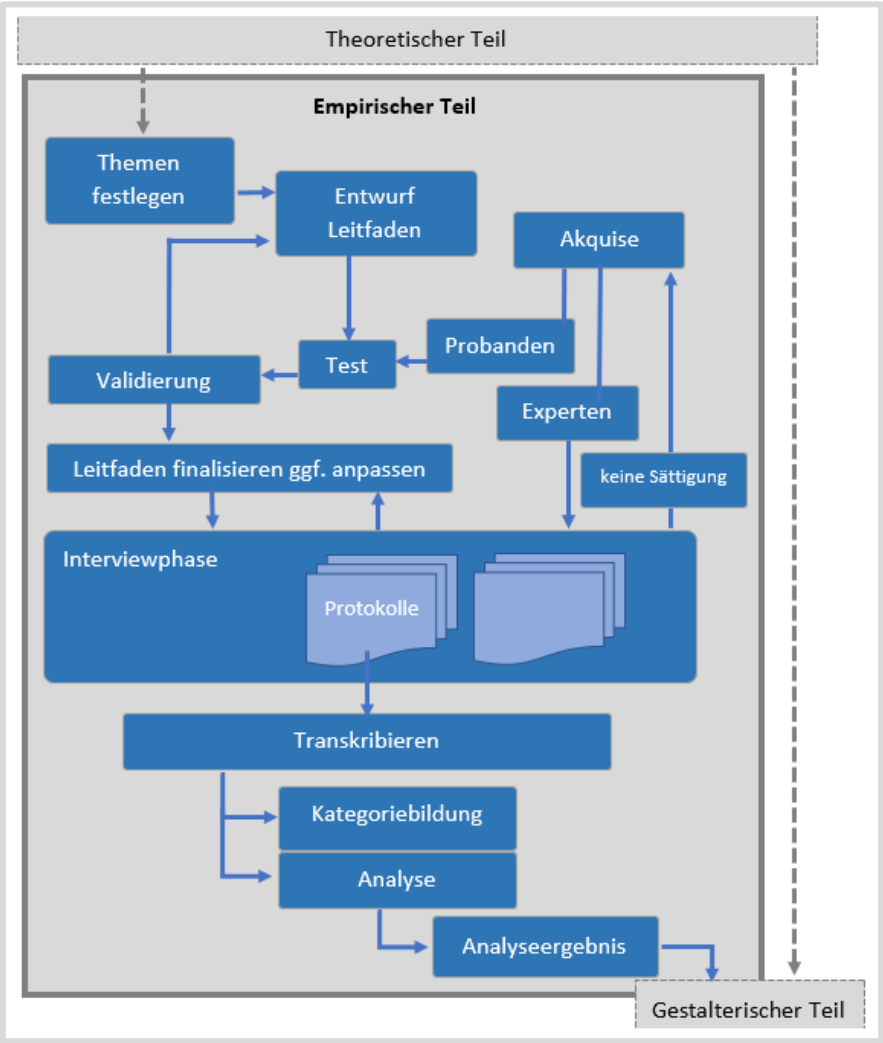


Abbildung 23 – Visualisierung des Vorgehens im empirischen Teil (Quelle: eigene Darstellung)

Zu den Aussagen im gestalterischen Teil war jeweils ein Bezug zu den theoretischen Grundlagen und Erkenntnissen herzustellen, so dass die Theorie, wie auf der Abbildung durch die gestrichelten Pfeile ersichtlich, nicht ausschließlich für die Gestaltung der Empirie genutzt wurde. Damit bilden das Analyseergebnis und die theoretischen Ergebnisse die Grundlage zur Ausarbeitung und Beantwortung der gestaltungsgeleiteten Fragestellungen.

Der Vorbereitungszeitraum von Dezember 2021 bis April 2022 nahm zirka fünf Monate in Anspruch. Die Hauptphase der Interviewdurchführung von April 2022 bis November 2022 dauerte zirka acht Monate. Als besonders zeitaufwändig erwiesen sich hier die

Transkriptionsarbeit und die Codierung des Materials. Die Codierungs- und Analysearbeit begann bereits nach den ersten Interviews und dauerte insgesamt zirka ein Jahr an, bevor die Ergebnisse im Rahmen der Erstellung der Dissertationsschrift verfasst wurden. Damit ist der Ablauf des gesamten Vorgehens in der empirischen Phase erläutert. Es schließen sich die Kapitel zum Ablauf der Experteninterviews sowie zur Codierung und Analyse an.

1.4.2 Ablauf Experteninterviews

Die Experteninterviews wurden im Zeitraum von April 2022 bis November 2022 durchgeführt. Die verschiedenen Wege, um geeignete Experten anzusprechen und mit ihnen einen Interviewtermin zu vereinbaren, wurden bereits im Unterkapitel zur Operationalisierung dokumentiert.

Vor dem Termin zur Interviewdurchführung wurden keine inhaltlichen Fachdiskussionen zum Business Continuity Management oder zur Digitalisierung geführt. Es wurde allerdings das Forschungsvorhaben per Gespräch, Telefonat oder per E-Mail vorab vorgestellt und die Einverständniserklärung auf Basis der Datenschutzgrundverordnung (DSGVO) erbeten, die auch zu Beginn eines jeden Interviews zusätzlich besprochen wurde. Den Erläuterungen von Döring folgend wurden alle Teilnehmer gründlich und verständlich über die Studie informiert und erklärten ihr ausdrückliches Einverständnis zur Teilnahme (2023, S. 121-122). Dabei wurde die Anonymisierung zugesagt und die Möglichkeit offeriert, das Interview jederzeit beenden zu können. Auch dass nachträglich noch ein Widerrufen der Einwilligungserklärung erfolgen kann, wurde erwähnt. Aufwandentschädigungen wurden nicht gezahlt. Interviewabbrüche oder Rücktritte von der Einverständniserklärung gab es nicht. Der Text der Einverständniserklärung ist als Anlage IV. beigefügt.

Die Terminvereinbarung erfolgte per E-Mail mit der entsprechenden Person oder dem Sekretariat. Es war in allen Fällen eine Durchführung als Videokonferenz mit elektronischer Aufzeichnung des Audiosignals vereinbart. Der prinzipielle Ablauf wurde bei allen Interviews in der gleichen Form eingehalten. Zu Beginn und noch vor Aufzeichnung erfolgte die obligatorische Begrüßung. In dieser Einleitungsphase wurden alle Punkte, wie von Bogner et al. (2014, S. 59-60) beschrieben, angesprochen: Nach einem Dank für die Gesprächsbereitschaft folgten eine Kurzvorstellung des Interviewers und des institutionellen Hintergrunds sowie eine Erläuterung des halboffenen Interviewleitfadens und der zeitlichen Planung.

Danach entsprach der Ablauf dem Leitfaden, wie er in Kapitel III 1.3.2 vorgestellt wurde. Die detaillierten Gesprächsführungen sind dieser Arbeit als Anlage III. beigefügt. Anfangs wurden die drei Fragen zur Erfahrungszeit im Bereich Business Continuity Management, zum Behördenbezug und zum persönlichen Sicherheitsempfinden gestellt. Anschließend erfolgte der erste Themenblock zum Business Continuity Management mit offenen Fragestellungen, damit der Experte diesen Bereich mit hoher Relevanz für die Forschungsfragen unbeeinflusst aus seiner Sicht darstellen konnte. Im Ablauf schlossen sich sodann die vorgesehenen Fragestellungen im zweiten Block aus dem Bereich der allgemeinen und der behördenrelevanten Digitalisierung an.

Herausfordernd für den Ablauf der Experteninterviews war es hier, dass im dritten Block die fokussierte Betrachtung von Argumenten aus dem ersten und zweiten Block gemeinsam angesprochen werden sollte. In vielen Fällen thematisierten die Experten allerdings unaufgefordert sofort diese kontextbezogenen Zusammenhänge. Da genau diese Erkenntnisse einen Schwerpunkt der Datenerhebung darstellen, wurde nicht steuernd durch die Interviewmoderation eingegriffen. Der Ablauf in später durchgeführten Interviews wurde dahingehend optimiert. Fortan wurde anfangs mitgeteilt, dass die Experten im Verlauf des Gesprächs sich ergebende direkt Zusammenhänge zwischen Business Continuity Management, Digitalisierungsprojekten und Behörden-IT oder Empfehlungen hierfür jederzeit nennen können.

Der zeitliche Verlauf bis zum dritten Block gemäß Leitfaden gestaltete sich unterschiedlich, so dass fallweise mehr oder weniger stark eingegriffen werden musste, damit in der gleichen Art noch die vorgesehenen Themengebiete zu Standards, Normen und Gesetzen behandelt werden konnten. Abschließend wurden die zusammenfassenden Fragenstellungen angesprochen und hier argumentierten viele Experten reflektierend zu den bereits getätigten Äußerungen und gaben ihre Prognosen ab. Als Letztes wurde gefragt, ob aus Sicht des Teilnehmers relevante Aspekte vergessen wurden (Bogner et al., 2014, S. 59-60). Damit wurde das Ende des Interviews eingeleitet, und sobald es keine weiteren Beiträge gab, wurde die Aufzeichnung des Interviews angekündigt beendet. Nach dem Interview konnten noch Fachthemen diskutiert werden, die teilweise die Sichtweisen des Interviewleiters beinhalteten und somit nicht in den Datenbestand des Forschungsvorhabens eingeflossen sind. Alle Interviews endeten mit der Verabschiedung und dem Hinweis, dass das schriftliche Protokoll in den drauffolgenden Wochen zur Verfügung gestellt wird.

1.4.3 Ablauf Codierung und Analyse

Ergänzend zur bereits in Kapitel III 1.3.5 dargestellten prinzipiellen Codierung mittels MAXQDA wird hier der Ablauf der Codierung und der Analyse beschrieben. Die Codierung konnte erst erfolgen, nachdem die Transkripte in ausreichender Qualität vorlagen. Vor der ersten Codierung wurde, basierend auf den Forschungsfragen und den daraus abgeleiteten Interviewfragen, ein erstes Code-Set erstellt und damit das Codesystem aufgebaut. Dies erfolgte in MAXQDA mit der Funktion ‚Neuen Code einfügen'. Die neuen Codes wurden hierarchisch strukturiert und als sogenannte Subcodes mit Beschreibung und Farbgebung hinterlegt, um auf diese Weise ein dokumentiertes Kategoriesystem zu erzeugen. Es wurden Codes wie ‚persönliches Sicherheitsempfinden', ‚Bedeutung BCM aus Sicht der Geschäftsführung' oder ‚Cloud-Computing' angelegt, die anschließend mittels Drag-and-Drop selektierten Textpassagen zugewiesen werden konnten. Der weitere Ablauf und die wiederkehrende Überarbeitung des Kategoriesystems folgten dem Ablaufmodell nach Mayring:

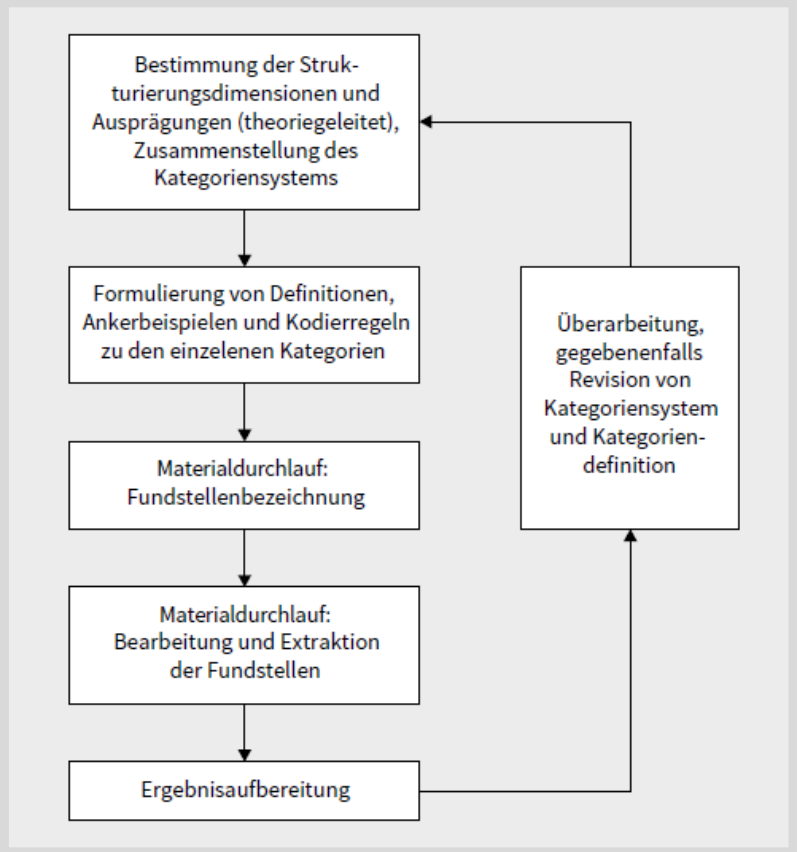


Abbildung 24 – „Ablaufmodell strukturierender qualitativer Inhaltsanalyse" (Quelle: Mayring, 2023, S. 103)

Mit den ersten erstellten Codes folgte der Materialdurchlauf, wobei das Kategoriesystem direkt induktiv ergänzt wurde. Die Extraktion und die Aufbereitung gestalten sich in MAXQDA

einfach, da sich alle codierten Segmente in verschiedenen Ansichten und mit Exportfunktion beliebig arrangieren lassen. Damit wurden die qualitative Analyse und die Ergebnisaufbereitung deutlich erleichtert. Wie in der Abbildung vorgesehen, wurde nach der Ergebnisaufbereitung das Kategoriesystem wiederholend überarbeitet, wonach stets wieder ein Materialdurchlauf erfolgen musste, damit keine inhaltlich nicht mehr gültigen Codierungen im System bestehen blieben.

Es wurden teilweise auch Gesprächssegmente mehreren Codes zugewiesen und gleiche Codes wurden in einem Interview an verschiedenen Stellen markiert. Mittels der Funktionalität ‚Codierte Segmente' von MAXQDA konnte in jedem Interview schnell verifiziert werden, ob die gesuchten Codes gefunden wurden oder ob bei dieser manuellen Codierung noch Fundstellen übersehen wurden. Es gab durchaus die Situation, dass Experten an wenigen erwarteten Stellen keine Aussagen getätigt hatten und somit für einzelne Aspekte in diesem Interview keine Markierung vorlag. Da in der späteren Analyse jeweils der Gesamtüberblick über alle Segmente zur Verfügung stand, konnte die Aussagefähigkeit aller oder einzelner Experten stets berücksichtigt werden.

Gleichzeitig erfolgte bereits die Markierung von bemerkenswerten Textstellen, die im Rahmen der Analyse berücksichtigt werden sollten, für die aber noch kein konkreter Code angelegt worden war. Insbesondere bei den Empfehlungen wurde jeweils ein übergreifendes Schlagwort aus dem Text ermittelt, das dann in diesem und anderen Interviews codiert wurde. Beispiele hierfür sind ‚Verständnis schaffen', ‚Transparenz' oder ‚Beübungen' auf deren Herleitung und Auswertung im Ergebniskapitel eingegangen wird.

Ebenso erfolgte in diesem Codierungsschritt das Erstellen von Codes zur Digitalisierung und bei der freien Äußerung zur Gesamtsituation des Business Continuity Managements im Zeitalter der Digitalisierung. Diese dann jeweils erstmalig erstellten Codes wurden anschließend in allen Interviews gesucht, geprüft und markiert, womit eine objektive Beurteilung des Sättigungsgrades vorgenommen werden konnte.

Die qualitative Inhaltsanalyse des Materials erfolgte nach Zusammenstellung aller codierten Segmente zu einer Kategorie. Der konkrete Ablauf stellte sich so dar, dass ein strukturierter Export aller codierten Segmente aus MAXQDA nach Microsoft Excel durchgeführt wurde. Hier konnte nach mehrfachem Lesen, Bewerten und Kommentieren zu allen Kategorien eine Zusammenfassung auf Basis aller Interviews erarbeitet werden. Diese wurde für das nachfolgende Kapitel als Ergebnis aufbereitet.

Bereits während der Erarbeitung der Ergebnisse wurde darauf geachtet, dass Gütekriterien einer empirischen Forschung eingehalten werden. Nach Mayring (2023, S. 119) sollte am Ende der Forschungsarbeit diese Einschätzung der Qualität der Ergebnisse vorgenommen werden. Bereits im Exposé zu dieser Arbeit wurde die konkrete Umsetzung hierzu in Abhängigkeit von der tatsächlich erzeugten Kategorien genannt, so dass die Auswahl, die Umsetzung und das Ergebnis in Kapitel III 3.2.1 nach der Ergebnisdarlegung folgen.

2 Ergebnisse

Nach Anwendung der im vorherigen Kapitel erläuterten Forschungsmethode und der gewählten Analysemethoden werden in diesem Kapitel die erarbeiteten Ergebnisse dargestellt. Im Fokus befinden sich hier die fachspezifischen Auswertungen, die zur Beantwortung der Forschungsfragen führen und in Verbindung mit den theoretischen Grundlagen die Basis für nachvollziehbare und valide Empfehlungen bilden. Nach einer kurzen Darstellung der Auswertung mit Teilergebnissen in Kapitel III 2.1 liegt der Schwerpunkt in Kapitel III 2.2 auf der Präsentation aller relevanten Ergebnisse.

2.1 Auswertung der Ergebnisse

Die Nutzung des Tools MAXQDA und die Anwendung der qualitativen Inhaltsanalyse nach Mayring wurden bereits im vorherigen Kapitel beschrieben. Wie sich durch Anwendung dieser Methode die Ergebnisse und Teilergebnisse ableiten lassen, ist in den folgenden zwei Unterkapiteln zur Codierung des Materials und zur inhaltlichen Auswertung beschrieben. Es wird der Gesamtumfang der Codierung erläutert und darauf eingegangen, wie anschließend die Selektion der relevanten Anteile erfolgte, die ausführlich in Kapitel III 2.2 kontextbezogen zu den Forschungsfragen dargestellt sind.

2.1.1 Codierung des Materials

Deduktive Codierung

Die Codierung erfolgte durch Zuordnung von Textpassagen zu Codes, mit denen das Kategoriesystem bereits vorbereitend aufgebaut war. In einem ersten Schritt wurde die Codierung auf Basis der Forschungsfragen (IF01 bis IF18) und der erwartbaren Ergebnisse zu den jeweiligen Themenkomplexen durchgeführt. In beiden Fällen waren die Kategorien vorab bekannt und es konnten die vorbereiteten Codes zugewiesen werden. Für den ersten Teil war der Interviewleitfaden der Bezug. Aufwändiger war der zweite Teil, bei dem die deduktive Codierung auf Basis der aus der Theorie herausgearbeiteten Punkte vorzunehmen war. Hierzu waren die verschiedenen Aspekte der Digitalisierung, die im Theoriekapitel bereits genannt wurden, der erwartete Bereich der Antworten, auch ohne dass diese durch den Interviewleiter aktiv angesprochen wurden. Für das Beispiel der Interviewfrage 08 (IF08) zu den relevanten

Aspekten der Digitalisierung aus Sicht der Experten ist dieser Ausschnitt des Kategoriesystems in der nachfolgenden Abbildung dargestellt:

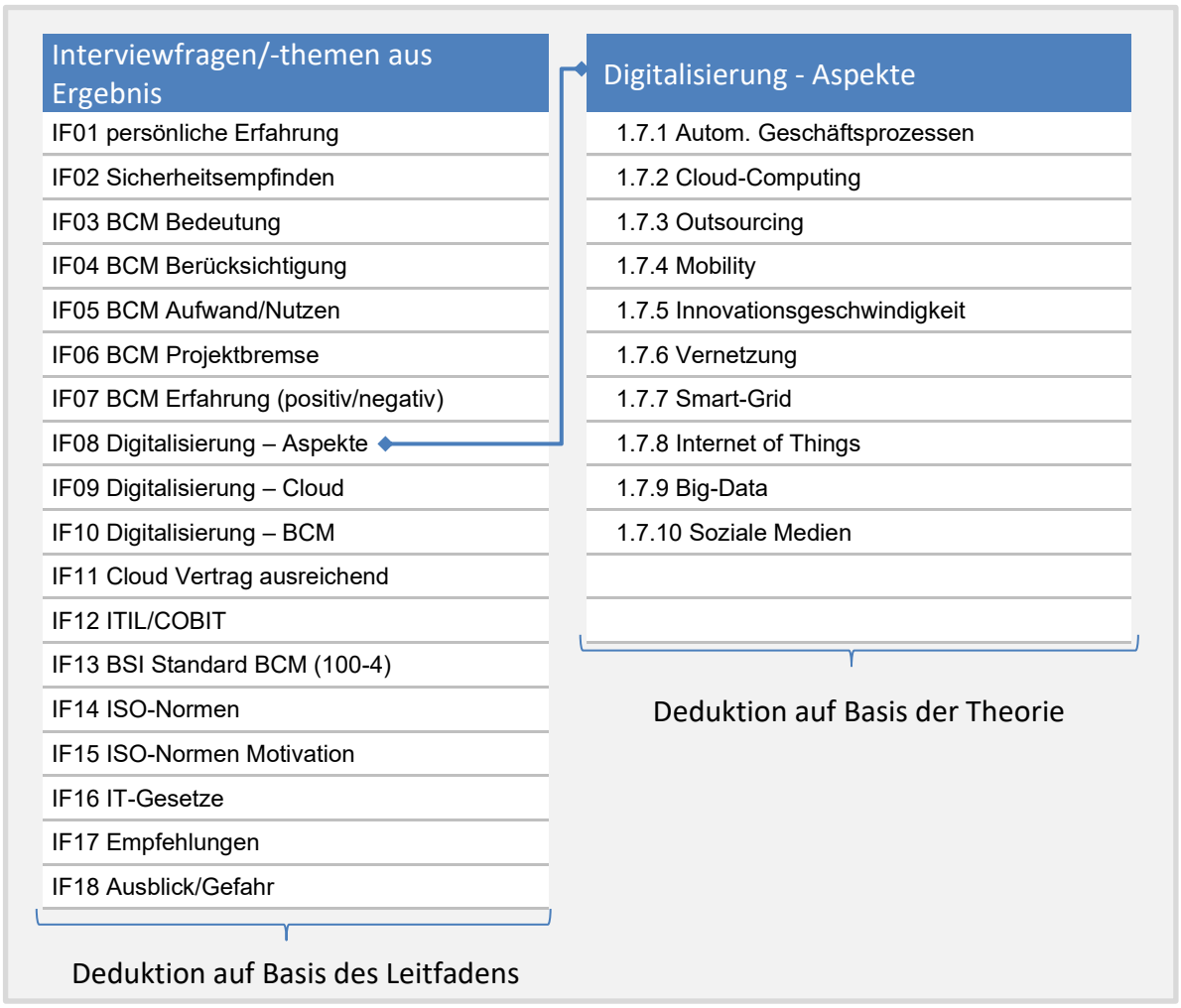


Abbildung 25 – Auszug deduktive Codierung (Quelle: eigene Darstellung)

Alle Codes des Kategoriesystems sind im Codebuch in Anlage IV. dokumentiert. Diese deduktive Codierung erfolgte für alle Forschungsfragen und in weiteren Unterkategorien mit Subcodes, wenn hierzu bereits aus der Theorie Aussagen erwartet wurden. In allen Bereichen war es während der qualitativen Inhaltsanalyse möglich, auch neue Codes zu erstellen. Bei dem hier erläuterten Beispiel war das unter anderem der Aspekt ‚Digitales Mindset', der von mehreren Experten zur Fragestellung genannt oder umschrieben wurde. Solche Codes ergänzten induktiv das Kategoriesystem.

Induktive Codierung

Neben den genannten induktiven Erweiterungen von vorhandenen Kategorien durch Subcodes wurden auch Hierarchieknoten vorbereitet, für die grundsätzlich noch keine Codes mit Bezug zu erwartbaren Antworten angelegt worden waren. In der nachfolgenden Abbildung sind angelegte Codes aufgelistet, die sich erst auf Basis der Auswertung des

Datenmaterials ergeben haben. Für die Bereiche ‚Beiträge zum Erkenntnisgewinn' und ‚Empfehlungen konkret' wurden als Codebezeichnungen kurze Schlagworte gewählt, unter denen die verschiedenen Aussagen der Experten zur gemeinsamen Betrachtung gruppiert werden konnten. Wesentlich ist hier, dass aus dieser prägnanten Kurzbezeichnung noch keine Schlüsse zu ziehen sind. Weder eine Reihenfolge oder Gewichtung noch inhaltliche Aussagekraft sind damit verbunden. Die Bedeutung des gewählten Begriffes ist ausführlich im Ergebnisteil herausgearbeitet. Die Herleitung von Erkenntnisgewinnen und deren Ausarbeitung bilden einen wesentlichen Teil der Forschungsarbeit. Die übergeordneten Schlagworte sind in Abbildung 26 aufgelistet.

Beiträge zum Erkenntnisgewinn und konkrete Empfehlungen	
2 02 Beiträge zum Erkenntnisgewinn	3 03 Empfehlungen konkret
2.1 Fachkräftemangel	3.1 Verständnis schaffen
2.2 Digitalisierung verstehen	3.2 wann berücksichtigen
2.3 neue Methoden	3.3 Transparenz
2.4 digitale Souveränität	3.4 technische Aspekte
2.5 Treiber Privatwirtschaft	3.5 Beübungen
2.6 ISO-Normen Umsetzung	3.6 Vorgehen
2.7 ISO-Normen Motivation	3.7 Digitalisierung ganzheitlich verstehen
2.8 BCM in der Praxis	3.8 BCM-Stellenwert erhöhen
2.9 BCM in aktuellen Krisen	3.9 Personal
2.9.1 Pandemie	
2.9.2 Hochwasser	
2.9.3 Ukraine-Konflikt	

Abbildung 26 – Auszug induktiv erstellter Codes (Quelle: eigene Darstellung)

Beispielgebend sind hier die aktuellen Krisen zu nennen, die seitens verschiedener Experten genannt wurden. Diese waren im Interviewleitfaden nicht vorgesehen, wurden aber mehrfach im Zusammenhang zu einigen Interviewfragen durch die Teilnehmer angesprochen.

Mit der Coronapandemie, dem Ahrtal-Hochwasser oder dem Ukraine-Konflikt wurde geschildert, wie unerwartete Schadensgroßereignisse stattfinden können, und passend zur Forschungsthematik wurden dann Zusammenhänge zur IT und zum Business Continuity Management aus Sicht des Experten dargelegt. Durch diese neu erstellten Codes und deren Zuordnung in allen Interviews ermöglichte MAXQDA eine schnelle Betrachtung und Analyse der relevanten Aussagen unterschiedlicher Experten hierzu. Insgesamt ergab sich das in Abbildung 27 dargestellte Kategoriesystem.

1 01 Interviewanalyse
1.1 Erfahrungszeit
1.2 Behördenbezug
1.3 persönliches Sicherheitsempfinden
1.4 Bedeutung BCM
1.4.1 ausreichende Berücksichtigung?
1.4.2 Geschäftsführung
1.4.3 Aufwand/Nutzen
1.4.4 Projektbremse?
1.5 positive Erfahrungen
1.6 negative Erfahrungen
1.7 Digitalisierung
1.7.1 Autom. von Geschäftsprozessen
1.7.2 Cloud-Computing
1.7.3 Outsourcing
1.7.4 Mobility
1.7.5 Innovationsgeschwindigkeit
1.7.6 Vernetzung
1.7.7 Smart-Grid
1.7.8 Internet of Things
1.7.9 Big Data
1.7.10 soziale Medien
1.8 Kombination BCM u. Digitalisierung
1.8.1 Verträge Dienstleistung Hosting
1.8.2 IT-Projekte
1.9 Standards und Vorgehensmodelle
1.9.1 ITIL, COBIT
1.9.2 BSI-Standards
1.9.3 ISO-Normen
1.9.4 Gesetze
2 02 Beiträge zum Erkenntnisgewinn
2.1 Fachkräftemangel
2.2 Digitalisierung verstehen
2.3 neue Methoden
2.4 digitale Souveränität
2.5 Treiber Privatwirtschaft
2.6 ISO-Normen Umsetzung
2.7 ISO-Normen Motivation
2.8 BCM in der Praxis
2.9 BCM in aktuellen Krisen
2.9.1 Pandemie
2.9.2 Hochwasser
2.9.3 Ukraine-Konflikt
2.10 Ausblick
2.10.1 Sicherheitsniveau zukünftig
3 03 Empfehlungen konkret
3.1 Verständnis schaffen
3.2 wann berücksichtigen
3.3 Transparenz
3.4 technische Aspekte
3.5 Beübungen
3.6 Vorgehen
3.7 Digitalisierung ganzheitlich verstehen
3.8 BCM-Stellenwert erhöhen
3.9 Personal

Abbildung 27 – Strukturiertes Kategoriesystem (Quelle: eigene Darstellung)

Unterhalb der drei Hauptkategorien ‚01 Interviewanalyse', ‚02 Beiträge zum Erkenntnisgewinn' und ‚03 Empfehlungen konkret' wurden in weiteren Hierarchien die Codes arrangiert, die in MAXQDA beschrieben und Textpassagen zugeordnet wurden.

2.1.2 Qualitativ-inhaltliche Auswertung der Interviews

Nach der Codierung erfolgte die Auswertung durch inhaltliche Analyse der Interviews. Kuckartz und Rädiker (2020, S. 81) bezeichnen es als vertiefende Analyse, die damit beginnt,

dass die codierten Segmente zu einer Kategorie von allen Teilnehmenden zusammengestellt werden. Die Autoren sehen als nächsten Schritt das Systematisieren und Analysieren dieser Segmente vor, wobei die Ergebnisse als freier Text erfasst werden und damit bereits verwendbare Bausteine für den Ergebnisbericht vorliegen (2020, S. 82). In dieser Arbeit wurden für den folgenden Ergebnisteil die codierten Segmente tabellarisch exportiert. Es wurden nicht relevante Satzteile durch eine Kennzeichnung ‚[…]' entfernt und das Analyseergebnis wurde schriftlich verfasst. Damit stehen die abgeleiteten Ergebnisse aus dem empirischen Teil nachvollziehbar und transparent zur Verfügung und sind zusätzlich in Form von Mindmaps skizziert. Mit den hier genannten Bausteinen folgt die Darlegung der Ergebnisse ab Kapitel III 2.2.

Für den ersten Block der Interviews mit den Aufwärm- und Einstiegsfragen IF01 und IF02 wurde das Analyseergebnis nicht in einer derart ausführlichen Form aufbereitet, da Erkenntnisse hieraus nicht unmittelbar zur Beantwortung der Forschungsfragen dienen. Diese Fragen waren zur Einschätzung der Expertise notwendig und das Ergebnis ist zusammenfassend im nächsten Kapitel beschrieben.

2.1.3 Einstiegsfragen und Sicherheitsempfinden

Die Einstiegsfragen zur persönlichen Erfahrungszeit und zum Bezug zu IT-Dienstleistungen für Behörden wurden dahingehend analysiert, dass sowohl der Expertenstatus als auch die Eignung aus Sicht der Zielgruppe verifiziert wurden. Alle Experten hatten entsprechende Erfahrungszeit und berichteten von ihrem Behördenbezug aus dem Bereich von IT-Dienstleistungen. Die Überprüfung anhand der transkribierten Interviews erfolgte lediglich zur Sicherstellung der konsistenten Dokumentation der Forschungsarbeit, da ungeeignete Interviewpartner nicht weiter berücksichtigt worden wären. Zwei Experten berichteten von einer Erfahrungszeit im Bereich der IT-Sicherheit und des Business Continuity Managements von weniger als zehn Jahren (Experte_07, 2022, Anlage III. 7; Experte_11, 2022, Anlage III. 11). Weitere zwei Experten konnten auf einen Erfahrungshorizont von über 30 Jahren zurückblicken (Experte_03, 2022, Anlage III. 3; Experte_14, 2022, Anlage III. 14). Alle weiteren Interviewpartner nannten einen Zeitpunkt vor zirka zehn bis zwanzig Jahren, seitdem sie sich intensiv damit beschäftigen.

Als dritte Einstiegsfrage wurden alle Experten nach ihrem persönlichen Sicherheitsempfinden gefragt. Die Teilnehmer waren sich der Situation bewusst, dass es hier unterschiedliche Grundeinstellungen geben kann. Sich selbst haben sie in den meisten Fällen „in der Mitte"

(Experten_12, 2022, Anlage III. 12; Experten_14, 2022, Anlage III. 14) einsortiert oder ihre Positionierung bewusst differenziert: Entweder wurde zwischen dem beruflichen und dem privaten Agieren unterschieden (Experten_07, 2022, Anlage III. 7) oder projekt- bzw. situationsspezifisch (Experten_14, 2022, Anlage III. 14; Experten_11, 2022, Anlage III. 11) argumentiert. Auf eine weitere Analyse und Aufbereitung wurde hier verzichtet, da diese Informationen lediglich unterstützend im Rahmen der Analyse genutzt wurden. Fallspezifisch wurde reflektiert, ob bereits aus der persönlichen Einschätzung zum Sicherheitsempfinden ableitbar war, dass die Aussagen zu anderen Interviewfragen dadurch beeinflusst sein könnten. Unter Berücksichtigung der in Kapitel II 2.1.6 im Theorieteil genannten geringen Aussagekraft von Sicherheitsempfinden und -prognosen und der zusammenfassenden Selbsteinschätzung, dass die Experten zwar risikobewusst, aber nicht fanatisch sind, mussten hier keine Segmente mit dieser Erkenntnis in ihrer Aussagekraft modifiziert interpretiert werden.

Als Ergebnis kann aber festgehalten werden, dass die Experten im Bereich Business Continuity Management nicht aufgrund ihrer Tätigkeit automatisch vehement die IT-Sicherheit postulieren, sondern zur Nutzung von Chancen eine entsprechende Abwägung empfehlen (Experten_08, 2022, Anlage III. 8; Experten_14, 2022, Anlage III. 14). Eine absolute Sicherheit kann es nicht geben, wie bereits in Kapitel II 2.1.6 erläutert. Unter dieser Annahme und den Erläuterungen zum persönlichen Sicherheitsempfinden der Experten folgend, ergibt sich auch für das Business Continuity Management, dass hier stets eine Abwägung erfolgen sollte und dass es keine allgemeingültige Empfehlung für ein erreichbares Sicherheitsniveau geben kann. An diese Einstiegsfragen schlossen sich in den Interviews die sich aus den Forschungsfragen ergebenden Fachthemen an, deren Ergebnisse im nachfolgenden Kapitel dargelegt werden.

2.2 Darlegung der Ergebnisse

Orientiert an den drei Nebenforschungsfragen erfolgte die qualitative Analyse der Interviews in der Reihenfolge des teilstandardisierten Interviewverlaufes. Dazu gliedert sich dieses Kapitel in die Betrachtung der Ergebnisse zu den Nebenforschungsfragen in Kapitel III 2.2.1 und die Vorbereitung der Beantwortung der Hauptforschungsfrage in Kapitel III 2.2.2 mit der Auswertung der Empfehlungen. Die Auswertung der Sättigungsanalyse und die Evaluation der Ergebnisse sind ebenfalls in diesem Kapitel dargelegt. Die Zusammenfassung, die Interpretation, die Betrachtung der Gütekriterien und die konkrete Beantwortung der

Hauptforschungsfrage folgen auf Basis dieser Darlegung in Kapitel III 3.3 ‚Diskussion, Interpretation und Konklusion'.

2.2.1 Darstellung der Ergebnisse zu den Forschungsfragen

In der Anlage VIII. sind die reduzierten und codierten Segmente des jeweiligen Untersuchungsschrittes in Form von Tabellen dargestellt, die die Aussagen der Experten enthalten und das nun folgende Analyseergebnis nachvollziehbar machen. Die mittelbar oder unmittelbar relevanten Interviewfragen werden passend zur Nebenforschungsfrage vorab genannt. Die jeweilige Analyse bezieht sich darüber hinaus auf weitere Informationen aus anderen Teilen der Interviews oder der Theorie, die dann als Referenz angegeben sind.

2.2.1.1 NFF1 Wie ist die Situation des BCM mit Blick auf die Digitalisierung?

Dieser Nebenforschungsfrage sind direkt die Interviewfragen 3 (IF03, Bedeutung BCM) und 4 (IF04, Berücksichtigung BCM) zuzuordnen und die Aussagen der Experten dazu sind in den zwei Tabellen der Anlage VIII. 1 und Anlage VIII. 2 dargestellt. Ebenfalls gehören die Fragen nach Aufwand/Nutzen (IF05), Projektbremse (IF06) und positiven sowie negativen Erfahrungen (IF07) inhaltlich hierzu und sind sowohl separat als auch zusammenfassend analysiert. Als Erstes folgt das Ergebnis zur Interviewfrage: ‚Welche Bedeutung messen Sie dem Notfallmanagement bzw. Business Continuity Management im IT-Geschäft allgemein zu?'.

Mittels der qualitativen Inhaltsanalyse der Interviewdaten ergibt sich die nachfolgend beschriebene aktuelle Situation des Business Continuity Managements aus Sicht der Experten aus der Praxis. Die Bedeutung wurde insgesamt als hoch bewertet. Experte_01 (2022, Anlage III. 1) und Experte_02 (2022, Anlage III. 2) sprachen von einer sehr hohen bzw. sehr großen Bedeutung und einem sehr hohen Stellenwert, wie Experte_03 (2022, Anlage III. 3) es bezeichnete. Experte_04 (2022, Anlage III. 4) bewertete es als ein extrem wichtiges Thema und Experte_05 (2022, Anlage III. 5) wies bereits auf eine steigende Bedeutung in diesem Zusammenhang hin, dass beständig weitere Geschäftsprozesse mit IT unterstützt werden. Sowohl Experte_07 (2022, Anlage III. 7) als auch Experte_08 (2022, Anlage III. 8) teilten diese Einschätzung und wiesen ebenfalls auf die gestiegene und steigende Bedeutung im Zusammenhang mit aktuellen Ereignissen hin. Experte_02 (2022, Anlage III. 2) nannte in diesem Zusammenhang das Ahrtal, wo sich 2021 eine

Hochwasserkatastrophe ereignet hat, bei der auch IT-Infrastruktur zerstört wurde. Mehrere Experten gewichteten das Business Continuity Management mit Begriffen wie „business-kritisch“ (Experte_10, 2022, Anlage III. 10) und wiesen ihm eine existenzielle Rolle zu (Experte_11, 2022, Anlage III. 11). Sogar die Möglichkeit für etwaige Straftatbestände wurde vom Experten_10 (2022, Anlage III. 10) genannt, falls die Geschäftsführung hier Versäumnisse zu verantworten hat, womit die Brisanz der Thematik verdeutlicht wird. Wiederholt hat auch Experte_13 (2022, Anlage III. 13) darauf hingewiesen, dass mit wachsenden Gefahren die Bedeutung steigt.

Zusammenfassend wurde die Bedeutung in der Praxis grundsätzlich deckungsgleich zu den Definitionen aus der Theorie beschrieben. Festzustellen ist, dass aktuell in der Praxis mit einer Zunahme der Bedeutung gerechnet wird. Diese wurde hauptsächlich durch zwei Faktoren beschrieben: die weitere Digitalisierung und aktuelle Ereignisse, die die Notwendigkeit einer Resilienz und die Verwundbarkeit des IT-Betriebes deutlich machen.

Die Schlüsselwörter der Aussagen sind in der Mindmap in Abbildung 28 aufgeführt. Die Tatsache, dass viele Experten bereits begründet darauf hingewiesen haben, dass die Bedeutung zukünftig steigen wird, wurde ebenfalls hervorgehoben dargestellt. Dazu sind in der Abbildung mit den zusammenfassenden Begriffen ‚aktuelle Ereignisse‘ und ‚weitere Digitalisierung‘ diese als Einflussfaktoren berücksichtigt.

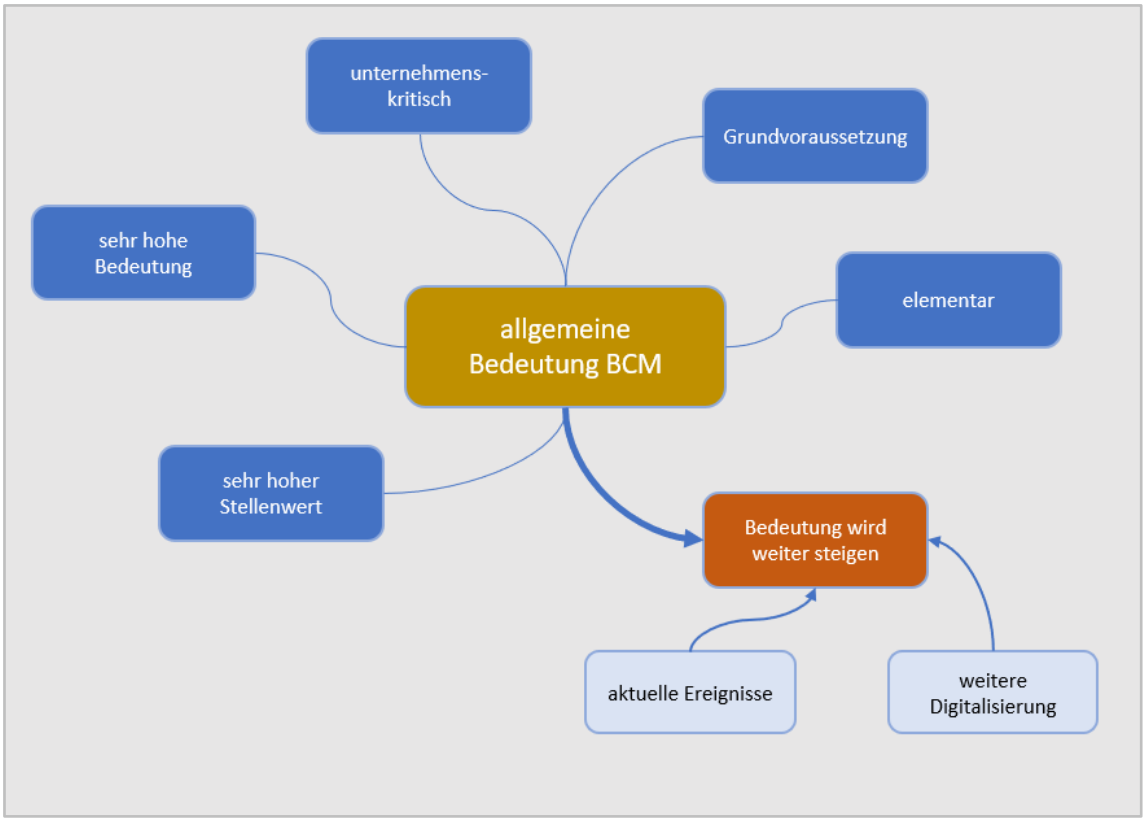


Abbildung 28 – Mindmap Bedeutung des BCM aus Sicht der Experten 2022 (Quelle: eigene Darstellung)

Mit Stand 2022 wird die herausragende Bedeutung eines Business Continuity Managements in der Praxis bestätigt. Ein zukünftiger Handlungsbedarf wurde ebenfalls angezeigt, da mit einer steigenden Abhängigkeit von der IT durch die Digitalisierung auch die Anforderungen zunehmen werden. Von hoher Relevanz ist es nun, zu wissen, wie die Berücksichtigung aktuell in der Praxis etabliert ist. Dies wurde mit der nächsten Interviewfrage ‚Wird das BCM stets ausreichend berücksichtigt?' angesprochen und die Antworten der Teilnehmer sind in der Anlage VIII. 2 aufgelistet.

Die Experten sagten mehrheitlich, dass in der Praxis das Business Continuity Management noch nicht ausreichend berücksichtigt wird. Lediglich zwei Experten sahen es in folgenden Punkten etwas positiver. Einmal wurde eine sich dahingehend verbessernde Situation erläutert, dass zumindest die Awareness auf der Executive-Ebene nun vorhanden sei (Experte_04, 2022, Anlage III. 4). Es wurde auch allgemein von einer zunehmenden Sensibilisierung in den letzten Jahren berichtet (Experte_01, 2022, Anlage III. 1). Des Weiteren wurde genannt, dass bei stark regulierten Branchen bereits seit Jahren vermehrt ein Augenmerk darauf gelegt wird (Experte_08, 2022, Anlage III. 8). Direkt übertragen wurde die Fragestellung von mehreren Experten auf den Bereich der Behörden-IT. Experte_11 (2022, Anlage III. 11) differenzierte hier zwischen Kommunen und Landesbehörden und erläuterte es mit den zur Verfügung stehenden Mitteln. Dieser fiskalische Faktor wurde auch von Experte_10 angeführt und Experte_02 bestätigte, dass hier „am falschen Ende gespart" (Experte_02, 2022, Anlage III. 2) wird. Experte_07 (2022, Anlage III. 7) berichtete aus dem Projektgeschäft, dass die üblichen Redundanztechnologien wie Hochverfügbarkeit und Ausfallsicherheit nicht vom Kunden angefordert werden, sondern erst aktiv durch die Beratung thematisiert werden. Auch die letzten drei Interviewpartner berichteten wiederholt, dass hier ein Defizit besteht. Sogar in IT-Großprojekten, wie Experte_14 (2022, Anlage III. 14) ausführte, sind Fallback-Lösungen noch kurz vor der Inbetriebnahme ungelöst. Experte_12 (2022, Anlage III. 12) hat es aktuell „immer wieder" erlebt und bescheinigte dem Business Continuity Management in den meisten Unternehmen eine eher untergeordnete Rolle. Diese Situation steht damit im Widerspruch zur Theorie, die die Sicherheitsaspekte als eine wesentliche Voraussetzung für die Digitalisierung nennt.

Auffallend in der Analyse waren die ersten spontanen Antworten auf diese Fragestellung. Oft wurde direkt mit einem Nein angefangen, bevor dazu ausgeführt wurde. Alle Experten hatten unmittelbar einen Bezug zu der Fragestellung und konnten ihre Position begründen und herleiten. Hierdurch wurde die in der Problematik und der Theorie bereits dargestellte

Situation, dass in Deutschland ein Nachholbedarf besteht (Schmid, 2019, S. 8), auch aus der Praxis heraus bestätigt.

Zur Verdeutlichung dieses Ergebnisses dient die nachfolgende Mindmap, die zu den drei prinzipiellen Antwortmöglichkeiten ‚ja', ‚nein' und ‚teilweise' darstellt, wo es entsprechende Beiträge gab. Es ist zu erkennen, dass in der Praxis ein ausreichend etabliertes Business Continuity Management nicht gesehen wurde. Nur einmal wurden branchenspezifische Situationen genannt, in denen es teilweise vorhanden ist (Experte_08, 2022, Anlage III. 8). Grundsätzlich berichteten alle Experten deutlich über eine noch fehlende ausreichende Berücksichtigung.

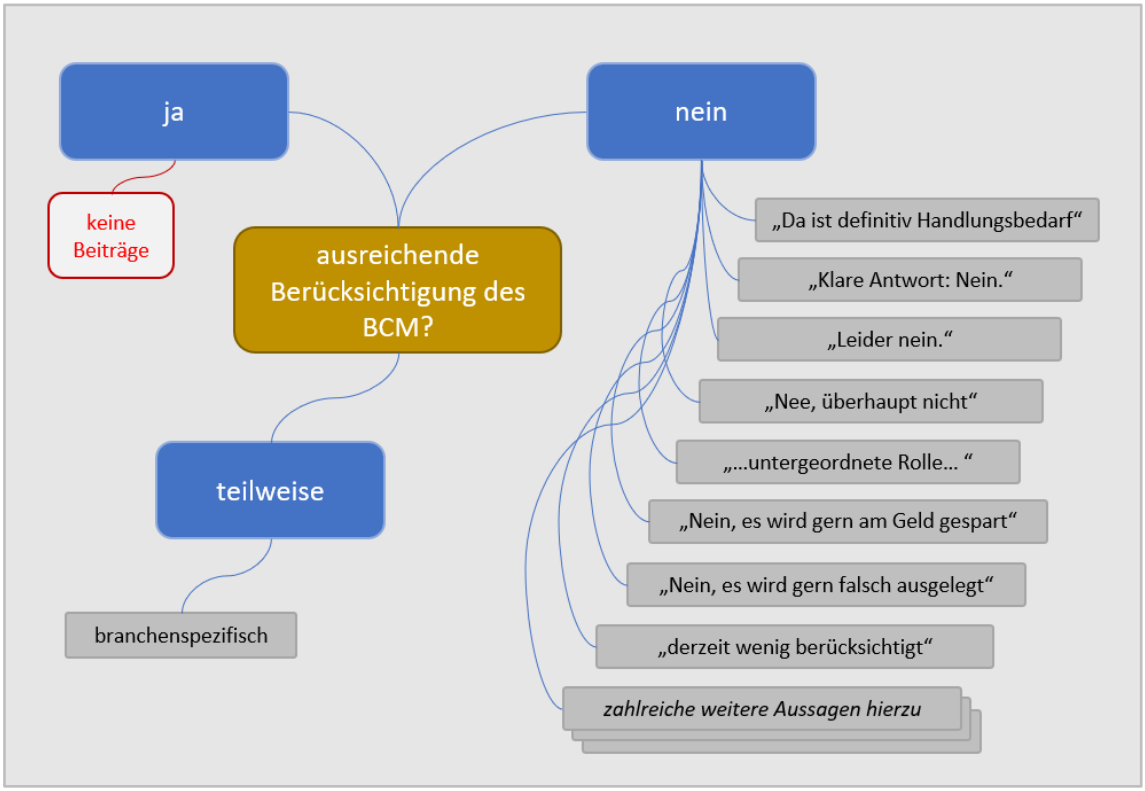


Abbildung 29 – Mindmap zur Frage ausreichender Berücksichtigung des BCM (Quelle: eigene Darstellung)

Damit wurden die ersten beiden Anteile zur Beantwortung der Forschungsfrage erschlossen. Eine weitere und ebenfalls bereits aus der Theorie bekannte Herausforderung ist in allen Projekten die Kosten- und Nutzenbetrachtung. Hier galt es herausfinden, wie sich das Verhältnis in der Praxis gestaltet und inwiefern diese Aspekte bei den Empfehlungen zu berücksichtigen sind. Aus der Theorie wurde bereits berichtet, dass Business Continuity Management auch neue geschäftliche Möglichkeiten eröffnen kann. Hierzu wurden die Aussagen zu dieser und der darauffolgenden Interviewfrage analysiert. Im Vordergrund der Analyse bleibt aber die Ergebnisdarstellung in Bezug auf die Hauptforschungsfrage. Zu der

Interviewfrage ‚Wie schätzen Sie das Aufwand/Nutzen-Verhältnis hier ein?' wurden die in der Anlage VIII. 3 aufgelisteten Textpassagen im Gesamtkontext analysiert.

Vorab ist anzumerken, dass diese Fragestellung seitens der Experten als schwierig klassifiziert wurde. Experte_12 (2022, Anlage III. 12) konnte hierzu zuerst keine Bewertung abgeben, diskutierte dann jedoch für den Bankensektor den Aufwand als potenziell zu hoch. Als einen zu hohen Aufwand bezeichneten andere Experten die Situation zwar nicht pauschal, aber von einem sehr hohen Aufwand wurde übereinstimmend berichtet. Zwei Experten reflektierten direkt mögliche Schadensfälle und stellten den Nutzen in den Vordergrund, der sich erst ergibt, wenn ein solcher Fall eingetreten ist (Experte_04, 2022, Anlage III. 4; Experte_02, 2022, Anlage III. 2). Experte_05 (2022, Anlage III. 5) empfahl hier eine geschäftsprozessspezifische Differenzierung bei der Entscheidung, welche Aufwände investiert werden. Experte_07 (2022, Anlage III. 7) blickte konkret auf Behörden und sicherheitsrelevante Services und sah vor diesem Hintergrund die Aufwände grundsätzlich als gerechtfertigt und notwendig an. Zwei Experten zogen den Vergleich zu Versicherungen (Experte_08, 2022, Anlage III. 8; Experte_09, 2022, Anlage III. 9) und damit wurde deutlich, dass von einem unmittelbarem Return on Invest hier nicht auszugehen ist. Beispielhaft merkte Experte_13 07 (2022, Anlage III. 13) zum Aufwand an, dass diesen doch „niemand letztendlich bezahlen" möchte. Er berichtete aber auch, dass meist die Kosten nach einem Schaden deutlich höher ausfallen, als wenn vorher entsprechende Aufwände für ein Business Continuity Management getätigt worden wären.

Strategisch wird hieraus gefolgert, dass für eine Kosten/Nutzen-Analyse im Bereich Business Continuity Management vorrangig der vorab nur schwer oder nicht bezifferbare Nutzen zu betrachten ist. Kosteneinsparungen oder Gewinnerzielungsabsichten sind aus den Berichten der Praxis kein priorisierter Ansatz, um die Ausgaben zu rechtfertigen. Mit dem Fokus auf die sicherheitsrelevanten Verwaltungs- und Behördenservices ist es daher eine große Herausforderung, die notwendigen Aktivitäten bei konkreten IT-Projekten für den Anteil des Business Continuity Managements zeit- und wirkungsgerecht einzubringen.

Insgesamt sahen die Experten hier einen hohen Aufwand, der differenziert dargestellt wurde und als ein Hemmnis für die Etablierung eines Business Continuity Managements angesehen werden kann. Eine Konkretisierung des Nutzens ist insbesondere deshalb schwierig, weil in der IT-Notfallprävention der Eintritt möglicher Schadensfälle geringgehalten werden soll. Wie bereits genannt, ist der Nutzen erst im Schadensfall erkennbar. Experte_07 (2022, Anlage III. 7) bewertete die Einsatzfähigkeit der deutschen Behörden inkl. der Bundeswehr

allerdings mit einem so hohen Stellenwert, dass das Risiko eines Ausfalls nicht tragbar ist; somit sah er den Nutzen als „sehr, sehr hoch“ an.

Der im Beratungsgeschäft auch bei Behörden erfahrene Experte_11 bezeichnete diese schwierige Kosten/Nutzen-Situation sogar als das „größte Problem“ (2022, Anlage III. 7). Experte_02 (2022, Anlage III. 2) sensibilisierte dahingehend, dass der Aufwand vor allem am Anfang besonders hoch ist, sich anschließend jedoch ein BCM-System mit „nicht mehr so hohem“ Aufwand betreiben lasse.

Bildlich zusammengefasst sind die Stichworte der Experten auf Basis der erfolgten Analyse in Abbildung 30 gruppiert nach Themengebieten dargestellt.

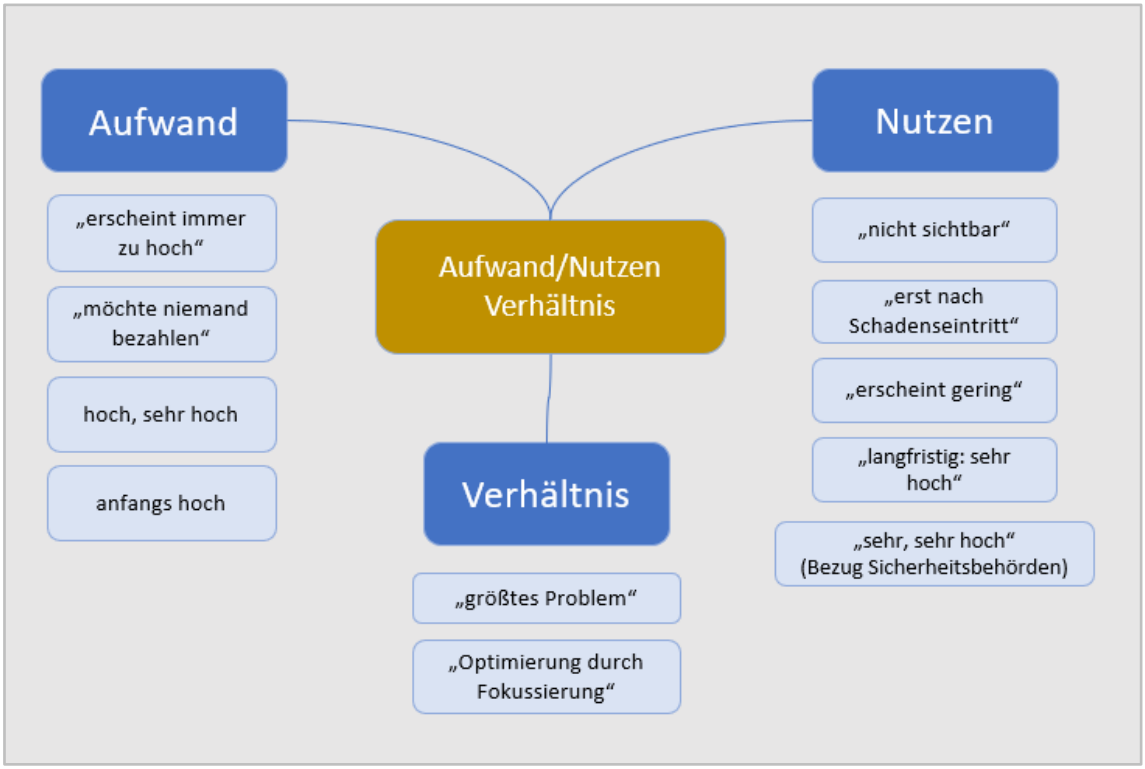


Abbildung 30 – Mindmap zur Frage Aufwand/Nutzen (Quelle: eigene Darstellung)

Zur weiteren Unterstützung der Beantwortung der ersten Nebenforschungsfrage wurde im Interview gefragt, wie das Business Continuity Management in IT-Projekten wahrgenommen wird. Hiermit wird bereits der zweite Block der Interviews zu den zukünftigen Digitalisierungserwartungen verknüpft. Zur Vermeidung einer Beeinflussung wurde einerseits erfragt, ob es negativ als Projekthemmnis oder andrerseits positiv als Projekt-Enabler in der Praxis wahrgenommen wird. In Anlage VIII. 4 sind die codierten Segmente zur Interviewfrage ‚Wird das BCM in der Praxis eher als Projektbremse oder -Enabler wahrgenommen?‘ aufgelistet. Das Ergebnis stellt sich inhaltlich wie folgt dar:

Zu dieser Fragestellung gab es kein einheitliches Ergebnis der Experten, was auch auf die Zusammensetzung der Expertenauswahl zurückzuführen ist. Experten aus dem Bereich der

Beratung von Behörden zu Digitalisierungsprojekten äußerten sich eher in die Richtung, dass das Business Continuity Management in IT-Projekten als lästig (Experte_08, 2022, Anlage III. 8) und als Projektbremse empfunden wird (Experte_13, 2022, Anlage III. 13). Experten aus dem Bereich der Lösungsanbieter wiederum sahen hier auch positive Aspekte. Es lässt sogar mehr Geschäft zu (Experte_04, 2022, Anlage III. 4; Experte_05, 2022, Anlage III. 5) bzw. kann das Business Continuity Management in IT-Projekten als Enabler verstanden werden. Weitere Einschätzungen wurden dahingehend getätigt, dass es in IT-Projekten derzeit wenig berücksichtigt wird und noch nicht adressiert ist (Experte_11, 2022, Anlage III. 11). Ein Experte berichtete von der konkreten Erfahrung, dass es in einem großen IT-Projekt mit mehrjähriger Laufzeit „schlichtweg überhaupt nicht betrachtet“ (Experte_14, 2022, Anlage III. 14) wurde. Experte_04 empfahl, Business Continuity Management frühzeitig in den IT-Projekten zu berücksichtigen und bereits in die Architekturüberlegungen einfließen zu lassen, um so auch Kosten zu sparen (2022, Anlage III. 4). Experte_05 schilderte dazu passend die Situation, in der sich bei rechtzeitiger Berücksichtigung auch ganz andere Lösungsansätze zeigen können (2022, Anlage III. 5).

Zu dieser Interviewfrage ergaben sich durch die Analyse drei Gruppierungsmöglichkeiten. Zu der These, dass Business Continuity Management in IT-Projekten als Hemmnis wahrgenommen wird, gab es passende Berichte und Ausführungen aus der Praxis. Bemerkenswerterweise teilten diese Einschätzung nicht alle Experten. Die Bezeichnung als ‚Bremse‘ wurde relativiert oder es wurde darüber hinaus sogar als Chance gesehen. In der zweiten Gruppierung nach der Bewertung des Business Continuity Managements in IT-Projekten als ‚Projekt-Enabler‘ gab es einerseits auch ablehnende Meinungen, andererseits Einschätzungen und Empfehlungen, dass es IT-Projekte ermöglichen kann oder sollte. Im Rahmen der Auswertung wurde deutlich, dass eine dritte Tendenz aufzuzeigen ist. In der Praxis ist in einigen Bereichen das Business Continuity Management bei IT-Projekten aktuell wenig oder gar nicht berücksichtigt. In Abbildung 31 ist das Ergebnis mit Stichworten visualisiert.

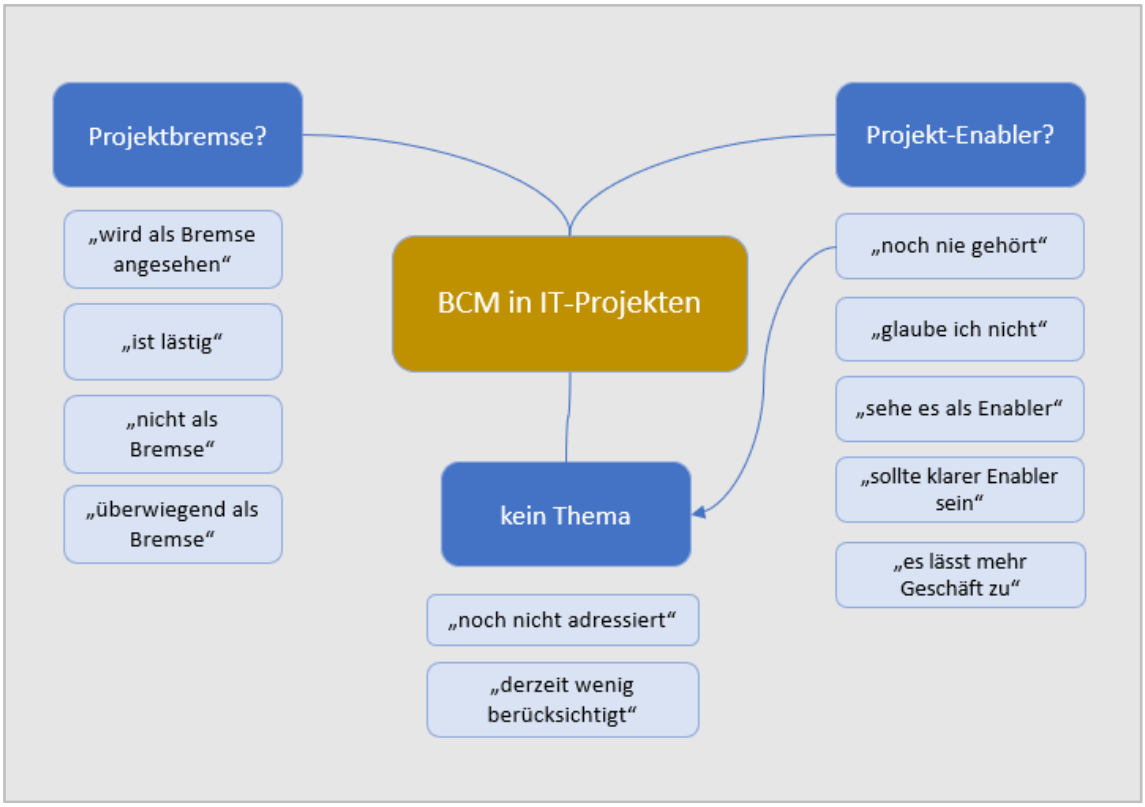


Abbildung 31 – Mindmap zur Frage nach BCM in IT-Projekten (Quelle: eigene Darstellung)

Damit wurden die Ergebnisse von vier Interviewfragen thematisch passend zur ersten Nebenforschungsfrage dargelegt. Die weitere Einordnung in den Gesamtzusammenhang und die Diskussion erfolgen in den später dafür vorgesehenen Kapiteln zur Beantwortung der Forschungsfragen. Als Nächstes werden die Ergebnisse aus den Experteninterviews zu den Auskünften mit hoher Relevanz zur zweiten Nebenforschungsfrage dargestellt.

2.2.1.2 NFF2 Welche Aspekte der Digitalisierung sind hier kritisch?

Die zweite Forschungsfrage betrachtet die Digitalisierung. Zu dieser allgemeinen Fragestellung wurden die Experten gebeten, vorerst unabhängig vom Business Continuity Management zu bewerten, welche Herausforderungen hier zu erwarten sind. In der ersten Frage wurde um die Nennung von Themen und Aspekten der Digitalisierung gebeten. Insgesamt wurde, je nach Interviewverlauf, nur diese Einstiegfrage gestellt und dann wurden mit vorbereiteten Subfragen die aus der Theorie abgeleiteten Aspekte hinterfragt. Wenn die Experten nicht bereits selbst darauf eingingen, wurde ergänzend eine Einschätzung zum Cloud-Computing eruiert, das, wie in der Theorie beschrieben, von herausgehobener Bedeutung für die Digitalisierung sein soll.

Die codierten Segmente zur Interviewfrage ‚Welche Herausforderungen sehen Sie bei der weiteren Digitalisierung auf uns allgemein und die Behörden in Deutschland zukommen?‘ sind

derart umfangreich, dass eine weitere deduktive Kategorienbildung wie in Kapitel III 2.1.1 beschrieben erfolgte. Es wurde ein übergeordneter Code ‚Automatisierung/Digitalisierung von Geschäftsprozessen' gewählt, der sich einerseits aus den thematisch übereinstimmenden Beiträgen der Experten ergab, und andrerseits wurde bereits die Hauptforschungsfrage dahingehend fokussiert, dass die weitere Digitalisierung zukünftig manuelle und analoge Vorgänge ersetzen wird. Dieser Aspekt wurde von den Experten unterschiedlich umschrieben und erläutert und es wurde auf Gefahren oder Möglichkeiten hingewiesen. Die hierzu codierten Segmente sind in Anlage VIII. 5 in einer weiter gekürzten Form dargestellt. Das Ergebnis lautet folgendermaßen:

Mehrere Experten beschrieben hier den weiteren Weg, wie Behördenvorgänge, die aktuell noch auf Papierbasis erfolgen, weiter digitaler werden. Experte_08 sprach von einer massiven Automatisierung, die bei den Geschäftsprozessen zu erwarten ist (Experte 08, 2022, Anlage III. 8). Experte_07 wies in diesem Zusammenhang direkt darauf hin, dass die Digitalisierung auch durch geeignete Schnittstellen behördenübergreifend erfolgen muss (2022, Anlage III. 7). Experte_09 (2022, Anlage III. 9) erwartete, dass sogenannte „stumpfe" Vorgänge zukünftig auch mit KI automatisiert werden, und Experte_05 (2022, Anlage III. 5) sah sogar pauschalisiert alles, was Menschen heute machen, zukünftig digitalisiert, wobei hier unterschiedliche Einstufungen zu treffen sind. Experte_02 (2022, Anlage III. 2) beschrieb und kritisierte ein unvollständiges Vorgehen: Es werde zwar einerseits auf digitale Lösungen gesetzt, aber weiterhin solle auf Papierdokumente nicht verzichtet werden.

Im internationalen Vergleich erläuterte Experte_14 (2022, Anlage III. 14), passend zu den in der Theorie dargelegten Ergebnissen der DESI-Studien, wie in anderen Ländern bereits Geschäftsprozesse digital automatisiert ablaufen, wie sie in Deutschland noch nicht denkbar sind. Interessanterweise diskutierte Experte_13 (2022, Anlage III. 13) eine Situation, in der es trotz Digitalisierung auch zu einer Verlangsamung von Behördenvorgehen durch die Digitalisierung kommen kann. Mit dieser Erkenntnis werden Hemmnisse oder Vorbehalte bei der weiteren Digitalisierung einfach erklärbar und es zeigt sich die Notwendigkeit einer gesamten Prozessbetrachtung. Vergleichbar argumentierte Experte_11 (2022, Anlage III. 11) und sah die von ihm genannte „digitale Rendite […] verpufft" (Experte_11, 2022, Anlage III. 11), wenn zwar digitalisiert wird, aber man als Backup an den alten analogen Vorgängen festhält. Experte_12 (2022, Anlage III. 12) warnte vor einem Trugschluss. Man dürfe nicht davon ausgehen, dass durch die Automatisierung alles einfacher und damit

weniger fehleranfällig werde. Er sah die Notwendigkeit, die daraus resultierenden neuen und speziellen Anforderung genau zu betrachten.

Damit ergibt sich ein Überblick aus der Praxis auf die Situation der behördlichen Prozesse, die im Rahmen der Digitalisierung weiter automatisiert werden. Hierzu wurden Auszüge aus dem Datenmaterial nach Meinungen zur Situation und zur Tendenz sowie nach relevanten Hinweisen gruppiert und in der nachfolgenden Abbildung dargestellt.

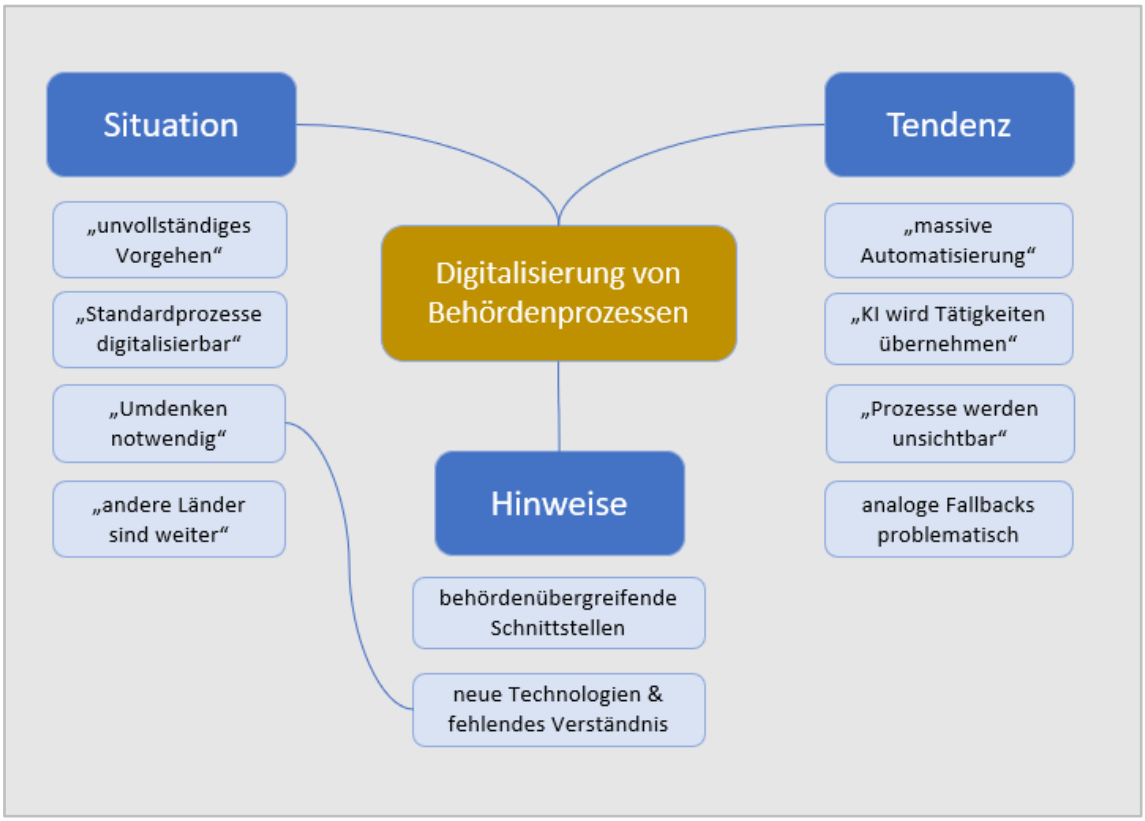


Abbildung 32 – Mindmap zur Digitalisierung von Behördenprozessen (Quelle: Anlage III., eigene Darstellung)

Trotz der Tendenz zu einer erwarteten massiven weiteren Automatisierung wurde aktuell ein noch unvollständiges Vorgehen gesehen, wozu ein Umdenken und ein Erlernen der neuen Technologien notwendig ist. Behördenübergreifend wurde auf den Bereich ‚Schnittstellen‘ hingewiesen und festgestellt, dass insbesondere Standardprozesse digitalisierbar sind. Allerdings werden die Prozesse dann auch unsichtbar, und als Rückfallposition die alten Prozesse in analoger Form vorzuhalten, wurde kritisch betrachtet. Damit wird in diesem Bereich der Handlungsbedarf deutlich und die Begründungen und Darstellungen der Experten werden im gestalterischen Teil die formulierten Handlungsempfehlungen ergänzen.

Neben dieser prozessualen Betrachtung der Digitalisierung wurde auf die für einen Betrieb notwendige Infrastruktur eingegangen. Wie in der Theorie bereits dargelegt, kommt der Cloud-Technologie eine zentrale Rolle bei der Digitalisierung zu (Faber, 2019, S. 20; Abolhassan, 2016, S. 149). Dies wurde daher als Teil der Experteninterviews aktiv mit der

Interviewfrage IF09 hinterfragt, falls es nicht bereits durch den Experten proaktiv thematisiert worden war. Es wurden die in der Anlage VIII. 6 aufgeführten Aussagen codiert, unter deren Bezugnahme die drauffolgende Analyse ausformuliert ist.

Zu diesem Bereich gab es zahlreiche Aussagen der Experten mit Meinungen, Erfahrungsdarstellungen und Prognosen. Der Begriff ‚Cloud-Computing' und das vorherrschende Verständnis davon in der Praxis wurden als sehr unterschiedlich dargestellt. Dazu bezeichnete Experte_01 (2022, Anlage III. 1) es als Kunstwort und ein Interviewpartner sprach direkt an, dass hier teilweise über Dinge entschieden wird, die die Entscheider nicht verstehen (Experte_14, 2022, Anlage III. 11). Gleichzeitig wurde der Begriff als eine Technologie aufgefasst, die schon lange präsent und bekannt ist und sich vorrangig auf die Rechenzentrumskapazitäten bezieht. Experte_03 (2022, Anlage III. 3) empfahl die Unterscheidung nach den großen Cloud-Anbietern und dem Betreiben von Cloud-basierender Technologie in einem eigenen Rechenzentrum. Experte_02 (2022, Anlage III. 2) sah hier ebenfalls eine Differenzierungsnotwendigkeit bei der Frage, ob die Systeme innerhalb oder außerhalb Deutschlands betrieben werden sollten. Zum vorherrschenden Verständnis führte ein Experte aus, dass teilweise auf der Geschäftsführerebene Entscheidungen für die Cloud nur aus Kostengründen getroffen werden, dass man aber nicht verstehe, was man da überhaupt entscheide (Experte_14, 2022, Anlage III. 14). Experte_01 (2022, Anlage III. 1) konstatierte bereits Entwicklungen bei den Cloud-Anbietern, wie diese von sich aus den Sicherheitsaspekt zunehmend in den Produkten berücksichtigen und auch länderspezifische Anforderungen, z. B. an den Datenschutz, integrieren. Auch Experte_09 (2022, Anlage III. 9) sah hier positive Anzeichen, indem Sicherheitsaspekte durch die Hersteller zunehmend berücksichtigt würden. Mehrere Experten wiesen darauf hin, dass bereits an vielen Stellen Cloud-Technologien in Betrieb seien, auch wenn diese nicht allgemein wahrgenommen werden.

Als interessante Lösung im Cloud-Umfeld für Behörden thematisierten zwei Experten das GAIA-X-Cloud-Projekt. Experte_04 (2022, Anlage III. 4) bewertete es als Initiative, mit der die Cloud vorangebracht werden kann, da in diesem Projekt auch eine Auseinandersetzung mit Datenmanagement und Datensicherheit erfolgt. Experte_06 (2022, Anlage III. 6) berichtete von Behörden, die in diese Richtung gehen wollen, da hier die Daten im europäischen Rechtsraum verbleiben. Zum aktuellen Sachstand des GAIA-X-Projektes wurde im theoretischen Kapitel II 2.1.7 bereits berichtet, wobei an dieser Stelle auch auf die kritischen Meinungen zur Transparenz und zum Projektfortschritt hinzuweisen ist. Die hier erhobenen

Informationen ergänzen damit den Erkenntnisstand aus Sicht der Praxis. Übereinstimmend mit der Theorie wurde genannt, dass das Projekt aktuell noch nicht zur Anwendung kommt, aber im Kontext der Sicherheit als interessante Lösung einzustufen ist.

Das sehr umfassende Lagebild zur Bewertung des Cloud-Computings aus der Praxis ist in der nachfolgenden Abbildung skizziert und erleichtert damit das Verständnis der Thematik Cloud-Computing im Zusammenhang des Forschungsprojektes. Es erfolgte eine Gruppierung der verschiedenen Aussagen nach den Punkten ‚Sachstand und Bewertung', ‚Ausblick', ‚Betrieb' sowie ‚Sicherheit'. Direkte Zusammenhänge bei Einzelaussagen in den Gruppen wurden mit entsprechenden Verbindungslinien gekennzeichnet. Beispielsweise wurde eine Verbindung in der Gruppe ‚Ausblick' zum ‚Betrieb' gezogen. Hiermit wird die aktuelle Herausforderung im Betrieb deutlich, die zukünftig gelöst werden muss.

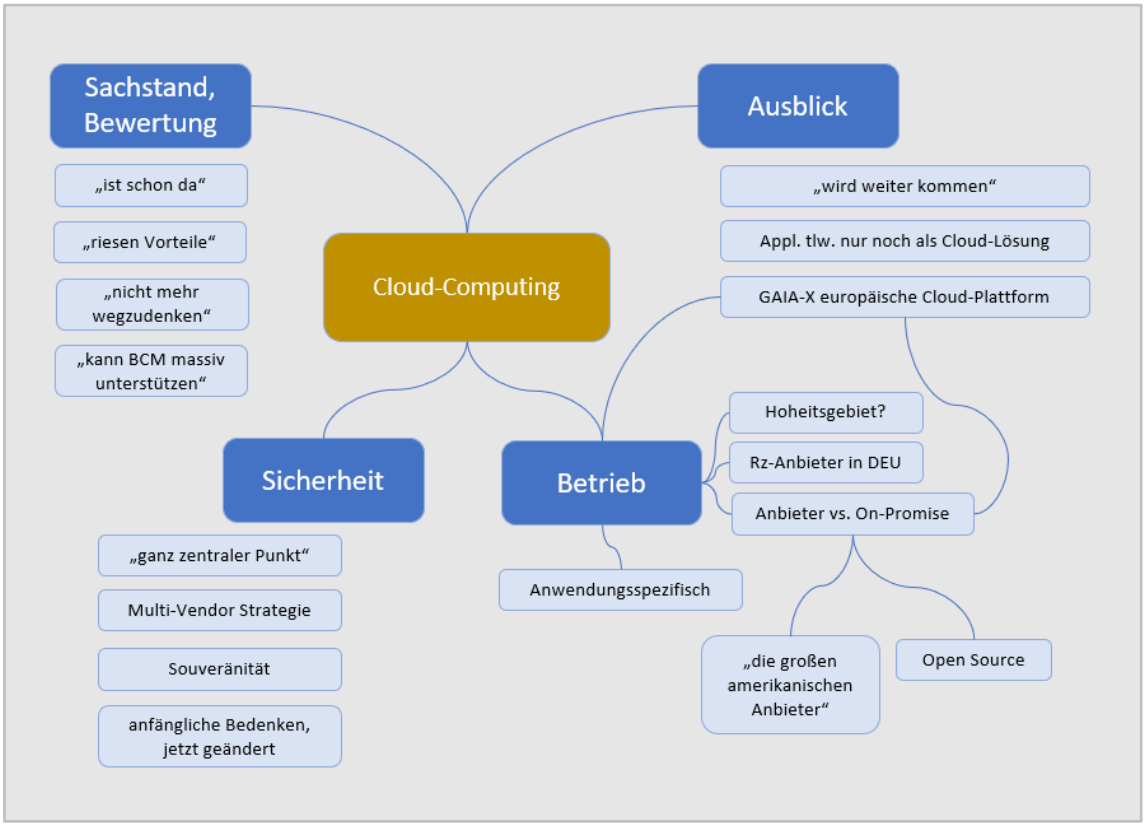


Abbildung 33 – Mindmap zur Thematik Cloud-Computing in der BCM-Praxis (Quelle: eigene Darstellung)

Bemerkenswert ist, dass aus Sicht der BCM-Experten mit dem Cloud-Computing Vorteile für ein Business Continuity Management gesehen werden. Dazu sagte ein Experte: „[…] rein technisch gesehen ist Cloud-Computing für BCM […] wirklich ein Vorteil" (Experte_12, 2022, Anlage III. 12). Experte_07 (2022, Anlage III. 7) sensibilisierte in diesem Zusammenhang jedoch dafür, dass es keine Rückfallposition gibt, wenn eine Organisation sich allein von einem Anbieter abhängig macht. Es wurden Multi-Cloud- und Multi-Vendor-Strategien diskutiert und empfohlen (Experte_09, 2022, Anlage III. 9; Experte_07, 2022, Anlage III. 7).

Zusammenfassend kann das Cloud-Computing als bereits vorhandene Technologie als vorteilhaft für die IT-Notfallprävention angesehen werden. Es bringt aber auch neue Anforderungen im Bereich der Sicherheit mit sich. Datensouveränität, eine anwendungsspezifische Differenzierung und die Entscheidung für geeignete IT-Partner und Rechenzentrumsdienstleister wurden als jeweils zu lösende Herausforderungen gesehen. Von aktuellen Produkt- und Weiterentwicklungen berichteten mehrere Experten, so dass hier davon auszugehen ist, dass Empfehlungen zurzeit nur auf Basis eines Zwischenstandes der jeweils aktuell verfügbaren Portfolios der Anbieter erfolgen können. Zielführender kann es hier sein, die eigenen Anforderungen in diese Weiterentwicklungen einfließen zu lassen.

Dies wird im Diskussions- und Gestaltungsteil noch genauer betrachtet werden. Hervorzuheben sind die komplexen Situationen, die sich nach dieser Erhebung für das Cloud-Computing in der Praxis ergeben haben. Einerseits wir Cloud-Computing als bereits vorhandene und genutzte Technologie bezeichnet, andrerseits wird von zahlreichen noch offenen Fragestellungen und Unsicherheiten für den Betrieb berichtet, wie in Abbildung 33 auf Seite 138 dargestellt. Damit ergibt sich, dass aktuell keine explizite Empfehlung dazu abgeleitet werden kann, welche Cloud wie aus Sicht eines Business Continuity Management einzusetzen wäre. Hier sind folglich weiterhin je Unternehmen und Behörde individuelle Auswahlentscheidungen zu treffen, die die eigenen Anforderungen und ggf. anwendungs-spezifische Schwerpunkte berücksichtigen, damit die Vorteile der Cloud-Technologie sicher genutzt werden können.

Neben den dargestellten Aussagen zur Automatisierung von Geschäftsprozessen und dem Cloud-Computing nannten die Experten weitere Aspekte bezüglich der Digitalisierung, die aus ihrer Sicht relevant sind. Die Aussagen zu Künstlicher Intelligenz (KI), Internet of Things (IOT), sozialen Medien, Smart-Grid, Big-Data, Mobility und Vernetzung werden nachfolgend kurz erläutert. Aufgrund der vielen unterschiedlichen Thematiken wurde hier auf die Zusammenstellung einer separaten Tabelle in Anlage VIII. mit den codierten Segmenten verzichtet. Es wird auf die Textpassagen in den Interviewprotokollen der Anlage III. verwiesen. Experte_09 (2022, Anlage III. 9) nannte KI, mit der sogenannte „stumpfe“ Tätigkeiten des Menschen zukünftig in fortgesetztem Maße durch die IT übernommen werden. Damit verbunden sah er eine qualitative Verbesserung der Arbeit und für den Mitarbeiter einen zunehmenden Interessengrad an der eigenen Arbeit. Experte_14 (2022, Anlage III. 14) merkte dazu an, dass grade die Absicherung dieser Komponenten eine wachsende Herausforderung

darstellt, wenn weitere Anteile durch KI geleistet werden. KI werde auch schon heute in Behörden eingesetzt, wobei sie nicht immer sichtbar sei (Experte_10, 2022, Anlage III. 10).

Für den Bereich IOT verwies Experte_05 (2022, Anlage III. 5) auf komplett neue Gefährdungen, sobald weit exponierte Bestandteile mit vernetzt werden und eine zunehmende Automatisierung erfolgt, ohne hierbei eine mögliche Steuerung durch den Menschen zu erhalten. Experte_06 sah noch nicht abschätzbare zukünftige Herausforderungen (2022, Anlage III. 6). Heute werde IOT grundsätzlich ohne Redundanzen ausgeprägt; so berichtete Experte_10 vom Einsatz von Sensoriken, die nur einfach installiert werden und nicht doppelt oder dreifach, um vor Ausfällen geschützt zu sein. Dies wurde als eine Herausforderung für das Business Continuity Management gesehen und dazu wurde die Notwendigkeit von BCM-Plänen erläutert (Experte_10, 2022, Anlage III. 10).

Für den Bereich der sozialen Medien erachtete Experte_04 (2022, Anlage III. 4) die Möglichkeiten der Kommunikation von Behörden mit der Bevölkerung als positiven Aspekt. Allerdings wurde es auch als kritisch betrachtet, wenn Behördenmitarbeiter z. B. mit Messenger-Diensten behördliche Vorgänge unterstützen (Experte_03, 2022, Anlage III. 3). Darüber hinaus wurden soziale Medien von den BCM-Experten nicht thematisiert, womit sie im empirischen Teil dieser Arbeit nicht weiter zu untersuchen sind.

Mit Big-Data sah Experte_06 (2022, Anlage III. 6) eine zunehmende Herausforderung auf das Business Continuity Management zukommen, um die Masse der Daten sicher zu halten. Mit Blick auf die Digitalisierung insgesamt stufte dieser Experte es als größte Herausforderung ein. Es wurden auch Gefahren darin gesehen, wenn Milliarden Sensordaten von vernetzten IOT-Geräten untereinander ausgetauscht werden. Zudem wurde von Erfahrungen berichtet, dass hier auch Angriffe von Geräten untereinander durchgeführt werden (Experte_06, 2022, Anlage III. 6).

Die Bereiche Mobility und Vernetzung wurden von den Experten so dargestellt, dass diese massiv zunehmen werden, womit auch neue Angriffsflächen entstehen können. Experte_11 (2022, Anlage III. 11) skizzierte ein mit zahlreichen Schnittstellen und Abhängigkeiten heranwachsendes Ökosystem im Rahmen der Digitalisierung. Eine Kompromittierung an nur einer Stelle könne dabei das gesamte System gefährden. Ausdrücklich wurde nicht nur ein gezielter Angriff betrachtet, sondern auch aus der Betriebssicht kann der Ausfall einzelner Komponenten zukünftig weitreichendere Folgen haben (Experte_11, 2022, Anlage III. 11). Diese Schlagworte zu den weiteren Aspekten der Digitalisierung sind nachfolgend skizziert:

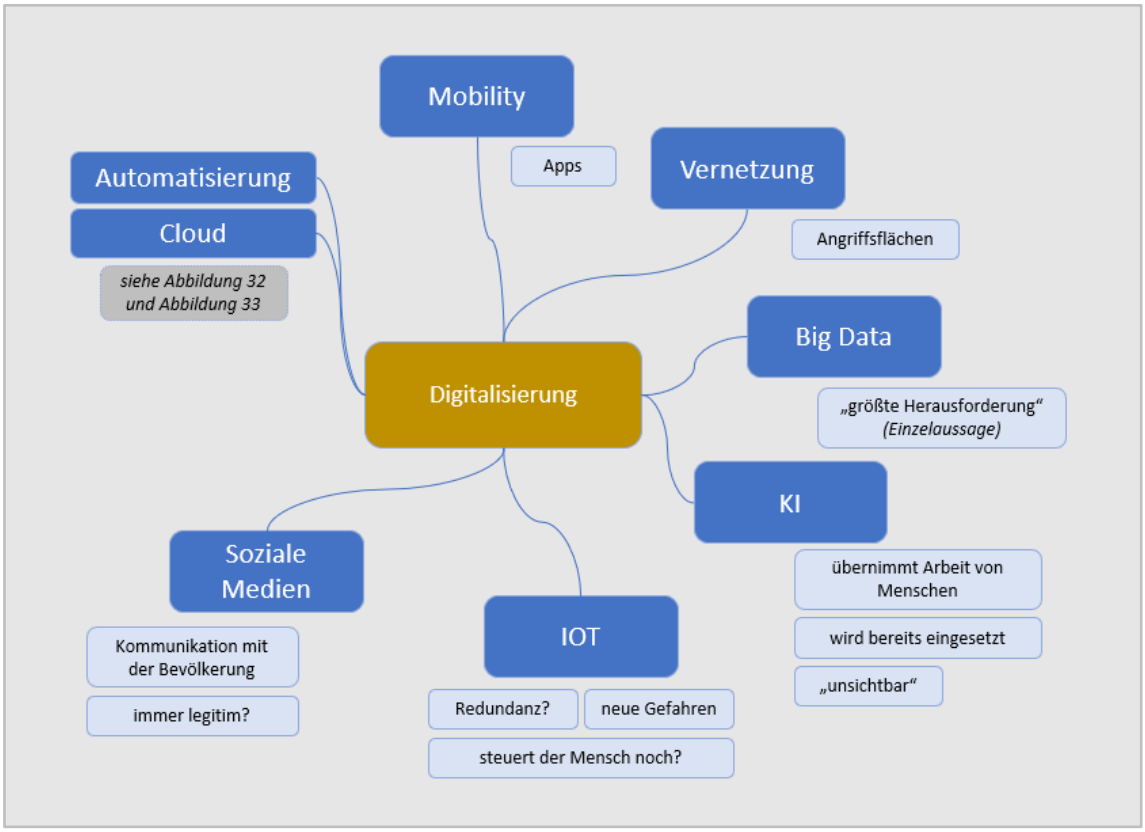


Abbildung 34 – Weitere Aspekte der Digitalisierung mit Schlagworten (Quelle: eigene Darstellung)

Zusammenfassend wurden hiermit wesentliche Aussagen zu den Aspekten der Digitalisierung dargestellt, die aus dem empirisch erhobenen Datenmaterial erhoben wurden. Als geschäftskritisch im Sinne des Business Continuity Managements wurden damit vorrangig die erwarteten Digitalisierungsschritte genannt und erläutert, die sich auf die weitere Automatisierung der Geschäftsprozesse beziehen. Für die Umsetzung der dafür notwendigen IT-Lösungen wurden die Herausforderungen im Bereich der Applikations- und Datenhaltung in Rechenzentren und der Nutzung von Cloud-Technologien praxisnah erläutert. Ebenfalls als relevant eingestufte Punkte wie die Vernetzung, mobile Endgeräte, neue Möglichkeiten mit KI und IOT wurden von den Experten kritisch angesprochen und hier zusammenfassend dargestellt. Für begründete Aussagen in der Interpretation der Ergebnisse wird neben Einzelbezügen auf diese zusammenfassende Gesamtsicht referenziert, womit die Nebenforschungsfrage 2 beantwortet werden kann.

2.2.1.3 NFF3 Welche Lösungsmöglichkeiten gibt es hier aus der Praxis?

In diesem Kapitel werden die Ergebnisse dargelegt, die sich aus Interviewfrage 17 (IF17) zum Ende der Interviews ergeben haben. Wichtig ist, dass die hier genannten Ergebnisse noch keine Beantwortung der Forschungsfragen darstellen, sondern lediglich den empirisch

erhobenen Anteil repräsentieren. Zudem wurden chronologisch davor weitere Themenfelder in den Interviews angesprochen, bis abschließend die Lösungsmöglichkeiten als Empfehlungen erfasst wurden. Die Ergebnisse zu diesen weiteren Interviewfragen, die sich den Forschungsfragen nicht direkt zuordnen lassen, werden ab Kapitel III 2.2.2 dargelegt.

Die von den Experten genannten Lösungsmöglichkeiten wurden codiert und inhaltlich im Gesamtzusammenhang analysiert. Es erfolgte eine Zuordnung zu Bereichen, auf die sich die Lösungsansätze beziehen. Dabei konnten die Empfehlungen in drei Bereiche aufgeteilt werden: Personal, Technologie und Vorgehen. Die Zuordnung der Textpassagen zu diesen Bereichen und die codierten Segmente sind in der Tabelle der Anlage VIII. 7 abgebildet.

Auffallend ist, dass nur wenige Experten bei den ersten Aussagen hinsichtlich der Empfehlungen die Technologiedimension angesprochen haben. Die Bereiche Wissen und Verständnis für die Digitalisierung und Personalmanagement in unterschiedlichen Ausprägungen wurden hingegen regelmäßig beginnend erläutert. Experte_12 (2022, Anlage III. 12) bezeichnete es als „Mindset“, womit neue Umgangs- und Denkweisen gemeint sind, die für die Digitalisierung erforderlich sind. Diese seien in der Praxis noch nicht vorhanden. Technologische Aspekte, wie Redundanzen (Experte_03, 2022, Anlage III. 3), Multi-Vendor-Strategien oder Endgerätesicherheit (Experte_09, 2022, Anlage III. 9) wurden ebenso erläutert wie verschiedene Managementmethoden. Bei den Vorgehensweisen wurden ein zu praktizierendes Risikomanagement (Experte_02, 2022, Anlage III. 2), ein angemessenes Kosten/Nutzen-Verhältnis (Experte_05, 2022, Anlage III. 5) und das Beüben als kritische Erfolgsfaktoren für ein gutes Business Continuity Management genannt (Experte_08, 2022, Anlage III. 8). Zur Unterstützung der weiteren Erläuterung sind in der nachfolgenden Abbildung die wesentlichen Themenfelder mit Stichworten aus dem empirischen Material dargestellt.

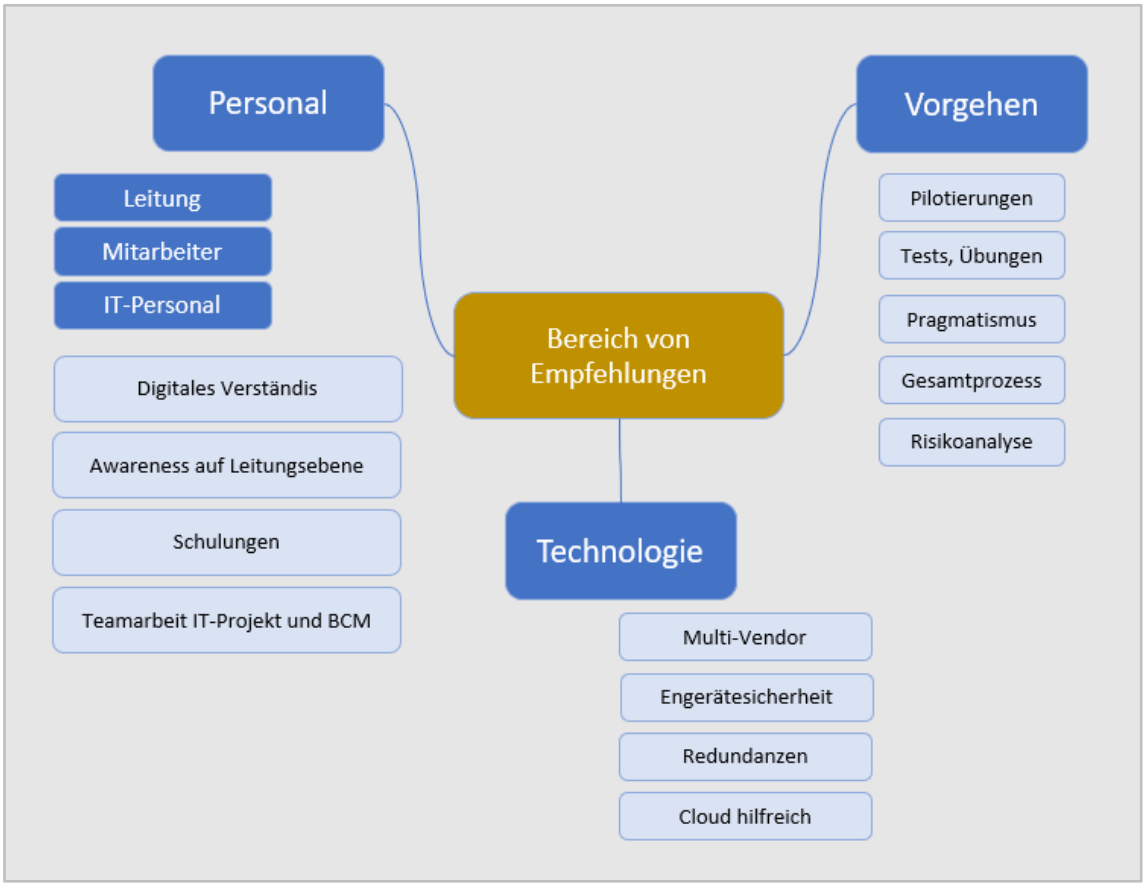


Abbildung 35 – Mindmap zu Themenbereichen für Empfehlungen (Quelle: eigene Darstellung)

Bei dem Personal in den Leitungsfunktionen, so empfahl Experte_01 (2022, Anlage III. 1), sollte der Bereich Business Continuity Management in der Hierarchie höher angesiedelt werden. Er stufte es als Aufgabe des CEO ein und nicht, wie aus der Praxis berichtet, eine oder zwei Ebenen tiefer. Für alle Mitarbeiter seien Schulungen vorzusehen. Experte_10 (2022, Anlage III. 10) empfahl für das Verständnis, die Prozesse sichtbar zu machen. Experte_08 (2022, Anlage III. 8) sah die Gefahr, dass das Business Continuity Management in der IT-Projektarbeit nicht angenommen wird, wenn es als kontrollierendes Organ auftritt. Hier wurde empfohlen, offen aufeinander zuzugehen und konstruktiv mitzuarbeiten (Experte_08, 2022, Anlage III. 8).

Weitere Empfehlungen bezogen sich auf das allgemeine Vorgehen. Hier wurden die auch aus der Theorie bekannten Tests und Übungen praxisorientiert erläutert. Für Pilotierungen wurde ausdrücklich empfohlen, nicht zu viele Voranalysen durchzuführen, sondern einen überschaubaren Teilbereich zu wählen, der aber auch eine Relevanz für die Behörde hat (Experte_14, 2022, Anlage III. 14). Passend dazu bezeichnete Experte_08 (2022, Anlage III. 8) dies als pragmatisches und zielorientiertes Vorgehen und schlug eine Orientierung an den möglichen Gefährdungen vor. So hob auch Experte_02 (2022, Anlage III. 2) die Bedeutung des Risikomanagements hervor und erinnerte daran, auch die unwahrscheinlichen Risiken und

zusätzlich den Gesamtprozess zu betrachten. Für den technologischen Anteil fasste es Experte_03 (2022, Anlage III. 3) so zusammen, dass Alternativen geschaffen werden müssen, sobald das Hauptsystem nicht mehr zur Verfügung steht. Das Prüfen, wo dafür eine Cloud-Technik eingesetzt werden kann (Experte_08, 2022, Anlage III. 8), wurde genannt, allerdings sollte man sich hierfür nicht nur auf einen Hersteller verlassen (Experte_09, 2022, Anlage III. 9). Der Bereich der Endgerätesicherheit wurde besonders hervorgehoben (Experte_09, 2022, Anlage III. 9), wenn zukünftig durch die weitere Vernetzung immer mehr Endgeräte in die Systeme integriert werden. Weitere Empfehlungen zu technologischen Aspekten aus Sicht des Business Continuity Managements werden später in der Diskussion genannt.

Damit sind die wesentlichen Bereiche der Empfehlungen für Lösungsmöglichkeiten aufgeführt und mit Ankerbeispielen belegt. Aufgrund der hohen Bedeutung der Nebenforschungsfrage 3 für die Hauptforschungsfrage und die Zielstellung dieser Arbeit erfolgt eine weitere ausführliche Darstellung der Ergebnisse in Kapitel III 2.2.3 nach der Vorstellung weiterer Erkenntnisse aus dem Bereich relevanter Vorgaben.

2.2.2 Relevante Vorgaben und Arbeitshilfen aus Sicht der Experten

Nach der Darlegung der Ergebnisse, die sich unmittelbar auf die Forschungsfragen beziehen, werden nachfolgend weitere Ergebnisse erläutert, die mittelbar im Gesamtkontext von hoher Bedeutung sind. Es wurde in den Interviews nach Standards und Vorgaben für das Business Continuity Management gefragt, ohne dabei konkrete Angaben zu tätigen. Damit kann die tatsächliche Etablierung in der Praxis mit erforscht werden und in die Analyse einfließen. Ziel war es, damit die zu formulierenden Lösungsmöglichkeiten derart zu gestalten, dass sie zu den in der Praxis angewandten Vorgaben und Methoden passen. Nach der offenen Einstiegsfrage wurde geprüft, ob zu den vier Themenblöcken BSI-Vorgaben, Best Practices, Gesetze und Normen Aussagen erfolgt sind; falls nein, wurde hierzu ergänzend nachgefragt.

Für diese nicht mehr unmittelbar den Forschungsfragen zuordenbaren codierten Segmente wurde auf eine tabellarische Auflistung in der Anlage VIII. verzichtet. Die relevanten Aussagen sind in Anlage VI. ab dortigem Unterkapitel 2.9 aufgeführt. Die Auswertung ist nach der folgenden und zusammenfassenden Abbildung beschrieben.

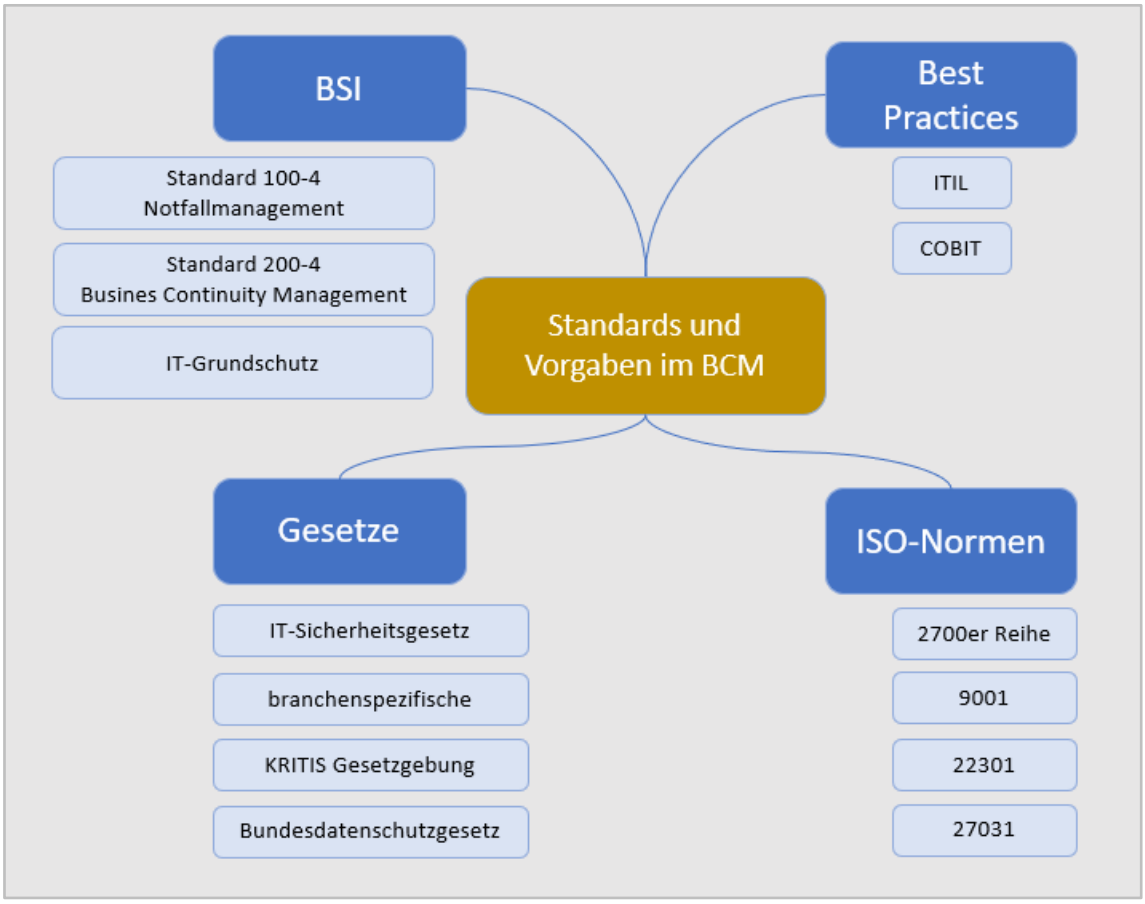


Abbildung 36 – Mindmap zu relevanten Vorgaben (Quelle: eigene Darstellung)

Die Gruppe der Experten setzte sich ausschließlich aus IT-Dienstleistern zusammen, die auch Erfahrung mit Behörden-IT haben. Erwartungsgemäß wurden die Vorgaben des BSI genannt und aus der Praxis erläutert. Der Standard 100-4 und der zum Zeitpunkt der Interviewführung noch zukünftig erwartete Standard 200-4 wurden von fast allen Experten aktiv angesprochen. Experte_02 bewertete diesen Standard als grundsätzlich gut (2022, Anlage III. 2). Ein Experte empfahl diese Standards explizit im Zusammenhang mit der weiteren Digitalisierung (Experte_05, 2022, Anlage III. 5). Den Standard 200-4 bewertete Experte_08 als wesentlich erneuert und verbessert gegenüber dem Standard 100-4 (Experte_08, 2022, Anlage III. 8). Hier war die Notwendigkeit einer Differenzierung zu erkennen, so dass aus Sicht eines Experten die vollständige Umsetzung der Standards 100-4 und 200-4 in kleineren Behörden, auch aufgrund des benötigten Personals, noch schwierig sei (Experte_11, 2022, Anlage III. 11). Schwierigkeiten in der Umsetzung dieser Standards konstatierte auch Experte_12, da dies aus Sicht der Organisation oft nicht leistbar ist (Experte_12, 2022, Anlage III. 12), und er empfahl, die Standards als Orientierungshilfe zu nutzen. Experte_14 äußerte sich zum Standard 200-4 kritisch und empfahl eher internationale Standards wie die ISO-Norm 22301 (Experte_14, 2022, Anlage III. 14). Mit konkreten Anhaltspunkten, um ein Business Continuity Management

praktisch aufzubauen, bewertete Experte_10 den BSI-IT-Grundschutz positiv und hob die dort aus seiner Sicht sehr gut behandelten Beispiele hervor (2022, Anlage III. 10).

Für die Best-Practices nach ITIL und COBIT, wie in Kapitel II 2.1.5 dargestellt, wurden die verschiedenen Aussagen der Experten gemeinsam betrachtet. Experte_13 (2022, Anlage III. 13) berichtete, wie aus seiner Erfahrung eher ITIL statt COBIT zur Anwendung kommt. Ebenfalls zurückhaltend äußerte sich Experte_14 (2022, Anlage III. 14) zu COBIT, verwies aber auf dort vorhandene Kennzahlen, die für das Business Continuity Management betrachtet werden können. Experte_12 (2022, Anlage III. 12) erwähnte lediglich ITIL als Richtschnur und Experte_10 (2022, Anlage III. 10) erläuterte ein Problem, dass zwar Mitarbeiter danach ausgebildet und zertifiziert würden und das Wissen anfangs auch angewendet werde, die Umsetzung dann aber regelmäßig nicht bis zum Ende fortgeführt werde. Experte_08 (2022, Anlage III. 8) grenzte COBIT hier klar ab und sagte, dass es aus seiner Sicht für die Umsetzung eines Business Continuity Managements nicht hilfreich sei. Als „super Handwerkszeug“ bezeichnet Experte_06 (2022, Anlage III. 6) das ITIL-Framework und wies auf den bereits in der Theorie dargestellten Plan-Do-Check-Act-Zyklus hin. Subjektive Abneigung führte Experte_05 (2022, Anlage III. 5) gegenüber COBIT an, nannte allerdings keine Details. Auf ITIL und die ISO 20000 wies er empfehlend hin. Experte_02 (2022, Anlage III. 2) bezeichnete ITIL als gängigen Standard und Experte_01 (2022, Anlage III. 1) hält diesen ebenfalls für wichtig. Übereinstimmend mit bereits genannten Aussagen zu COBIT bewertete auch Experte_01 (2022, Anlage III. 1) diesen Standard als hier weniger nützlich. Interessanterweise wurde das im Theorieteil genannte TOGAF-Framework seitens der Experten überhaupt nicht angesprochen.

Bei den Gesetzen wurde mehrfach das IT-Sicherheitsgesetz angeführt (Experte_14, 2022, Anlage III. 14; Experte_12, 2022, Anlage III. 12; Experte_11, 2022, Anlage III. 11; Experte_1, 2022, Anlage III. 1). Differenziert erläuterte Experte 14 (2022, Anlage III. 14) die Situation, dass es zwar anfangs gut entworfen wurde, sich in der Praxis aber viele Kritikpunkte zeigen. Beispielsweise sah er die Gefahr, dass sich Unternehmen nicht vollumfänglich resilient aufstellen, wenn gesetzlich nur die Absicherung von bestimmten Prozessen vorgesehen ist. Verschiedene branchenspezifische Gesetze wurden genannt und im Kontext betrachtet, beispielsweise das Kreditwesengesetz (Experte_01, 2022, Anlage III. 1). Experte_06 (2022, Anlage III. 6) führte dazu das Krankenhauszukunftsgesetz an. Auch Experte_08 (2022, Anlage III. 8) reflektierte hierzu passend die KRITIS-Gesetzgebung und sagte, Gesetze könnten einen „Anschub leisten“ (Exerte_08, 2022, Anlage III. 8) und seien als positiv zu

sehen. Als Ausnahme und übereinstimmend mit Aussagen aus der Theorie (Kipker und Scholz, 2021, S. 42) kritisierte Experte_05 (2022, Anlage III. 5) die Gesetze grundsätzlich als zu wenig konkret. Argumentativ führte er die Lobbyarbeit an, die dann die ursprünglichen Gesetze beeinflusse, so dass diese anschließend nicht mehr konkret genug verfasst seien (Experte_05, 2022, Anlage III. 5).

Das Bundesdatenschutzgesetz wurde mehrfach genannt (Experte_08, 2022, Anlage III. 8; Experte_13, 2022, Anlage III. 13) und mit einer großen Reichweite und weitreichenden Vorgaben auch für den Bereich Business Continuity Management bewertet. Die NIS-Richtlinie der EU wurde lediglich von einem Experten angesprochen und dieser erläuterte dazu, dass sie Grundlagen für den Bereich der IT-Sicherheit schafft (Experte_05, 2022, Anlage III. 5).

Als letzter Block werden hier die ISO-Normen betrachtet, die im empirischen Teil von den Experten genannt wurden. Erwartungsgemäß wurde sehr oft direkt Bezug auf die ISO-Norm 22301 genommen. Experte_14 (2022, Anlage III. 14) empfahl diesen internationalen Standard sogar deutlich vor nationalen Standards wie dem BSI 200-4 und argumentierte dazu, dass keine nationalen Standards nötig seien. Ein Experte bestätigte die in der Theorie herausgearbeitete Situation mit den Worten „Die meisten haben es überhaupt gar nicht auf dem Schirm“ (Experte_12, 2022, Anlage III. 12). Zusammenfassend wurden positive und erläuternde Aussagen der Experten zu den ISO-Normen 22301, 27031, 9001 und 27000er getätigt, die eine Vereinfachung und ein Gütesiegel darstellen können (Experte_04, 2022, Anlage III. 4). In den Anlagen sind alle Aussagen zu den ISO-Normen in Kapitel VI. 2.9.3 aufgelistet.

Damit wurden die aus Sicht der Experten gängigen und relevanten Vorgaben sowie Arbeitshilfen, die aktuell in der Praxis zur Anwendung kommen, aufgeführt und die Sicht aus der Praxis auf diese Vorgaben wurde erläutert.

2.2.3 Darlegung der Empfehlungen

Basierend auf den drei zugeordneten Bereichen für Lösungsmöglichkeiten in Bezug auf Personal, Vorgehen und Technologie, die sich aus der Analyse der Aussagen zur dritten Nebenforschungsfrage ergeben haben, werden hier die verschiedenen Empfehlungen der Experten weiter analysiert und ausführlich dargestellt.

<u>Dimension Personal</u>

Für den Bereich Personal und Personalmanagement haben die Experten sowohl zur Ebene Führungskräfte, Vorgesetzte, Geschäftsführer bzw. Amtsleiter Aussagen getroffen als auch zu

betroffenen Mitarbeitern und Kunden von Unternehmen und Behörden. Ebenso wurden Aussagen zur Rolle des IT-Fachpersonals im Zusammenhang mit IT-Projektleitungen getätigt und die Funktion der BCM-Experten in dem Zusammenhang wurde thematisiert. Wie bereits zitiert, forderte Experte_01 die Erhöhung des Stellenwerts im Management und hält es für notwendig, die Thematik in der Unternehmenssteuerung zu verankern (Experte_01, 2022, Anlage III. 1). Experte_13 (2022, Anlage III. 13) berichtete, wie durch die zunehmende Digitalisierung die sogenannte Awareness aktuell weiter steigt. Auch Experte_01 (2022, Anlage III. 1) sah eine verstärkte Aufmerksamkeit in den letzten drei Jahren. Er argumentierte dies im Zusammenhang mit der Coronapandemie. Durch aktuelle Ereignisse wie den Ukrainekrieg steigt das empfundene Risiko im Zusammenhang mit einem Business Continuity Management, sagte auch Experte_07 (2022, Anlage III. 7). Es müsse hier noch mehr sensibilisiert werden, um auch in Behörden und bei entsprechenden IT-Dienstleistern das Business Continuity Management zu stärken (Experte_07, 2022, Anlage III. 7). Die Mitarbeiterebene umfänglich einzubinden, schlug Experte_08 (2022, Anlage III. 8) vor und verband damit eine Förderung zum selbstverantwortlichen Handeln. Dadurch sollen die Mitarbeiter auch dann weiter agieren können, wenn etwas in der IT nicht wie geplant funktioniert. Er bewertete diesen Aspekt als Kernkomponente einer guten Resilienz. Zur Einhaltung von einfachen IT-Sicherheitsstandards sah Experte_06 die Notwendigkeit der Sensibilisierung der Mitarbeiter auf menschlicher und psychologischer Ebene (2022, Anlage III. 6).

Auf das IT-Fachpersonal kommt damit eine besondere Rolle zu, dass die Anforderungen des Business Continuity Managements stets mitberücksichtigt werden sollen. Es scheint, das Business Continuity Management in Digitalisierungsprojekten noch nicht immer ausreichend berücksichtigt wird. Hierzu sind die IT-Projektleitungen frühzeitig mit den BCM-Experten zusammenzubringen, damit nicht, wie Experte_14 aus seinen Erfahrungen berichtete, bei Großprojekten über Jahre die Aspekte der technischen Ausfallsicherheit vergessen werden (2022, Anlage III. 14).

Mit den Schulungen sah Experte_07 auch einen aufklärenden Zusammenhang, durch den der hinter den Maßnahmen stehende Nutzen klar wird (2022, Anlage III. 7). Für Experte_10 waren Schulungen im Bereich des Denkens in Prozessen essenziell (2022, Anlage III. 10). Gleichzeitig berichtete er von Erfahrungen, dass Ausbildungen zwar durchgeführt werden und Mitarbeitern entsprechende Prozessschulungen ermöglicht werden, dass aber anschließend keine ausreichende Umsetzung des Erlernten in der Firma oder der Behörde erfolgt. Ebenfalls

warnte Experte_11, dass Schulungen grundsätzlich besucht werden und die Thematik initial angegangen wird, jedoch werde sie wegen des großen Aufwandes danach nicht weiter vorangetrieben (2022, Anlage III. 11).

Im Bereich des Business Continuity Managements kommt den Tests und Übungen eine besondere Bedeutung zu, wie auch in der Theorie schon dargestellt. Nach Experte_08 (2022, Anlage III. 8) wird sonst „nur Papier erzeugt“. Die aufgeschriebenen Prozesse werden erst durch Tests und Übungen in das Bewusstsein der Mitarbeiter gelangen und können so eingeübt und trainiert werden. Experte_11 (2022, Anlage III. 11) sah bei diesen Simulationen den Vorteil, dadurch auch über die möglichen Bedrohungslagen zu informieren und bei den Mitarbeitern das notwendige Verständnis zu schaffen. Er hob hervor, hier auch die Führungsebene direkt in entsprechende Simulationen einzubeziehen. Experte_08 (2022, Anlage III. 8) nannte es Überzeugungsarbeit, die geleistet werden muss, und sah es als Priorität an, zunächst die Unterstützung durch die Geschäftsleitungen und die Amtsleitungen sicherzustellen. Da bei der Suche nach IT-Fachkräften und angesichts des schnellen Wandels der Technologien nur bedingt sofort passendes Personal auf dem Markt zu finden ist, empfahl Experte_13 (2022, Anlage III. 13), sowohl auf eigene Ausbildung zu setzen als auch eingestellte Fachkräfte durch Weiterbildungen zu schulen. Für einen Überblick sind diese Empfehlungen strukturiert in Abbildung 37 dargestellt.

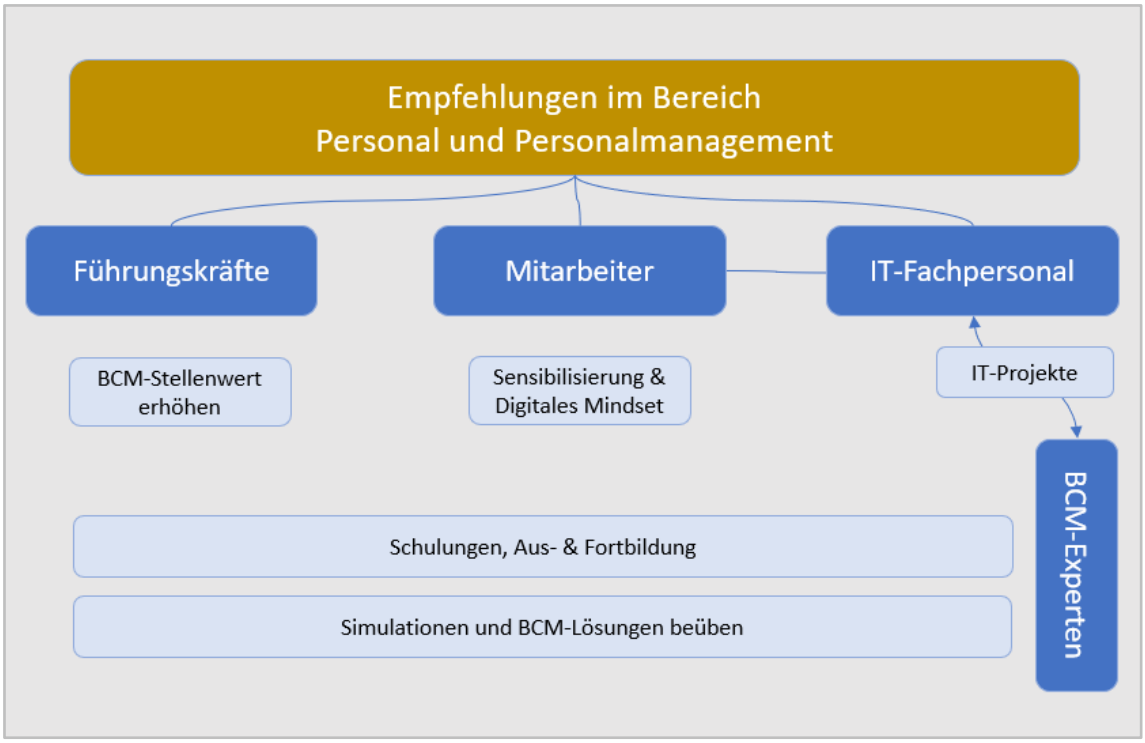


Abbildung 37 – Empfehlungen im Bereich Personal (Quelle: eigene Darstellung)

Im Bereich Personal und Personalmanagement wurden die Bereiche Führungskräfte, eigene Mitarbeiter sowie explizit das IT-Fachpersonal und die BCM-Experten als eigene Gruppen angesprochen. Die wesentlichen und mehrfach genannten Empfehlungen für diese Personalgruppen wurden hier zugeordnet. In der Abbildung 37 sind unten die durch die BCM-Experten zu unterstützenden Themenbereiche, wie Ausbildung und Schulungen sowie Simulationen und Übungen querschnittlich wirkend für alle Mitarbeitergruppen dargestellt.

Dimension Vorgehen, Teil 1: BCM einführen

Weitere Empfehlungen betrafen das allgemeine Vorgehen, um ein Business Continuity Management zu etablieren. Wie im vorherigen Absatz beschrieben, ist es wesentlich, die notwendige Aufmerksamkeit für die Aktivitäten zu schaffen. Experte_13 hoffte auf eine steigende Awareness und sah bei entsprechend hoher Aufmerksamkeit für ein Business Continuity Management auch die Sicherheitsaspekte bei der Digitalisierung allgemein als mehr berücksichtigt (2022, Anlage III. 13). Nach der Sensibilisierung sollen, so Experte_06, notwendige Ressourcen und Budget bereitgestellt werden. Er bezeichnete das als zentralen Punkt (Experte_06, 2022, Anlage III. 6). Im Unterschied zum Vorgehen nach BSI-Standard 200-4 schlug Experte_14 hinsichtlich der Einführung vor, dass zunächst einen Bereich der Behörde herausnehmen sei, der bereits relevant für den Betrieb ist und der gut abgeschätzt werden kann. Dort sollen die entwickelten Methoden ausprobiert werden (Experte_14, 2022, Anlage III. 14). Ebenfalls stufte es Experte_02 (2022, Anlage III. 2) als problematisch ein, wenn man, statt zu beginnen, mit der Digitalisierung immer direkt alles umgesetzt haben möchte, und schlug vor, mit kleinen Schritten anzufangen. Ein dokumentiertes Business Continuity Management zu erstellen, es aber nicht zu nutzen, erachtete Experte_08 (2022, Anlage III. 8) als problematisch und bezeichnete es aus der Praxis heraus als größten Fehler im Notfallmanagement. Er sah eine gute Vorgehensweise erst durch regelmäßige Tests und Übungen abgesichert. Ebenfalls als relevant bezeichnete Experte_11 (2022, Anlage III. 11) solche Übungen und Simulationen, um ein Gespür dafür zu erwerben, wo die Bedrohungen liegen.

Dimension Vorgehen, Teil 2: Risikomanagement

Ein praktiziertes Risikomanagement nannten viele der Experten im Zusammenhang mit dem Vorgehen, ein Business Continuity Management zielorientiert einzuführen. Experte_02 (2022, Anlage III. 2) bezeichnete es als eine Analyse der Störgrößen, die vorgenommen werden sollte und eine Abschätzung welche Probleme davon erwartbar oder nicht erwartbar

sind, um dann weitere Schritte abzuleiten. Experte_05 (2022, Anlage III. 5) verglich die Gesamtthematik mit einem generellen Risikomanagement, so dass stets alles eine Abwägung ist, ob ein Risiko tolerierbar ist oder nicht. Bemerkenswert hier ist, dass es in der Praxis auch Situationen geben kann, wonach das Risikomanagement die benötigten Budgets nicht rechtfertigen würde. Experte_07 (2022, Anlage III. 7) argumentiert hierzu, dass diese Einschätzung dann von der Geschäftsführung übersteuert werden müsse, um solche IT-bezogenen Notfallmaßnahmen mit einzuplanen.

Dimension Vorgehen, Teil 3: Allgemein

Bei den allgemeinen Empfehlungen schlugen mehrere Experten einen pragmatischen Ansatz vor. Experte_11 (2022, Anlage III. 11) reflektierte die fundierten Grundlagen aus dem BSI-Standard und den ISO-Normen, sah diese aber eher als Orientierungshilfe und praktiziert selbst pragmatischere Alternativen, um z. B. ein IT-Notfallhandbuch in wenigen Wochen statt in vielen Jahre zu erstellen. In diesem Zusammenhang verwies Experte_08 (2022, Anlage III. 8) auf weitere Standards, die praxisorientierte und pragmatische Implementierungsmethoden beinhalten, wie die Good Practice Guidelines, die im Theorieteil bereits genannt wurden. Deutlich im Zusammenhang mit den neuen Produkten der Digitalisierung stellte Experte_01 (2022, Anlage III. 1) die Notwendigkeit pragmatischer Methoden heraus, da hier alte Ansätze nicht mehr funktionieren würden und andere, neue Lösungen erforderlich seien.

Ein Experte sah einen hohen Nutzen, wenn durch die eigene Motivation zur Einhaltung der ISO-Normen ein adäquates Sicherheitsniveau erreicht werden soll (Experte_07, 2022, Anlage III. 7). Als eine Art Gewissheit, um das betreffende Unternehmen bestmöglich zu schützen, bezeichnete Experte_09 (2022, Anlage III. 9) die ISO-Normen. Als „starke Stütze“ (Experte_10, 2022, Anlage III. 7) könne eine ISO-Zertifizierung auch für die internen Zwecke angesehen werden. Kritisch erläuterte Experte_11 (2022, Anlage III. 11) diese Motivation dahingehend, dass diese zwar wünschenswert wäre, aber eine Zertifizierung aktuell eher regulatorisch von Vertragspartnern oder Gesetzgebern getrieben werde.

Direkte Empfehlungen, den COBIT-Standard für ein Business Continuity Management anzuwenden, gab es von den Experten nicht. ITIL als Prozess-Framework hingegen wurde von einigen Experten als positiv und in diesem Zusammenhang als hilfreich diskutiert. Experte_14 (2022, Anlage III. 14) befürwortete den Zusammenhang von Business Continuity Management und ITSCM. Das IT-Service-Continuity als Teil des IT-Notfallmanagements wurde seitens des Experten_05 (2022, Anlage III. 5) als nutzbar angesehen. Erst auf Nachfrage äußerte sich Experte_08 (2022, Anlage III. 8) zu diesen Standards, sagte aber, dass Business Continuity

Management aus seiner Sicht dort nicht der Schwerpunkt ist, wobei ITIL als Standard in diesem Bereich zu nennen sei. COBIT stufte er nicht als hilfreichen Standard für das Business Continuity Management ein. Experte_10 (2022, Anlage III. 10) berichtete von Erfahrungen zu mangelnden Umsetzungen. Es würden zwar Schulungen zu diesen Standards besucht, jedoch erfolge anschließend keine ausreichende Umsetzung in der Praxis. Von einer langen Erfahrungszeit und einem positiven Nutzen berichtete Experte_13 (2022, Anlage III. 13) zur Anwendung von ITIL. Zudem verwies er auf Kundenanforderungen, die dazu geführt hätten, dass man damals in bestimmten Prozessen, wie dem Störungsmanagement (Incident-Management), besser werden musste. Zusammenfassend kann somit ITIL im Vorgehen als hilfreiches Werkzeug angesehen werden, das zwar nicht im Schwerpunkt die Herausforderungen des Business Continuity Managements im Rahmen der Digitalisierung löst, aber mit den etablierten Anteilen des ITSCM dort unterstützen kann. TOGAF und COBIT wurden von den Experten nicht spontan als passendes Werkzeug genannt. Hier ist von einem Zusammenhang zwischen dem in Kapitel II 2.1.5 bereits genannten Fokus und den Stärken dieser Standards auszugehen. Der Aufbau von Unternehmens- und IT-Architekturen mittels TOGAF sowie die Unterstützung der Unternehmenssteuerung nach Vorgaben gemäß COBIT haben die Experten nicht unmittelbar mit den Herausforderungen der Einführung eines Business Continuity Managements verbunden. Da aber beide Standards grundsätzlich ein Continuity Management im Rahmen ihrer Empfehlungen vorsehen, kann ihre Anwendung im entsprechenden Kontext empfohlen werden. Von hoher Relevanz hierbei ist, dass die jeweils aus Sicht des Business Continuity Managements relevanten Aspekte nicht vernachlässigt werden. Mit Verweis auf die Tabelle 6 auf Seite 72 dieser Arbeit sind das für TOGAF die Architekturprinzipien der ‚Business Continuity', für ITIL die ‚Service-Continuity-Management-Praktiken' und für COBIT die Vorgaben der ‚Managed Continuity' aus den Bereichen Deliver, Service und Support.

Erwartungsgemäß wurde der BSI-Standard in den Interviews umfangreich von den Teilnehmern angesprochen. Die Erkenntnisse daraus werden nachfolgend erläutert.

Dimension Vorgehen, Teil 4: BSI-Standards

Wie eingangs in Kapitel II 2.1.5 dieser Forschungsarbeit umfangreich dargestellt, sind die BSI-Standards 100-4 und 200-4 als Vorgabedokument von besonderer Bedeutung in Deutschland. Die Erfahrungen aus der Praxis dazu wurden erfasst. Ein Experte in der Funktion als Geschäftsführer eines IT-Dienstleisters traf im Rahmen der Interviews zu den Standards

nach BSI keine konkreten Aussagen bzw. verwies für weitere Fachexpertise hierzu auf seine Mitarbeiter (Experte_04, 2022, Anlage III. 4). Dass der Standard auch in diesem Unternehmen präsent ist, wurde damit indirekt bestätigt. Ein weiterer Experte machte ebenfalls keine Aussagen, sondern assoziierte den Bereich der Standards ausschließlich mit den ISO-Normen (Experte_13, 2022, Anlage III. 13). Alle weiteren Experten erläuterten in Bezug auf Standards ihre Sicht zu den BSI-Dokumenten und berichteten von Erfahrungen. Damit ist ersichtlich, dass diese BSI-Standards für den Bereich des Business Continuity Managements bei den behördenerfahrenen IT-Dienstleistern grundsätzlich entsprechend bekannt sind. Aus der praxisorientierten Erfahrung berichteten allerdings einige Experten, dass deren Anwendung nicht ohne wichtige Anmerkungen zu empfehlen ist. In der Anlage VIII. 8 sind die entsprechenden Aussagen als codierte Segmente aufgeführt.

Insgesamt werden diese Standards zwar als hilfreich bewertet, allerdings ist eine direkte Umsetzung aufgrund ihres Umfanges schwierig. Experte_11 (2022, Anlage III. 11) bezeichnete dem Umfang als „oversized“ für die Zielgruppe am Beispiel von Landratsämtern und Polizeibehörden. Experte_12 (2022, Anlage III. 12) bewertete die Vorgaben als nicht umsetzbar, aber gleichzeitig nannte er es als Orientierung „sehr, sehr hilfreich“. Kritisch diskutierte Experte_14 (2022, Anlage III. 14) diese Standards und empfahl, internationale Reglungen vorzuziehen. Im Gegensatz dazu stufte Experte_10 (2022, Anlage III. 10) die Standards als konkreten Anhaltspunkt positiv ein und Experte_09 (2022, Anlage III. 9) bezeichnete sie darüber hinaus als „ganz wichtig“. Als grundsätzlich gut bewertete Experte_02 (2022, Anlage III. 2) diese Vorgaben und auch Experte_01 (2022, Anlage III. 1) thematisierte die Standards und bezeichnete sie als erwähnenswerte Methodensammlung. Auf Basis dieser Aussagen sind die BSI-Standards 100-4 und 200-4 für ein zielführendes Vorgehen im Business Continuity Management bei der weiteren Digitalisierung als praxisrelevante Richtlinien zu bewerten.

Experte_06 (2022, Anlage III. 6) sah die Notwendigkeit einer kontinuierlichen Bearbeitung der Herausforderungen durch regelmäßige Tests und auch Experte_14 (2022, Anlage III. 14) wies auf einen Lifecycle hin, der sich jedes Jahr wiederholt. Dem folgend werden die Empfehlungen im Vorgehen grundsätzlich als notwendige Daueraufgabe statt als einmalige Aktivität betrachtet. Für diese Ergebnisse wurde die folgende Übersicht in Abbildung 38 erstellt, deren Bestandteile soeben erläutert wurden:

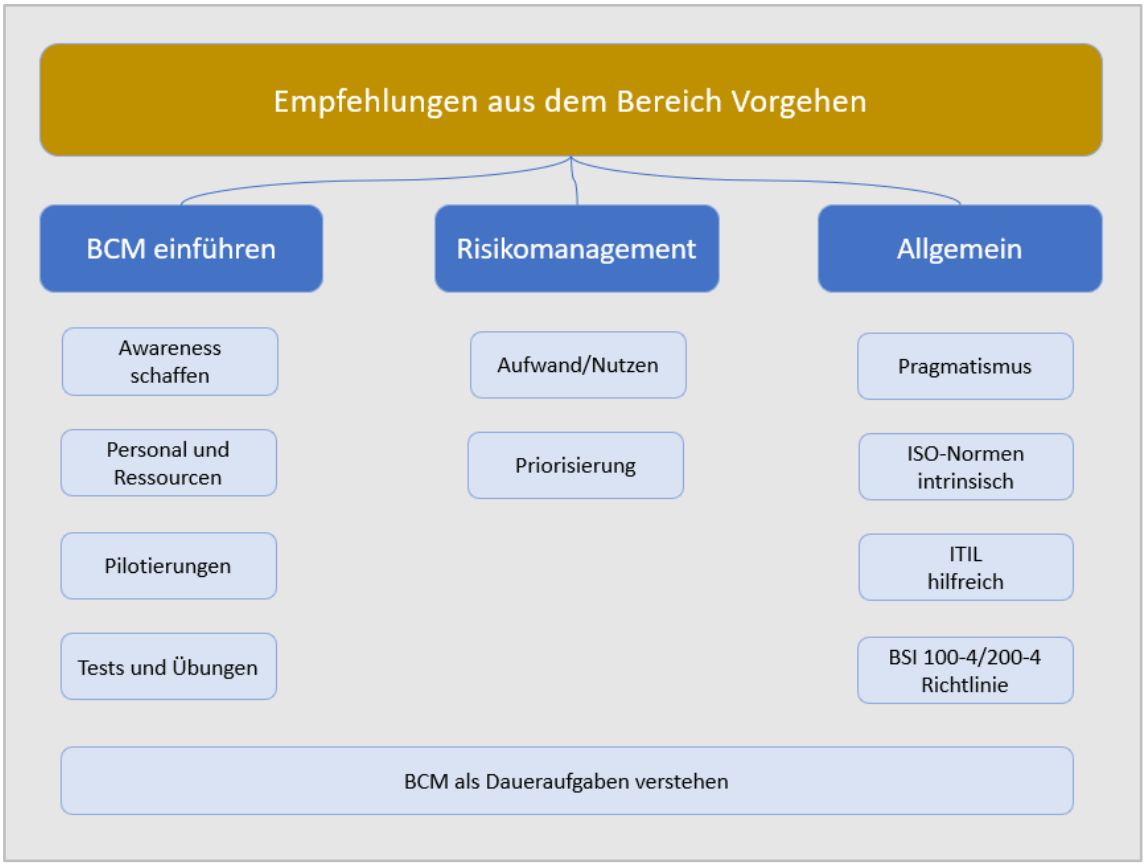


Abbildung 38 – Übersicht Empfehlungen zum Vorgehen (Quelle: eigene Darstellung)

Damit sind die Empfehlungen aus den zwei Bereichen Personal und Vorgehen dargestellt. Es folgt der Anteil der Technologien, für den die Experten Empfehlungen und Hinweise zu technischen Aspekten der Digitalisierung gegeben haben.

Dimension Technologien

In diesem Bereich wurden Hinweise und Empfehlungen aus der Praxis erhoben. Diese wurden auf wesentliche Aspekte reduziert, die im Rahmen der Zusammenfassung im Kapitel der theoretischen Grundlagen ermittelt wurden. Die Erläuterungen werden zur Begründung und Herleitung der relevanten Handlungsempfehlungen genutzt. Im Mittelpunkt stehen bei den technologischen Überlegungen die Fragen, mit welchen neuen Herausforderungen ein Business Continuity Management zukünftig konfrontiert sein wird und welche Lösungsansätze es dazu bereits gibt. Um herauszuarbeiten, wie sich die erwarteten weiteren Schritte in der Digitalisierung technisch und organisatorisch ausreichend resilient ausplanen lassen, werden für den empirischen Anteil die Empfehlungen der Experten nachfolgend dargestellt.

Dem Cloud-Computing kommt eine zentrale Rolle bei der Digitalisierung zu, wie bereits in der Theorie recherchiert und hier aus der Praxis bestätigt. Damit beginnend wurden die Aussagen der Experten in den Bereichen Hosting, Betrieb von Cloud-Applikationen, Souveränität, Rechenzentren sowie Empfehlungen zu Multi-Vendor-Strategien und Multi-Clouds analysiert.

Experte_03 erläuterte die Strategien der amerikanischen Konzerne, die durch ein Hosting in Europa die hier einzuhaltenden rechtlichen Regelungen erfüllen möchten, bewertete die Gesamtsituation aber noch als „Grauzone“. Er erachtete es als notwendig, diesen Konzernen eine Konkurrenz zu bieten, um die Souveränität über die Daten zu behalten (Experte_03, 2022, Anlage III. 3). Experte_05 (2022, Anlage III. 5) schlug dazu vor, Behördendaten alternativ zu einer Auslagerung bei Google besser in Rechenzentren der Telekom in Deutschland zu betreiben. Er merkte aber gleichzeitig an, dass es lediglich Rechtsthemen sind, bei denen Organisationen in Bezug auf einen inländischen Betrieb an Vertrauen gewinnen können. Eine besondere Unterscheidung und Prognose sah Experte_07 (2022, Anlage III. 7) bei der Verarbeitung von Daten der sogenannten Klassifikation ‚Verschlusssachen‘. Auch perspektivisch ergebe sich hier keine Lösung durch die großen amerikanischen Cloud-Anbieter für deutsche Behördendaten. Experte_03 (2022, Anlage III. 3) führte als Möglichkeit auch die Gründung von Unternehmen in Deutschland an, die den Betrieb übernehmen können, und diskutierte in dem Zusammenhang die Lösung „Nextcloud“ (Experte_03, 2022, Anlage III. 3). Das Open-Source-Programm nannte er als eine mögliche Option. Ebenso argumentierte Experte_02 (2022, Anlage III. 2), dass sich mit einem Unternehmen aus dem Staatsdienst solche Technologien entwickeln und einsetzen lassen. Experte_04 (2022, Anlage III. 4) zog hierzu einen Vergleich zu den USA, wo mittels behördlicher Ausschreibungen eine sogenannte GovCloud entstanden ist, die den behördlichen Ansprüchen genügt. Diese wurde allerdings von einem großen Cloud-Anbieter umgesetzt. Im Nachgang zu dem Interview wurde hierzu die Firma Amazon mit dem Produkt AWS als Cloud-Anbieter recherchiert. Experte_05 (2022, Anlage III. 5) empfahl in diesem Zusammenhang die Strategie, nicht nur einen Cloud-Anbieter zu nutzen, sondern mehrere einzuplanen. Der Experte würdigte den erhöhten Aufwand und wies dabei darauf hin, dass bei den verteilten Daten dann auch an allen Lokationen die Sicherheitsaspekte hinterfragt werden müssen. Für besonders schützenwerte Systeme sah er im Zweifelsfall dann aber weiterhin die Möglichkeit, sie auch zukünftig als On-Premises-Lösungen zu betreiben. Die Komplexität des Betriebes einer Cloud für höher eingestufte Daten erläuterte auch Experte_07 (2022, Anlage III. 7) und nannte als eine mögliche europäische Lösung das Projekt GAIA-X, das im theoretischen Teil dieser Arbeit bereits dargestellt wurde. Experte_08 (2022, Anlage III. 8) wies auf die Gefahr hin, dass bei der Cloud-Technologie davon ausgegangen wird, automatisch über abgesicherte und notfallfähige Datensicherungen zu verfügen, was aber nicht der Fall sei. Beispielhaft führte er den in der Einleitung dieser Forschungsarbeit genannten Vorfall des Rechenzentrumbrandes in

Straßburg an. Er sah hier seine Vermutung bestätigt, dass Kunden sich darauf verlassen hatten, aber die Dienstleister nur dann Datensicherungen bei den Cloud-Diensten durchgeführt hatten, wenn sie dazu beauftragt waren. Als hybride Cloud bezeichnete ein Experte die Möglichkeit, je nach Sensibilität der Daten zu unterscheiden und gemischte Szenarien zu realisieren, in denen Teile noch in On-Premises-Lösungen verbleiben (Experte_09, 2022, Anlage III. 9).

Das allgemeine Risiko des Abgreifens von Daten sprach er ebenfalls an (Experte_09, 2022, Anlage III. 9). Als Vorteil bewertete Experte_10 (2022, Anlage III. 10) die Möglichkeit, bei Clouds sogenannte Availability-Zonen zu buchen, um damit Anforderungen des Business Continuity Managements zu erfüllen. Unter diesem Fachbegriff finden sich bei Cloud-Anbietern Angebote, bei denen mehrere Rechenzentren an verschiedenen Standorten weltweit verteilt betrieben werden, was für die IT-Services Redundanzen bieten. Für Experte_12 wird Cloud-Computing zunächst mit einer internen Cloud und der Auswahl von Anbietern innerhalb Deutschlands verbunden, bei denen die Verträge im Gegensatz zu Microsoft als Hoster eher überprüfbar sind (Experte_12, 2022, Anlage III. 12). Allerdings wurde auch von Erfahrungen berichtet, bei denen eine On-Premises-Lösung aus BCM-Sicht Schwierigkeiten bereitete und in einer Microsoft Azure Cloud bestimmte Probleme als viel leichter zu lösen bewertet wurden (Experte_12, 2022, Anlage III. 12).

Auch Experte_13 (2022, Anlage III. 13) berichtete von der Herausforderung, die Kontrolle für einen Fallback zu behalten und sicherzustellen, dass der Cloud-Anbieter selbst keinen Zugriff auf die Daten erhält. Insgesamt stehen damit die Aspekte Hosting, Souveränität und mögliche Multi-Cloud-Lösungen aus technologischer Sicht im Vordergrund der Empfehlungen. Abschließend verdeutlichte auch Experte_14, dass er die von amerikanischen Unternehmen angebotenen Public-Cloud-Lösungen im Behördenkontext entschieden nicht befürworten kann, sondern alternativ eine gemeinsame Cloud von deutschen IT-Dienstleistern empfiehlt (Experte_14, 2022, Anlage III. 14).

Die Nutzung der Applikationen oder Services der Cloud erfolgt zunehmend durch den Einsatz von verschieden Zugriffsgeräten. Dazu zählen vor allem mobile Endgeräte, so dass Mobility eine Technologie ist, die für die weitere Digitalisierung von hoher Bedeutung ist. Mit den Begriffen ‚mobil' und ‚bring your own device' sieht Resch (2020, S. 154) es als Teil der Digitalisierung. Passend dazu erachtete Experte_03 (2022, Anlage III. 3) es gegenwärtig als notwendig, dass Vorgänge, beispielsweise von Polizisten, mit dienstlichen oder sogar privaten Smartphones unter Nutzung bestimmter Applikationen bearbeitet werden können. Aus Sicht

des Business Continuity Managements bezeichnete Experte_09 (2022, Anlage III. 9) die Endgerätesicherheit noch als Schwachstelle. Er nannte dazu auch die vermehrte Nutzung des Homeoffice und der damit verbundenen privaten IT und wies darauf hin, wie beispielsweise der Zugangsrouter zum Internet als Einfallstor genutzt werden kann. Für Experte_09 (2022, Anlage III. 9) war dieser Punkt für jede Cloud-Strategie von essenzieller Bedeutung. Experte_04 (2022, Anlage III. 4) hob die einfache Möglichkeit der Kommunikation von Behörden mit der Bevölkerung über soziale Medien hervor und Experte_07 (2022, Anlage III. 7) sah es sogar als notwendig an, dass Behörden den Bürgern solche Services anbieten. Gleichzeitig stufte er hierbei die Themen Identifizierung und den Umgang mit sensiblen Daten noch als große Herausforderungen ein.

Das Internet der Dinge (Internet of Things, IOT) bewertete Experte_10 (2022, Anlage III. 10) für das Business Continuity Management als Herausforderung, da Sensoren beispielsweise grundsätzlich nicht redundant ausgelegt werden. Es sei nicht üblich, zwei Sensoren zu verbauen, um bei einem Ausfall den Defekt direkt überbrücken zu können. Er betonte einerseits, dass das IOT bereits stark verbreitet ist, andererseits sprach er hier von Vernachlässigungen in der Praxis aus BCM-Sicht. Ebenfalls das Wort ‚Vernachlässigung' nutzte hier Experte_09 (2022, Anlage III. 9), der IOT als wichtigen Punkt in der Digitalisierung bezeichnete, und er wies darauf hin, dass Computerviren im IOT in deutlich anderen Formen auftreten als bekannte Schadsoftware im Office-IT-Bereich. Experte_14 (2022, Anlage III. 14) verband das IOT mit der künstlichen Intelligenz (KI) und damit die weitere Automatisierung von Prozessen, sah aber eine zunehmende Herausforderung in der Absicherung der darunterliegenden Infrastrukturkomponenten. Experte_08 (2022, Anlage III. 8) hinterfragte die Update-Fähigkeit von IOT-Devices und erläuterte, dass es viele Geräte gibt, die nicht aktualisiert werden können, so dass eine Sicherheitslücke über Jahre offen bleiben kann.

Experte_11 (2022, Anlage III. 11) forderte die Erarbeitung von Kontinuitätsstrategien für den Bereich der zunehmenden Vernetzung. Als einen Ansatz hierfür nannte er eine ausreichende Dokumentation, auf deren Basis die Bewertungen von Ausfallszenarien erfolgen können. Als große Herausforderung stufte Experte_01 (2022, Anlage III. 1) bei der Vernetzung auch datenschutzrechtliche Anforderungen ein. Eine steigende Bedeutung für das Business Continuity Management und das IT-Notfallmanagement sah in diesem Zusammenhang auch Experte_05 (2022, Anlage III. 15). Experte_14 (2022, Anlage III. 14) forderte bei zukünftig durch KI gemanagten Prozessen, dass weiterhin der Mensch sie kontrollieren und verstehen muss. Hier verortete er das Business Continuity Management und das ITSCM in einer starken

Rolle. Diese BCM-relevanten Handlungsfelder zu den von den Experten genannten Aspekten der Digitalisierung wurden in der nachfolgenden Abbildung skizziert. Damit ist ein Überblick über die Digitalisierungsanteile und deren Herausforderungen, wie sie in der Praxis gesehen werden, gegeben.

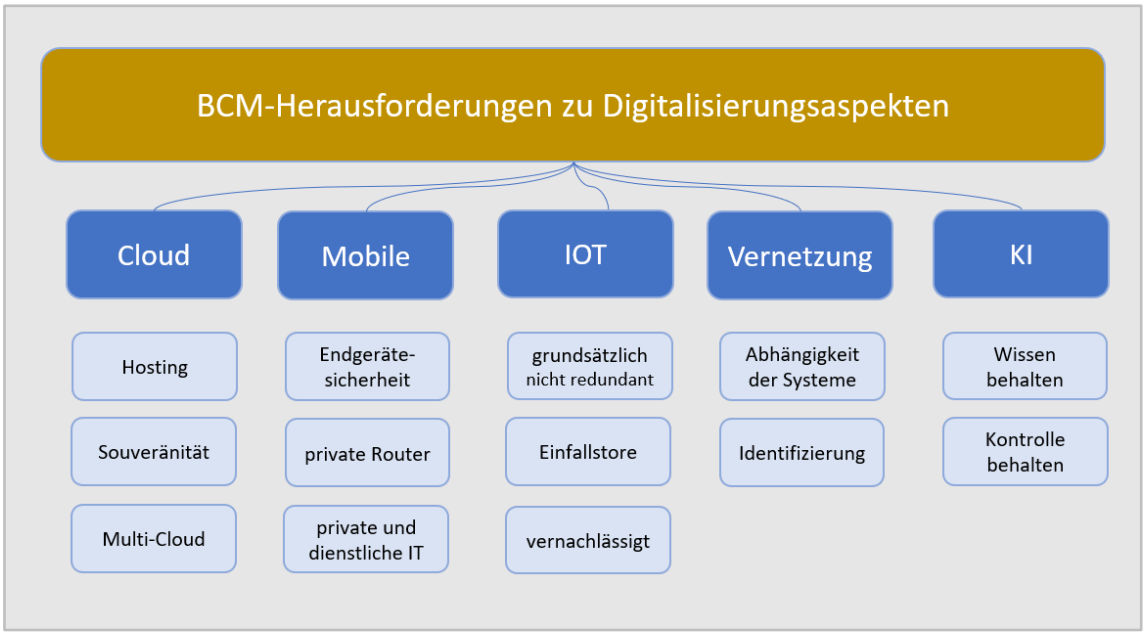


Abbildung 39 – Handlungsfelder zu Digitalisierungsaspekten aus Sicht der Experten (Quelle: eigene Darstellung)

Bis hierhin wurden die Ergebnisse dargestellt, die sich aus der Praxis ergeben haben und sich konkret auf die Nebenforschungsfragen beziehen und damit bei deren Beantwortung unterstützen können. Zusätzlich wurde erfragt, wo in der Praxis zukünftige Herausforderungen gesehen werden. Hierzu wurden die Teilnehmer zum Ende der Experteninterviews um einen Ausblick gebeten.

2.2.4 Darlegung des Ausblickes

Es wurde um einen begründeten Ausblick gebeten, ob sich mit der weiteren Digitalisierung nach Einschätzung der Experten das allgemeine Sicherheitsniveau eher verschlechtert oder sogar verbessert. Einer weiteren Erläuterung der Fragestellung bedurfte es in den Interviews nicht, da unmittelbar zuvor bereits die Themenfelder Sicherheit und Digitalisierung im Fokus waren. Für die weitere Interpretation der Ergebnisse insgesamt wurde erfragt, ob die Experten in diesem Kontext eher pessimistisch oder optimistisch in die Zukunft blicken. Dies sollte sowohl aus Sicht der Digitalisierung als auch konkret aus Sicht des Business Continuity Managements betrachtet werden. Interviewfrage 18 (IF18) wurde je nach Interviewverlauf grundsätzlich wie folgt gestellt: ‚Ist mit der Digitalisierung automatisch ein erhöhtes Sicherheitsniveau bei IT-Notfällen verbunden oder wo ist durch einen Kontrollverlust die

Sicherheit eher gefährdet?‘. Interessanterweise gab es hier ein divergierendes Meinungsbild. Im ersten Interview wurde die Frage noch nicht gestellt. Bei den weiteren Teilnehmern sahen fünf Experten die Möglichkeit für eine grundsätzliche Verbesserung, vier Teilnehmer stellten die Gefahren in den Vordergrund. Die anderen vier Teilnehmer sahen beide Möglichkeiten und argumentierten entsprechend. Von besonderer Bedeutung war neben der grundsätzlichen Tendenz hier die jeweilige Darlegung von Begründungen. In gekürzter Form sind die Aussagen in der Anlage VIII. 9 zusammengefasst in einer Tabelle aufgelistet.

Wie bereits erwähnt, waren die Prognosen der Experten nicht einheitlich. Es wurden sowohl positive Entwicklungen als auch negative Auswirkungen prognostiziert und erläutert. Experte_02 (2022, Anlage III. 2) sah eine konditionierte Verbesserung des allgemeinen Sicherheitsniveaus, wenn bei der Digitalisierung eine Risikobeurteilung korrekt berücksichtigt wird. Experte_03 (2022, Anlage III. 3) fokussierte einen weiterführenden und geopolitischen Lösungsansatz in Richtung einer Unabhängigkeit Europas, die er als Voraussetzung erachtete. Gleichzeitig kann dies auch als mögliche Verschlechterung interpretiert werden, wenn es nicht gelingt, sich von diesen Abhängigkeiten zu lösen. Experte 04 (2022, Anlage III. 4) nannte einen zusätzlichen Aufwand, der nötig ist, damit die Gefahren nicht größer werden. Auch Experte_05 (2022, Anlage III. 5) und Experte_06 (2022, Anlage III. 6) sprachen die Gefahren an und erkannten ein höheres Risiko. Im Gegensatz dazu meinte Experte_07 (2022, Anlage III. 7), dass im behördlichen Umfeld auch die IT-Sicherheit zukünftig zunehmen wird, und nahm damit eine eher positive Einstufung vor. Auch Experte_08 (2022, Anlage III. 8) bezeichnete die Digitalisierung als Chance für mehr Sicherheit, war sich der Gefahren aber auch bewusst. Gleichlautend positiv prognostizierte Experte_09 (2022, Anlage III. 9) die weitere Entwicklung, nannte allerdings eine politische Weichenstellung als Voraussetzung. Die ausdrückliche Möglichkeit, mit der Digitalisierung ein erhöhtes Sicherheitsniveau erhalten zu können, führte Experte_10 (2022, Anlage III. 10) an. Wiederum im Gegensatz dazu sah Experte_11 (2022, Anlage III. 11) die Zukunft kritisch und forderte konsequentes Mitdenken von Security und Resilienz, um nicht in fünf bis zehn Jahren vor beträchtlichen Problemen zu stehen. Experte_12 (2022, Anlage III. 12) betonte die Chance für eine erhöhte Sicherheit, diskutierte aber auch einen möglichen Kontrollverlust. Experte_13 (2022, Anlage III. 13) koppelte die Prognose an die bereits in den vorherigen Kapiteln beschriebene Awareness, die notwendig ist, damit keine Risiken eintreten. Abschließend äußerte sich Experte_14 (2022, Anlage III. 14) dahingehend, dass sich durch falsche Strategien, wie z. B. das Nutzen der amerikanischen Clouds für Behördendaten, die Unsicherheit definitiv erhöht. Er machte es aber auch von der

Geschwindigkeit abhängig und ging bei einer eher langsamen und gründlichen Umsetzung im Rahmen von deutschen Behördendaten davon aus, dass die Digitalisierung entsprechend sicher gestaltet werden kann.

Hierzu wurde eine Mindmap entwickelt, auf der die Experten kontextbezogen mit ihrer Meinung positioniert sind. Dabei wurde das Stimmungsbild in drei Bereiche eingeteilt. Neben der eher positiven Erwartungshaltung sind die Experten gruppiert, die von einem schlechteren Sicherheitsniveau ausgingen. Zudem ist ein Bereich angelegt, in dem die unentschlossenen Experten dargestellt sind.

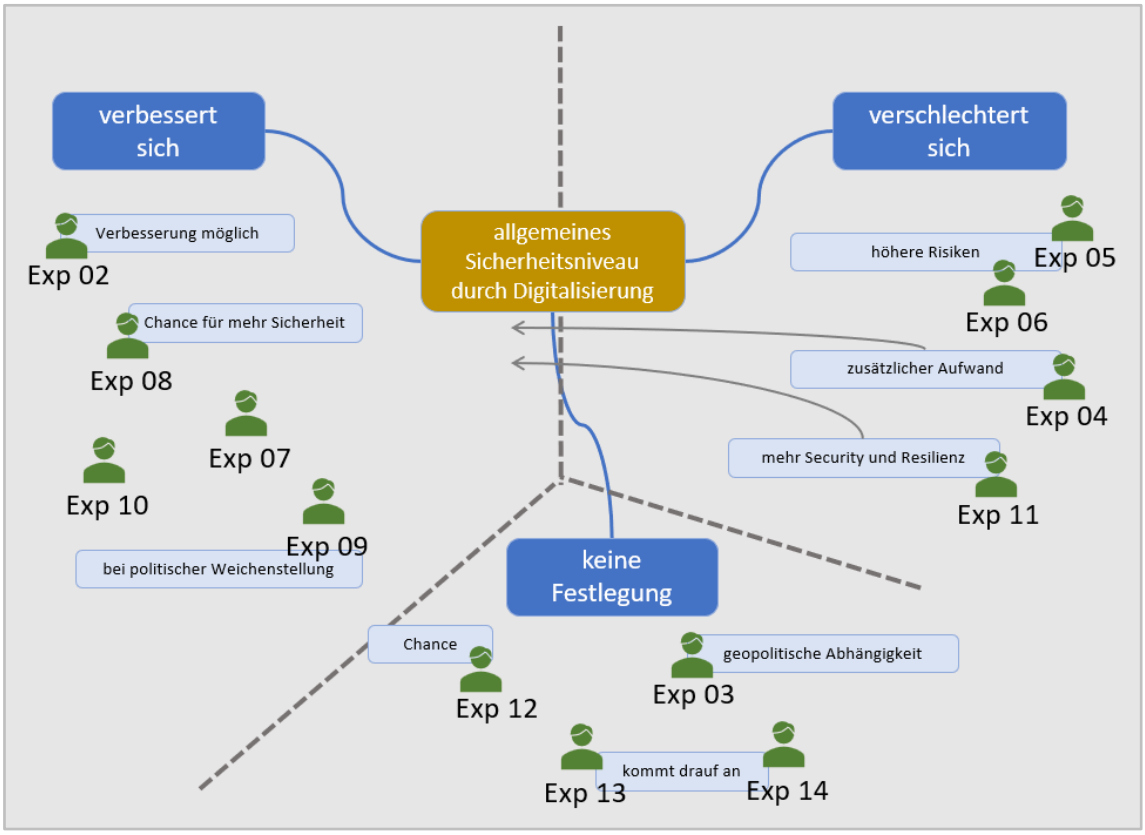


Abbildung 40 – Mindmap zur Prognose der Experten zum Sicherheitsniveau (Quelle: eigene Darstellung)

Mit den grauen Pfeilen sind Tendenzen der Experten gekennzeichnet, die zwar eher negativ prognostizierten, unter den genannten Bedingungen aber auch die Möglichkeit für eine Verbesserung sahen. Zur Verdeutlichung sind beispielhaft wörtliche Aussagen der Experten als Ankerbeispiele in die Abbildung aufgenommen.

Zusammenfassend zeigt sich ein heterogenes Meinungsbild dazu, ob sich das Sicherheitsniveau zukünftig verbessern wird. Zur Einordnung wurde mit der Bezeichnung ‚allgemeines Sicherheitsniveau' in den Interviews auch stets die Situation definiert, ob die Sicherheitsorganisationen in Deutschland durch die weitere Digitalisierung weiterhin einsatzfähig bleiben und ihre Aufgaben erfüllen können oder ob durch zunehmende IT-Ausfälle eine begründete Gefahr für die Einsatzbereitschaft zu erwarten ist. Nach den

ersten Meinungsäußerungen erfolgten in allen Fällen auch Begründungen und Relativierungen durch die Experten. Die Teilnehmer hatten grundsätzlich Meinungen und Argumente für beide Prognosen. Damit ist ersichtlich, dass die Experten auch die in der Problemstellung und der Ausgangslage beschriebenen Gefahren wahrnehmen. Somit ist unstrittig, dass auf Basis der Praxisberichte zum Business Continuity Management mit der weiteren Digitalisierung auch negative Auswirkungen auf die Sicherheit verbunden sein können. Zu diesem zentralen Punkt der Forschungsarbeit werden mit den abgeleiteten Handlungsempfehlungen Lösungswege als Erfolgsfaktoren vorgeschlagen.
Die weitere Diskussion und Interpretation dieser und aller zuvor dargelegten Ergebnisse folgen in Kapitel III 3. Zunächst wird erläutert, weshalb mit weiteren als den bis dahin durchgeführten Interviews keine neuen Erkenntnisse mehr zu erwarten waren.

2.2.5 Auswertung der Sättigungsanalyse

Anhand der in Kapitel III 1.3.7 beschriebenen Prinzipien wurde die Sättigung fortlaufend überprüft. Es wurden so lange weitere Interviews durchgeführt, bis die Analyse keine weiteren Einflussfaktoren mehr hervorbrachte. Die Datenerhebung wurde dann beendet und die Stichprobe mit den durchgeführten Interviews gilt als gesättigt (Hussy et al., 2013, S. 196). Danach wäre mit weiteren Interviews kein zusätzlich Erkenntnisgewinn mehr zu erwarten gewesen. Eine vollumfängliche Darstellung der Sättigungsanalyse auf Basis aller einzelnen Interviewfragen würde den Rahmen des Kapitels überschreiten, so dass sich die nachfolgende Auswertung auf die Ebene der Nebenforschungsfragen und den hierfür notwendigen Erkenntnisgewinn beschränkt. Damit werden auch die Antworten zur persönlichen Erfahrungszeit und zum persönlichen Sicherheitsempfinden von der Analyse, ob neue Erkenntnisse zu erwarten sind, ausgeschlossen.
Im Detail verlief die Analyse hierzu wie folgt. Beginnend ab April 2022 wurden bis Juni 2022 fünf Interviews durchgeführt und in einer Voranalyse ausgewertet. Nach der vorläufigen Datenauswertung ergab sich die Situation, dass sich bei den ersten Interviews bereits die Problemstellung mit den Berichten aus der Praxis nachvollziehen ließ. Die Bedeutung des Business Continuity Managements, passend zur Nebenforschungsfrage 1, wurde als sehr hoch und essenziell bezeichnet und begründet dargelegt. Je nach beruflichem Hintergrund des Experten wurde dies unterschiedlich begründet, aber es gab hier keine konträren Aussagen. Zu den relevanten Bereichen der Digitalisierung, die mit der Nebenforschungsfrage 2 zu bearbeiten waren, wurden noch unterschiedliche Themenfelder genannt. Einige

Themenbereiche, beispielsweise Big Data und künstliche Intelligenz waren noch nicht genannt. Auch für die Frage nach Standards und praxisorientierten Lösungsmöglichkeiten, deren Beantwortung das Ziel der Nebenforschungsfrage 3 ist, wurde mit weiteren Experten ein zusätzlicher Erkenntnisgewinn erwartet. Zusätzlich waren noch nicht alle geplanten Bereiche der Fokusgruppe vertreten, so dass der Eintritt der Sättigung auszuschließen war. Die Ergebnisanalyse wurde dann unterbrochen und es galt zunächst, weitere Interviews zu führen. Nach sieben Interviews wurde eine erneute Auswertung auf sich wiederholenden Aussagen und Empfehlungen vorgenommen. Als objektives Kriterium wurde geprüft, ob bei der qualitativen Auswertung des nächsten Interviews jeweils neue Codes induktiv anzulegen waren. Mit dieser Methode arbeiteten auch Guest et al. und es wurde festgestellt, dass in deren Experiment 73 % Vollständigkeit nach sechs Interviews und 92 % Vollständigkeit nach zwölf Interviews erreicht wurden (Guest et. al, 2006, S. 66). Auf diesen theoretischen Grundlagen basierend sollten hier in jedem Fall mehr als zwölf Interviews abgehalten werden. Nach Durchführung und Analyse der bereits genannten weiteren sieben Interviews im Zeitraum bis August 2022 wiederholten sich die genannten Aspekte und Empfehlungen, wie nachfolgend mit Beispielen belegt. Alle vorgesehenen Bereiche der Fokusgruppe waren jetzt involviert. Es haben Experten von kleinen, mittleren und großen Unternehmen an den Interviews teilgenommen. Sowohl Produktanbieter für sichere Digitalisierungslösungen als auch IT-Dienstleister und Beratungsunternehmen zur Digitalisierung mit Erfahrung bei öffentlichen Auftraggebern waren involviert. Hierbei ist anzumerken, dass die Unternehmensgröße kein entscheidendes Kriterium war, sondern die Experten mit ihrer langjährigen Erfahrung, auch bei vorherigen Arbeitgebern, im Vordergrund standen. Es wurde ein längerer Zeitraum für die Analyse und die Codierung dieser sieben Interviews eingeplant.

In den ersten Fragen wurden ergebnisoffen die Aspekte des Business Continuity Managements und der Digitalisierung erfragt und es wurde um Auskünfte zu positiven oder negativen Erfahrungen gebeten. Bei den positiven Erfahrungen wiederholten sich schnell die Reflexionen des Business Continuity Managements in Verbindung mit der Digitalisierung am Beispiel der Coronapandemie. Hier wurde wiederholend dargestellt, dass und wie ein Unternehmen oder eine Behörde schnell arbeitsunfähig wurde, wenn die Mitarbeiter nicht wie gewohnt in die Arbeitsstätte kommen konnten, um dort mit Ihrer IT-Ausstattung und IT-Anbindung zu arbeiten.

Bei der Situation und der Berücksichtigung des Business Continuity Managements gab es wiederkehrende Aussagen, dass der Thematik zwar eine hohe Bedeutung zugemessen wird,

dass diese aber in der Praxis noch zu wenig Berücksichtigung erfährt. Zur Digitalisierung und zu deren relevanten Aspekten wurden, je nach Experte und beruflichem Hintergrund, grundsätzlich unterschiedliche Punkte genannt, die sich im Gesprächsverlauf und bei der späteren Analyse zu bereits angelegten Kategorien zuordnen ließen. Zur allgemeinen weiteren Automatisierung von Geschäftsprozessen, zur zunehmenden Vernetzung, zum Cloud-Computing und zu den anderen Anteile der Digitalisierung wurden jeweils von mehreren Experten argumentativ Aussagen getroffen, die bei den letzten Interviews keinen substanziell neuen Erkenntnisgewinn erzeugten. Im Bereich Standards, Normen, Vorgaben und Gesetze gab es unterschiedliche Erfahrungen und Berührungspunkte bei den Experten. Hier war es von Bedeutung, so lange Interviews zu führen, bis zu allen Themenbereichen ausreichendes Material für die Analyse zur Verfügung stand.

Nach den zwölf Interviews ergab sich, dass sowohl alle erwarteten Aspekte angesprochen waren als auch dass sich die Erfahrungen, Hinweise, Empfehlungen und Argumentationen wiederholten. Es wurde somit bereits von einer Sättigung ausgegangen, die in zwei weiteren Interviews bestätigt werden sollte.

Durch die Codierungen in MAXQDA und die Abbildung der aus den ersten Interviews induktiv erzeugten Kategorien erfolgte die Analyse der zwei im November 2022 durchgeführten Interviews. Im Ergebnis haben diese, abgesehen von persönlichen oder firmenspezifischen Neuerungen, lediglich die vorhandenen Kategorien bestätigt oder in Nuancen ergänzt, aber keine neuen Erkenntnisse geliefert. Damit ist, wie eingangs dargestellt, von der theoretischen Sättigung auszugehen. Quantitativ entspricht diese Anzahl der durchgeführten Interviews auch dem nach Döring genannten Umfang von 10 bis 20 zu involvierenden Personen bei Leitfadeninterviews (2023, S. 369). Mit dem Datenmaterial dieser insgesamt 14 Interviews wurden ab November 2022 die detaillierte Analyse, Aufbereitung und Darlegung der Ergebnisse durchgeführt, wie es ausführlich in den vorherigen Kapiteln beschrieben ist. Insgesamt wurde damit eine Gruppe von Experten interviewt, die sich dadurch auszeichnet, dass die Teilnehmer jahrelange Erfahrungen im Business Continuity Management haben und diese Thematiken auch schon im behördlichen Umfeld angebracht haben.

Vor einer Ableitung von Handlungsempfehlungen wurden die Resultate dahingehend evaluiert, inwiefern sie sachgerecht im Bereich der erwarteten Ergebnisse liegen.

2.2.6 Evaluation dieser Ergebnisse

Im Ergebnis des empirischen Teils haben sich Handlungsempfehlungen zum Bereich Personal und Personalmanagement und zum Vorgehen sowie Hinweise zu bestimmten technologischen Anteilen der Digitalisierung ergeben. Anhand der Literatur wurde verglichen, ob diese Handlungsfelder sachgerecht zur Problemstellung passen und hinsichtlich der Grundlagen aus der Theorie stimmig sind. Schmid wurde schon zitiert, der von einem fehlenden konzeptionellen Grundverständnis für die Digitalisierung im Zusammenhang mit E-Government spricht (2019, S. 8). Dazu passen die Hinweise und Erkenntnisse aus dem empirischen Teil, die ein digitales Mindset fordern und den Menschen sowie die Ausbildung an erster Stelle der Empfehlungen anführen.

Das Vorgehen wurde ebenfalls in der Literatur bereits entsprechend diskutiert. So berichten Hoberg et al., dass zwei Drittel der Unternehmen einer weltweiten Umfrage keine klare Transformationsstrategie besitzen (2018, S. 71-72). Zahlreiche Hinweise und Empfehlungen der Interviewpartner fokussierten diesen Aspekt, womit auch dieser Anteil in einem erwarteten Bereich liegt. Die einzelnen Hinweise zu den Digitalisierungstechnologien, wie dem Cloud-Computing, reicherten die ebenfalls bereits aus der Theorie abgeleiteten Faktoren zielführend an. Schon Faber (2019, S. 20) diskutiert den möglichen Kontrollverlust und mehrere Experten haben dazu passend in den Interviews ihre Sichtweisen und Empfehlungen aus der Praxis dargelegt.

Damit ergibt sich, dass die Resultate im Bereich der grundsätzlich erwarteten Ergebnisse liegen, wie sie aus der Theorie erschlossen wurden. Die herausgearbeiteten Ergebnisse passen mittelbar und teilweise unmittelbar zu den Forschungsfragen, womit eine korrekte Wahl der Methodik verdeutlicht wird. Gleichzeitig wird die Eignung des Fragebogens für den Forschungszweck bestätigt, da die Auskünfte der Experten sich auf die aus der Theorie erwartbaren offenen Handlungsfelder fokussierten. Im Detail und durch die Berücksichtigung der praxisbezogenen Ausführungen sind die erhobenen Informationen neu und bilden die Grundlage zur Erarbeitung von Handlungsempfehlungen. Damit lässt sich für die Evaluation feststellen, dass die Ergebnisse in einem Bereich liegen, in dem sie plausibel zur Beantwortung der Forschungsfragen genutzt werden können. Der Weg zu erfolgversprechenden Handlungsempfehlungen ist im nächsten Kapitel mit der Interpretation und der Diskussion der Ergebnisse beschrieben.

3 Diskussion, Interpretation und Konklusion

In diesem Kapitel werden die soeben dargelegten Ergebnisse der Empirie unter Berücksichtigung der theoretischen Grundlagen weiter diskutiert. Die von den Experten getätigten Äußerungen aus der Praxis werden in Bezug auf die Problemstellung im Business Continuity Management interpretiert. Dabei werden die wesentlichen Handlungsfelder herausgearbeitet und die Vorschläge aufgenommen, verglichen und verifiziert.

Zur Einleitung in dieses Kapitel wurde das Zielbild der Forschungsarbeit auf Basis der Prognosen der Experten reflektiert. Mit dem Vorliegen der empirischen Ergebnisse konkretisiert sich die Zielstellung dahingehend, dass nicht nur die Problemstellung bestätigt wurde, sondern auch die Prognosen der Experten den Handlungsbedarf weiter geschärft haben. Die Abbildung aus Kapitel III 2.2.4 „Darlegung des Ausblicks“ wurde um die Ziele ergänzt, die durch Umsetzung der Ergebnisse dieser Arbeit erreicht werden sollen. Eine vollständig sichere Digitalisierung ohne negative Auswirkungen in IT-Notfällen bleibt utopisch, aber die erstellten Handlungsempfehlungen und Erkenntnisse für Forschung und Praxis können bei der weiteren Digitalisierung unterstützen.

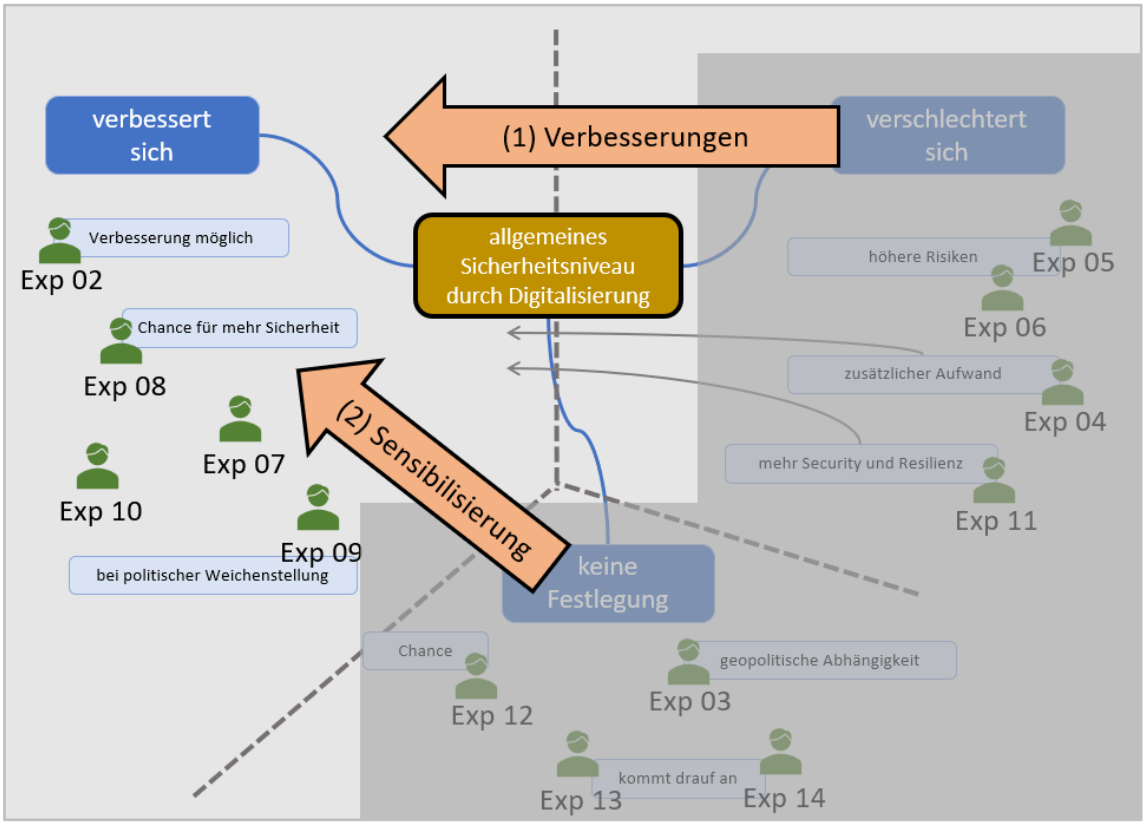


Abbildung 41 – Aktualisiertes Zielbild (Quelle: eigene Darstellung)

Insgesamt bleibt es das Ziel, dass sich durch die Digitalisierung keine weiteren Gefahren ergeben, die Staat und Gesellschaft vor neue und große Probleme stellen werden. Das allgemeine Sicherheitsniveau soll durch die Einsatzbereitschaft von Behörden, Sicherheitsorgangen und auch der Wirtschaft weiterhin gegeben sein. Hierzu sind Verbesserungen in den Bereichen notwendig, in denen die Experten begründete Argumente genannt haben, wonach sie mit einer Verschlechterung des allgemeinen Sicherheitsniveaus rechnen, wenn die Digitalisierung weiter voranschreitet. Experten, die sich in den Interviews dazu noch nicht festlegen wollten, stehen damit auch stellvertretend für IT-Fachkräfte und Manager, die sich ebenfalls noch nicht mit der Situation auseinandergesetzt haben. Hier soll mit einer Sensibilisierung für die Problemstellung und deren Lösungsmöglichkeiten erreicht werden, dass die notwendige Aufmerksamkeit für ein effektives Business Continuity Management zukünftig frühzeitig erbracht wird.
Orientiert an dem aktualisierten Zielbild erfolgen ab dem nächsten Kapitel III 3.1 die Diskussion und die Interpretation der Ergebnisse.

3.1 Diskussion und Interpretation der Ergebnisse

Die Diskussion erfolgt zunächst orientiert an den Hauptthematiken ‚Business Continuity Management' und ‚Digitalisierung'. Von besonderer Bedeutung ist die Interpretation der Empfehlungen in Verbindung mit den dargelegten Hinweisen und Fakten aus der Theorie. Ergänzend wird dann in Kapitel III 3.1.4 die Problemstellung explizit in Bezug zu den erarbeiteten Ergebnissen gesetzt. Am Ende des Kapitels werden die Forschungsfragen beantwortet, so dass die Voraussetzungen für den Gestaltungsteil gegeben sind.
Hervorzuheben sind bereits zwei Analyseergebnisse, die so vorher nicht in dieser Deutlichkeit erwartbar waren und die einen maßgeblichen Einfluss auf die weitere Interpretation und Gestaltung haben. Zunächst wurde übereinstimmend berichtet, dass ein Business Continuity Management im Kontext der Digitalisierung überhaupt nicht, noch nicht oder zumindest nicht im erforderlichen Maße zur Anwendung kommt. Zweitens und im direkten Zusammenhang mit dem ersten Punkt wurden bei den Empfehlungen in allen Fällen zuerst das noch notwendige ‚Mindset', die notwendige Awareness und das Verständnis in den Vordergrund gerückt. Auf Basis der Theorierecherche und der Hinweise aus der Literatur, der Gesetzestexte, der ISO-Normen und etablierten Standards konnte angenommen werden, dass dieses Grundverständnis für ein Business Continuity Managements auch in der Praxis und

insbesondere bei Digitalisierungsprojekten gegeben ist. Mit dieser Situation werden die Phänomene aus der Problemstellung erklärbar und die zentralen Handlungsempfehlungen können darauf aufbauend zielorientiert verfasst werden. Es folgt die Interpretation der Ergebnisse nach den einzelnen Themengebieten.

3.1.1 Die Situation des Business Continuity Managements

Als lebenswichtig für zahlreiche Unternehmen bezeichnet Königs das Business Continuity und empfiehlt, es in die strategische Zielsetzung von Unternehmen einzubinden (2017, S. 308). Aus der Perspektive der behördenerfahrenen IT-Dienstleister wird dem Business Continuity Management ebenfalls eine solch hohe Bedeutung eingeräumt. Die Experten sprechen von einem unternehmenskritischen, überlebenswichtigen und essenziellen Stellenwert, der dem Business Continuity Management beizumessen ist. Bemerkenswert und zu Beginn des Forschungsprojektes noch nicht zu erwarten war die Situation, dass mehrere Experten aktuell eine steigende Bedeutung des Business Continuity Managements in der Praxis sehen. Eine höhere Relevanz aufgrund der fortschreitenden Digitalisierung war bereits im Rahmen der theoretischen Grundlagen absehbar, allerdings wurden in den Interviews neben der Covid-Pandemie auch aktuelle Naturkatastrophen und die Ukrainekrise genannt, wodurch die Eintrittswahrscheinlichkeit von IT-Notfällen allgemein als höher angenommen werden könnte. Gezielte Angriffe von Aggressoren auf kritische Infrastruktur in Deutschland waren vor 2022 kein viel diskutiertes Risiko. Im Rahmen der ab April 2022 durchgeführten Interviews sahen mehrere Experten den Schutz der IT-Komponenten in der Wirtschaft, bei kritischen Infrastrukturen und bei Behörden mit als wesentliche Aufgabe des Business Continuity Managements und sagten vor dem genannten Hintergrund eine steigende Bedeutung vorher. Der aus der Theorie bekannte Stellenwert wurde seitens der BCM-Experten insgesamt bestätigt, wonach zusammenfassend in dieser Studie dem Business Continuity Management eine sehr hohe und elementare Bedeutung zugemessen wurde.

Dass das Business Continuity Management aktuell ausreichend berücksichtigt wird, wurde von keinem Experten bestätigt. Vielmehr wurde in allen Fällen ein Handlungsbedarf aufgezeigt und diskutiert. Hier waren vor allem die Argumente der Experten für die weitere wissenschaftliche Analyse aufschlussreich. Technologieaspekte wurden dabei weniger genannt. Stattdessen wurden vorrangig die Bereiche Personal und das sogenannte notwendige ‚Mindset' thematisiert.

Ein solches „digitales Mindset im Veränderungsprozess“ (Hasenbein, 2020, S. 28) wurde auch schon in der Literatur beschrieben. Aus wirtschaftspsychologischer Sicht ist damit die Forderung nach einer kulturellen Veränderung in Organisationen gemeint und es geht um das Verständnis für digitale Zusammenhänge (Hasenbein, 2020, S. 28). Für das Business Continuity Management im Zeitalter der Digitalisierung ergibt sich damit als Haupterfolgsfaktor für eine Etablierung und Verbesserung, dass zunächst die Awareness und das Verständnis dafür zu fördern sind. Die konkreten Empfehlungen werden in Kapitel III 3.1.3 detaillierter diskutiert. Mit den Aussagen der Experten bedeutet dies im Ergebnis, dass vor etwaigen technischen Lösungen der Problematik noch kulturelle Veränderungen erforderlich sind und nicht die technischen Lösungsmöglichkeiten im Vordergrund stehen. Im Bezug zur Problemstellung kann damit interessanterweise geschlussfolgert werden, dass die real eingetretenen Schadensereignisse der Ausgangslage ursächlich nicht auf technische Unzulänglichkeiten zurückzuführen sind. Sie wären im Vorhinein durch eine ausreichende Awareness und ein Ergreifen von Gegenmaßnahmen vermeidbar gewesen.

Diese Awareness bedarf eines Grundverständnisses für die digitale Transformation und wurde in der Literatur und im empirischen Teil dieser Arbeit als ‚digitales Mindset‘ bezeichnet. Zusammenfassend kann festgehalten werden, dass zwar ein Bewusstsein für die Notwendigkeit eines Business Continuity Managements besteht, dass aber durch fehlendes Verständnis, auch bezüglich der digitalen Transformation, derzeit noch keine ausreichenden Maßnahmen ergriffen werden. Dabei sind die technologischen Aspekte, die im nächsten Kapitel betrachtet werden, nicht der bestimmende Faktor.

Die Übertragbarkeit der BCM-Studie von Sawalha aus dem Jahr 2020 ist nur bedingt möglich. In Jordanien existiert ein höheres Bewusstsein für die Thematik (Sawalha, 2020, S. 88-89), als es für deutsche Behörden aus Sicht der Experten in der vorliegenden Arbeit ermittelt wurde. Übereinstimmend kann jedoch auch für Deutschland festgehalten werden, dass noch ein Defizit im Wissen besteht, wie sich ein Business Continuity Management effektiv implementieren lässt (Sawalha, 2020, S. 83). Ebenfalls bestand Übereinstimmung darin, dass ISO-Zertifizierungen ein Treiber oder ein Initiator sein können. Damit sind diese beiden Punkte bei der Herausarbeitung der Erfolgsfaktoren zu berücksichtigen. Im internationalen Vergleich gilt es für Deutschland allerdings, an erster Stelle die Sensibilität für das Business Continuity Management insgesamt weiter zu steigern. Als Handlungsfelder konnten notwendige Aktivitäten hierzu in den Ebenen Personal, Technologie und Vorgehen, wie in der Abbildung 35 auf Seite 143 dargestellt, herausgearbeitet werden. Die dort genannten Stichworte werden

im Gestaltungsteil aufgenommen, um auf deren Basis das Business Continuity Management besser etablieren zu können.

3.1.2 Relevante Aspekte der Digitalisierung

Die Digitalisierung hat zahlreiche Facetten. Es ist davon auszugehen, dass alle Bereiche eines Unternehmens davon betroffen sind und mit der digitalen Transformation eine hohe Komplexität verbunden ist (Hess et al., 2016, S. 124). Von den Experten erfolgte zur Digitalisierung eine Beschreibung der weiter zu erwartenden Automatisierung der Tätigkeiten und behördlichen Vorgänge. Diese Betrachtung war zwar durch die Auswahl der Experten und der Zielrichtung des Forschungsthemas beabsichtigt, um fokussierte Empfehlungen erarbeiten zu können, dennoch wurden Beispiele aus diversen Lebensbereichen und der beruflichen Praxis angeführt. Viele dieser zusätzlich genannten Aspekte der Digitalisierung müssen im vorliegenden Rahmen nicht weiter interpretiert werden, wenn sie nicht zum Erkenntnisgewinn bezüglich der Problemstellung beitragen. Es wird auf die Automatisierung und die Digitalisierung von Geschäftsprozessen fokussiert. Hierzu erfolgen sowohl eine prozessuale Betrachtung dieses Aspektes als auch eine Diskussion der Sicht des Managements. Bei diesem wesentlichen Punkt der Digitalisierung, der weiteren Automatisierung von Geschäftsprozessen, gibt es in der Verwaltungspraxis aber auch schon Fortschritte. Bizer berichtete schon 2019 von ausgewählten Verwaltungsprozessen in einigen Bundesländern, die bereits „soweit wie möglich“ automatisiert sind und teilweise vollautomatisch ablaufen (2019, S. 120). Der Autor weist auf die Relevanz der digitalen Souveränität hin und darauf, dass bei der dynamischen Digitalisierung der Staat stets die Hoheit über die Daten behalten muss (Bizer, 2019, S. 124). Für die Speicherung von Daten wurde bei der Ergebnisdarstellung aus der Praxis hervorgehoben, dass der Cloud-Technologie eine Schlüsselrolle zukommt, um die Digitalisierung weiter voranzubringen. Es wurde der Aspekt der Sicherheit und der IT-Sicherheit thematisiert, womit einer sicheren und ausfallsicheren Cloud-Lösung die entscheidende Bedeutung zukommt. Gleichzeitig muss die Datensouveränität erhalten bleiben.

Es wurde die Empfehlung herausgearbeitet, aus Sicht des Business Continuity Managements zunächst die unternehmenskritischen Geschäftsprozesse zu priorisieren und damit die Betrachtung der auszuwählenden Digitalisierungsanteile zu beschränken. Behörden oder Unternehmen, die vorrangig auf Kommunikationsservices angewiesen sind oder diese anbieten, haben dann auch anfangs mehr in redundante Auslegungen von Mobility-Services,

Vernetzungen und Endgerätesicherheit zu investieren. Für IOT werden noch Herausforderungen gesehen, da diese oft nicht ausfallsicher ausgebracht werden. Hier kann eine Verbesserung einfach durch redundante Komponenten und Sensorik erzielt werden. Für den Bereich der KI ist die weitere Entwicklung vielfach noch nicht absehbar. Als Herausforderung wurde hier die Problematik hervorgehoben, inwiefern der Mensch noch die Kontrolle behalten kann. In der gemeinsamen Betrachtung mit der noch fehlenden Awareness für ein Business Continuity Management und einem unzureichenden Verständnis für die digitale Transformation werden hier große Herausforderungen gesehen. Bezogen auf den Aufbau und den Betrieb von KI wird auf die Annahmen und Empfehlungen zum Bereich Hosting, Cloud-Computing und Vorgehen verwiesen, da diese in gleichem Maße für den Betrieb der KI-relevanten IT-Komponenten notwendig sind. Eine fachliche Auseinandersetzung mit KI und Business Continuity Management wird im Forschungsausblick vorgeschlagen.

Zusammen mit dem Aspekt Big Data als große Herausforderung für das Business Continuity Management lassen sich als relevante Punkte der Betrieb der IT in einer sicheren Backend-Infrastruktur, ausfallsichere zentrale und dislozierte Komponenten und die Sicherstellung von geeigneten Zugangsmöglichkeiten zu den Services festhalten. Als kurze Reflexion zur Problemstellung kann konstatiert werden, dass die in der Ausgangslage geschilderten Fälle aus rein technischer Sicht einfach vermeidbar gewesen wären. Das verstärkt das Gesamtergebnis dieser Arbeit, dass die im nächsten Kapitel dargestellten Empfehlungen von deutlich höherer Bedeutung für eine sichere Digitalisierung sind als die singuläre Betrachtung der technischen Aspekte.

3.1.3 Interpretation der Empfehlungen

Die dargelegten Empfehlungen konzentrieren sich auf die Bereiche Personal, Vorgehen und Technologie. Wie bereits zu den technologischen Aspekten ausgeführt, wären die in der Problemstellung geschilderten Phänomene vermeidbar gewesen. Mit dem notwendigen Verständnis und einer Sensibilisierung beginnend ab der Managementebene kann mit einem geeigneten Vorgehen die Digitalisierung sicherer gestaltet werden. Interessant dabei ist, wie sich die digitale Transformation zukünftig entwickeln wird und welche Empfehlungen bereits in der Literatur existieren. Dazu wurden für die nun folgende Diskussion zwei Veröffentlichungen analysiert. Diese betrachten nur einzelne Teile der Themenstellung und bieten damit noch keine Antworten auf die hier definierte Forschungslücke.

Die von Stember und Hasenkamp 2019 (S. 48) veröffentlichte Abbildung zeigt Herausforderungen, die auch in der hier durchgeführten empirischen Untersuchung bestätigt wurden. Die dort als Government to Customer (G2C), Government to Government (G2G) und Government to Business (G2B) dargestellten Beziehungen wurden von den BCM-Experten diskutiert und alle dort genannten Handlungsfelder – Ressourcen, Komplexität, mangelnde Kooperation, externe Akzeptanz, Qualifikation von Personal, interne Akzeptanz und rechtliche Regelungen – wurden nach der qualitativen Auswertung der Interviews als relevante Handlungsfelder mit Begründungen und Lösungsvorschlägen herausgearbeitet.

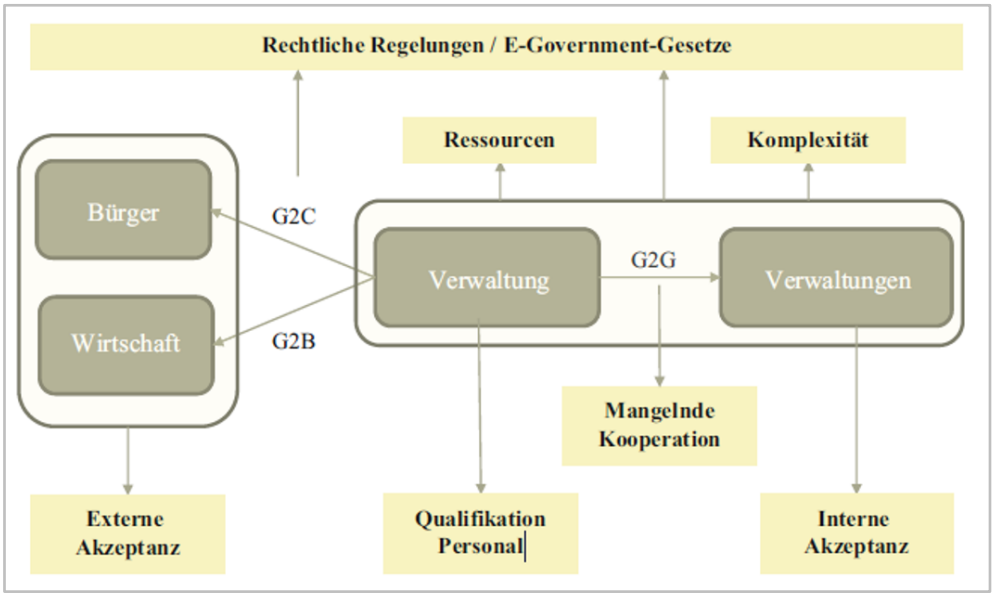


Abbildung 42 – „Empirisch belegte Herausforderungen beim E-Government“ (Quelle: Stemper & Hasenkamp, 2019, S.48)

Insgesamt bemerkenswert ist, dass hier keine technischen Aspekte genannt sind. Die Digitalisierung am Beispiel E-Government ist nach dieser Studie im Wesentlichen von den dort genannten Herausforderungen abhängig. Trotz des Hinweises auf die Komplexität fehlen aus hiesiger Sicht die Herausforderungen der IT-Sicherheit allgemein und des Business Continuity Managements explizit. Solange es nicht als Herausforderung angesehen und entsprechend bearbeitet wird, wird es auch zukünftig zu den Situationen aus der Problemstellung kommen. Passend zu der Darstellung und den Ergebnissen aus der Empirie werden als Erfolgsfaktoren auch die in dieser Abbildung genannten Herausforderungen berücksichtigen.

In der Betrachtung des Business Continuity Managements steht nicht das E-Government im Vordergrund, sondern grundsätzlich müssen alle Facetten der Digitalisierung bedacht werden. Dazu wurde die weitere Veröffentlichung von Saarikko et. al. aus dem Jahr 2020 gesichtet, die Empfehlungen für die Digitalisierung erarbeitet hat. An dieser Studie nahmen unter anderem Connectivity- und Cloud-Anbieter teil und die Entwicklungen im IOT-Bereich wurden

fokussiert. Im Ergebnis wurden fünf Aussagen erarbeitet, um ein digitales Bewusstsein zu entwickeln. Diese Empfehlungen sind in der nachfolgernden Abbildung rechts aufgeführt.

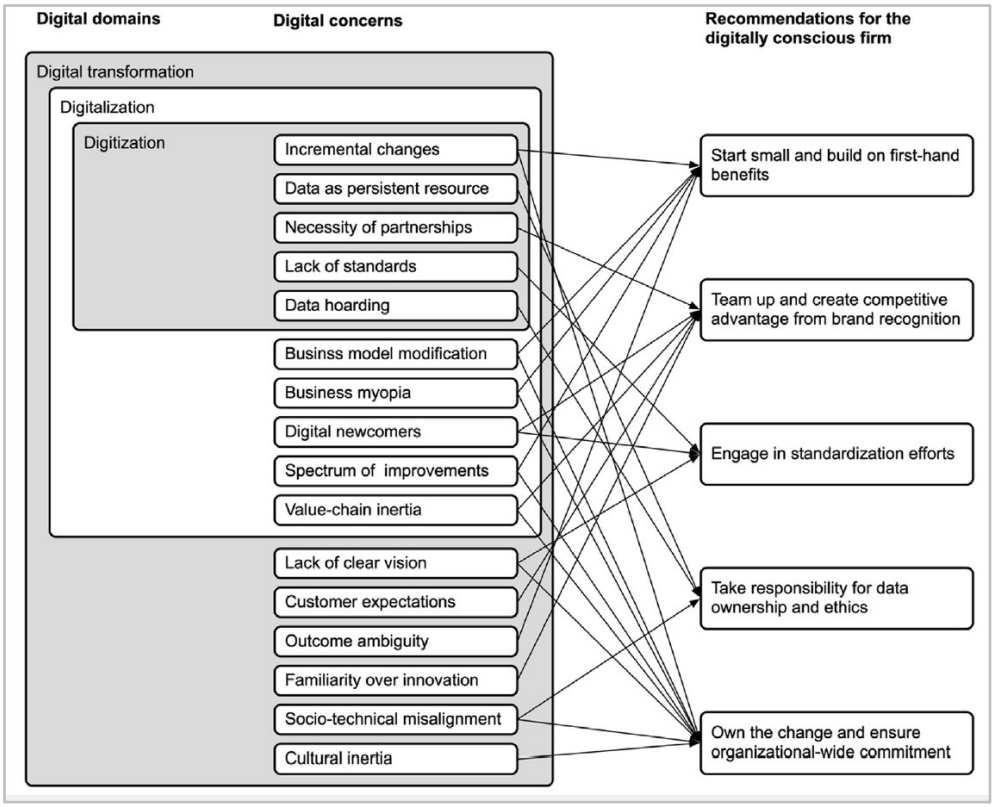


Abbildung 43 – „Digital domains and becoming digitally conscious“ (Quelle: Saarikko et al., 2020, S. 837)

Einige aus dem Bereich der BCM-Experten herausgearbeiteten Hinweise können hier direkt zu Empfehlungen dieser Studie zugeordnet werden und sind damit auch aus dieser Perspektive betrachtet. Der Hinweis, dass zunächst mit kleinen Schritten begonnen werden soll, ist in beiden Untersuchungen identisch. Der zweite Punkt kann mit Blick auf das GAIA-X-Projekt ebenfalls als vorteilhaft für das Business Continuity Management angenommen werden. Übereinstimmungen sind auch bei der Thematik der Standardisierung zu sehen, wobei im Business Continuity Management mit den vorgestellten Standards und Normen kein wesentliches Defizit vorhanden ist. Die Empfehlung für ein Engagement zur weiteren Standardisierung kann aber grundsätzlich übernommen werden und ergänzt damit die Aussagen der BCM-Experten. Eine deutliche Übereinstimmung ist im Bereich der letzten beiden Empfehlungen zu sehen. Der vierte von fünf Punkten kann mit der von den BCM-Experten geforderten und diskutierten Datensouveränität in Übereinstimmung gebracht werden und verstärkt damit die Handlungsempfehlung aus der Praxis mit den Hinweisen aus der Literatur. Bemerkenswert ist, dass mit dem letzten Punkt deutlich wird, wie bei dieser Fokusgruppe der Faktor Mensch, das Verständnis der Digitalisierung und der Umgang damit ebenfalls ein wesentliches Handlungsfeld darstellt.

Von den Experten wurde die Souveränität angesprochen und gefordert, wie bereits in der Ergebnisdarstellung andiskutiert. Passend dazu haben Lepping und Palzkill (2017, S. 25) die Situation mit Bezug zum Digitalisierungsgrad skizziert.

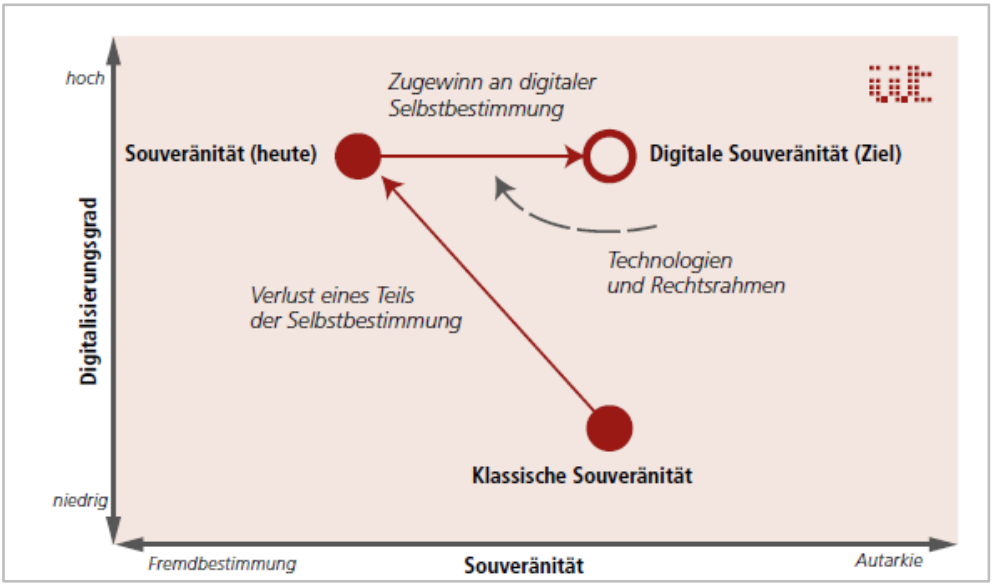


Abbildung 44 – Souveränität und Digitalisierungsgrad (Quelle: Lepping und Palzkill, 2017, S. 25)

Als Ziel ist hier die digitale Souveränität bezeichnet, die bei steigendem Digitalisierungsgrad abnimmt, so dass sich eine Entwicklung von einer Autarkie hin zu einer Fremdbestimmung vollziehen kann. Durch Technologien und Rechtsrahmen kann ein Zugewinn an digitaler Selbstbestimmung erreicht werden. Die hier dargestellte Situation wurde auch in der Praxis als Herausforderung eingestuft und die digitale Souveränität aus Sicht des Business Continuity Managements gefordert.

Zusammenfassend zeigt sich, dass die Empfehlungen auf Basis der Praxiserfahrungen und der theoretischen Grundlagen in anderen Studien einerseits ähnlich formuliert wurden. Andrerseits ist kritisch anzumerken, dass die hier zusätzlich herausgearbeitete essenzielle Bedeutung eines Business Continuity Managements bei der weiteren Digitalisierung in vergleichbaren Studien nicht eindeutig angesprochen wird.

3.1.4 Bezug zur Problemstellung

In diesem Kapitel werden die Problemstellung allgemein und die beiden Beispiele aus der Ausgangslage zu den Ergebnissen reflektiert. Das Problem, wenn ein nicht ausreichend ausgeprägtes Business Continuity Management in Unternehmen oder Behörden auf eine immer schneller voranschreitende Digitalisierung trifft, wurde mit den Ergebnissen zur Situationsdarstellung verdeutlicht. Solange die notwendige Aufmerksamkeit noch nicht

vorhanden ist, werden die Herausforderungen nicht proaktiv untersucht und es werden keine vorbereitenden Maßnahmen ergriffen. Für das Beispiel des Großbrandes in einem Rechenzentrum zeigen die Ergebnisse eindeutig den Handlungsbedarf auf, der vor der Nutzung dieser Cloud-Services hätte geklärt werden müssen. Dazu zählen die Datensouveränität, ein ausfallsicherer Betrieb und das Ergreifen von Maßnahmen für die Worst-Case-Szenarien. Mit der Nutzung von externen IT-Services oder dem Umzug ganzer IT-Landschaften zu externen Anbietern ist nicht automatisch ein ausreichend sicherer Betrieb aus Sicht des Business Continuity Managements verbunden. Offensichtlich war sich das Management der betroffenen Unternehmen und Behörden dieser Herausforderung nicht in ausreichendem Maße bewusst, so dass es im Ergebnis zu Datenverlusten und großen Betriebseinschränkungen kam. Technische Lösungen, wie ein georedundanter Betrieb, das automatische Erstellen und Rückladen von Backups aller Systeme und Daten an anderen Standorten, sind hier nicht das Problem. Der Rechenzentrumsanbieter hat diese sogar explizit offeriert, sie wurden allerdings in vielen Fällen nicht genutzt. Hiermit wird die aktuell noch notwendige weitere Sensibilisierung deutlich.

Zu erheblichen Einschränkungen kam es auch im zweiten Beispiel der Ausgangslage, in dem sogar der IT-Katastrophenfall in Deutschland erstmals für einen Landkreis ausgerufen wurde. Hier fehlte es an redundanten Lösungen, die ein aus Sicht des Business Continuity Managements erwartbares Schadensgroßereignis in Form eines Verschlüsselungstrojaners entsprechend absichern. Auch hier stellt die dafür notwendige IT nicht das Problem dar. Es ist davon auszugehen, dass mit geeigneten Offline-Archiven und Backups eine solche Herausforderung vergleichsweise schnell gelöst werden kann. Es fehlte an einer frühzeitigen Berücksichtigung und daher am digitalen Verständnis für derartige Angriffsszenarien. Daraus ergibt sich, dass die Handlungsempfehlungen in einer entsprechenden Reihenfolge und Priorisierung verfasst werden müssen, um damit zukünftige Digitalisierungsprojekte möglichst ausfallsicher gestalten zu können.

Auf Basis der Ergebnisdarstellung, der Interpretation und Diskussion werden im folgenden Kapitel die Forschungsfragen beantwortet, womit dann nachvollziehbare Grundlagen zur Formulierung der konkreten Handlungsempfehlungen als Erfolgsfaktoren zur Verfügung stehen.

3.1.5 Beantwortung der Forschungsfragen

Mit den Informationen aus der Theorierecherche und dem Erkenntnisgewinn aus der analysierten empirischen Datenerhebung können die Forschungsfragen beantwortet werden. Hierzu wurden zunächst die Nebenforschungsfragen einzeln betrachtet, um anschließend damit die Hauptforschungsfrage zu beantworten.

3.1.5.1 Beantwortung der Nebenforschungsfragen

Mit der ersten Nebenforschungsfrage wurde die aktuelle Situation des Business Continuity Managements untersucht und in einem direkten Zusammenhang mit der fortschreitenden Digitalisierung betrachtet. Es galt herauszufinden, wie die Annahmen und Bewertungen hierzu in der Theorie aussehen und was die Experten aus der Praxis dazu berichten. Diese erste Forschungsfrage bereitet damit die weiteren Fragestellungen und die Möglichkeit der Erarbeitung von wissenschaftlich fundierten Empfehlungen vor.

- Nebenforschungsfrage 1: Wie ist die Situation des Business Continuity Managements mit Blick auf die Digitalisierung?

Hierzu waren grundsätzlich der allgemeine Stellenwert und die damit zusammenhängende tatsächliche Berücksichtigung und Umsetzung in Unternehmen und Behörden interessant. Wie von Königs bereits zitiert, wird dem Business Continuity eine überlebenswichtige Bedeutung für Unternehmen zugemessen und es wird empfohlen, es in Verbindung mit der IT-Notfallplanung in der strategischen Zielsetzung der Unternehmen zu berücksichtigen (2017, S. 308). Übereinstimmend berichteten die Experten von einer sehr hohen und essenziellen Bedeutung des Business Continuity Managements aus der Praxis. Laut Studien, wie in Kapitel II 1.1.5 zitiert, sind die Verbreitung und die Umsetzung allerdings noch auf einem niedrigen Niveau. Aus der Praxis wurde diese Problematik deutlich verschärft dargestellt, indem kein Experte von einer ausreichenden Berücksichtigung des Business Continuity Managements mit Blick auf die noch weiter erwartete Digitalisierung berichten konnte. Das Verständnis, die sogenannte Awareness dafür, müsse auf allen Ebenen noch geschaffen werden. Diese Awareness für das Business Continuity Management wächst zunehmend durch aktuelle Krisen und weltweite Ereignisse, bei denen Situationen tatsächlich eintreten, deren Eintrittswahrscheinlichkeit als sehr gering bzw. unmöglich angenommen wurde. Damit besteht aktuell eine Chance, die sehr hohe Bedeutung an die verantwortlichen Stellen zu adressieren, um die benötigten Ressourcen und Aktivitäten generieren zu können. Gleichzeitig

wird die Bedeutung mit der weiteren Digitalisierung zunehmen, insbesondere wenn geschäftskritische Prozesse mehr und mehr automatisiert und damit von der IT abhängig gemacht werden. Bemerkenswert sind hier auch die zunehmenden Gefahren, von denen berichtet wurde, durch die Organisationen bei der weiteren Digitalisierung zusätzlich angreifbarer werden. Zusammenfassend ist die Situation aktuell sehr dynamisch. Das Business Continuity Management muss sich neben der weiteren Etablierung auch kurzfristig an neue Herausforderungen anpassen. In Stichworten lässt sich die Situation des Business Continuity Managements im Zeitalter der Digitalisierung wie folgt skizzieren:

- die sehr hohe Bedeutung wurde bestätigt
- diese steigt mit der weiteren Digitalisierung
- ein allgemeines Verständnis dafür ist noch nicht vorhanden
- aktuelle Krisen schaffen Awareness und erhöhen die Notwendigkeit
- die Umsetzung in der Praxis ist nicht ausreichend
- ein großer Handlungsbedarf, sowohl methodisch als auch praktisch, wurde bestätigt
- ein dynamischer Anpassungsprozess ist notwendig
- bei Vernachlässigung sind schwerwiegende Folgen absehbar

Diese Auflistung ist allgemeingültig formuliert, fokussiert aber bereits den Bereich der behördennahen IT-Dienstleister, um damit mittelbar die Entwicklungen in der zukünftigen behördlichen IT zu steuern und um den Betrieb resilienter zu machen.

Mit der zweiten Nebenforschungsfrage waren im Kontext der ersten Nebenforschungsfrage diejenigen Aspekte der Digitalisierung herauszuarbeiten, die hier von besonderem Interesse sind.

- Nebenforschungsfrage 2: Welche Aspekte der Digitalisierung sind hier kritisch?

Der Cloud-Technologie kommt eine zentrale Rolle bei der Digitalisierung zu (Faber, 2019, S. 20; Abolhassan, 2016, S. 149). Ebenso haben die Experten, wie in Abbildung 33 in Kapitel III 2.2.1.2 dargestellt, das Cloud-Computing als zentralen Punkt diskutiert, der auch Chancen für das Business Continuity Management bietet. Gleichzeitig sind damit Gefahren verbunden und es gibt noch ungeklärte Fragen für ein sicheres Hosting dieser Technologien. Diese Situation ist in den Handlungsempfehlungen an zentraler Stelle aufzunehmen. Grundsätzlich haben die Experten im Rahmen der Digitalisierung zuerst die Automatisierung angesprochen, die sie, jeweils unterschiedlich ausgedrückt, in verschiedenen Szenarien beschrieben haben. Dabei wird die aktuell noch durch menschliche Arbeit zu erledigende Vorgangsbearbeitung zunehmend digitalisiert und dann auch automatisiert

werden. Speziellere Themen, wie Big Data, KI oder Smarthome, Smart City und IOT wurden zwar ebenso genannt, aber noch nicht vorrangig als kritische Themen in diesem Zusammenhang bewertet. Für die weitere Automatisierung von Geschäftsprozessen wurde die technische, sichere und rechtlich vertretbare Realisierbarkeit hinterfragt. Hierzu berichteten die Experten von differenzierten Erfahrungen mit der als unumgänglich bewerteten Cloud-Technologie, die Vorteile für das Business Continuity Management bringen kann, aber auch noch mit großen Herausforderungen verbunden ist. Mehrfach haben die Experten auch den technologischen Fortschritt im privaten Bereich und in der Wirtschaft mit dem Einsatz von IT in Behörden verglichen und prognostizierten, dass diese Entwicklungen entsprechend Einzug halten werden und der private Bereich weiter direkt mit der behördlichen IT vernetzt werden wird. Damit sind diese Aspekte als Erstes in der nachfolgenden Auflistung zu nennen. Die Nutzung privater Hard- und Software als Teil der behördlichen Vorgangsbearbeitung wurde als kritisch, aber unvermeidlich betont und damit einhergehend ebenso die zunehmende Nutzung unterschiedlicher mobiler Devices.

Zusammenfassend bedürfen somit die nachfolgenden Themenfelder der Digitalisierung im Zusammenhang mit dem Business Continuity Management aus der Perspektive der behördennahen IT-Dienstleister einer besonderen Aufmerksamkeit:

- vollständige Automatisierung von behördlichen Geschäftsprozessen und Nutzung digitaler Lösungen in allen Bereichen der Leistungserbringung
- sicherer Betrieb Cloud-basierender IT-Lösungen
- Vernetzung, Integration und Datenaustausch über unterschiedliche Domänen
- Endgerätesicherheit und sichere mobile Kommunikation

Damit sind die wesentlichen hier relevanten Punkte der Digitalisierung mit Bezug zum Business Continuity Management herausgearbeitet. Mit der nachfolgenden Forschungsfrage werden Lösungsmöglichkeiten ermittelt, um zukünftig Risiken gemäß der Problemstellung zu minimieren.

- Nebenforschungsfrage 3: Welche Lösungsmöglichkeiten gibt es aus der Praxis?

Diese praxisbezogene Nebenforschungsfrage lässt sich durch die Analyse der Interviews beantworten, da die Experten in den halboffen geführten Interviews auch stets ihre Erfahrungen, Ideen und Empfehlungen für die genannten Problemstellungen mitteilten. Die Erfahrungen waren nicht nur negativ, sondern es wurde auch direkt von Lösungsmöglichkeiten berichtet, die sich bewährt haben. Für eine prägnante Beantwortung dieser Frage mussten die Hinweise der Experten auf die in den ersten beiden Neben-

forschungsfragen herausgearbeiteten Aspekte beschränkt werden. Die Interpretation und der Vergleich mit den theoretischen Ergebnissen erfolgten bereits in Kapitel III 3.1.3, so dass die Frage nun folgendermaßen beantwortet wird.

Voraussetzung für alle Lösungsmöglichkeiten sind

- eine Sensibilisierung des Managements und der Mitarbeiter sowie
- das Schaffen von organisatorischen, personellen und finanziellen Voraussetzungen.

Auf Basis dieser Voraussetzungen können die folgenden Lösungsansätze verfolgt werden, um die weitere Digitalisierung auch bei Schadensgroßereignissen möglichst sicher zu gestalten:

- Digitalisierungsprojekte müssen bereits zu Beginn aus Sicht des Business Continuity Managements betrachten werden.
- IT-Lösungen sind kritikalitätsspezifisch konsequent redundant zu realisieren.
- Abhängigkeiten (technologisch, vom Hersteller, geographisch) sind zu minimieren.
- Die schrittweise Einführung eines Business Continuity Managements wird empfohlen.
- Standards müssen genutzt werden, aber nicht als verpflichtende Belastung, sondern intrinsisch, indem ihr Mehrwert erkannt und umgesetzt wird.
- Business Continuity Management muss als Daueraufgabe verstanden und regelmäßig aktualisiert und eingeübt werden.
- Durch technische oder manuelle Fallback-Lösungen kann eigenständig die Fähigkeit behalten werden, auch bei einem Ausfall der IT handlungsfähig oder wieder anlauffähig zu sein.

Als konkrete Empfehlungen nach Darlegung dieser Ergebnisse können folgende Punkte abgeleitet werden, die später in den Handlungsempfehlungen aufgenommen werden:

- Aufklärung des Managements zur Verantwortung insgesamt und im Rahmen der erwarteten NIS-2-Gesetzgebung,
- Erweiterung oder Anpassung der Organisation durch Benennung von BC-Beauftragten oder Continuity-Managern,
- Start der Aktivitäten mit einer dokumentierten Business-Impact-Analyse,
- Durchführung von Schulungen aller Mitarbeiter im Bereich IT-Sicherheit,
- Durchführung von Schulungen zum Business Continuity Management für relevante Bereiche und Mitarbeiter,
- Anstreben und Durchführung einer Zertifizierung nach ISO-Norm 22301 durch Beauftragung externer Zertifizierungsinstitute,

- Vermeiden von Digitalisierungsprojekten ohne gleichzeitige Einführung ausreichender Redundanzen aus Sicht des Business Continuity Managements durch Berücksichtigung verpflichtender Prüfpunkte im IT-Projektmanagement,
- Einführen und Testen alternativer IT-Lösungen, mit denen ein Ausfall der primären IT in seiner Auswirkung reduziert werden kann, beispielsweise eine zweite und unabhängige Cloud-Umgebung,
- konsequente Anwendung und Wiederholung des PDCA-Zyklus für die Aspekte des Business Continuity Managements durch regelmäßiges Controlling.

Damit haben sich nach Abschluss des empirischen Teils zur Beantwortung der Forschungsfragen Resultate ergeben, die vorab so nicht erwartet wurden. In der Theorie und nach Analyse der qualitativen sowie der quantitativen Studien wurde davon ausgegangen, dass es zwar einen Nachholbedarf bei der Thematik gibt und sich die Herausforderungen ggf. auf technische Aspekte konzentrieren, aber nicht, dass zunächst noch das Business Continuity Management vorrangig in der Gesamtsicht adressiert werden muss. Die Antworten auf die dritte Forschungsfrage bilden daher einen wesentlichen Bezug für die erstellten Handlungsempfehlungen.

3.1.5.2 Beantwortung der Hauptforschungsfrage

Die Antworten auf die Hauptforschungsfrage setzen sich inhaltlich aus den Erkenntnissen zu den Nebenforschungsfragen zusammen und geben einen kompakten und zukunftsweisenden Blick auf die Thematik.

- HFF: Wie ist die Situation des Business Continuity Managements im Zeitalter der Digitalisierung und mit welchen Erfolgsfaktoren kann eine möglichst sichere Digitalisierung, auch in der öffentlichen Verwaltung, ermöglicht werden?

Die Situation ist allgemein so, dass der Stellenwert in Unternehmen und Behörden noch deutlich erhöht werden muss. Die Bedeutung wird durch aktuelle Krisen zunehmend erkannt, allerdings wird sie zusätzlich auch durch die weitere Digitalisierung rapide zunehmen. Daher muss die Anwendung des Business Continuity Managements sich wie folgt entwickeln:

- die Etablierung muss deutlich erhöht werden
- es muss als verpflichtender Standard in Digitalisierungsprojekten berücksichtigt sein
- IT-Notfallpläne müssen erstellt, beübt und regelmäßig aktualisiert werden
- eine Orientierung an den Standards nach BSI und ISO wird empfohlen

Zur weiteren Erläuterung wurde auf Basis der Ergebnisse die nachfolgende Abbildung erstellt. Die unaufhaltsame weitere Entwicklung im Bereich der Digitalisierung, die in Behörden in Deutschland mit entsprechenden IT-Dienstleistern erfolgen wird, wurde skizziert. Die Situation des Business Continuity Managements insgesamt ist aktuell so, dass damit noch keine Resilienz gegeben ist und die Risiken weiter steigen. Als Erfolgsfaktoren, um eine möglichst sichere Digitalisierung zu ermöglichen, wurden die Themenblöcke ‚Verständnis schaffen', ‚Technologieentscheidungen' und die Berücksichtigung in ‚Digitalisierungsprojekten' aus den Erkenntnissen dieser Arbeit abgeleitet.

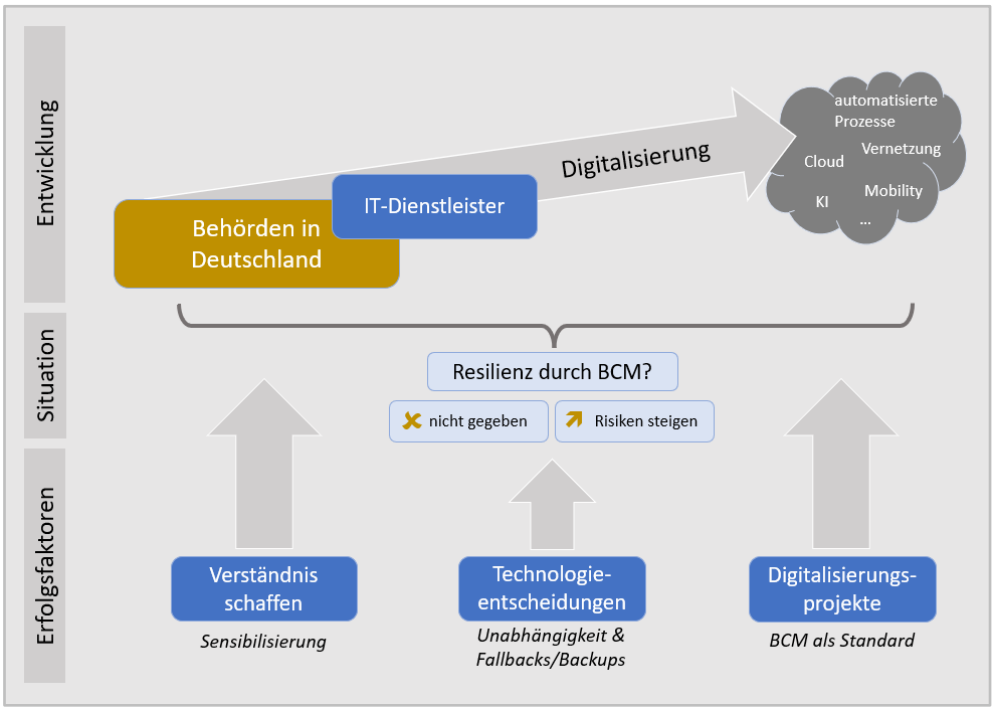


Abbildung 45 – Ergebnis zur Hauptforschungsfrage (Quelle: eigene Darstellung)

Die weitere Digitalisierung muss insgesamt, hier speziell im Bereich der deutschen Behörden, resilienter ausgeplant werden und dabei sind die Standards des Business Continuity Managements hinreichend zu berücksichtigen, damit durch die Digitalisierung keine neuen Risiken heranwachsen. Es dürfen keine Problemfelder entstehen, die die Handlungsfähigkeit der Behörden und Organisationen im Bereich der kritischen Infrastrukturen, der Polizei, der Bundeswehr, der Krankenhäuser, des technischen Hilfswerks oder der Feuerwehren durch Ausfall der IT stark gefährden. Durch ein praktiziertes Business Continuity Management, das ausreichende Rückfallpositionen schafft, bestehen Chancen, durch die Digitalisierung gesamtgesellschaftlich und explizit im Bereich der inneren und äußeren Sicherheit einen Mehrwert zu schaffen und das Sicherheitsniveau zu erhöhen.

Der Erkenntnisgewinn nach der Beantwortung der Forschungsfragen wird im nächsten Teil IV dieser Arbeit zur Darstellung von Erfolgsfaktoren genutzt. Zunächst werden noch die Gütekriterien betrachtet und angewendet, um die Qualität der Ergebnisse abzusichern.

3.2 Gütekriterien und methodische Abgrenzung

In diesem Kapitel werden die Gütekriterien dargelegt, die für das qualitative Vorgehen zur Anwendung gekommen sind. Anschließend wird das methodische Vorgehen dahingehend kritisch betrachtet und abgegrenzt, womit sich auch Handlungsfelder für weiterführende qualitative oder quantitative Forschungen ergeben.

3.2.1 Auswahl und Anwendung der Gütekriterien

Für ein qualitativ hochwertiges Ergebnis muss mit der gewählten Forschungsmethode auch eine entsprechende Güte der Ergebnisse sichergestellt werden. Flick (2022b, S. 534) diskutiert die Frage, wie sich aus subjektiven Sichtweisen ausreichend unabhängige Schlussfolgerungen erarbeiten lassen. In dieser Arbeit wurden im Rahmen der Interviews grundsätzlich persönliche Erfahrungen der Experten erfasst und analysiert, die damit durchaus auch subjektive Bestandteile beinhalten. Nach Mayring (2023, S. 119) ist am Ende der Forschungsarbeit eine Einschätzung der Qualität der Ergebnisse vorzunehmen. Bereits im Exposé zu dieser Arbeit wurde die konkrete Umsetzung hierzu in Abhängigkeit von den tatsächlich erzeugten Kategorien genannt, so dass die Anwendung der ausgewählten Gütekriterien nun erfolgen kann.

Mayring (2023, S. 123-125) hat sechs allgemeine Gütekriterien für die qualitative Forschung erläutert: „Verfahrensdokumentation“, „argumentative Interpretationsabsicherung“, „Regelgeleitetheit“, „Nähe zum Gegenstand“, „kommunikative Validierung“ und „Triangulation“. Aufgrund der Erhebungsmethode in Form von Experteninterviews, der Zielgruppe und des Untersuchungsgegenstandes wurden die Kriterien „Verfahrens-dokumentation“, „Nähe zum Gegenstand“ , „argumentative Interpretationsabsicherung“ und hier „Regelgeleitetheit“ explizit angewandt.

<u>Verfahrensdokumentation</u>

Das Verfahren wurde insgesamt mit dieser Dissertation und den Anlagen ausführlich dokumentiert. Beginnend mit der Ausgangslage und der Problemstellung wurde über die Theorierecherche die Methode ermittelt, ein Leitfaden für Experteninterviews abgeleitet und

die Interviewvorbereitung und -durchführung nachvollziehbar dokumentiert. Es waren sowohl als Pflichtinhalte der Dissertation als auch nach den Vorgaben der Datenschutzgrundverordnung (DSGVO) entsprechende Verfahrensdokumentationen verpflichtend einzuhalten. Die Zusammenstellung der Analyseinstrumente und die Auswertung, wie Mayring (2023, S. 123) es für die Verfahrensdokumentation vorsieht, wurden hier ebenfalls nachvollziehbar dokumentiert.

Nähe zum Gegenstand

Die Nähe zum Gegenstand wurde dadurch erreicht, dass der empirische Teil der Arbeit die Personen involviert hat, die hier über Expertenwissen verfügen und dieses bereits im Bereich der behördlichen IT angewendet haben. Von Bedeutung war ebenfalls, dass die Teilnehmer auch aktuell im Bereich IT-Sicherheit und Business Continuity Management tätig sind und hier aus der Praxis berichten können. Dem Forschungszweck entsprechend wurden damit die Nähe zum Gegenstand um der notwendige Faktor *aktuelle* Nähe zum Gegenstand erweitert. Die Interviews wurden als Audiokonferenz durchgeführt, so dass die Teilnehmer aus ihrer aktuellen Arbeitswelt heraus ihre Erfahrungen berichten konnten. Zusätzlich waren die Fragestellungen in den Interviews aus der Problemstellung, der Ausgangslage und der Theorie abgeleitet, um eine hohe und aktuelle Nähe zum Gegenstand zu wahren.

Argumentative Interpretationsabsicherung

Interpretationen sind in der qualitativen Forschung von besonderer Bedeutung, können jedoch nicht bewiesen werden (Mayring, 2023, S. 123). Im Rahmen der Analyse des Datenmaterials waren die Aussagen insbesondere in der Gesamtsicht entsprechend zu interpretieren. Ein wissenschaftlich anerkanntes Ablaufmodell zur Inhaltsanalyse wurde in Kapitel 1.4.3. erläutert und ist hier zur Anwendung gekommen. Zur Absicherung wurden die Interpretationen argumentativ im Kapitel der Ergebnisdarlegung aufgearbeitet. Dazu wurden sowohl die Argumente der Experten als auch die Grundlagen aus der Theorie gemeinsam betrachtet, um die herausgearbeiteten Ergebnisse qualitativ abzusichern.

Regelgeleitetheit

Auch in der qualitativen Forschung sind die Arbeitsschritte systematisch abzuarbeiten. In der Analyse wird das Vorgehen nach einem Ablaufmodell empfohlen (Mayring, 2023, S. 123-124). Nach den Regeln, wie im Modell in Kapitel III 1.4.3 dargestellt, wurde die Analyse für den Anteil der Codierung und der Kategoriebildung durchgeführt. Ebenfalls erfolgte die Erstellung des Interviewleitfadens nach der Regel, dass, basierend auf den Erkenntnissen der Theorie, die Themenbereiche der Forschungsfragen im Vordergrund standen. Weitere feste Regeln in

der Interviewführung ergänzten das Regelset für den empirischen Teil. Hierzu gehörte es, die Interviewpartner zunächst frei berichten zu lassen, um die Schwerpunkte in der Praxis abschätzen zu können. Für einen Themenwechsel während der Interviews kamen grundsätzlich nur vorbereitete Nachfragen zur Anwendung, um systematisch auswertbares Datenmaterial zu erzeugen.

Eine weitere Möglichkeit zur Überprüfung der Codierung ist die Berechnung eines Reliabilitätsmaßes, z. B. nach Cohens Kappa, das nach einer erneuten Codierung des Materials durch einen zweiten Codierer berechnet werden kann (Züll & Menhold, 2022, S. 1131). Kuckartz (2019, S. 17) sieht die Anwendung dieser Maße in der qualitativen Forschung allerdings als problematisch an und verweist auf die Abhängigkeit von der Anzahl der Haupt- und Unterkategorien. Ebenfalls von Bedeutung hier ist, dass, wie bei der Operationalisierung bereits vorgestellt, neben der deduktiven Codierung auch eine induktive Kategoriebildung erfolgen musste, um ergebnisoffen die Hinweise aus der Praxis zu erfassen. Nach Rädiker und Kuckartz (2019, S. 103) ist es nicht sinnvoll, bei diesem Vorgehen in der qualitativen Analyse eine Koeffizientenbestimmung vorzunehmen. Die Autoren bezeichnen den Anspruch, wonach sich die gleichen Kategorien bei der induktiven Codierung durch mehrere Personen ergeben sollen, als nicht erfüllbar. Bogner et al. (2014, S. 93) sehen anstelle der klassischen Gütekriterien hier die Transparenz im Auswerteprozess und bei der Erhebung des Datenmaterials als Mittel des Nachweises der Objektivität und der Güte der Untersuchung. Dem folgend wurde die Operationalisierung bereits detailliert beschrieben und die Erhebungsmethode, die Expertenauswahl sowie die Interviewdurchführung wurden ausführlich dargestellt. Die Ergebnisdarstellung wurde erläutert und um die kontextbezogenen Aussagen der Experten in tabellarischer Form jeweils ergänzt. Zusätzlich sind der Interviewleitfaden (Anlage II.) und alle geführten Interviews in Anlage III. vollständig beigefügt, um die von Bogner et al. empfohlene Transparenz herzustellen.

3.2.2 Methodische Abgrenzung

Wie bereits im Forschungsdesign dokumentiert, wurden sensible Thematiken zum Sachstand des Business Continuity Managements hinterfragt. Es wurde nicht mit einem Fragebogen eine Ist-Situation erhoben und ausgewertet, sondern die Sachlage, die Hintergründe und Bewertungen wurden ermittelt. Damit besteht eine deutliche Abgrenzung gegenüber einem quantitativen Forschungsdesign, bei dem mit einer repräsentativen Stichprobengröße auf die

Gesamtheit geschlossen werden kann. Dieser Aspekt wird im Rahmen des Forschungsausblicks aufgenommen.

Um möglichst praxisnahe Auskünfte zu erhalten und Empfehlungen ableiten zu können, wurden Experten aus dem Bereich der IT-Dienstleistungsbranche interviewt, die über Behördenerfahrungen verfügen. Damit wurden zwar einerseits nicht die betroffenen Bereiche selbst in die Datenerhebung direkt eingebunden, andererseits waren dadurch genau solche IT-Dienstleister involviert, die auch für das Business Continuity Management Beratungs- und Entwicklungsleistungen anbieten. Auf diese Weise konnte ein Mehrwert generiert werden, der in der späteren Umsetzung genau die dort bekannten Herausforderungen anspricht und Lösungswege aufzeigt.

Sowohl bei der Digitalisierung als auch, wie diese empirische Studie gezeigt hat, im Bereich des Business Continuity Managements steht Deutschland noch am Anfang und vor großen Herausforderungen und Veränderungen. Objektiv kann nur das gemessen und analysiert werden, was vorhanden oder eingetreten ist. Schwerpunkt dieser Arbeit war es somit, Gründe für Defizite zu finden und proaktiv Lösungsmöglichkeiten zu erarbeiten, anstatt faktenbasierend Schlussfolgerungen zu ziehen. Mit der gewählten Methode und der qualitativen Auswertung war dies möglich, die Arbeit grenzt sich aber von Untersuchungen in Bereichen ab, in denen in der Praxis bereits mehr Erfahrungen vorliegen und erfasst werden können.

Die Untersuchung war auf behördenerfahrene IT-Dienstleister in Deutschland mit Blick auf die Digitalisierung und Services deutscher Behörden und Organisationen eingeschränkt. Die zitierten Umfragen und Studien aus anderen Ländern oder mit internationalem Fokus haben deutliche Unterschiede im Fortschritt der Digitalisierung gegenüber dem Sachstand in Deutschland gezeigt. Ebenfalls wurde deutlich, dass die Verbreitung und Etablierung eines praktizierten Business Continuity Managements, beispielsweise anhand der ISO-Zertifizierungen, in anderen Ländern teilweise auf einem deutlich höheren Niveau liegt. Damit sind die Analyseergebnisse und Empfehlungen vorrangig auf den deutschen Bereich anwendbar, es wurde allerdings darauf geachtet, dass die wesentlichen Erkenntnisse auch international und unabhängig von der Organisation übertragbar sind. Zudem wurde das Business Continuity Management grundsätzlich nicht nur aus der Perspektive eines Unternehmens oder einer Behörde betrachtet, sondern in erster Linie aus Sicht der Digitalisierung.

Damit sind die methodischen Einschränkungen genannt und es wurde aufgezeigt, wie mit diesen umgegangen wurde, um fokussiert die Forschungsfragen beantworten zu können und einen generalisierbaren Erkenntnisgewinn zu erzeugen. Durch Anpassung der Methodik und Änderung an diesen limitierenden Faktoren können weiterführende und andere Forschungsziele er- und bearbeitet werden, auf die im Forschungsausblick eingegangen wird. Nach dieser Betrachtung der Gütekriterien und der methodischen Abgrenzung können im nächsten Kapitel die empiriegeleiteten Fragestellungen beantwortet werden.

3.3 Konklusion und Beantwortung der empiriegeleiteten Fragestellungen

In diesem Kapitel wird der empirische Teil mit den wesentlichen Erkenntnissen zusammengefasst und mit dem Übergang zum Gestaltungsteil abgeschlossen. Die Erkenntnisse aus der Untersuchung bestimmen neben der Theorie maßgeblich die erstellten Empfehlungen und den Ausblick.

3.3.1 Zusammenfassung der relevantesten Erkenntnisse der Empirie

Eine wesentliche Erkenntnis aus dem empirischen Teil ist, dass es aus der Praxis keine Berichte gab, die ein Business Continuity Management in Unternehmen oder Behörden als etabliert beschreiben und diese für die weitere Digitalisierung in Deutschland als gut vorbereitet ansehen. Im Rahmen der Theorie wurden Studien gesichtet, in denen von einem vorhandenen IT-Notfallmanagement in Unternehmen und Behörden berichtet wird. Prozentual zeigte sich dort bereits eine Verbreitung auf einem niedrigen Niveau. Allerdings ist fokussiert auf das Business Continuity Management auf Basis der Praxiserhebung noch von einem deutlich schlechteren Lagebild auszugehen. Von einer ausreichenden Berücksichtigung in Behörden oder bei behördennahen IT-Dienstleistern konnte kein Experte berichten. Gleichzeitig wurden der Stellenwert und die Bedeutung eines Business Continuity Managements in der Praxis, hier übereinstimmend mit den Rechercheergebnissen aus der Theorie, als besonders hoch und unternehmenskritisch herausgearbeitet. Von den Experten wurde ausnahmslos von einem Handlungsbedarf berichtet, um das Business Continuity Management zukünftig und vor dem Hintergrund der weiteren Digitalisierung ausreichend in Behörden und Unternehmen zu etablieren. Die Begründungen und Argumentationsketten der Experten zeigten hierzu ein einheitliches Bild. In allen Fällen wurde berichtet, dass das Verständnis sowohl für ein Business Continuity Management als auch für die weitere Digitalisierung noch nicht ausreichend

vorhanden ist. Die Praxis empfiehlt hierzu zunächst die weitere Sensibilisierung und Schaffung eines sogenannten Mindsets als erste Voraussetzung, um zukünftig IT-Projekte unter Berücksichtigung eines Business Continuity Managements sicher zu gestalten und resilient umsetzen zu können.

Eine weitere relevante Erkenntnis aus der technischen Betrachtung ist, dass eine eindeutig empfehlenswerte Lösung für einen sicheren Betrieb von Cloud-Lösungen offensichtlich noch nicht vorhanden ist, sobald die Resilienzfähigkeit hinterfragt wird. Es wurde berichtet, dass z. B. mit dem Projekt GAIA-X verschiedene Lösungen in Vorbereitung sind, aber es aktuell keine klare Empfehlung gibt, wie eine Organisation sicher und unabhängig die eigene IT-Infrastruktur auf Cloud-Technologien umstellen kann. Vorhandene Lösungen der großen amerikanischen Anbieter wurden kritisch diskutiert und es wurde wiederkehrend auf die Notwendigkeit hingewiesen, die IT-Systeme durchaus weiterhin in eigenen Rechenzentren zu betreiben, um die Datensouveränität zu wahren. Eine weitere Erkenntnis aus der Praxis ist, dass mit weiteren Digitalisierungstechnologien wie IOT oder KI auch völlig neue Gefahren erwartet werden, auf die sich das Business Continuity Management erst einstellen muss. Das bezieht sich dabei nicht nur auf neue Angriffsmöglichkeiten oder Einfallstore, sondern explizit aus Sicht des IT-Notfallmanagements auf neue notwendige Strategien. Konträr dazu, aber ebenfalls aus der empirischen Analyse, hat sich ergeben, dass die Experten für die aktuell genutzten IT-Systeme keine unlösbaren Herausforderungen sehen. Mit den Möglichkeiten moderner Backup- und Redundanzsysteme wären die Probleme der Ausgangslage vermeidbar gewesen.

Konkret bedeutet das, dass zunächst noch eine weitere Aufklärung und Sensibilisierung auf allen Ebenen erfolgen muss. Für viele technologische Herausforderungen aus Sicht des Business Continuity Managements gibt es bereits Lösungen, die wegen fehlenden Problembewusstseins nicht zur Anwendung kommen. Für weitere Schritte der Digitalisierung und rechtliche Fragestellungen besteht noch Handlungs- und Entscheidungsbedarf, um die weitere Digitalisierung dadurch nicht aufzuhalten. Mögliche Lösungen und empfohlene Vorgehensweisen dazu sind im Rahmen der Handlungsempfehlungen im nächsten Teil IV dokumentiert.

3.3.2 Beantwortung der empiriegeleiteten Fragestellungen

In der Zielstellung waren die nachfolgenden Fragen für den erwarteten Erkenntnisgewinn aus dem empirischen Teil definiert:

- Wie und wann wird in der Praxis ein Business Continuity Management angewendet, um den neuen Herausforderungen der Digitalisierung gerecht zu werden?
- Welche Einflussfaktoren, Herausforderungen und Erfahrungen stehen hierzu in Unternehmen in welchem Zusammenhang?
- Welche bewährten Praktiken existieren, um die IT-Sicherheit mit den Methoden eines Business Continuity Managements bei der weiteren Digitalisierung zu erhöhen?

Zur ersten Frage lässt sich feststellen, dass der direkte Zusammenhang und die Handlungsnotwendigkeiten in der Praxis von den verantwortlichen Personen noch nicht gesehen werden. Auch ohne den konkreten Fokus auf Digitalisierungsprojekte ist ein Business Continuity Management nicht in dem Maße präsent, wie es zu empfehlen wäre. Hier muss zuerst ein Problembewusstsein auf allen Ebenen geschaffen werden, um die Anforderungen an eine resiliente IT-Landschaft, auch bei Eintritt von Schadensgroßereignissen, rechtzeitig in die weitere digitale Transformation einzubringen. Erst mit dem Verständnis für sichere IT-Digitalisierungsprojekte auch auf Ebene der Geschäfts- und Behördenleitungen können entsprechende Mittel dafür zur Verfügung gestellt werden.

Als ein außergewöhnlicher Einflussfaktor sind die aktuellen Krisen wie die COVID-19-Pandemie, das Ahrtal-Hochwasser und der Ukrainekrieg zu nennen. Auch wenn in allen Fällen dort die Digitalisierung nicht im Vordergrund steht, wurde durch das Auftreten undenkbarer Situationen gezeigt, dass Risiken eintreten können, deren Eintrittswahrscheinlichkeit als sehr gering bewertet werden konnte. Am Beispiel der Pandemie zeigte sich zudem, dass mit der Digitalisierung und mit vorbereiteten Notfallplänen die Krise aus Unternehmenssicht leichter zu bewältigen war. Experten berichteten hierzu aus Erfahrungen, wie Unternehmen und Behörden mit bereits ausgeprägter mobiler IT-Ausstattung weniger Einschränkungen hatten, die Arbeitsfähigkeit aufrechtzuerhalten. Als weitere Herausforderung ist das allgemeine Kosten/Nutzen-Verhältnis zu bewerten. Durch anfangs hohe Investitionen in ein Business Continuity Management werden grundsätzlich weder Gewinne erwirtschaftet noch neue Geschäftsfelder erschlossen. Es werden auch keine neuen IT-Services im Rahmen der Digitalisierung des Staates damit ermöglicht, sondern es sichert in beiden Fällen lediglich den Weiterbetrieb nach entsprechenden Ereignissen oder Angriffen ab. Die konkreten Kundenanforderungen sind ein wesentlicher Einflussfaktor, an die die IT-Dienstleister gebunden sind. Als weitere Herausforderung ist die Zusammenarbeit mit Partnern und Providern zu nennen, sobald die rechtlichen Fragestellungen im Zusammenhang mit Datensouveränität und Datenschutz betrachtet werden.

Aus der Beantwortung der dritten Frage können direkt praxisbewährte Empfehlungen abgeleitet werden, die unter Berücksichtigung der Gesamtanalyse und des theoretischen Rahmens in die Handlungsempfehlungen eingeflossen sind. In Ergänzung zu der schon ausführlich dargestellten Interpretation der Empfehlungen in Kapitel III 3.1.3 sind folgende Erkenntnisse aus der empirischen Untersuchung zu nennen. Es wurden Vorgabedokumente wie die ISO-Norm, der BSI-Standard oder ITIL als hilfreich empfohlen. Diese Standards sind als Empfehlung zu sehen und stellen keine vollumfänglich und zwingend einzuhaltenden Vorgaben dar. Hier einen Ansatz zu wählen, der in einem Unternehmen oder einer Behörde vorsieht, umgehend sämtliche Anforderungen in allen Abteilungen und Bereichen umzusetzen, ist nicht erfolgversprechend. Stattdessen wurde aus der Praxis ein schrittweises Vorgehen empfohlen. Auch Mandl (2021, S. 555) rät, zunächst einen einfachen Ansatz zu wählen, der anschließend verbessert werden kann. Es sollte zunächst mit einer Business-Impact-Analyse begonnen werden, wie es auch in der Theorie vorgesehen ist. Eine Umsetzung kann anschließend priorisiert nach Abteilungen, Anwendungen oder kritischen Geschäftsprozessen erfolgen, um dabei für den weiteren Ausbau zu lernen und die Mitarbeiter nicht zu überlasten. Mit dieser komprimierten Beantwortung der dritten Frage ist die grundsätzliche Ausrichtung von aktuellen Empfehlungen dargestellt. Der nachfolgende Teil IV dient in seiner Gesamtheit ergänzend der Beantwortung der Frage, welche bewährten Methoden in der Praxis existieren, um die IT-Sicherheit durch Anwendung eines Business Continuity Managements bei der weiteren Digitalisierung zu erhöhen.

Zusammenfassend sind damit die empiriegeleiteten Fragestellungen beantwortet, die einerseits den aktuellen Handlungs- und einen weiteren Forschungsbedarf aufzeigen und andererseits Hinweise liefern, wie das Business Continuity Management in der Fokusgruppe erfolgversprechend eingebracht werden kann.

3.3.3 Wie wurde die Zielstellung erreicht?

Bereits nach den ersten Erkenntnissen aus der Theorierecherche wurde transparent, dass in vielen Bereichen noch Handlungsbedarf besteht, wenn die weitere Digitalisierung aus Sicht des Business Continuity Managements betrachtet wird. Eine quantitative Erhebung und Analyse oder Befragung von Experten mit hauptsächlich geschlossenen Fragen wäre hier nicht zielführend gewesen, da die Fragestellung für den praxisorientierten Teil noch unbekannte Antwortmöglichkeiten, Zusammenhänge und Hintergründe ermitteln sollte.

Die Zielstellung wurde dadurch erreicht, dass durch Auswahl der Interviewpartner und die Methode der leitfadengestützten Experteninterviews fokussiert das Wissen und die Erfahrungen im relevanten Beriech dokumentiert werden konnten. Durch die offenen Einstiegsfragen in Block 2 und 3 der Interviews nannten und erläuterten die Experten direkt die aus ihrer Sicht relevanten Themenfelder. Für die Thematiken, die sich aus der Theorie als in jedem Fall relevant gezeigt haben, konnten durch vorbereitete Nachfragen im Verlauf des Interviews Informationen zu allen relevanten Bereichen erhoben werden.
Wie bereits als Gütekriterium erläutert, war die Nähe zum Gegenstand zur Zielerreichung von besonderer Bedeutung. Die interviewten Personen konnten aus ihrer beruflichen Praxis heraus im Rahmen einer Video- oder Audiokonferenz, wie es im Jahr 2022 im beruflichen Alltag der IT-Dienstleistungsbranche schon üblich war, mit ihrem Expertenwissen Auskunft geben und beratend tätig sein. Das war für die empiriegeleiteten Fragstellungen von entscheidender Bedeutung, um für die Auswertung ein Datenmaterial hoher Qualität zu erzeugen.
Abschließend war die Zielstellung durch Anwendung der wissenschaftlichen Standards im Rahmen der Auswertung zu erreichen, damit ein regelbasiertes, transparentes und nachvollziehbares Ergebnis generiert werden konnte.

3.4 Gestaltungsgeleitete Fragestellung

Nach der Erhebung, der Auswertung und der Diskussion des empirischen Datenmaterials stehen Erkenntnisse, Informationen und Empfehlungen zur Verfügung, die die Digitalisierung aus Sicht von behördennahen IT-Dienstleistern mit Blick auf das Business Continuity Management fokussieren. Aus gestalterischer Perspektive stellt sich die Fragen, welche Empfehlungen auf dieser Basis wie formuliert als Erfolgsfaktoren zu erfassen sind und welche Reihenfolge oder Priorisierung dabei vorzunehmen ist. Nach der Feststellung, welche Aktivitäten oder Defizite sich in der Praxis durch die Beeinflussung der Digitalisierung ergeben, sind die Empfehlungen dahingehend zu gewichten. Fachlich betrachtet lässt sich die gestaltungsgeleitete Fragestellung wie folgt zusammenfassen:

- Welche Erfolgsfaktoren in Form von Handlungsempfehlungen zur weiteren Digitalisierung im behördlichen Umfeld sind zu formulieren, damit diese in Verbindung mit den theoretischen Grundlagen und einem effektiven Business Continuity Management anwendbar sind?

Eine weitere gestaltungsgeleitete Fragestellung in diesem Kontext ist, ob und in welchem Maße das durch die Digitalisierung zunehmende Outsourcing geschäftskritischer Anwendungen zu empfehlen ist und welches Mindestmaß an Notfallpräventionsmaßnahmen hier vorzusehen ist. Für weitere Schritte der Digitalisierung sind zumindest strategische Vorschläge zu formulieren, damit ein Kontrollverlust zukünftig durch entsprechende Absicherungen vermieden werden kann. Insgesamt lassen sich durch die Beantwortung dieser Fragestellung und die Anwendung der erarbeiteten Empfehlungen die in der Ausgangslage und der Problemstellung dargestellten Situationen vermeiden oder zumindest in ihren negativen Auswirkungen reduzieren.

IV GESTALTUNGSTEIL

In diesem Teil werden die Empfehlungen und Lösungsansätze basierend auf den empirischen Ergebnissen und unter Einbezug der Theorie beschrieben und begründet. Für einen praktischen Nutzen sind aus den Ergebnissen der Untersuchung Handlungsempfehlungen durch den Forschenden abzuleiten (Döring, 2023, S. 90). Im ersten Kapitel dieses Teil IV werden entsprechend den drei wesentlichen Themenfeldern dieser Arbeit drei Handlungsempfehlungen für die Forschung generiert. Für die Praxis werden sechs Handlungsempfehlungen erstellt, die sich initial aus dem empirischen Teil und den dort untersuchten Praxiserfahrungen ergeben haben. Anschließend wird im dritten Kapitel der Gestaltungsteil zusammengefasst und zum Schlussteil übergeleitet.

1 Handlungsempfehlungen/Lösungsansätze Forschung

Dieses Kapitel gliedert sich in die Unterkapitel Business Continuity Management, Digitalisierung und IT-Management, für die sich jeweils im Ergebnis ein Handlungsbedarf ergeben hat. Diese wurden um Lösungsansätze ergänzt, um den hier erlangten Erkenntnisgewinn auch für andere Forschungsvorhaben verfügbar zu machen. Dazu wurden drei Empfehlungen für die Forschung erstellt, die sich an den drei Hauptthematiken orientieren. Eine Priorisierung war hier nicht vorzunehmen.
Dadurch soll erreicht werden, dass die Relevanz des Business Continuity Managements in allen Bereichen und bei neuen wissenschaftlichen Ausarbeitungen zum IT-Management präsent ist. Zusätzlich wird empfohlen, das Business Continuity Managements bereits bei der Erforschung und Entwicklung von neuen digitalen Lösungen zu berücksichtigen.

1.1 Empfehlung (1) für die Forschung im Bereich BCM

Einleitend wird auf die Verwendung der Begrifflichkeit ‚Business Continuity Management' auch in Deutschland hingewiesen. Im Jahr 2023 wurde vom Bundesamt für Sicherheit in der Informationstechnik der so betitelte neue BSI-Standard 200-4 veröffentlicht. Dieser löst den BSI-Standard 100-4 „Notfallmanagement" ab und gilt zukünftig als Teil des BSI-Grundschutzes als Standard in Deutschland, explizit für die Notfallvorsorge im Bereich der IT. Mit dem alleinigen Begriff ‚Notfallmanagement' wird in der Gesellschaft, wie die Recherche in der wissenschaftlichen Literatur gezeigt hat, der medizinische Bereich assoziiert. Von hoher

Bedeutung ist hier das Wort ‚Continuity', womit die Möglichkeit zur Geschäftsfortführung gemeint ist. Mit der deutschen Übersetzung im Sinne einer Kontinuität ist es ebenfalls allgemein verständlich. Die kontinuierliche Geschäftstätigkeit kann durch den Eintritt eines Schadensgroßereignisses, beispielsweise die Vernichtung aller Unternehmensdaten, nicht mehr gegeben sein. Das grenzt klar von erwartbaren und kleineren IT-Störungen ab und die Bezeichnung ‚Continuity Management' ist international gebräuchlich. Nach dieser Vorbemerkung kann für die Forschung im Bereich Business Continuity Management Nachfolgendes empfohlen werden.

Wissenschaftliche Untersuchungen, die ein tatsächlich etabliertes Business Continuity Management in Deutschland mit Blick auf die IT-Infrastruktur tiefgründig untersucht haben, konnten nicht recherchiert werden. In Abgrenzung zur vorliegenden Arbeit ist damit die grundsätzliche und quantitative Verbreitung des Business Continuity Managements in Unternehmen und Behörden gemeint, ohne die hervorgehobenen Herausforderungen der IT und der digitalen Transformation. Es lassen sich im Internet Umfrageergebnisse recherchieren, die auf Selbstauskünften basieren und eine interessante und positive Tendenz zeigen. Indikatoren aus dieser Dissertation deuten allerdings darauf hin, dass hier mit Differenzen im Sinne einer negativen Situation zu rechnen ist. Interessant wäre hierzu ebenfalls eine internationale Analyse der ISO-Zertifizierungen nach der Norm 22301 „Business Continuity Management System", wie im Theorieteil bereits diskutiert. Ein weiterer Lösungsansatz wäre eine wissenschaftlich begleitete und öffentlich beauftragte großflächige Untersuchung in den relevanten kritischen Sektoren und Behörden, um die Resilienzfähigkeit der genutzten IT-Systeme transparent zu untersuchen und zu fördern.

Auch Neugebauer (2018, S. 6) sieht dauerhaft einen hohen Forschungsbedarf im Bereich der Sicherheit und der Digitalisierung. Mit den Erkenntnissen aus den hier empirisch aus der Praxis erhobenen Informationen wird empfohlen, ebenfalls permanent die Sachstände und die Möglichkeiten im Business Continuity Management wissenschaftlich zu begleiten. Thematisch von hoher Relevanz ist in diesem Zusammenhang die Betrachtung der digitalen Souveränität bei der weiteren Digitalisierung im Bereich des Cloud-Computing, der KI und den Planungen zum Projekt GAIA-X. Mithilfe wissenschaftlicher Untersuchungen können hier konkrete Gefahren herausgearbeitet und es kann bewertet werden, inwiefern die digitale Souveränität abnimmt und mit einem Verlust der Selbstbestimmung verbunden sein kann. Dadurch können die im Rahmen der weiteren Digitalisierung, die im nächsten Kapitel betrachtet wird, noch

nicht abschätzbaren Veränderungen frühzeitig erkannt werden, um für sicherheitskritische Herausforderungen die notwendigen Lösungen zu erarbeiten.

1.2 Empfehlung (2) für die Forschung im Bereich Digitalisierung

Zur Digitalisierung existieren, wie auch quantitativ in Kapitel II 1.1.1 „Recherchevorgehen“ dargestellt, zahlreiche wissenschaftliche Veröffentlichungen. Für die Forschung wird hier empfohlen, die Aspekte der Ausfallsicherheit, der Redundanz und der Fallback-Alternativen bei der weiteren Entwicklung von IT-Lösungen stets vordergründig mit zu untersuchen. Es ist davon auszugehen, dass Diversität auch im Bereich der Hersteller und Anbieter von IT-Lösungen zukünftig an Bedeutung gewinnt. Aus Sicht des Business Continuity Managements haben die Experten in dieser Studie davon abgeraten, sich für die wichtigen IT-Systeme an nur einen Hersteller oder Anbieter zu binden. Lösungen, die ‚by Design‘ nicht redundant ausgelegt sind, wurden kritisch diskutiert. Eine weitere Forschung im Bereich von IT-Systemen, die trotz des Verlusts oder des Ausfalls zentraler Komponenten die Arbeitsfähigkeit nicht einschränken, wäre zu begrüßen. In diesem Zusammenhang ist das Projekt GAIA-X zu nennen, das bereits wissenschaftlich begleitet wird. Aus Sicht des Business Continuity Managements könnten damit Herausforderungen gelöst werden, die sowohl in der Theorie als auch bei den interviewten Experten als Schlüsseltechnologien für eine sichere und souveräne Digitalisierung bewertet wurden. Wissenschaftliche Untersuchungen mit Fokus auf die Nutzbarkeit, die Ausfallsicherheit und die juristischen Aspekte insbesondere zur Nutzung durch deutsche Behörden und Sicherheitsorganisationen wird empfohlen. Damit ist bereits das Themenfeld IT-Management angesprochen, zu dem im nächsten Kapitel Empfehlungen herausgearbeitet werden.

1.3 Empfehlung (3) für die Forschung im Bereich IT-Management

Das IT-Management befindet sich analog zur digitalen Transformation im Wandel, wie es in Kapitel II 2.1.2 anhand verschiedener Autoren zitiert und für dieses Forschungsprojekt reflektiert wurde. Analog zu den Empfehlungen zur Forschung im Bereich der Digitalisierung kann auch hier eine Verbesserung erzielt werden, wenn das Business Continuity Management eine größere Berücksichtigung erfährt. Die Erkenntnisse aus der Theorie und die Berichte der Experten verorten dies als Managementaufgabe im Bereich der Geschäftsführungen. Die Verantwortung, die Geschäftsfortführung auch nach Eintritt von Schadensgroßereignissen zu

wahren, liegt jeweils auf höchster Ebene. Konsequent ist es dann, dass sowohl das strategische Management als auch das IT-Management diese Aufgaben und Verantwortlichkeiten klar benennen und strukturell berücksichtigen. Es bieten sich diesbezüglich verschiedene Handlungsfelder für die Forschung an. Auf Basis von Analysen im Unternehmensmanagement kann eine zielführende Abgrenzung oder Integration der Aufgaben und Verantwortlichkeiten zu geeigneten Rollenträgern, beispielsweise CEO, CIO oder CISO, erfolgen. Quantitative Studien können den jeweiligen Handlungsbedarf transparent machen.

Die Bedeutung des Business Continuity Managements wurde als überlebenswichtig und essenziell herausgearbeitet. Nachvollziehbarerweise sieht das IT-Management in den Kernprozessen (Allweyer, 2020, S. 38; Abbildung 9 in Kapitel II 2.1.2) alle Aktivitäten auf die IT ausgerichtet. Zukünftig die Notfallvorsorge bei ausgefallener IT ebenfalls als festen Bestandteil im IT-Management auf dieser Ebene anzusiedeln, könnte Unternehmen und Behörden durch ein so praktiziertes IT-Management resilienter machen. Es sollte erforscht werden, ob und wie lange Unternehmen heute und insbesondere zukünftig nach Ausfall der IT-Infrastruktur noch arbeitsfähig sind. Außerdem stellt sich die Frage, welche Vorgaben das IT-Management in Bezug auf Reaktionsgeschwindigkeit, maximale Ausfallzeiten und Datenverluste nach Worst-Case-Szenarien zukünftig machen muss und wie diese in Unternehmen und Behörden organisatorisch, personell und technisch angemessen zu berücksichtigen sind. Forschungsgegenstand können hier die steigende Abhängigkeit von der IT sowie der Umgang damit aus Sicht des IT-Managements sein. Zusätzlich kann empfohlen werden, die Kompatibilität der erläuterten Standards nach ITIL, COBIT und TOGAF mit den zukünftigen Anforderungen NIS-2 und dem neuen BSI-Standard 200-4 tiefgründig aus Sicht des IT-Managements zu untersuchen.

Zusammenfassend sind hiermit die Empfehlungen für die Forschung dargelegt, die sich nach der Theorie und der Analyse der empirisch erhobenen Daten ergeben haben, um durch weitere Forschungen die Probleme und Risiken aus der Problemstellung zukünftig weiter vermeidbar zu machen oder in ihren Auswirkungen zu minimieren. In die Lösungsansätze sind die in dieser Arbeit gemachten Erfahrungen eingeflossen.

Abschließend wird empfohlen, den hier angewendeten Forschungsansatz mit Experten-interviews und einer qualitativen Inhaltsanalyse ebenfalls mit Fokus auf andere Zielgruppen durchzuführen. Involviert waren behördenerfahrene IT-Dienstleister mit entsprechender Erfahrung auch im IT-Umfeld des öffentlichen Sektors, um die Forschungsfragen für dieses

Umfeld mit Blick auf die digitale Transformation zu beantworten. KRITIS-Betreiber oder ausgewählte Behörden mittels Fallstudien zu untersuchen oder qualitativ auszuwertende Interviews mit Fokus- oder Mitarbeitergruppen eines bestimmten Bereiches können Gegenstand weiterer Forschung sein.

2 Handlungsempfehlungen/Lösungsansätze Praxis

Für den praxisorientierten Anteil wurden fünf Empfehlungen als Erfolgsfaktoren abgeleitet, die sich aus der Darlegung der Ergebnisse ergeben haben. Die von den Experten geäußerten Empfehlungen wurden verglichen und zusammen mit den Sachständen und Hinweisen aus der Theorierecherche zu allgemeingültigen Handlungsempfehlungen aufbereitet. Die vorgestellten Standards zum Business Continuity Management haben ebenfalls zum Ziel, geeignete Methoden und Vorgehensweisen für die Einführung eines Business Continuity Managements zu erläutern. Von diesen Standards wird dahingehend abgegrenzt, dass die vorliegende Untersuchung eine zielgruppenorientierte Analyse und empirische Datenerhebung zu Grunde liegt. Allerdings wurden Teile der Standards inhaltlich in die Empfehlungen aufgenommen. Diese sind entsprechend gekennzeichnet und um den Mehrwert aus dieser Arbeit ergänzt.

Für eine übersichtliche Aufstellung und Beschreibung der Empfehlungen wurde in diesem Gestaltungsteil auf die erneute Ableitung und Schlussfolgerung zu den Sachständen und konkreten Empfehlungen, wie sie bereits in Kapitel III 3 erfolgt ist, verzichtet. Ergänzende Überlegungen für geeignete Handlungsempfehlungen und Lösungsansätze sind hier dokumentiert. Einleitend wird auf die Grundprinzipien im Business Continuity Management hingewiesen, wie den PDCA-Zyklus, das Risikomanagement oder die am Anfang stehende Business-Impact-Analyse, die sowohl von den Standards vorgesehen sind als auch von den Experten aus der Praxis nicht kritisiert wurden.

Für die darüber hinausgehenden Empfehlungen wurden auf Basis der Auswertung folgende Handlungsempfehlungen ausgearbeitet:

- Top down Awareness schaffen — Bezug: Kapitel III 2.2.1.3
- IT-Projekte mit BCM im Standard — Bezug: Kapitel III 2.2.1.1
- Digitalisierung vorteilhaft für BCM nutzen — Bezug: Kapitel III 2.2.3
- Digitale Souveränität wahren — Bezug: Kapitel III 2.2.1.3
- BCM-Standards kontextbezogen nutzen — Bezug: Kapitel III 2.2.2

Dieser Auflistung entsprechend gliedern sich die Kapitel in die so bezeichneten Unterkapitel. Die Reihenfolge (1) bis (5) stellt dabei keine Priorisierung oder Bewertung dar. Es bietet sich allerdings von der Logik her an, den ersten Punkt vorranging zu berücksichtigen, um die Voraussetzung für alle weiteren Maßnahmen zu schaffen. Vorab wird die Zielgruppe für diese Empfehlungen festgelegt.

2.1 Zielgruppe der Empfehlungen

Die Zielgruppe für die hier ausgearbeiteten Empfehlungen sind verschiedene Personengruppen mit unterschiedlichen Verantwortlichkeiten. Es wurden BCM-Experten im empirischen Teil involviert, die über Erfahrungen im Projektgeschäft zur Digitalisierung in Behörden verfügen. Vermeintlich kann angenommen werden, dass diese Klientel der BCM-Berater sich der nachfolgenden Empfehlungen grundsätzlich bewusst ist. Hier gilt es insbesondere für Personen, die sich neu in die Thematik einarbeiten, aktuelle und zielorientierte Hinweise zu geben, welche Defizite in der Praxis bestehen, um diese zu vermeiden. Gezielt angesprochen werden sollen auch IT-Projektleiter, um die Notwendigkeit und die Herausforderungen frühzeitig im Rahmen von neuen IT-Projekten zu erkennen. Für die in Unternehmen und Behörden ausgeprägte Rolle des CIO und CISO ergänzen die Empfehlungen die Verantwortlichkeiten im Bereich der IT-Sicherheit. Für die jeweils höchste Managementebene sollen die Empfehlungen ebenfalls hilfreich sein. Hierzu wird in Empfehlung (1) noch auf die Verantwortlichkeiten eingegangen. Mit dieser Erläuterung sind die Empfehlungen zusammenfassend fokussiert auf:

- BCM-Berater, -Verantwortliche, -Experten
- IT-Projektleiter insbesondere für Digitalisierungsprojekte im öffentlichen Dienst
- CIO, CISO, Führungskräfte im Bereich BCM und IT-Sicherheit
- Unternehmensleitungen, CEO, Behördenleitungen oder vergleichbar
- Wissenschaftler (als Ergänzung zu Kapitel IV 1)

2.2 Handlungsempfehlung (1): Top down Awareness schaffen

Wie schon Uhl und Loretan in ihrem Kapitel „Die Menschen sind entscheidend bei der Digitalisierung“ (2019, S. 2) beschrieben haben, sind es nicht die technischen Voraussetzungen und Analysen, sondern der Faktor Mensch ist das Wesentliche. Diese auf schweizerische KMU ausgerichtete Ausarbeitung betrachtet zwar nicht im Fokus das Business Continuity Management, aber eine Übertragung auf die hier analysierte Problemstellung ist uneingeschränkt möglich. Ergebnisoffen wurden die Experten zur Situation des Business Continuity Managements befragt und es wurde von Defiziten berichtet, die in der Analyse und nach direkten Aussagen unmittelbar auf eine fehlende Awareness schließen lassen. Neben dem geforderten allgemeinen Verständnis aller Mitarbeiter für digitale Prozesse und der IT-Sicherheit wurden auch explizit die Führungsebenen angesprochen, in denen nach Aussagen

der Experten die notwendige Aufmerksamkeit noch nicht vorhanden ist. Einzelaussagen dazu wurden bereits in der Ergebnisdarstellung erläutert.

Die vorangestellte Bezeichnung ‚top down' wurde hinzugefügt, um deutlich zu machen, dass sich zunächst die Führungsebenen klar zum Business Continuity Management bekennen müssen, da dort sowohl die strategischen Entscheidungen getroffen werden als auch die benötigten Ressourcen freigegeben werden können. Ausdrücklich anzusprechen sind auch die Ebenen darunter, da ebenfalls IT-Projektleitungen, Mitarbeiter, Kunden und Nutzer idealerweise die Notwendigkeiten verstehen, um etwaige Einschränkungen und Mehraufwände zu akzeptieren. Damit wird die erste Handlungsempfehlung hergeleitet: Die Aufrechterhaltung des Betriebes liegt in der Verantwortung der Führungskräfte. Mit der digitalen Transformation steigt die weitere Abhängigkeit von der IT. Durch ein rechtzeitig initiiertes Business Continuity Management können die Auswirkungen von IT-Notfällen entsprechend minimiert werden, damit die Handlungsfähigkeit auch in Extremsituationen weiterhin gegeben ist. Eine Vernachlässigung in diesem Bereich kann eklatante Auswirkungen haben. Für das hierfür notwendige Verständnis (die ‚Awareness') ist beginnend mit den Leitungsebenen grundsätzlich noch deutlicher zu sensibilisieren. Dies kann initial durch eine Information an die Geschäftsführungen und die Behördenleitungen zu der erwarteten NIS-2 Gesetzgebung erfolgen. Ergänzend können Schulungen der Mitarbeiter zu Digitalisierung, IT-Sicherheit und – für die relevanten Mitarbeiter – zum Business Continuity Management das notwenige Verständnis steigern. Neben diesen aus dem Aspekt ‚Awareness' abgeleiteten Ratschlägen wird auf das empfohlene „Digitale Mindset im Veränderungsprozess" (Hasenbein, 2020, S. 28) hingewiesen, um dauerhaft den zukünftigen Herausforderungen gerecht werden zu können.

2.3 Handlungsempfehlung (2): IT-Projekte mit BCM im Standard

Aus der Praxis wurde berichtet, dass aktuell noch immer IT-Großprojekte realisiert werden, bei denen die technische Ausfallsicherheit im Sinne eines Business Continuity Managements nicht berücksichtigt wird (Experte_14, 2022, Anlage III. 14). Mit der im Ergebnisteil dargestellten grundsätzlich unzureichenden Berücksichtigung eines Business Continuity Managements in der Praxis und der zu erwartenden hohen Anzahl von notwendigen IT-Projekten in der Zukunft kann empfohlen werden, bereits vor der Realisierung die BCM-Anforderungen zu berücksichtigen. Als Lösungsansatz kann hier eine zukunftsorientierte

Business-Impact-Analyse vorgenommen werden. Es wird davon ausgegangen, dass maximal tolerierbare Ausfallzeiten und Datenverluste auch vor einer Inbetriebnahme ermittelt werden können. Damit stehen, wie in der klassischen Business-Impact-Analyse für vorhandene IT-Services, die notwendigen Parameter zur Verfügung, um die Anforderungen an Redundanz-, Ersatz- oder Notfallsysteme frühzeitig in die Projektplanung einzubringen. Wenn zukünftig IT-Projekte nur dann realisiert werden, wenn vorab die Anforderungen aus Sicht des Business Continuity Managements in das Projekt eingebracht und ausreichend berücksichtigt sind, kann damit die Eintrittswahrscheinlichkeit einer Handlungsunfähigkeit aufgrund von IT-Störungen reduziert werden. Es ist also zusammenfassend empfehlenswert, geplante IT-Lösungen bereits vor Projektierung aus Sicht der Ausfallsicherheit dahingehend zu betrachten, dass das Unternehmen oder die Behörde auch bei Totalausfall dieser IT weiterhin handlungsfähig bleibt oder nur tolerierbare Ausfallzeiten erleidet. Durch die Einführung von BCM-Meilensteinen im IT-Projektmanagement kann diese Empfehlung in der Praxis umgesetzt werden. Projekt- und organisationsspezifische Meilensteine lassen sich hierzu auf Basis der Inhalte und der Struktur des in Kapitel II 2.1.5 erläuterten BSI-Standards 200-4 für die eigenen Bedürfnisse ermitteln.

2.4 Handlungsempfehlung (3): Digitalisierung vorteilhaft für das BCM nutzen

Interessanterweise lassen sich einige Herausforderungen der Digitalisierung in Bezug auf die Ausfallsicherheit mit den neuen Möglichkeiten der Digitalisierung lösen. So wurde in den Interviews erfragt, welche weiteren Schritte in die Digitalisierung gesehen oder erwartet werden. Hierbei gab es keine Tendenzen, dass die weitere Digitalisierung aus Sicht eines Business Continuity Managements nicht beherrschbar wäre. Besonders hervorzuheben ist hier erneut die Cloud-Technologie. Die Vorteile liegen nicht nur im Bereich einer einfachen Skalierung, der schnellen Nutzbarkeit oder eines verhältnismäßig einfacheren Bereitstellens von Applikationen. Ein schnelles Auslagern von Leistungen ist damit ebenfalls verbunden, wodurch das Business Continuity Management massiv unterstützt werden kann (Experte_10, 2022, Anlage III. 10). Kommerzielle Lösungen sind hier bereits vorhanden. Die Anbieter werben in ihren Cloud-Angeboten mit sogenannten Availabilty-Zonen, mit denen neben einer Performance-Verbesserung auch explizit die Notfallvorsorge adressiert wird. Hiermit wird deutlich, dass durch Nutzung von Teilen der Digitalisierung das Business Continuity

Management für ebendiese weitere Digitalisierung genutzt und empfohlen werden kann. Sparen Unternehmen und Organisationen allerdings an dieser Stelle und betreiben die Cloud-Lösung nur in einem Rechenzentrum, werden sie zwar digitaler und flexibler, allerdings aus Sicht des Business Continuity Managements nicht besser. Hierzu wurde indirekt bereits mit den Handlungsempfehlungen (1) und (2) sensibilisiert. Zusätzlich ist im Rahmen dieser Empfehlung auf die beschriebenen Gefahren hinzuweisen, die mit der Cloud-Nutzung verbunden sein können, beispielsweise ein Verlust oder eine Minderung der Kontrolle, der Souveränität oder der Unabhängigkeit. Wesentlich ist ein gewisses Umdenken dahingehend, dass für neue Herausforderungen eventuell auch neue Technologien zur Absicherung zu nutzen sind, statt an alten Absicherungsmaßnahmen festzuhalten.

Ein weiteres Beispiel für diese Empfehlung kann aus dem Bereich der Verschlüsselungstechnologien mit den Möglichkeiten der Ende-zu-Ende-Verschlüsselung abgeleitet werden. Die notwendige weitere Vernetzung und Integration unterschiedlicher Geräte, Endgeräte und Sensoren im Rahmen der Digitalisierung birgt grundsätzlich die Gefahr, dass Daten an vielen Stellen abgegriffen oder vernichtet werden. Ebenfalls erhöht es die Gefahr, dass von außen in die Systeme eingedrungen wird. Verschlüsselte Datenübertragung und verschlüsselte Speichersysteme können zwar bereits als Standard angesehen werden, für neue Anwendungsfälle bei der Digitalisierung können aber auch neue Verschlüsselungs-ansätze auf allen Ebenen zur Anwendung kommen, um beispielsweise aus Datenschutzsicht einen bestimmten Digitalisierungsschritt zu ermöglichen. Damit kann dann ein Business Continuity Management unterstützt werden, falls lediglich entsprechend sicher verschlüsselte Datenbestände gesichert, gespeichert, gehostet, verwaltet und ggf. ausgelagert werden sollen. Zusammenfassend wird empfohlen, bei der weiteren Digitalisierung nicht nur die neuen Möglichkeiten zu fokussieren, sondern im gleichen Maße innovative Optionen zur Absicherung der IT-Systeme mit zu betrachten.

2.5 Handlungsempfehlung (4): Digitale Souveränität wahren

Diversität ist aus der Perspektive des Business Continuity Managements bei der Digitalisierung nach Auswertung der Ergebnisse von hoher Bedeutung. Experten hatten am Beispiel der Cloud-Technologie eine Multi-Vendor-Strategie angesprochen, um mögliche Abhängigkeiten von nur einem Anbieter zu vermeiden. In diesem Zusammenhang wird auch auf die anzustrebende digitale Souveränität nach Lepping und Palzkill (2017, S. 24) hingewiesen, die

bei der Diskussion in Kapitel III 3.1.3 bereits zitiert und diskutiert wurde. Es ist für die digitale Transformation daher zu empfehlen, dass Unternehmen und Organisationen sich trotz der unvermeidlichen Abhängigkeit von IT-Dienstleistern, Produktanbietern, Providern und Partnern dieser Herausforderung bewusst sind. Dennoch ist eine vollständige Unabhängigkeit oder Autarkie schon heute und insbesondere mit der weiteren Digitalisierung als utopisch anzunehmen. Es ist nicht davon auszugehen, dass ein Unternehmen oder eine Behörde beispielsweise einen weltweiten Ausfall des Internets durch eigene IT-Infrastrukturen kompensieren kann. Von daher wurde die Empfehlung so formuliert, dass zumindest ein Bewusstsein hinsichtlich der Herausforderung bestehen sollte. Dann können aus Sicht des Business Continuity Managements dort, wo es möglich ist, entsprechende Risiken toleriert werden oder an den Stellen, wo eine Rückfallposition dringend notwendig wäre, muss auf alternative Lösungsansätze ausgewichen werden. In jedem Fall wird empfohlen, für geschäftskritische Prozesse keine Abhängigkeiten von nur einer Technologie, einem Anbieter, Provider oder Dienstleister einzugehen, um bei Ausfall dieser Services oder Vereinbarung nicht handlungsunfähig zu werden. Für die bereits genannte Cloud-Technologie bietet sich hier eine Multi-Vendor-Strategie an, die unter Umständen durch Notfallsysteme auf eigenständig betriebener Hard- und Software zu ergänzen ist.

Das ebenfalls bereits genannte Projekt GAIA-X hat hierzu in der sogenannten ‚Domäne Öffentlicher Sektor' einige Ziele formuliert, um explizit Abhängigkeiten zu minimieren. Die Entwicklungen des Projektes zu verfolgen und eine Nutzbarkeit im eigenen Bereich zu prüfen, wird daher grundsätzlich empfohlen. Damit wird diese Handlungsempfehlung wie folgt zusammengefasst: Je geschäftskritischer die im Rahmen der Digitalisierung zu modernisierenden Prozesse sind, desto sensibler sollte die Abwägung stattfinden, ob ein Unternehmen sich in unkontrollierbare Abhängigkeiten von IT-Systemen oder Anbietern begibt. Unter Umständen ist, wie es Experte_11 (2022, Anlage III. 11) bezeichnet hat, mit einem Verlust der „digitalen Rendite" zu rechnen. Gemeint sind hiermit die zu erzielenden Einsparpotenziale, die sich mit einer Digitalisierung ergeben können. Als Empfehlung kann damit insgesamt genannt werden, dass dem „Verlust eines Teils der Selbstbestimmung" (Lepping & Palzkill, 2017, S. 25) durch die weitere Digitalisierung entgegenzuwirken ist. Konkret können alle expliziten Veränderungen an der genutzten IT durch eine Vorher-/Nachher-Betrachtung aus dieser Perspektive untersucht werden.

2.6 Handlungsempfehlung (5): BCM-Standards kontextbezogen nutzen

Die Standards im Business Continuity Management wurden vorgestellt. Neben dem zum Zeitpunkt der Datenerhebung noch gültigen BSI-Standard 100-4 ‚Notfallmanagement' wurde der im Jahr 2023 in Kraft gesetzte Standard BSI 200-4 ‚Business Continuity Management' sowohl anhand der Literatur als auch mit den Feedbacks aus der Praxis analysiert. Es wurde in der Interpretation der Ergebnisse in Kapitel III 2.2.3 festgestellt, dass die Inhalte dieser Standards grundsätzlich mit dem empfohlenen Vorgehen aus der Praxis übereinstimmen. Kritisch wurde der jeweilige Umfang diskutiert und die Bedeutung hervorgehoben, zumindest klein anzufangen, bevor versucht wird, umfänglich die Standards in ein ganzes Unternehmen oder alle Abteilungen einer Behörde einzuführen. Als Erfolgsfaktor hat sich in der Analyse der Ergebnisse ein daran orientiertes Vorgehen ergeben. Auf dieser Basis wird empfohlen, die Umsetzung und Anwendung dieser Standards zunächst nur auf einzelne Bereiche zu beziehen. Über diese deutschen Standards hinaus wurden auch die Standards nach BCI GPG und die ISO-Norm 22301 aus der Praxis als zielführend für ein Business Continuity Management bewertet. Kritische Bewertungen aus der Praxis bezogen sich dabei auf den bereits diskutierten, teilweise hohen Umfang. Insbesondere bei der ISO-Zertifizierung ist darauf hinzuweisen, dass für einen nachhaltigen Effekt nicht lediglich die Zertifizierungsbestätigung das vorrangige Ziel darstellen soll, sondern das tatsächliche Berücksichtigen der Anforderungen und Veränderungen in den Unternehmen. Zusammenfassend lässt sich für diese Handlungsempfehlung schlussfolgern, dass ein Vorgehen nach BCM-Standards grundsätzlich als ein möglicher Erfolgsfaktor zu nennen ist. Auf Basis der Praxiserfahrungen wird empfohlen, diese Standards nicht zwingend direkt vollumfänglich einzuführen, sondern iterativ vorzugehen.

2.7 Strukturierte Darstellung der Handlungsempfehlungen nach TOM

Als eine wesentliche Aufgabe des Wissensmanagements für einen langfristigen Erfolg sieht Müller (2022, S. 57) das Erstellen einer Strategie auf den Ebenen Technik, Organisation und Menschen (TOM). Nachfolgend sind die Inhalte der Handlungsempfehlungen eins bis vier strukturiert in dieser Form dargestellt. Die fünfte Handlungsempfehlung als Erfolgsfaktor bezieht sich jeweils auf die Anwendung der referenziert genannten Standards der Theorie in der Praxis. Auf dieser Basis können je nach Behörde, Organisation oder IT-Dienstleister entsprechende Maßnahmenpakete entwickelt werden, mit denen das Business Continuity Management im Kontext der Digitalisierung gestärkt werden kann. Für eine übersichtliche Darstellung wurden die hier erläuterten Begriffe und Empfehlungen anschließend in der nachfolgenden Abbildung 46 mit einem kurzen Stichwort zur jeweiligen Ebene aufgenommen.

Technik

Aus technischer Sicht ist zunächst die Ausfallsicherheit der vorhandenen IT-Systeme zu prüfen und die maximal tolerierbaren Ausfallzeiten für die davon abhängigen Geschäftsprozesse sind zu ermitteln. Das kann im Rahmen der erläuterten Business-Impact-Analyse erfolgen. Bei neuen IT-Systemen und -Architekturen, die im Rahmen der weiteren Digitalisierung erst noch aus- oder aufgebaut werden, sind direkt die Anforderungen des Business Continuity Managements zu berücksichtigen (Handlungsempfehlung 2). Konkret sind entsprechende Redundanzen zu schaffen, mit denen bei Ausfall einzelner IT-Systemen die Arbeitsfähigkeit kontinuierlich aufrechterhalten werden kann. Von hoher Bedeutung ist die Cloud-Technologie, für die Multi-Cloud-Ansätze empfohlen werden. Zusätzlich ist hier die Wahrung der digitalen Souveränität (Handlungsempfehlung 4) ein kritischer Faktor. Gleichzeitig bietet die Cloud-Technologie technische Lösungen für die Anforderungen des Business Continuity Managements, beispielsweise eine ortsunabhängige Datenhaltung, mit der lokale Ausfälle kompensiert werden können (Handlungsempfehlung 3).

Damit ergeben sich für die Ebene Technik die nachfolgenden Stichworte: IT-Systeme bewerten (BIA), Redundanzen schaffen, sichere Cloud-Strategie, digitale Lösungen für BCM nutzen und neue IT-Systeme BCM-konform realisieren.

Organisation

Für den Bereich Organisation sind aus den Handlungsempfehlungen die nachfolgenden Punkte als Erfolgsfaktoren zu nennen. Solange noch keine Organisationselemente für das Business Continuity Management ausgeprägt sind, wurde empfohlen, hierfür entsprechende

Stellen zu schaffen. Sowohl der Betrieb als auch die IT-Projekte in der Organisation müssen mit diesen Bereichen zusammenarbeiten (Handlungsempfehlung 2), um stets die Anforderungen aus Sicht des Business Continuity Managements zu berücksichtigen. Hierzu sind entsprechende Zusammenarbeitsbeziehungen in der Organisation zu definieren.

Neben dieser Aufbauorganisation ist eine besondere Aufbauorganisation (BAO) konzeptionell festzulegen, wie es der BSI-Standard 200-4 vorsieht, um organisatorisch den Situationen eines IT-Notfalls gerecht werden zu können. Abhängigkeiten der Organisation von anderen Organisationen, Unternehmen und speziell von IT-Dienstleistern sind kritisch zu hinterfragen und auch für diese Beziehungen sind, soweit möglich, Redundanzen zu schaffen, um in einem definierten Umfang autark agieren zu können. Damit lassen sich für die Organisation folgende Stichpunkte nennen: BCM-Rollen ausprägen, BCM-Integration, BAO definieren, Autarkiefähigkeit.

Menschen

Diese Ebene wurde in der Handlungsempfehlung 1 als zentrale Komponente beschrieben. Es wird empfohlen, sowohl die ‚Awareness' für mögliche Gefahren im Bereich der IT als auch ein allgemeines ‚digitales Mindset' weiter auszuprägen. Dies kann durch Schulungen erfolgen und neben Fortbildungen zur IT-Sicherheit am Arbeitsplatz auch Weiterbildungen in neuen Digitalisierungstechnologien und damit verbundenen Veränderungen am Arbeitsplatz umfassen.

Auf Ebene der Geschäftsführungen und der Amtsleitungen ist für die Anforderungen und die Möglichkeiten des Business Continuity Managements zu sensibilisieren, um alle notwendigen Folgeaktivitäten zu ermöglichen. Als Stichworte für die nachfolgende Abbildung lassen sich zu dieser Ebene folgende Begriffe ableiten: Awareness steigern, Schulungen, digitales Mindset aufbauen, TOP-Management sensibilisieren. Für den zuletzt genannten Punkt wurde als Kurzbezeichnung in der nachfolgenden Abbildung der Begriff ‚Mgmt-Briefing' gewählt.

Alle zu den Ebenen abgeleiteten Stichworte sind in der nachfolgenden Abbildung dargestellt:

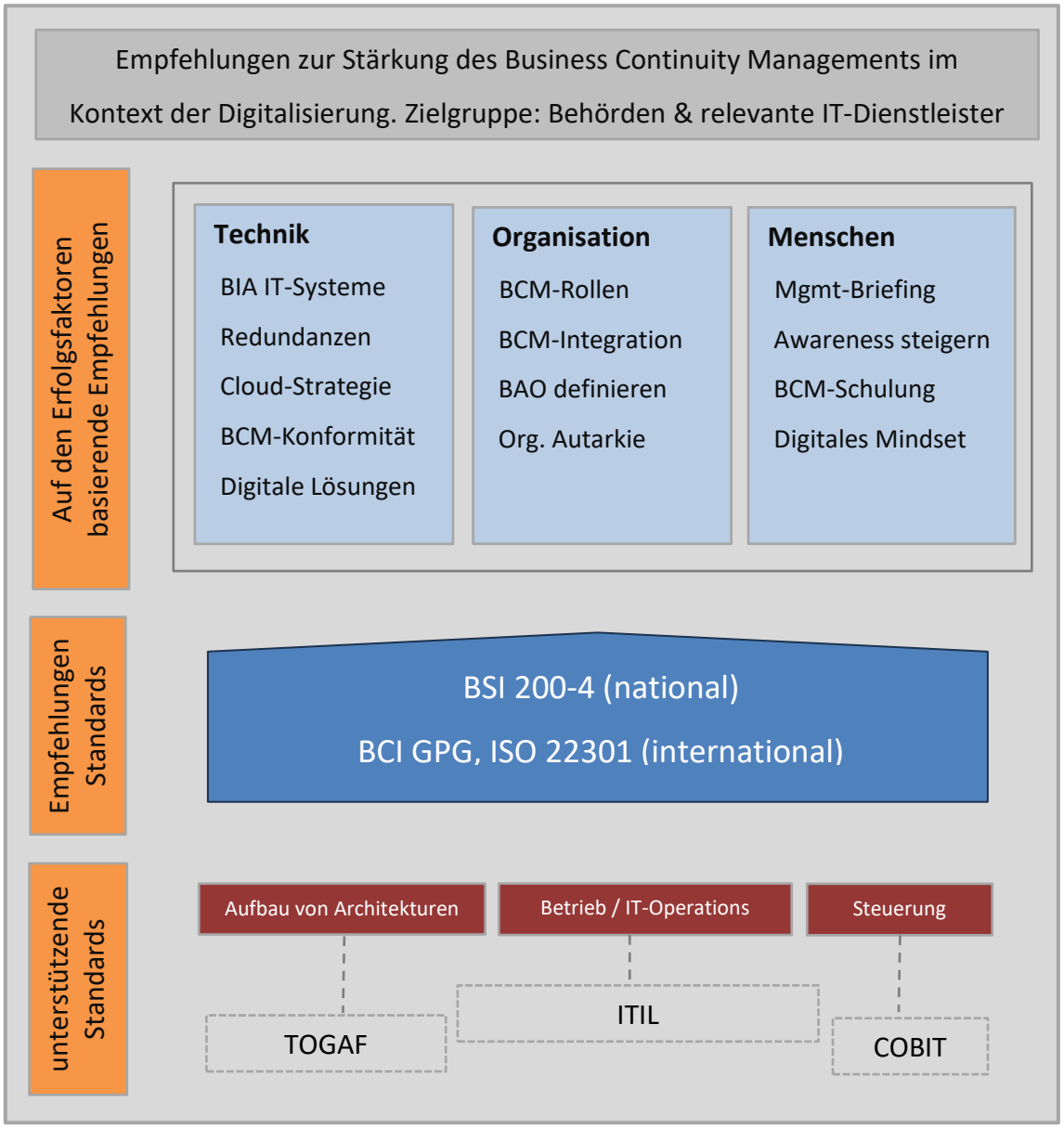


Abbildung 46 – Empfehlungen nach TOM mit Standards (Quelle: eigene Darstellung)

Damit sind die wesentlichen Erkenntnisse basierend auf den Erfolgsfaktoren dargestellt, um in der Zielgruppe das Business Continuity Management im Kontext der Digitalisierung stärken zu können. Für jede der Ebenen Technik, Organisation und Menschen wurden die herausgearbeiteten Stichworte genannt, ohne deren Berücksichtigung ein langfristiger Erfolg für eine sichere Digitalisierung gefährdet ist. Die betroffenen IT-Dienstleister und Behörden können auf dieser Basis für den eigenen Bereich die notwendigen Maßnahmen definieren. Als grundsätzlich empfehlenswerte Standards sind national für Deutschland der BSI-Standard 200-4 sowie international die BCI GPG und die ISO-Norm 22301 zu nennen. Damit sind geeignete Werkzeuge und Vorgehensweisen vorgeschlagen und die mindestens einzuhaltenden Standards festgelegt. Darüber hinaus finden sich in den etablierten Standards

TOGAF, COBIT und ITIL ebenfalls Hinweise und Anforderungen für ein Business Continuity Management, die, wenn diese Standards eingesetzt werden, bei entsprechender Berücksichtigung unterstützend eine entsprechend sichere Digitalisierung ermöglichen.
Nach dieser ergänzenden visualisierten und strukturierten Darstellung der Ergebnisse folgt im nächsten Kapitel die Zusammenfassung des Gestaltungsteils.

3 Zusammenfassung und Konklusion

Für die Forschung wurden drei Empfehlungen abgeleitet und vorgestellt. Für die Praxis konnten fünf Handlungsempfehlungen als Erfolgsfaktoren formuliert werden, die basierend auf den theoretischen Grundlagen und Analysen der Praxisberichte aktuell für die Zielgruppe von hoher Bedeutung sind. In diesem Kapitel wird, unterteilt nach Erkenntnissen und der Beantwortung der gestaltungsgeleiteten Fragestellung, der Gestaltungsteil IV zusammengefasst.

3.1 Erkenntnisse des Gestaltungsteils

Die wichtigsten Erkenntnisse und Ergebnisse dieses Teils werden in diesem Kapitel an der Erwartungshaltung zu Beginn der Dissertation gemessen. Es waren Handlungsempfehlungen als Erfolgsfaktoren zu formulieren, mit deren Berücksichtigung die in der Ausgangsplage und der Problemstellung dargestellten Situationen bei der weiteren Digitalisierung möglichst vermieden oder abgeschwächt werden können. Als zentrale Erkenntnis ist hervorzuheben, dass die Empfehlungen nicht in die Richtung gehen, wie sich im Detail ein Business Continuity Management bei der digitalen Transformation zur Anwendung bringen lässt. Stattdessen ist es aktuell noch notwendig, dass ein Business Continuity Management überhaupt zum Einsatz kommt und das Bewusstsein auf allen Ebenen geschärft wird. Die Sensibilisierung für die Themenfelder muss vorerst weiter ausgeprägt werden.

Konkretisiert wurde das Vorgehen durch die fünf Empfehlungen für die Praxis, die auf der nachfolgenden Abbildung in Stichworten skizziert sind:

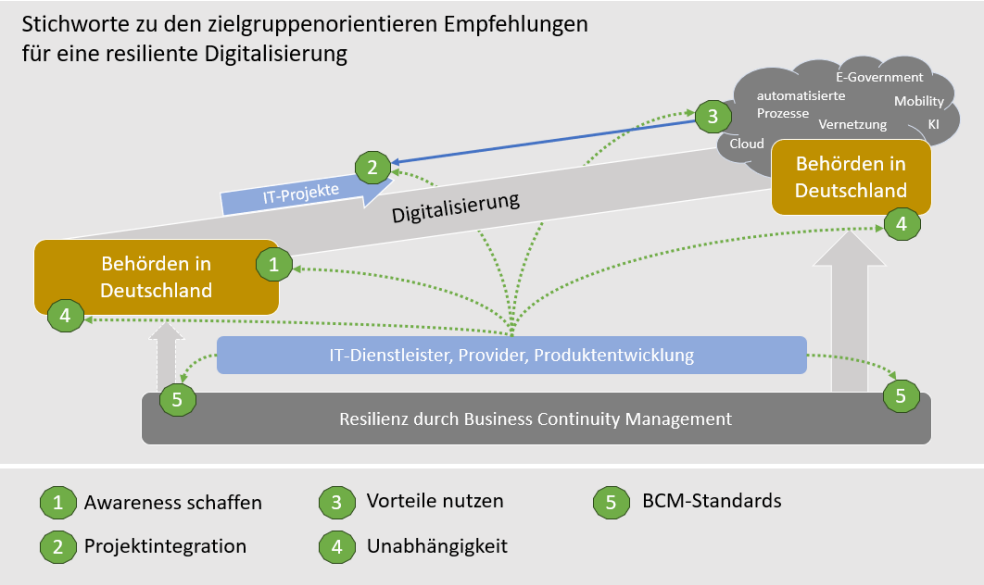


Abbildung 47 – Strukturierte Übersicht Praxisempfehlungen (Quelle: eigene Darstellung)

Die gestaltungsgeleitete Zielstellung wurde dadurch erreicht, dass die Hinweise aus der Theorie, den Vorgehensmodellen aus den Standards und dem empirisch erhobenen Material gemeinsam betrachtet wurden. Mit den Hinweisen zur Vorgehensweise aus der Theorie können bereits grundsätzliche Handlungsempfehlungen angenommen werden, die mit den Erfahrungen aus der Praxis und in Reflexion der Realität weiter ausgestaltet wurden. Dadurch konnten Handlungsempfehlungen und Lösungsansätze als Erfolgsfaktoren ausgearbeitet werden, die in dieser Form für die Zielgruppe einen Erkenntnisgewinn darstellen. Für die individuelle Maßnahmenentwicklung wurde mit der Abbildung 46 in Kapitel IV 2.7 eine praxisorientierte Unterstützung geschaffen, in der die aus den Erfolgsfaktoren abgeleiteten Empfehlungen strukturiert nach Technik, Organisation und Menschen dargestellt sind.

3.2 Beantwortung der gestaltungsgeleiteten Fragestellung

Das Hauptziel dieser Forschungsarbeit wurde im Einleitungsteil ausführlich dargestellt, mit dem zusammenfassend ein Beitrag geleistet werden soll, um die weitere Digitalisierung in Deutschland auch aus Sicht der IT-Notfall- und Katastrophenfallprävention möglichst effektiv zu unterstützen. Aus der Theorie und der Analyse vorhandener Studien im Bereich der Digitalisierung und des Business Continuity Managements konnten Fragestellungen abgeleitet werden, zu denen Antworten und Erfahrungen aus der Praxis erhoben wurden. Insbesondere die dort ermittelten Fragestellungen und Situationen wurden für die Ausarbeitung des Gestaltungsteils genutzt und damit konnte die Hauptzielstellung erreicht werden.

Die gestaltungsgeleitete Fragestellung aus Kapitel III 3.4 wurde dann in der Form beantwortet, dass konkrete Empfehlungen erstellt wurden, die in den vorangegangenen Kapiteln erläutert sind. Für den Bereich der Forschung wurden mit dem Erkenntnisgewinn über die relevanten Themenfelder weitere Forschungen empfohlen, die ebenfalls Forschungslücken schließen können, die sich mit der weiteren Digitalisierung zukünftig noch ergeben. Die Erfolgsfaktoren für die Praxis wurden in Form von Handlungsempfehlungen erstellt, mit deren Anwendung die Hauptzielstellung erreicht werden kann. Als erster und maßgeblicher Erfolgsfaktor wurde herausgearbeitet, dass zunächst noch die notwendige Awareness zu schaffen ist. IT-Projekte im Rahmen der weiteren Digitalisierung sollen zukünftig möglichst direkt das Business Continuity Management mit betrachten und neue Möglichkeiten der Digitalisierung bieten auch Chancen für eine effektive Notfallprävention. Eine besondere Bedeutung, der man sich bewusst sein muss, kommt der Unabhängigkeit und der Datensouveränität zu. Als letzter

Punkt wurde die gestaltungsgeleitete Fragestellung damit beantwortet, dass und wie die Anwendung von BCM-Standards für die Zielgruppe empfohlen werden kann.

Die ergänzenden gestaltungsgeleiteten Fragestellungen aus Kapitel III 3.4 bezüglich des Outsourcings von geschäftskritischen Prozessen und des Mindestmaßes an Notfallprävention wurden durch den Erfolgsfaktor ‚Digitale Souveränität wahren' in Kapitel III 2.5 beantwortet und technisch diskutiert.

V SCHLUSSTEIL

In diesem Teil wird die gesamte Arbeit rückblickend ab Beginn des Forschungsvorhabens betrachtet, wie Kornmeier (2021, S. 162) es für den Schlussteil einer wissenschaftlichen Arbeit empfiehlt. Dabei werden von den Ergebnissen lediglich die relevantesten Erkenntnisse kurz dargestellt, da für eine ausführliche Darlegung die vorangegangenen Kapitel vorgesehen waren (Kornmeier, 2021, S. 162).

1 Zusammenfassung und Fazit

Im Jahr 2020 haben wir weltweit und damit auch in deutschen Behörden die Auswirkungen der Coronapandemie erlebt. Petersen und Bluth (2020, S. 9) sprechen von einem Ausmaß an prognostizierbaren ökonomischen Schäden, wie es sie seit dem Ende des Zweiten Weltkrieges nicht mehr gegeben hat. Die Autoren sehen große Veränderungen des weltweiten Gesellschaftssystems und heben dabei die steigende Bedeutung der Digitalisierung hervor. Eine funktionierende IT-Infrastruktur kann in diesem Zusammenhang mittlerweile als „systemrelevant“ bezeichnet werden (Klös, 2020, S. 17). Bertscheck (2020, S. 653) spricht hierzu von einem krisenstabilisierenden Effekt der Digitalisierung.

Vor diesem Hintergrund wurde beginnend ab dem Jahr 2020 intensiv recherchiert, inwiefern digitale Lösungen zukünftig resilient betrieben werden können. Mit besonderem Blick auf sicherheitsrelevante Behörden, wie Polizei und Bundeswehr, sowie Betreiber kritischer Infrastruktur wird die besondere Relevanz der Thematik für unsere Sicherheit deutlich. Für außergewöhnliche Schadensgroßereignisse, beispielsweise die Zerstörung eines Rechenzentrums, sollen mit einem Business Continuity Management auch schwierigste Situationen beherrschbar bleiben. In der Literatur und in Studienergebnissen zeigte sich, dass ein durch ein effektives Business Continuity Management abgesicherter IT-Betrieb in Unternehmen und Behörden noch nicht überall Standard ist. Es stellt sich zusätzlich die Frage, ob wir uns zu sehr von der Technik abhängig machen. Die gemeinsame Betrachtung der Sicherheit, der Digitalisierung und des Managements in Unternehmen und Behörden kristallisierte sich als Forschungslücke heraus. Es wurden daraufhin Forschungsfragen formuliert und ein Forschungsdesign erstellt. Auf Basis der theoretischen Erkenntnisse folgte im Jahr 2022 die empirische Phase der Datenerhebung, in der BCM-Experten zu den herausgearbeiteten Themenfeldern interviewt wurden. Die Interviewteilnehmer verfügten sowohl über

Behördenerfahrung als auch über langjährige Erfahrungen im Bereich Business Continuity Management. Aus der Praxis wurde berichtet, dass Unternehmen und Behörden, die für eine Pandemie entsprechende Notfallpläne hatten, die Corona-Krise besser und schneller im Sinne der Aufrechterhaltung der Arbeitsfähigkeit bewältigen konnten. Ein zentraler Punkt war hier, die Mitarbeiter mit der benötigen Hard- und Software auszustatten, womit ein sicheres Arbeiten aus dem Homeoffice heraus genehmigt werden konnte. Gleichzeitig wurde in den Interviews von großen Defiziten im Bereich der Anwendung des Business Continuity Managements berichtet, welche die Erwartungshaltung nach der Literaturrecherche noch im negativen Sinn übertroffen haben. Kontextbezogen wurden Empfehlungen aus der Praxis formuliert und erläutert. Ende 2022 und Anfang 2023 folgte die qualitative Inhaltsanalyse des erhobenen Materials und mit den Ergebnissen unter Berücksichtigung der theoretischen Grundlagen konnten Handlungsempfehlungen ausgearbeitet werden.

Im Verlauf der Forschungsarbeit ergaben sich 2021 mit dem Ahrtal-Hochwasser und 2022 mit dem Ukrainekrieg erneut weitere unvorstellbare Situationen, die die Notwendigkeit von Notfallpräventionsmaßnahmen allgemein zeigten. Übertragen auf die Anforderungen an einen sicheren IT-Betrieb rückte damit das Business Continuity Management weiter in den Fokus des IT-Managements. Aus dem empirischen Teil lässt sich schließen, dass durch diese Krisen eine erhöhte Aufmerksamkeit für eine Resilienz in den Führungsebenen von Behörden und Unternehmen entstanden ist.

Zusammen mit den herausgearbeiteten relevanten Aspekten der Digitalisierung wurde die aktuelle Situation des Business Continuity Managements abgeleitet. Als Fazit der gesamten Arbeit kann Folgendes festgehalten werden: Mit der weiteren Digitalisierung in sicherheitskritischen Bereichen steigt auch die Bedeutung für ein effektives Business Continuity Management deutlich. In der Praxis ist das Business Continuity Management in Deutschland noch nicht etabliert, allerdings steigt die Awareness durch aktuelle Krisen. Im Jahr 2023 wurde der neue BSI-Standard 200-4 ‚Business Continuity Management' in Kraft gesetzt, womit mehrere Einflussfaktoren entstanden sind, um sich mit der weiteren Digitalisierung möglichst resilient aufzustellen. Ziel ist es, dass sich zukünftig IT-Katastrophenfälle, wie in der Ausgangslage geschildert, nicht wiederholen. Es sind weitere Aktivitäten sowohl bei der wissenschaftlichen Grundlagenarbeit als auch in der praktischen Umsetzung notwendig. Fundierte Handlungsempfehlungen liegen als Ergebnis dieser Arbeit vor. Das nächste Kapitel fasst die Erkenntnisse und Ergebnisse zusammen, bevor im dritten Kapitel ein abschließender Ausblick gegeben wird.

2 Ergebnisse und Erkenntnisse

In diesem Kapitel werden die relevantesten Ergebnisse, die auf den Erkenntnissen des theoretischen und des empirischen Teils basieren, zusammengefasst. Damit wird abschließend der Mehrwert dargestellt, der für die Forschung und für die Praxis entstanden ist.

Das bestimmende Ergebnis für beide Bereiche ist, dass die notwendige Awareness für ein funktionierendes Business Continuity Management bei der weiteren Digitalisierung von erheblicher Bedeutung ist und zunehmend relevanter wird. Durch die Erstellung und die Erprobung geeigneter Notfallplänen kann vermieden werden, dass bei einem Ausfall der IT die hoheitliche Aufgabenwahrnehmung für die innere und die äußere Sicherheit in Deutschland gefährdet wird. Das konnte bereits auf Basis der Literaturrecherche herausgearbeitet werden und wurde durch die Befragung von Experten um praxisorientierte Detailaspekte angereichert. Es gilt vor allem, die neue Erkenntnis zu berücksichtigen, dass die Zielgruppe sich der Grundsätze zwar bewusst ist, aber ein ausreichender Einbezug von Absicherungsmaßnahmen bislang nicht im möglichen oder notwendigen Umfang erfolgt, wie die Experten berichtet haben.

Für die beiden Bereiche Forschung und Praxis wird die fehlende Notfallprävention aktuell nicht als technische Herausforderung im Rahmen der Digitalisierung angesehen. Es sind das Unternehmens- und das IT-Management, bei denen zunächst ein deutlich höheres Engagement für ein Business Continuity Management erreicht werden muss. Diese grundlegende Erkenntnis impliziert die weiteren Ergebnisse, die in den Folgekapiteln in die beiden Bereiche Forschung und Praxis aufgeteilt sind.

2.1 Wichtige Ergebnisse und Erkenntnisse für die Forschung

Für die Forschung ist, wie im Einleitungsteil bereits vorgestellt, von Interesse, wie sich die relevanten Themenfelder Digitalisierung, Management und Sicherheit beeinflussen und welche Wechselwirkungen hier bestehen. Es wurde herausgearbeitet, dass durch die weitere Digitalisierung nicht automatisch mit sichereren IT-Systemen zu rechnen ist, die eine Resilienz von Behörden, Betreibern kritischer Infrastruktur, Institutionen oder Partnerunternehmen erhöhen. Entscheidend ist hier zunächst das Management, das für die weitere Digitalisierung noch mehr den Sicherheitsaspekt für einen resilienten Betrieb berücksichtigen muss, damit keine Handlungsunfähigkeit durch einen Kontrollverlust droht. Im Allgemeinen kann davon

ausgegangen werden, dass die Ausfallsicherheit und die Robustheit von IT-Systemen aktuell nicht in dem Maße ausgeprägt sind, wie es aus Sicht eines Business Continuity Managements vorzusehen wäre. Forschungen zur Weiterentwicklung und Analyse des strategischen und operativen Managements müssen zukünftig mehr das IT-Management berücksichtigen. Es liegt im Verantwortungsbereich des Managements, bei der weiteren Digitalisierung für IT-Notfallsituationen Vorsorgen zu treffen, die entweder mit ebenfalls neuen Digitalisierungstechnologien oder mit Hilfe manueller Alternativen sicherzustellen sind. Im Speziellen ist für die Forschung relevant, dass auch dann, wenn Notfalloptionen zur Verfügung stehen, diese in der Praxis nicht immer genutzt werden. Es besteht eine Diskrepanz zwischen den quantitativen Erhebungen mit Selbstauskünften, ob ein IT-Notfallmanagement vorhanden ist, und den Ergebnissen der vorliegenden qualitativen Untersuchung. Für weitere Forschungen ist es von hoher Relevanz, wenn einerseits Unternehmen selbst erklären, ein Notfallmanagement zu haben, und andererseits Experten die Vorsorgemaßnahmen überwiegend als nicht ausreichend bewerten.

Die Standards für ein Business Continuity Management entwickeln sich weiter. Im Jahr 2023 wurde vom BSI ein neuer Standard in Kraft gesetzt. Auch wenn bereits vorab eine Version dazu veröffentlicht wurde, können eine fundierte Prüfung und eine Adaption der Anforderungen auf Behörden und Unternehmen erst beginnend mit dem Jahr 2023 erfolgen. Laufende und geplante Untersuchungen zur IT-Sicherheit und zur Digitalisierung in Deutschland müssen berücksichtigen, dass sich die Behörden und Unternehmen erst seit der finalen Veröffentlichung dem neuen Standard widmen werden.

Die konkrete Forschungslücke bestand aus der gemeinsamen Betrachtung der weiteren Digitalisierung und der notwendigen Maßnahmen aus Sicht des Business Continuity Managements, konzentriert auf die Zielgruppe der behördenerfahrenen IT-Dienstleister. Von einer Etablierung kann bei dieser Zielgruppe explizit bislang noch nicht gesprochen werden, so dass bei wissenschaftlichen Erhebungen aktuell nur von einer Bestätigung der in Deutschland noch rückständigen Digitalisierung auszugehen ist. Zusammen mit dem im vorherigen Absatz genannten neuen Standard wird die aktuelle Dynamik, der sich die Wissenschaft stellen muss, deutlich, um die weiteren Entwicklungen in der digitalen Transformation unterstützen zu können. Die Studie hat zudem ergeben, dass die Cloud-Technologie als ein zentraler Punkt der Digitalisierung aus Sicht des Business Continuity Managements noch zu diskutieren ist. Neben positiven Aspekten bei der Ausfallsicherheit wurden auch Gefahren genannt. Damit hat die Empirie die theoretischen Erkenntnisse

insbesondere für die Zielgruppe der Behörden und der behördenerfahrenen IT-Dienstleister geschärft. Konkret benannt werden können hierzu rechtliche Fragen, Souveränität sowie die Unabhängigkeit von Herstellern als offene Handlungsfelder für die Forschung.

Als neue Erkenntnis ist das von den Experten genannte Defizit im Bereich des digitalen Verständnisses bei der Zielgruppe anzusehen. Es wurde damit nachvollziehbar erklärt, weshalb die Etablierung eines Business Continuity Managements in Deutschland noch rückständig ist. Hieraus lässt sich schlussfolgern, dass die in der Ausgangslage dargestellten Situationen ursächlich in einem fehlenden Gesamtverständnis begründet sind. Lediglich zu versuchen, ein Business Continuity Management einzuführen, ohne diesen Gesamtzusammenhang zu berücksichtigen, erscheint nicht zielführend.

Zusammenfassend sind es nicht die technischen Erkenntnisse, mit denen die Forschungslücke im Ergebnis zu schließen war. Vielmehr sind Anpassungen im IT-Management von Unternehmen und Behörden der entscheidende Erfolgsfaktor. Unterstützt durch Detailausführungen zum Cloud-Computing, das GAIA-X-Projekt und die hier im Gestaltungsteil ausformulierten Empfehlungen zur Nutzung der Standards kann die digitale Transformation damit wissenschaftlich fundiert weiterentwickelt werden. Allerdings bleibt es für die Forschung eine Herausforderung, bei Weiterentwicklungen in der Digitalisierung stets zeitgerecht vor der Markteinführung und der Nutzung neuer Technologien verifizierte Absicherungsmaßnahmen empfehlen zu können.

2.2 Wichtige Ergebnisse und Erkenntnisse für die Praxis

Die wichtigsten Erkenntnisse für die Praxis sind, dass sich das Business Continuity Management als Teil des IT-Managements in Deutschland noch nicht etabliert hat. Hier muss aktiv auf das Management zugegangen werden, um entsprechende Überzeugungsarbeit zu leisten. Es kommen mit der weiteren Digitalisierung neue Gefahren, die die Handlungsfähigkeit von Behörden und Unternehmen massiv einschränken können. Auch für die klassischen Schadensgroßereignisse, wie Brände oder Naturkatstrophen, sind grundsätzlich keine ausreichenden Vorkehrungen getroffen, um die Auswirkungen gering zu halten. Die Beispiele aus der Ausgangslage haben dies deutlich gezeigt. Das Defizit wurde durch die Experten bestätigt und mit einer allgemein noch nicht ausreichend vorhandenen Sensibilität für ein Business Continuity Management erklärt. Von besonderer Bedeutung für die Praxis ist

die gestiegene Eintrittswahrscheinlichkeit derartiger Ausfälle und neuer Bedrohungen durch die weitere Digitalisierung. Jedes Unternehmen kann hiervon unmittelbar betroffen sein.
Durch die Coronapandemie, die Ahrtal-Hochwasserkatastrophe und den Ukrainekrieg sind mehrere Situationen eingetreten, die zeigen, wie auch als unwahrscheinlich anzunehmende Risiken Realität werden können. Wenn diese Situationen auch nicht unmittelbar IT-relevant waren, bieten sie aktuell eine Chance zur Sensibilisierung des Managements. Behörden und Unternehmen müssen sich grundsätzlich auch auf Risiken vorbereiten, deren Eintrittswahrscheinlichkeit als sehr gering angenommen wird. Die allgemeine Awareness für ein Business Continuity Management steigt derzeit laut den Experten. In der Praxis kann diese Tendenz genutzt werden, um nun ein Business Continuity Management bei allen weiteren Schritten zur Digitalisierung zu berücksichtigen und es rechtzeitig in das Projektgeschäft einzubringen. Damit wären die Beispiele aus der Ausgangslage vermeidbar gewesen, wie in den nächsten Absätzen erläutert wird.
Als weiteres bedeutsames Ergebnis wurde festgestellt, dass die Digitalisierung neben den Risiken auch Chancen für das Business Continuity Management bietet. Für viele Szenarien sind technische Lösungen bereits vorhanden, sie werden in der Praxis aber nicht genutzt. Insgesamt sind die fünf formulierten Handlungsempfehlungen als die zentralen Ergebnisse für die Praxis anzusehen. Wie damit die anfänglich dargestellte Problemstellung lösbar geworden ist, lässt sich wie folgt nachvollziehen. Mit der notwendigen Awareness (Handlungsempfehlung 1) im Rahmen eines Risikomanagements für mögliche Datenzerstörungen durch Brände oder Krytoptrojaner, wären die Gefahren rechtzeitig bewertet worden und mit Gegenmaßnahmen hätten die Auswirkungen geringgehalten werden können. Beim Auf- und Ausbau der IT in den betroffenen Behörden, beispielsweise bei einem Projekt zu Verlagerung der Daten zu einem Cloud-Anbieter, wären Datenverlustrisiken spätestens im IT-Projektmanagement mitberücksichtigt (Handlungsempfehlung 2). Im Fall des Rechenzentrumbrandes ist zu sehen, dass technische Backup-Lösungen vorhanden waren und dort direkt hätten mit beauftragt werden können (mittelbar Handlungsempfehlung 3). Insgesamt unterstützt auch das Bewusstsein für eine Datensouveränität (Handlungsempfehlung 4) die Problemlösung, da es ganzheitlich das Verständnis hinsichtlich der Bedeutung der elektronischen Datenbestände für die Arbeitsfähigkeit von Unternehmen und Behörden erhöht. Mit den Standards (Handlungsempfehlung 5) stehen schon seit vielen Jahren Vorgehensweisen und Empfehlungen zur Verfügung, wie sich ein Business Continuity Management grundsätzlich in Unternehmen einführen lässt. Die dort vorgesehenen

Praktiken, wie der PDCA-Zyklus und eine Business-Impact-Analyse, gelten bereits aus der Literatur und nach den hier erhobenen empirischen Daten als empfehlenswert für den Aufbau eines effektiven Business Continuity Managements, insbesondere um die weitere digitale Transformation sicher zu gestalten.

3 Ausblick

Abschließend wird in diesem Kapitel ein Ausblick aus Sicht der Praxis und für die weitere Forschung gegeben. Eine allgemeine fachliche Prognose, wie sich das Business Continuity Management und die weitere Digitalisierung entwickeln können, wurde im empirischen Teil bei den Experten erfragt. Deren Einschätzung ist in Teil III Kapitel 2.2.4 dargestellt. Darüber hinaus wird hier ein genereller Ausblick gegeben, der darauf aufbauend zusätzlich technologische Entwicklungsprognosen berücksichtigt und die wissenschaftlichen Handlungsfelder betrachtet.

3.1 Praxisausblick

Das untersuchte Business Continuity Management muss und wird in der Praxis einen höheren Stellenwert erlangen, damit IT-Notfälle zukünftig nicht zunehmend Behörden, Unternehmen oder Betreiber kritischer Infrastrukturen kurzfristig oder dauerhaft handlungsunfähig machen. Die Erkenntnisse machen den Sachstand hierzu transparent und die Empfehlungen bieten eine fundierte Unterstützung, um dieses Ziel zu erreichen. Es müssen zunächst die Voraussetzungen in den Bereichen Personal und Organisation sowie bezüglich benötigter Ressourcen geschaffen werden. Weitere Digitalisierungsprojekte sind zukünftig auch stets aus Sicht der Resilienz des Unternehmens zu bewerten. Nach einer Einführung der notwendigen BCM-Lösungen in Behörden und Unternehmen sollten diese dauerhaft betrieben und regelmäßig beübt, aktualisiert und hinterfragt werden. Dadurch wird sich die Thematik der Resilienzfähigkeit insbesondere für die IT-Unterstützung der Prozesse in der Praxis allgegenwärtig ausprägen.

Ob und wie sich weltweite oder europäische Lösungen und Standards in der Praxis etablieren werden, bleibt zwar einerseits abzuwarten, andrerseits können sie auch nur aus der Praxis heraus umgesetzt werden. Hier wird als Ausblick erwartet, dass zukünftig Teile der Anforderungen des Business Continuity Managements durch neue Lösungen unterstützt werden. Unternehmen und Behörden können sich aktiv an der Weiterentwicklung beteiligen und ihre Anforderungen einbringen. Dennoch ist davon auszugehen, dass eine gewisse Autarkie zur Aufrechterhaltung der Handlungsfähigkeit auch in IT-Notfallsituationen in der Praxis wieder an Bedeutung gewinnen wird. Das betrifft nicht nur die in dieser Arbeit fokussierten behördenerfahrenen IT-Dienstleister, sondern ist gleichermaßen für alle Unternehmen und Organisationen sowohl national als auch international relevant. Es wird

erwartet, dass damit die weitere Digitalisierung sicher gestaltet werden kann und keine neuen Unternehmensrisiken entstehen, die nicht beherrschbar sind.
Die EU fordert die Umsetzung der NIS2-Direktive in nationales Recht bis zum 17. Oktober 2024 (EU, 2022b, S. 9). Damit ist zusätzlich davon auszugehen, dass durch die nationale Gesetzgebung zur Umsetzung dieser europäischen Vorgaben ab dem Jahr 2024 die gesamte Thematik in der IT-Branche eine erhöhte Aufmerksamkeit erfahren wird und Business-Continuity-Management-Praktiken in der Praxis an Bedeutung gewinnen werden.

3.2 Forschungsausblick

Diese Arbeit hat gezeigt, dass im Bereich des Business Continuity Managements mit einer qualitativen Inhaltsanalyse Sachstände und Zusammenhänge zur IT-Notfallprävention hinterfragt und analysiert werden können, die durch eine quantitative Erhebung und Selbstauskünfte in dieser Tiefe nicht möglich sind. Anschließende Forschungsvorhaben können aufbauend auf dieser Methode gezielt weitere Wissenslücken schließen. Es bietet sich an, sowohl quantitative Erhebungen zur Digitalisierung und dem damit zusammenhängenden IT-Notfallmanagement durchzuführen als auch im Detail qualitativ die Effektivität der ergriffenen Maßnahmen zu untersuchen.
Der im Jahr 2023 veröffentliche BSI-Standard kann den Anlass dazu geben, die Einführung des neuen Standards in der öffentlichen Verwaltung, bei Unternehmen der kritischen Infrastruktur und den relevanten IT-Dienstleistern kritisch zu hinterfragen oder wissenschaftlich zu begleiten. Interessant wäre es, herauszufinden, ob und wie sich die länderspezifischen Unterschiede im europäischen und weltweiten Vergleich erklären lassen. Neben der DESI-Studie zur Digitalisierung können hier aus Sicht des Business Continuity Managements auch die Anzahl der ISO-22301-Zertifizierungen quantitativ und die Beweggründe für eine Zertifizierung qualitativ weiter erforscht werden. Dadurch lassen sich Tendenzen erkennen, Empfehlungen formulieren und Rückschlüsse auf die weitere Digitalisierung ziehen.
Ebenfalls wird erwartet, dass bei Eintritt weiterer IT-Katastrophen diese wissenschaftlich begleitet und analysiert werden, um für die Zukunft Maßnahmen für eine noch resilientere Digitalisierung vorschlagen zu können. Idealerweise werden potenzielle Notfallszenarien vor Eintritt analysiert und Lösungen können rechtzeitig berücksichtigt werden. Die vorliegende Arbeit ergänzt damit die Grundlagen der Standards im Business Continuity Management um

die aktuelle Situation. Die Handlungsempfehlungen für die Forschung sehen dabei vor, dass die drei Themenfelder Sicherheit, Digitalisierung und IT-Management jeweils auch im Zusammenhang betrachtet werden, um sich so den neuen Herausforderungen der Resilienz durch die steigende Abhängigkeit von der IT stellen zu können. Damit kann die fortgesetzte Digitalisierung in den deutschen Behörden zukünftig weiter zielorientiert und wissenschaftlich fundiert unterstützt werden. Es wird empfohlen, die Entwicklungen im Bereich der KI, das GAIA-X-Projekt und noch kommende Digitalisierungstrends stets frühzeitig auch aus Sicht der Resilienz mit zu bewerten und wissenschaftlich fundiert zu begleiten.

4 Verzeichnisse

4.1 Literaturverzeichnis

Abolhassan, F. (2016). *Was treibt die Digitalisierung? Warum an der Cloud kein Weg vorbeiführt.* Wiesbaden: Springer Gabler. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-10640-9

Adelskamp, P. (2018). Smart-City-Herangehensweisen einzelner Kommunen, Düsseldorf. In Heuermann, R., Tomenendal, M. & Bressem, C. (Hrsg.), *Digitalisierung in Bund, Ländern und Gemeinden* (S. 69–75). Berlin: Springer Gabler. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-54098-5

Ahlemann, F. (2018). IT Expertise Everywhere: Why the Single IT Department will Soon be History. In Urbach, N., Ahlemann F., Böhmann T., Drews, P., Brenner, W., Schaudel F. & Schütte, R. (Hrsg.), *The Impact of Digitalization on the IT Department.* Business & Information Systems Engineering, (61), 123–131. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1007/s12599-018-0570-0

Allweyer, T. (2020). IT-Management. Grundlagen und Perspektiven für den erfolgreichen Einsatz von IT im Unternehmen. Norderstedt: Books on Demand

Alvesson, M. & Sandberg, J. (2013). *Constructing Research Questions: Doing Interesting Research*. London: SAGE.

Baldwin, S. (2019). Business Continuity Management as an operational risk service provider: An approach to organisational resilience. *Journal of Business Continuity & Emergency Planning.* (13(2)), 102–110. Zugriff am 05.03.2024. Verfügbar unter: https://www.researchgate.net/publication/337651805

Baumgarth, C. & Evanschitzky, H. (2009). Erfolgsfaktorenforschung. In Baumgarth, C., Eisend, M., Evanschitzky, H. (Hrsg.). *Empirische Mastertechniken. Eine anwendungsorientierte Einführung für die Marketing- und Managementforschung* (S. 235–261). Wiesbaden: Gabler Verlag. Zugriff am 22.07.2024. Verfügbar unter: https://doi.org/10.1007/978-3-8349-8278-0

Bartsch, M. & Frey, S. (2017). *Cyberstrategien für Unternehmen und Behörden*. Wiesbaden: Springer Vieweg. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-16139-2

Baumann, S. & von Rössing, R. (2018). Business Continuity Management – unverzichtbares Element eines angemessenen Risikomanagements. In Hunziker, S. & Meissner, J. O. (Hrsg.). *Ganzheitliches Chancen- und Risikomanagement: Interdisziplinäre und praxisnahe Konzepte* (S. 163–194). Wiesbaden: Springer Gabler. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-17724-9

Baur, N. & Blasius, J. (2022). *Handbuch Methoden der Empirischen Sozialforschung* (3., vollständig überarbeitete und erweiterte Auflage). Wiesbaden: Springer VS. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-37985-8

BCI - Business Continuity Institute (2013). *Good Practice Guidelines 2013 Global Edition Edited Highlights*. Zugriff am 04.03.2024. Verfügbar unter: https://www.thebci.org/static/uploaded/5c0205f3-a9ff-4f81-9695c3813b674a3b.pdf

BCI - Business Continuity Institute (2018). *Good Practice Guidelines 2018 LITE*. Zugriff am 14.07.2023. Verfügbar unter: https://www.thebci.org/resource/gpg-lite-2018-edition.html

Bendiek, A. & Stürzer, I. (2022). Die digitale Souveränität der EU ist umstritten: warum die EU dennoch im EU-US Handels- und -Technologierat auf den Brüssel-Effekt setzen sollte. *SWP-Aktuell*, (30/2022), 1–8. Berlin: Stiftung Wissenschaft und Politik. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.18449/2022A30

Bengler, K. & Schmauder, M. (2016). Digitalisierung. *Zeitschrift für Arbeitswissenschaft*, (70(2)), 75–76. Zugriff am 04.03.2024. Verfügbar unter: https://link.springer.com/article/10.1007/s41449-016-0021-z

Bernhardt, J. & Steininger, M. (2021). Gaia-X - Wegbereiter einer digitalen und wettbewerbsfähigen Zukunft der EU? *ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München*, (74(05)), 66–71. Zugriff am 07.03.2024. Verfügbar unter: https://www.econstor.eu/handle/10419/250769

Bertschek, I. (2020). Digitalisierung - der Corona-Impfstoff für die Wirtschaft. *Wirtschaftsdienst*, (100), 653–656. Zugriff am 07.03.2024. Verfügbar unter: https://doi.org/10.1007/s10273-020-2732-1

Bitkom e. V. (2020). *Spionage, Sabotage Und Datendiebstahl - Wirtschaftsschutz in der vernetzten Welt*. Zugriff am 04.03.2024. Verfügbar unter: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

Bitkom e. V. (2021). *Sicherheitsmaßnahmen 2021. Wie sich Deutschlands Unternehmen gegen Diebstahl, Spionage und Sabotage schützen.* Zugriff am 04.03.2024. Verfügbar unter: https://www.bitkom.org/sites/main/files/2021-10/bitkom-charts-sicherheit-in-der-dt.-wirtschaft-14-10-2021_0.pdf

Bitkom e. V. (2022a). *Wirtschaftsschutz 2022*. Zugriff am 03.03.2024. Verfügbar unter: https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf

Bitkom e. V. (2022b). *Rechenzentren in Deutschland*. Zugriff am 03.03.2024. Verfügbar unter: https://www.bitkom.org/sites/main/files/2022-02/10.02.22-studie-rechenzentren.pdf

Bizer, J. (2019). Die Digitalisierung in der Verwaltungspraxis – wir sind weiter als gedacht, In Schmid, A. (Hrsg.), *Verwaltung, eGovernment und Digitalisierung: Grundlagen, Konzepte und Anwendungsfälle* (S. 115–126). Wiesbaden: Springer Vieweg. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10. 1007/978-3-658-27029-2

BMWi - Bundesministerium für Wirtschaft und Energie (2021). *Digitalisierung in Deutschland - Lehren aus der Corona-Krise.* Zugriff am 01.03.2024. Verfügbar unter: https://www.bmwk.de/Redaktion/DE/Publikationen/Ministerium/Veroeffentlichung-Wissenschaftlicher-Beirat/gutachten-digitalisierung-in-deutschland.pdf

Bogner, A. & Menz, W. (2009). Experteninterviews in der qualitativen Sozialforschung. In Bogner, A., Littig, B. & Menz, W. (Hrsg.), *Experteninterviews. Theorien, Methoden, Anwendungsfelder* (3., grundlegend überarbeitete Auflage) (S. 7–34 & S. 61–98). Wiesbaden: VS Verlag für Sozialwissenschaften. Zugriff am 03.03.2024. Verfügbar unter: https://link.springer.com/book/9783531162591

Bogner, A., Littig, B. & Menz, W. (2014). *Interviews mit Experten: Eine praxisorientierte Einführung.* Wiesbaden: Springer VS. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-531-19416-5

Brauner, F. & Fiedrich, F. (2018). Kritische Infrastrukturen und Business Continuity Management. In Reuter, C. (Hrsg.), *Sicherheitskritische Mensch-Computer-Interaktion* (S. 207–228). Wiesbaden: Springer Vieweg. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-19523-6

BSI - Bundesamt für Sicherheit in der Informationstechnik (2008). *BSI-Standard 100-4 – Notfallmanagement*. Zugriff am 03.03.2024. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf

BSI - Bundesamt für Sicherheit in der Informationstechnik (2019). *Die Lage Der IT-Sicherheit in Deutschland 2019*. Zugriff am 03.03.2024. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.html

BSI - Bundesamt für Sicherheit in der Informationstechnik (2022). *Die Lage der IT-Sicherheit in Deutschland 2022*. Zugriff am 03.03.2024. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf

BSI – Bundesamt für Sicherheit in der Informationstechnik (2023). *Business Continuity Management BSI-Standard 200-4*. Köln: Reguvis Fachmedien. Zugriff am 03.03.2024. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf

Cornish, M. (2011). Business Continuity Management Methodology. In Hiles, A. (Hrsg.), *The Definitive Handbook of Business Continuity Management* (3. Auflage) (S. 121–135). Hoboken: John Wiley & Sons Inc.

Demary, V., Engels, B., Röhl, K.-H. & Rusche, C. (2016). Digitalisierung und Mittelstand: eine Metastudie. *IW-Analysen*, (109). Köln: Institut der deutschen Wirtschaft. Zugriff am 04.03.2024. Verfügbar unter: https://www.econstor.eu/handle/10419/157156

DIN EN ISO 22301 (2020), Deutsches Institut für Normungsverfahren e.V.*, Sicherheit und Resilienz - Business Continuity Management System - Anforderungen (ISO 22301:2019);*

Deutsche Fassung EN ISO 22301:2019. Berlin: Beuth Verlag GmbH. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.31030/3087743

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, (04(02)), 92–100. Zugriff am 08.03.2024. Verfügbar unter: http://dx.doi.org/10.4236/jis.2013.42011

Döring, N. (2023). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (Lehrbuch, 6., vollständig überarbeitete, aktualisierte und erweiterte Auflage). Berlin, Heidelberg: Springer. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-64762-2

Draheim, D., Krimmer, R. & Tammet, T. (2021). On State-Level Architecture of Digital Government Ecosystems: From ICT-Driven to Data-Centric. In Hameurlain, A. & Tjoa, A. M. (Hrsg.), *Transactions on Large-Scale Data- and Knowledge-Centered Systems XLVIII* (S. 165–195). Berlin: Springer. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-63519-3

Eckert, C. (2023). *IT-Sicherheit. Konzepte - Verfahren - Protokolle* (11. Auflage). Berlin, Boston: De Gruyter. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1515/9783110985115

Ee, H. (2014). Business Continuity 2014: From Traditional to Integrated Business Continuity Management. *Journal of Business Continuity & Emergency Planning*, (8(2)), 102–105. Zugriff am 04.03.2024. Verfügbar unter: https://www.researchgate.net/publication/268794947

Eisend, M. & Kuß, A. (2021). *Grundlagen empirischer Forschung. Zur Methodologie in der Betriebswirtschaftslehre* (2., überarbeitete und erweitere Auflage). Wiesbaden: Springer Gabler. Zugriff am 09.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-32890-0

Elliott, D., Swartz, E. & Herbane, B. (2010). *Business Continuity Management: A Crisis Management Approach* (2. Ausgabe). New York: Routledge.

Engel, A. (2018). Die gewandelte Rolle des CIOs. In Heuermann, R., Tomenendal, M. & Bressem, C. (Hrsg.), *Digitalisierung in Bund, Ländern und Gemeinden IT-Organisation, Management und Empfehlungen* (S. 25–28). Berlin, Heidelberg: Springer Gabler. Zugriff am 09.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-54098-5

EU - Europäische Union (2022a). *Digital Economy and Society Index (DESI) 2022*. Zugriff am 03.03.2024. Verfügbar unter: https://digital-strategy.ec.europa.eu/en/policies/desi

EU - Europäische Union (2022b). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.* Zugriff am 07.03.2024. Verfügbar unter: http://data.europa.eu/eli/dir/2022/2555/oj

Eul, M., Röder, H. & Simons, E. (2010). Strategisches IT-Management - Vom Kostenfaktor zum Werttreiber. In Keuper, F., Schomann, M. & Zimmermann, K. (Hrsg.), Management von IT

und IT-gestütztes Management (2., überarbeitete und erweiterte Auflage) (S. 54–69). Wiesbaden: Gabler. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-8349-8803-4

Faber, O. (2019). Digitalisierung – ein Megatrend: Treiber & Technologische Grundlagen. In Erner, M. (Hrsg.), *Management 4.0 – Unternehmensführung im digitalen Zeitalter* (S. 3–42). Berlin, Heidelberg: Springer Gabler. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-57963-3

Faertes, D. (2015). Reliability of Supply Chains and Business Continuity Management. *Procedia Computer Science*, (55), 1400–1409. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1016/j.procs.2015.07.13

Fallenbeck, N. & Eckert, C. (2017). IT-Sicherheit und Cloud Computing. In Vogel-Heuser B., Bauerhnhansl, T. & ten Hompel M. (Hrsg.), *Handbuch Industrie 4.0. Bd. 4. Allgemeine Grundlagen* (2. Auflage). (S. 135–169). Berlin: Springer Vieweg. https://doi.org/10.1007 /978-3-662-53254-6

Fischer, C., Heuberger, M. & Heine, M. (2021). The impact of digitalization in the public sector: a systematic literature review. *dms - der moderne staat - Zeitschrift für Public Policy, Recht und Management*, (14(1-2021)), 3–23. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.3224/dms.v14i1.13

Flick, U. (2022a). Design und Prozess qualitativer Forschung. In Flick, U., Kardorff, E. von, & Steinke, I. (Hrsg.), *Qualitative Forschung. Ein Handbuch* (14. Auflage, Originalausgabe) (S. 252–264). Reinbek bei Hamburg: rowohlts.

Flick, U. (2022b). Klassische Gütekriterien im Kontext qualitativer Sozialforschung. In Baur, N. & Blasius, J. (Hrsg.), Handbuch Methoden der empirischen Sozialforschung (3., vollständig überarbeitete und erweiterte Auflage) (S. 533–547). Wiesbaden: Springer VS. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-37985-8

Foth, E. (2016). *Erfolgsfaktoren für eine digitale Zukunft: IT-Management in Zeiten der Digitalisierung und Industrie 4.0.* Berlin, Heidelberg: Springer Vieweg. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-53177-8

Frevel, B. (2016). *Sicherheit. Ein (un)stillbares Grundbedürfnis* (2. Auflage). Wiesbaden: Springer VS. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-12458-8

Früh, W. (2017). *Inhaltsanalyse. Theorie und Praxis* (9., überarbeitete Auflage). Konstanz: UVK Verlagsgesellschaft mbH.

Gadatsch, A. & Mangiapane, M. (2017). *IT-Sicherheit. Digitalisierung der Geschäftsprozesse und Informationssicherheit.* Wiesbaden: Springer Vieweg. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-17713-3

Gläser, J. & Laudel, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen* (4. Auflage). Wiesbaden: VS Verlag. Zugriff am 04.03.2024. Verfügbar unter: https://link.springer.com/book/9783531172385

Gleißner, W. (2022). Robustheit und Resilienz von Staaten und Unternehmen. In Roselieb, F. (Hrsg.), *Business Continuity Management in der Praxis: Mit Krisen professionell umgehen - erfolgreiche Konzepte und Fallbeispiele* (S. 249–261). Berlin: Erich Schmidt Verlag GmbH & Co. KG. Zugriff am 04.03.2024. Verfügbar unter: https://link.springer.com/book/10.37307/b.978-3-503-20961-3

Gobble, M. (2018). Digitalization, Digitization, and Innovation. *Research-Technology Management*, (61(4)), 56–59. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1080/08956308.2018.1471280.

Guest, G., Bunce, A. & Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods,* (18(1)), 59–82. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1177/1525822X05279903

Häder, M. (2019). *Empirische Sozialforschung. Eine Einführung* (4. Auflage). Wiesbaden: Springer VS. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-26986-9

Hamidian, K. & Kraijo, C. (2013). Digitalisierung – Status quo. In Keuper, F., Hamidian K., Verwaayen E., Kalinowski, T. & Kraijo C. (Hrsg.), *Digitalisierung und Innovation: Planung – Entstehung – Entwicklungsperspektiven* (S. 3–23). Wiesbaden: Springer Gabler. Zugriff am 25.02.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-00371-5

Harich, T. W. (2021). *IT-Sicherheitsmanagement. Das umfassende Praxis-Handbuch für IT-Security und technischen Datenschutz nach ISO 27001* (3. Auflage). Frechen: mitp.

Härtwig, C. & Sapronova, A. (2021). Keine Angst vor der Digitalisierung! Zum Stand digitalisierter Arbeitsanforderungen in verschiedenen Industriebranchen und Tätigkeitsfeldern sowie Zusammenhänge zwischen Belastung, Ressourcen und Beanspruchungsfolgen in Deutschland. *Zeitschrift für Arbeitswissenschaft*, (75(1)), 58–73. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/s41449-020-00205-y

Hasenbein, M. (2020). *Der Mensch im Fokus der digitalen Arbeitswelt. Wirtschaftspsychologische Perspektiven und Anwendungsfelder.* Berlin: Springer. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-61661-1

Hassel, H. & Cedergren, A. (2019). Exploring the Conceptual Foundation of Continuity Management in the Context of Societal Safety. *Risk Analysis,* (39(7)), 1503–1519. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1111/risa.13263

Helfferich, C. (2022). Leitfaden- und Experteninterviews. In Baur, N. & Blasius, J. (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung (3., vollständig überarbeitete und erweiterte Auflage)* (S. 875-892). Wiesbaden: Springer VS. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-37985-8

Hellmann, R. (2023). *IT-Sicherheit. Methoden und Schutzmassnahmen für sichere Cybersysteme* (2., aktualisierte und erweiterte Auflage). Berlin, Boston: De Gruyter.

Herbane, B. (2010). The Evolution of Business Continuity Management: A Historical Review of Practices and Drivers. *Business History*, (52(6)), 978–1002. Zugriff am 04.03.2024. Verfügbar unter: http://dx.doi.org/10.1080/00076791.2010.511185

Hersyah, M. H. & Derisma. (2018). A Literature Review on Business Continuity Based on ISO 22301, Six Sigma and Customer Satisfaction Evaluation. *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*. Bandung, Indonesia: IEEE, 392–397. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1109/ICITSI.2018.8696075

Hess, T., Matt, C., Benlian, A. & Wiesböck, F. (2016). Options for Formulating a Digital Transformation Strategy. *MIS Quarterly Executive*, (15(2), 123–139. Zugriff am 04.03.2024. Verfügbar unter: https://aisel.aisnet.org/misqe/vol15/iss2/6/

Heuermann, R. (2018), Bewertung Situation und Landesstrategien. In Heuermann, R., Tomenendal, M., Bressem, C. & Engel (Hrsg.), *Digitalisierung in Bund, Ländern und Gemeinden* (S. 132–136). Berlin: Springer Gabler. https://doi.org/10.1007/978-3-662-54098-5

Hiermaier, S. & Scharte, B. (2018). Ausfallsichere Systeme - Resilienz als Sicherheitskonzept im Zeitalter der Digitalisierung. In Neugebauer, R. (Hrsg.), *Digitalisierung. Schlüssel-technologien für Wirtschaft und Gesellschaft* (S. 295–310). Berlin, Heidelberg: Springer Vieweg. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-55890-4

Hippmann, S., Klinger, R. & Leis, M. (2018). Digitalisierung – Anwendungsfelder und Forschungsziele. In Neugebauer, R. (Hrsg.), *Digitalisierung. Schlüsseltechnologien für Wirtschaft und Gesellschaft* (S. 9–18). Berlin, Heidelberg: Springer Vieweg. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-55890-4

Hoberg, P., Welz, B., Oswald, G., & Krcmar, H. (2018). Digitale Transformation aus Sicht von IT-Entscheidern. In Oswald, G. & Krcmar, H. (Hrsg.), *Digitale Transformation. Fallbeispiele und Branchenanalysen* (S. 65–72). Wiesbaden: Springer Gabler. https://doi.org/10.1007/978-3-658-22624-4

Hochstein, A., Zarnekow, R. & Brenner, W. (2004). ITIL als Common-Practice-Referenzmodell für das IT-Service-Management. Formale Beurteilung und Implikationen für die Praxis. *Wirtschaftsinformatik*, (46(5)), 382–389. Zugriff am 05.03.2024. Verfügbar unter: https://link.springer.com/article/10.1007/BF03250951

Hofmann, E. & Staiger, F. (2020). Beschaffungskompetenzen 4.0. Berlin: Springer Gabler. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-61838-7

Honekamp, W. (2019). Cybercrime: Aktuelle Erscheinungsformen und deren Bekämpfung. In Lange, H.-J., Model, T., Wendekamm, M. (Hrsg.), *Zukunft Der Polizei: Trends und Strategien* (S. 47–59). Wiesbaden: Springer VS. Zugriff am 05.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-22591-9

Hug, T. & Poscheschnik, G. (2020). *Empirisch forschen.* (3. Überarbeitete und ergänzte Auflage). München: UVK Verlag. Zugriff am 05.03.2024. Verfügbar unter: https://doi.org/10.36198/9783838553030

Hussy, W., Schreier, M. & Echterhoff, G. (2013). *Forschungsmethoden in Psychologie und Sozialwissenschaften für Bachelor* (2., überarbeitete Auflage). Berlin, Heidelberg: Springer: Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-642-34362-9

ISO 22313 (2020). *Security and resilience — Business continuity management systems, Guidance on the use of ISO 22301*. International Organization for Standardization. Zugriff am 01.03.2024. Verfügbar unter: https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-2:v1:en

Janotta, F. (2019). Vom Chief Information Officer zum Chief Executive Officer. In Buchenau, P. (Hrsg.), *Chefsache Zukunft. Was Führungskräfte von morgen brauchen* (S. 255–267). Wiesbaden: Springer Gabler. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-26560-1

Järveläinen, J. (2012). Information Security and Business Continuity Management in Interorganizational IT Relationships. *Information Management & Computer Security*, (20(5)), 332–349. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1108/09685221211286511

Johanning, V. (2020). *Organisation und Führung der IT. Die neue Rolle der IT und des CIOs in der digitalen Transformation.* Wiesbaden: Springer Vieweg. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-12008-5

Kaiser, D. (2020). *Berufsbegleitend promovieren in den Wirtschaftswissenschaften: Ein Leitfaden für Berufstätige*. Berlin: Springer Gabler. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-61963-6

Kappelman, L., Johnson, V., Torres, R., Maurer, C. & McLean, E. (2018). A Study of Information Systems Issues, Practices, and Leadership in Europe. *European Journal of Information Systems*, (28(1)), 26–42. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1080/0960085X.2018.1497929

Karmasin, M. & Ribing, R. (2017). *Die Gestaltung wissenschaftlicher Arbeiten* (9. überarbeitete und aktualisierte Auflage). Wien: facultas.

Kerkmann, C. & Scheuer, S. (2021, 8. April). Die Lehren aus dem Feuer im Rechenzentrum. *Handelsblatt print*, (067), 19. Düsseldorf: Handelsblatt Media Group. Zugriff am 01.03.2024. Verfügbar unter: https://archiv.handelsblatt.com/document/HB__AB0F32CC-7E85-4352-BC20-B15B129403EE%7CHBPM__AB0F32CC-7E85-4352

Kersten, H. & Klett, G. (2017). *Business Continuity und IT-Notfallmanagement. Grundlagen, Methoden und Konzepte.* Wiesbaden: Springer Vieweg. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-19118-4

Kersten, H., Reuter, G. & Schröder, K.-W. (2013). *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz* (4., aktualisierte und erweiterte Auflage). Wiesbaden: Springer Vieweg. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-01724-8

Keuper, F. (2010). IT-Management im Kontext des Strategie-Struktur-Zusammenhangs Innovatives IT-Management. In Keuper, F., Schomann, M. & Zimmermann, K. (Hrsg.), Management von IT und IT-gestütztes Management (2., überarbeitete und erweiterte Auflage) (S. 4–29). Wiesbaden: Gabler. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-8349-8803-4

Kipker, D.-K. & Scholz, D. E. (2021). Das IT-Sicherheitsgesetz 2.0: Eine kritische Analyse. *Datenschutz und Datensicherheit - DuD*, (45(1)), 40–45. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/s11623-020-1387-9

Kirchmair, R. (2022). *Qualitative Forschungsmethoden. Anwendungsorientiert: vom Insider aus der Marktforschung lernen.* Berlin, Heidelberg: Springer. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-62761-7

Klenk, T., Nullmeier, F. & Wewer, G. (2019). Auf dem Weg zum Digitalen Staat? Stand und Perspektiven der Digitalisierung in Staat und Verwaltung. In Klenk, T., Nullmeier, F. & Wewer, G. (Hrsg.), *Handbuch Digitalisierung in Staat und Verwaltung* (S. 1–22). Wiesbaden: Springer VS. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-23669-4

Klös, H.-P. (2020). Nach dem Corona-Schock: Digitalisierungspotenziale für Deutschland. *IW-Policy Paper*, (14), Köln: Institut der deutschen Wirtschaft. Zugriff am 02.03.2024. Verfügbar unter: https://www.econstor.eu/handle/10419/219033

Kollmann, T., Kuckertz, A. & Stöckmann, C. (2016). *Das 1 x 1 des Wissenschaftlichen Arbeitens* (2. Auflage). Wiesbaden: Springer Gabler. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-10707-9

Königs, H.-P. (2017). *IT-Risikomanagement mit System. Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken* (5. Auflage). Wiesbaden: Springer Vieweg. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-12004-7

Kornmeier, M. (2021). *Wissenschaftlich schreiben leicht gemacht. Für Bachelor, Master und Dissertation* (9., aktualisierte und ergänzte Auflage). Bern: Haupt Verlag.

Kotlarsky, J., van den Hooff, B., Geerts, L. (2020). Under Pressure: Understanding the dynamics of coordination in IT functions under business-as-usual and emergency conditions. *Journal of Information Technology*, 35(2), 94–122. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1177/0268396219881461

Krcmar, H. (2018). Grundlagen der digitalen Transformation. In Oswald, G. & Krcmar, H. (Hrsg.), *Digitale Transformation. Fallbeispiele und Branchenanalysen* (S. 5–10). Wiesbaden: Springer Gabler. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-22624-4

Krishna Kaiser, A. (2018). *Reinventing ITIL in the Age of DevOps. Innovative Techniques to Make Processes Agile and Relevant.* Berkeley, CA: Apress. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-1-4842-3976-6

Krüger, D. & Riemeier, T. (2014)**.** Die qualitative Inhaltsanalyse - eine Methode zur Auswertung von Interviews. In Krüger, D., Parchmann, I. & Schecker, H. (Hrsg.), *Methoden in der naturwissenschaftsdidaktischen Forschung* (S. 133–145). Berlin, Heidelberg: Springer Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-642-37827-0

Kuckartz, U. (2018). *Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung* (4. Auflage). Weinheim Basel: Beltz Juventa.

Kuckartz, U. (2019). Qualitative Inhaltsanalyse: von Kracauers Anfängen zu heutigen Herausforderungen. *Forum Qualitative Sozialforschung*, (20(3)), Art. 12. Zugriff am 03.03.2024. Verfügbar unter: http://dx.doi.org/ 10.17169/fqs-20.3.3370

Kuckartz, U. & Rädiker, S. (2020). *Fokussierte Interviewanalyse mit MAXQDA. Schritt für Schritt.* Wiesbaden: Springer VS. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-31468-2

Kuckartz, U. & Rädiker, S. (2022). *Qualitative Inhaltsanalyse. Methoden, Praxis, Computer-unterstützung* (5. Auflage). Weinheim: Beltz Juventa.

Lambach, D. & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Governance*, (36(3)), 693–709. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1111/gove.12690

Lang, S. & Kneuper, R. (2022). Datenschutz und Informationssicherheit in Gaia-X. *Datenschutz und Datensicherheit - DuD*, (46(12)), 778–781. Zugriff am 07.03.2024. Verfügbar unter: https://doi.org/10.1007/s11623-022-1692-6

Lasar, A. (2019). Die Herausforderungen der Kommunen im Rahmen der Digitalisierung. In Schmid, A. (Hrsg.), *Verwaltung, eGovernment und Digitalisierung: Grundlagen, Konzepte und Anwendungsfälle* (S. 101–111). Wiesbaden: Springer Vieweg. Zugriff am 05.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-27029-2

Leimeister, J. M. (2012). *Dienstleistungsengineering und -management.* Berlin, Heidelberg: Springer Gabler. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-642-27983-6

Leitner, A. & Wroblewski, A. (2002). Zwischen Wissenschaftlichkeitsstandards und Effizienzansprüchen. In Bogner, A., Littig, B. & Menz, W. (Hrsg.), *Das Experteninterview. Theorie, Methode, Anwendung* (S. 241–256). Wiesbaden: Springer. Zugriff am 07.03.2024. Verfügbar unter: https://doi.org/ 10.1007/978-3-322-93270-9

Lepping, J. & Palzkill, M. (2017). Die Chance der digitalen Souveränität. In Wittpahl, V. (Hrsg.), *Digitalisierung* (S. 17–25). Berlin, Heidelberg: Springer Vieweg. Zugriff am 07.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-52854-9

Limaj, E. & Bernroider, E. W. N. (2022). A Taxonomy of Scaling Agility. *The Journal of Strategic Information Systems*, 31(3), 1–19. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1016/j.jsis.2022.101721

von Lucke, J. (2018). Digitalisierung in der Kernverwaltung - Konzepte. In Heuermann, R., Tomenendal, M. & Bressem, C. (Hrsg.), *Digitalisierung in Bund, Ländern und Gemeinden IT-Organisation, Management und Empfehlungen* (S. 28–40). Berlin: Springer Gabler. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-54098-5

Lundborg, M., Gull, I. & Baischew, D. (2022). *Strategische Bedeutung von Cloud-Diensten für die digitale Souveränität von KMU. Teil 1 - Marktübersicht Cloud-Anbieter.* Bad Honnef: WIK-Consult. Zugriff am 03.03.2024. Verfügbar unter: https://www.econstor.eu/handle/10419/268805

Mandl, T. (2021). IT-Notfallplanung und IT-Notfallmanagement in der Praxis. In Tiemeyer, E. (Hrsg.), *Handbuch IT-System- und Plattformmanagement, Handlungsfelder, Technologien, Managementinstrumente, Good Practices* (2. Auflage) (S. 553–584). München: Hanser.

Maindok, H. (2003). *Professionelle Interviewführung in der Sozialforschung* (2. Auflage). Herbolzheim: Centaurus Verlag & Media. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-86226-829-0

Mangiapane, M. & Büchler, R. P. (2015). *Modernes IT-Management. Methodische Kombination von IT-Strategie und IT-Reifegradmodell.* Wiesbaden: Springer Vieweg. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-03493-1

Mayer, H. O. (2013). Interview und schriftliche Befragung. Grundlagen und Methoden empirischer Sozialforschung (6., überarbeitete Auflage). München: Oldenbourg.

Mayring, P. (2023). *Einführung in die qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken* (7., überarbeitete Auflage). Weinheim: Beltz.

Mayring, P. (2022). *Qualitative Inhaltsanalyse: Grundlagen und Techniken*. (13., überarbeitete Auflage). Weinheim: Beltz.

Mergel, I. (2019). Digitale Transformation als Reformvorhaben der deutschen öffentlichen Verwaltung. *dms - der moderne staat - Zeitschrift für Public Policy, Recht und Management,* (12(1–2019), 162–171. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.3224/dms.v12i1.09

Merschbacher, A. (2018). *Sicherheitsfibel*. Wiesbaden: Springer Vieweg. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10. 1007/978-3-658-21141-7

Mierowski, S. (2021). *Datenschutz nach DS-GVO und Informationssicherheit gewährleisten. Eine kompakte Praxishilfe zur Maßnahmenauswahl: Prozess ZAWAS 4.0.* Wiesbaden: Springer Vieweg. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-33470-3

Mirkes, M. & Özcan, E. (2020). Business Continuity Management - Vorbereitung auf den Notfall. In Mahnke, A. & Rohlfs, T. (Hrsg.), *Betriebliches Risikomanagement und*

Industrieversicherung. Erfolgreiche Unternehmenssteuerung durch ein effektives Risiko- und Versicherungsmanagement (S. 191–211). Wiesbaden: Springer Gabler. Zugriff am 05.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-30421-8

Misoch, S. (2019). *Qualitative Interviews* (2., erweiterte und aktualisierte Auflage). Berlin, Boston: De Gruyter Oldenbourg.

Moeller, R. R. (2008). *Sarbanes-Oxley Internal Controls. Effective Auditing with AS5, CobiT and ITIL.* Hoboken, NJ: John Wiley & Sons.

Moen, R. & Norman, C. (2009). Evolution of the PDCA Cycle. *Proceedings of the 7th ANQ Congress.* Zugriff am 06.03.2024. Verfügbar unter: https://www.researchgate.net /publication/228475044

Mónica, R., Henry, Q., Estela, M. & Washington, F. (2020). Why implement continuity plans in Organizations? Approach of a prospective study based on ITIL. *2020 International Conference on Intelligent Systems and Computer Vision (ISCV).* 1–5. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1109/ISCV49265.2020.9204335

Moşteanu, N. R. (2020). Management of Disaster and Business Continuity in a Digital World. *International Journal of Management*, (11(4)), 169–177. Zugriff am 06.03.2024. Verfügbar unter: https://ssrn.com/abstract=3600760

Müller, J. R. (2015). *Die Formalisierte Terminologie der Verlässlichkeit Technischer Systeme*. Berlin, Heidelberg: Springer Vieweg. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-46922-4

Müller, K.-R. (2018). *IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement - Sichere Anwendungen - Standards und Practices* (6. Auflage). Wiesbaden: Springer Vieweg. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-22065-5

Müller, M. (2022). Wissensmanagement klipp & klar. Wiesbaden: Springer Fachmedien Wiesbaden. Zugriff am 27.07.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-38309-1

Nachrowi, E., Nurhadryani Y. & Sukoco H. (2020). Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, (4(4)), 764–774. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.29207/resti.v4i4.2265

Neugebauer, R. (2018). Digitale Information – der „genetische Code“ moderner Technik. In Neugebauer, R. (Hrsg.), *Digitalisierung. Schlüsseltechnologien für Wirtschaft & Gesellschaft* (S. 1–7). Berlin, Heidelberg: Springer Vieweg. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-55890-4

Newell, S. & Marabelli, M. (2015). Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of ‘Datification’. *The Journal of Strategic Information Systems,* 24(1), 3–14. Zugriff am 03.03.2024. Verfügbar unter: https://dx.doi.org/10.1016/j.jsis.2015.02.001

Niemimaa, M., Järveläinen, J., Heikkilä, M. & Heikkilä, J. (2019). Business Continuity of Business Models: Evaluating the Resilience of Business Models for Contingencies. *International Journal of Information Management*, (49), 208–216. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1016/j.ijinfomgt.2019.04.010

Njenga, K. & Brown, I. (2012). Conceptualising Improvisation in Information Systems Security. *European Journal of Information Systems*, (21(6)), 592–607. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1057/ejis.2012.3

Osterhage, W. W. (2017). *IT-Kompendium. Die effiziente Gestaltung von Anwendungs-plattformen.* Berlin: Springer Vieweg. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-52705-4

Osterhage, W. W. (2016). *Notfallmanagement in Kommunikationsnetzen.* Berlin, Heidelberg: Springer Vieweg. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-45660-6

Otto, B. (2022). The Evolution of Data Spaces. In Otto, B., Ten Hompel, M. & Wrobel, S. (Hrsg.), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (S. 3–15). Cham: Springer. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-030-93975-5

Păunescu, C. & Argatu, R. (2020). CRITICAL FUNCTIONS IN ENSURING EFFECTIVE BUSINESS CONTINUITY MANAGEMENT. EVIDENCE FROM ROMANIAN COMPANIES. *Journal of Business Economics and Management*, (21(2)), 497–520. Zugriff am 06.03.2024. Verfügbar unter: https://doi.org/10.3846/jbem.2020.12205

Pérez-Morote, R., Pontones-Rosa, C. & Núñez-Chicharro, M. (2020). The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries. *Technological Forecasting & Social Change*, (154), 1–14. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1016/j.techfore.2020.119973

Petersen, T. & Bluth, C. (2020). *Megatrend-Report #02: Die Corona-Transformation: Wie die Pandemie die Globalisierung bremst und die Digitalisierung beschleunigt. Gütersloh: Bertelsmann Stiftung*. Zugriff am 09.03.2024. Verfügbar unter: https://doi.org/10.11586/2020054

Petrenko, S. (2021). *Developing an Enterprise Continuity Program*. Gistrup: River Publishers.

Pickl, S. (2019). Interview with Erich Vad on “Political and Security Aspects of Digitization”. *Business & Information Systems Engineering*, (61(3)), 257–260. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/s12599-019-00597-0

Pilorget, L. & Schell, T. (2018). *IT Management. The art of managing IT based on a solid framework leveraging the company’s political ecosystem*. Wiesbaden: Springer Vieweg. Zugriff am 07.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-19309-6

Pohle, J. & Thiel, T. (2020). Digital Sovereignty. *Internet Policy Review*, (9(4)), 1–19. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.14763/2020.4.1532

Pohlmann, N. (2018). Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung. In Bär, C., Grädler, T. & Mayr, R. (Hrsg.), *Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht* (S. 195–212). Berlin: Springer Gabler. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-56438-7

Pohlmann, N. (2019). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.* Wiesbaden: Springer Vieweg. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-25398-1

Porath, R. (2020). *Internet, Cyber- und IT-Sicherheit von A-Z. Aktuelle Begriffe kurz und einfach erklärt - Für Beruf, Studium und Privatleben* (2. Auflage). Berlin: Springer Vieweg. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-60911-8

Proff, Harald, Ahrens, C., Neuroth, W., Proff, Heike, Knobbe, F., Szybisty, G. & Sommer, S. (2021). *Accelerating Digitalization. Chancen der Digitalisierung erkennen und nutzen*. Wiesbaden: Springer Gabler. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-31456-9

Przyborski, A. & Wohlrab-Sahr, M. (2021). *Qualitative Sozialforschung. Ein Arbeitsbuch* (5., überarbeitete und erweiterte Auflage). Berlin, Boston: De Gruyter Oldenbourg

Rädiker, S. & Kuckartz, U. (2019). Analyse Qualitativer Daten Mit MAXQDA. Text, Audio und Video. Wiesbaden: Springer VS. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-22095-2

Reinders, H. (2011). Interview. In Reinders, H., Ditton, H., Gräsel, C. & Gniewosz, B. (Hrsg.), *Empirische Bildungsforschung. Strukturen und Methoden* (S. 85–97). Wiesbaden: VS Verlag für Sozialwissenschaften. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-531-93015-2

Reinders, H. & Ditton, H. (2011). Überblick Forschungsmethoden. In Reinders, H., Ditton, H., Gräsel, C. & Gniewosz, B. (Hrsg.), *Empirische Bildungsforschung. Strukturen und Methoden* (S. 45–51). Wiesbaden: VS Verlag für Sozialwissenschaften. Zugriff am 02.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-531-93015-2

Renn, O. (2014). Risikowahrnehmung in der Bevölkerung - Implikationen für das Sicherheitsempfinden. *Zeitschrift für Außen- und Sicherheitspolitik*, (8(1)), 49–67. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/s12399-014-0436-6

Resch, O. (2020). *Einführung in das IT-Management: Grundlagen, Umsetzung, Best Practice* (5., neu bearbeitete Auflage). Berlin: Erich Schmidt Verlag.

Ridley, G.. Young, J. & Carroll, P. (2004). COBIT and its Utilization: A framework from the literature. *37th Annual Hawaii International Conference on System Sciences*. Big Island, USA: IEEE, 1–8. Zugriff am 20.02.2024. Verfügbar unter: https://doi.org/10.1109/HICSS.2004.1265566

Roselieb, F. (2022). *Business Continuity Management in der Praxis: Mit Krisen professionell umgehen - erfolgreiche Konzepte und Fallbeispiele*. Berlin: Erich Schmidt Verlag GmbH &

Co. KG. Zugriff am 20.02.2024. Verfügbar unter: https://link.springer.com/book/10.37307/b.978-3-503-20961-3

Saarikko, T., Westergren, U. H. & Blomquist, T. (2020). Digital Transformation: Five Recommendations for the Digitally Conscious Firm. In *Business Horizons*, (63(6)), 825–839. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1016/j.bushor.2020.07.005

Sawalha, I. H. (2020). Business Continuity Management: use and approach's effectiveness. *Continuity & Resilience Review*, (2(2)), 81–96. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1108/CRR-05-2020-0016

Schaefer C. & Gornas J. (2018). Öffentliche Betriebswirtschaftslehre (ÖBWL). In Voigt, R. (Hrsg.), *Handbuch Staat* (S. 53–64) Wiesbaden: Springer VS. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-20744-1

Schaudel, F. (2018). Digitalization Might Change the World, but Does it Really Fundamentally change how IT has to be Managed? In Urbach, N., Ahlemann F., Böhmann T., Drews, P., Brenner, W., Schaudel F. & Schütte, R. (Hrsg.), *The Impact of Digitalization on the IT Department.* Business & Information Systems Engineering, (61), 123–131. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1007/s12599-018-0570-0

Schewe, C. (2006). Subjektives Sicherheitsgefühl. In Lange, H.-J. (Hrsg.), *Wörterbuch zur Inneren Sicherheit* (S. 322–325). Wiesbaden: VS Verlag für Sozialwissenschaften.

Schmid, A. (2019). *Verwaltung, eGovernment und Digitalisierung. Grundlagen, Konzepte und Anwendungsfälle.* Wiesbaden: Springer Vieweg. Zugriff am 20.02.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-27029-2

Schmidt, F. A. & van der Giet, G. (2018). Digitalisierung auf Bundesebene. In Heuermann, R., Tomenendal, M. & Bressem, C. (Hrsg.), *Digitalisierung in Bund, Ländern und Gemeinden IT-Organisation, Management und Empfehlungen* (S. 137–152). Berlin: Springer Gabler. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-54098-5

Schneijderberg, C., Wieczorek, O. & Steinhardt, I. (2022). *Qualitative und quantitative Inhaltsanalyse: digital und automatisiert: eine anwendungsorientierte Einführung mit empirischen Beispielen und Softwareanwendungen*. Weinheim, Basel: Beltz Juventa.

Schumacher, A., Sihn, W. & Erol, S. (2016). Automation, Digitization and Digitalization and Their Implications for Manufacturing Processes. *International scientific Conference.* Zugriff am 03.03.2024. Verfügbar unter: https://www.researchgate.net/publication/318877006

Schumann, S. (2018). *Quantitative und qualitative empirische Forschung.* Wiesbaden: Springer VS. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-17834-5

Schwab, C., Kuhlmann, S., Bogumil, J. & Gerber, S. (2019). Digitalisierung der Bürgerämter in Deutschland. *Study der Hans-Böckler-Stiftung, No. 427.* Zugriff am 04.03.2024. Verfügbar unter: https://www.econstor.eu/handle/10419/204530

Schwab, K. (2016). *Die Vierte Industrielle Revolution*. München: Pantheon Verlag.

Schwer, K. & Hitz, C. (2018). Designing Organizational Structure. *Journal of Eastern European and Central Asian Research*, (5(1)), 11–21. Zugriff am 04.03.2024. Verfügbar unter: http://dx.doi.org/10.15549/jeecar.v5i1.213

Sofyana, L. & Putera, A. R. (2019). Business architecture planning with TOGAF framework. *Journal of Physics: Conference Series*, (1375(1)), 1–10. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1088/1742-6596/1375/1/012056

Specht, P. (2021). Die 50 wichtigsten Themen der Digitalisierung (5. Auflage). München: Redline Verlag.

Spilker, J. (2022). IT Service and Continuity Management am Beispiel DATEV. In Roselieb, F. (Hrsg.), *Business Continuity Management in der Praxis: Mit Krisen professionell umgehen - erfolgreiche Konzepte und Fallbeispiele* (S. 143–155). Berlin: Erich Schmidt Verlag GmbH & Co. KG. Zugriff am 04.03.2024. Verfügbar unter: https://link.springer.com/book /10.37307/b.978-3-503-20961-3

Spörrer, S. (2014). *Business Continuity Management. ISO 22301 und weitere Normen im Rahmen der Informationstechnologie* (Nachdruck 2018). Wiesbaden: Springer Gabler. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-23403-4

Stember, J. & Hasenkamp, V. (2019). Handbuch E-Government: Technikinduzierte Verwaltungsentwicklung. In Stember, J., Eixelsberger, W., Spichiger, A., Neuroni, A., Habbel F.-R. & Wundara, M. (Hrsg.), *Handbuch E-Government. Technikinduzierte Verwaltungs-entwicklung* (S. 31–52). Wiesbaden: Springer Gabler. Zugriff am 04.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-21402-9

Stier, W. (1999). *Empirische Forschungsmethoden* (2., verbesserte Auflage). Berlin, Heidelberg: Springer. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978 -3-642-58460-2

Supriadi, L. S. R. & Sui Pheng, L. (2018). *Business Continuity Management in Construction.* Singapore: Springer. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-981-10-5487-7

Suresh, N., Sanders, G. L. & Braunscheidel, M. J. (2020). Business Continuity Management for Supply Chains Facing Catastrophic Events. *IEEE Engineering Management Review*, (48(3)), 129–138. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1109 /EMR.2020.3005506

Tardieu, H. (2022). Role of Gaia-X in the European Data Space Ecosystem. In Otto, B., Ten Hompel, M. & Wrobel, S. (Hrsg.), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (S. 41–59). Cham: Springer. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-030-93975-5

Theis, D. (2012). Modernisierung in der Bundeswehr - Der Beitrag von HERKULES und SASPF. In Richter, G. (Hrsg.), *Neuausrichtung der Bundeswehr. Beiträge zur professionellen Führung und Steuerung* (S. 183–196). Wiesbaden: Springer VS. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-531-94331-2

Tiemeyer, E. (2020). *Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis* (7., überarbeitete Auflage). München: Hanser.

Uhl, A. & Loretan, S. (2019). *Digitalisierung in der Praxis: So schaffen KMU den Weg in die Zukunft*. Wiesbaden: Springer Vieweg. Zugriff am 08.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-26137-5

UN - United Nations (2020). *United Nations E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development*. New York: United Nations Department of Economic and Social Affairs. Zugriff am 03.03.2024. Verfügbar unter: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Re port).pdf

Urbach , N. (2018). Introduction. In Urbach, N., Ahlemann F., Böhmann T., Drews, P., Brenner, W., Schaudel F. & Schütte, R. (Hrsg.), *The Impact of Digitalization on the IT Department.* Business & Information Systems Engineering, (61), 123–131. Zugriff am 01.03.2024. Verfügbar unter: https://doi.org/10.1007/s12599-018-0570-0

Urbach, N. & Ahlemann, F. (2019). *IT Management in the Digital Age: A Roadmap for the IT Department of the Future.* Cham: Springer. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-319-96187-3

Urbach, N. & Ahlemann, F. (2016). *IT-Management im Zeitalter der Digitalisierung. Auf dem Weg zur IT-Organisation der Zukunft.* Berlin, Heidelberg: Springer Gabler. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-52832-7

Verlaine, B. (2017). Toward an Agile IT Service Management Framework. *Service Science*, (9(4)), 263–274. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1287/serv.2017.0186

Verlaine, B., Jureta, I. & Faulkner, S. (2016). How Can ITIL and Agile Project Management Coexist? In Borangiu, T., Dragoicea, M. & Nóvoa, H. (Hrsg.), *Exploring Services Science. IESS 2016. Lecture Notes in Business Information Processing* (247), 327–342. Cham: Springer. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-319-32689-4_25

Vial, G. (2019). Understanding Digital Transformation: A Review and a Research Agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1016/j.jsis.2019.01.003

Vogel, V. & Ziegler, N. (2023). Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie. *International Cybersecurity Law Review*, (4(1)), 1–19. Zugriff am 07.03.2024. Verfügbar unter: https://doi.org/10.1365/s43439-022-00077-4

Voigt, P. (2022). *IT-Sicherheitsrecht. Pflichten und Haftung im Unternehmen* (2. neu bearbeitete Auflage). Köln: Otto Schmidt.

Wan, S. H. C. & Chan, Y.-H. (2008). Adoption of Business Continuity Planning Processes in IT Service Management. *2008 3rd IEEE/IFIP International Workshop on Business-Driven IT*

Management. 21–30, Salvador, Brazil: IEEE. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1109/BDIM.2008.4540071

Watters, J. (2014). *Disaster Recovery, Crisis Response, and Business Continuity. A Management Desk Reference*. New York: Apress.

Weber, S. G. (2017). IT-Sicherheit und Nutzer: Chancen und Risiken in der Digitalisierung. In Wittpahl, V. (Hrsg.), *Digitalisierung* (S. 27–33). Berlin, Heidelberg: Springer Vieweg. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-52854-9

Weiß, J. (2019). Zwischen Alexa und Aktenmappe: Was lässt sich aus der Entwicklung des E-Governments für die Digitalisierung der öffentlichen Verwaltung lernen? In Schmid, A. (Hrsg.). *Verwaltung, eGovernment und Digitalisierung. Grundlagen, Konzepte und Anwendungsfälle* (S. 67–88). Wiesbaden: Springer Vieweg. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-27029-2

Wergen, J. (2019*). Promotionsplanung und Exposee: Die ersten Schritte auf dem Weg zur Dissertation* (3. Auflage). Opladen & Toronto: Verlag Barbara Budrich.

Wichmann, A. (2019). *Quantitative und Qualitative Forschung im Vergleich: Denkweisen, Zielsetzungen und Arbeitsprozesse.* Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-59817-7

Wimelius, H., Mathiassen, L., Holmström, J. & Keil, M. (2020). A Paradoxical Perspective on Technology Renewal in Digital Transformation. *Information Systems Journal,* 31(1), 198–225. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1111/isj.12307

Windoffer, A. (2018). Herausforderungen der Digitalisierung aus der Perspektive der öffentlichen Verwaltung. In Bär, C., Grädler, T. & Mayr, R. (Hrsg.), *Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht* (S. 363–376). Berlin: Springer Gabler. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-56438-7

Wirtz, B. & Daiser, P. (2018). E-Government. In Voigt, R. (Hrsg.), *Handbuch Staat.* (S. 981–995) Wiesbaden: Springer VS. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-20744-1

Witt, B. C. (2006). *IT-Sicherheit kompakt und verständlich. Eine praxisorientierte Einführung*. Wiesbaden: Vieweg.

Wittpahl, V. (2016). *Digitalisierung. Bildung, Technik, Innovation*. Berlin, Heidelberg: Springer Vieweg. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-662-52854-9

Zadeh, M. E., Millar, G. & Lewis, E. (2012). Mapping the Enterprise Architecture Principles in TOGAF to the Cybernetic Concepts - An Exploratory Study. *2012 45th Hawaii International Conference on System Sciences* (HICSS). Maui, USA: IEEE, 4270–4276. Zugriff am 07.03.2024. Verfügbar unter: https://doi.org/10.1109/HICSS.2012.422

Zhang, Z., Nan, G. & Tan, Y. (2020). Cloud Services vs. On-Premises Software: Competition Under Security Risk and Product Customization. *Information Systems Research*, (31(3)), 848–864. Zugriff am 03.03.2024. Verfügbar unter: https://doi.org/10.1287/isre.2019.0919

Zhenmin, L. (2020). Foreword. In United Nations Department of Economic and Social Affairs (Hrsg.). *United Nations E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development* (S. IV-V). New York: United Nations. Zugriff am 03.03.2024. Verfügbar unter: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

Zöller, S. (2019). *Ja zur Digitalisierung! Mit der richtigen Einstellung die Zukunftsfähigkeit des Unternehmens sichern.* Wiesbaden: Springer Gabler. Zugriff am 05.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-23959-6

Züll, C. & Menold, N. (2022). Offene Fragen. In Baur, N. & Blasius, J. (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung (3., vollständig überarbeitete und erweiterte Auflage)* (S. 1127-1134). Wiesbaden: Springer VS. Zugriff am 10.03.2024. Verfügbar unter: https://doi.org/10.1007/978-3-658-37985-8

4.2 Abbildungsverzeichnis

4.3 Tabellenverzeichnis

4.4 Abkürzungsverzeichnis

BAO	Besondere Aufbauorganisation
BCI	Business Continuity Institute
BC	Business Continuity
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
COBIT	Control Objectives for Information and related Technology
DESI	Digital Economy and Society Index
DIN	Deutsches Institut für Normung
DOAJ	Directory of Open Access Journals
DSGVO	Datenschutzgrundverordnung
ERP	Enterprise Resource Planning
EU	Europäische Union
GPG	Good Practice Guidelines
HFF	Hauptforschungsfrage
IKT	Informations- und Kommunikationstechnik
ISMS	Informationssicherheits-Managementsystem
ISO	International Standards Organization
ISSN	International Standard Serial Number
IT	Informationstechnik
IT-SiG	IT-Sicherheitsgesetz
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
NFF	Nebenforschungsfrage
PDCA	Plan Do Check Act
QS	Qualitätssicherung
TOGAF	The Open Group Architecture Framework
TOM	Technik Organisation Menschen

UN	United Nations / Vereinte Nationen
VHB	Verband der Hochschullehrer für Betriebswirtschaft