universität wien

MASTERARBEIT/MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

Risk Assessment als Ausgangspunkt für Business Continuity Planning

verfasst von / submitted by

Elena Volosova

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2020 / Vienna, 2020

Studienkennzahl lt. Studienblatt/: degree programme code as it appears on the student record sheet	UA 066 926
Studienrichtung lt. Studienblatt/: degree programme as it appears on the student record sheet	Masterstudium Wirtschaftsinformatik
Betreut von / Supervisor:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Zusammenfassung

In Unternehmen, insbesondere aus dem Finanzbereich, ist eine nahezu 100%ige Verfügbarkeit aller Services und Dienstleistungen fast eine Selbstverständlichkeit aus Kundensicht. Diese kann jedoch in der heutigen globalen und vernetzten Welt, welche eine Unzahl an Risiken birgt, oft nur durch viel Glück erreicht werden. Nur ausgereifte und durchdachte Pläne im Hintergrund können eine Hochverfügbarkeit garantieren und somit den Unternehmensfortbestand sichern.

Solche Pläne sind Teil des Business Continuity Managements (BCM) und werden Business Continuity Plan (BCP) genannt. Der Grundstein eines jeden BCP ist eine Ermittlung von Risiken. Diese werden nach modernen Vorgehensschemata mit Hilfe einer Risikoanalyse ermittelt. Dazu wird in dieser Arbeit eine Übersicht ausgewählter Ansätze zu solchen Risikoanalysen und Assessments gegeben. Von den Risiken ausgehend werden innerhalb eines BCM Maßnahmen ermittelt um einen Betrieb weiterzuführen und aufrecht zu erhalten.

Anschließend wird gezeigt, wie Ergebnisse des Risk Assessment in Form von Triggern als Ausgangspunkt für die Erstellung von Business Continuity Plänen eingesetzt werden können. Diese wird am Beispiel des Business Continuity Plannings (BCP) der Bank of Japan (BoJ) untermauert.

Um auch den BCM/BCP-Prozess zu beobachten und verbessern zu können, wird für diesen Zweck ein zugeschnittenes Maturity Modell entwickelt.

Die Erkenntnisse werden auch innerhalb einer Case Study für ein SME angewandt.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

„Just because the river is quiet it does not mean that all the crocodiles have left"

Malaiische Bauernregel

1.1 Background

Um in die spezifischen Bereiche dieser Arbeit einzusteigen, wird zuerst eine Definition für den Term Risiko benötigt. Risiko wird allgemein als Ereignis mit einer möglichen negativen Auswirkung angesehen (siehe auch Enisa [10]).

Der historische Ursprung des Risikobegriffes ist sehr alt. Risiko war der Menschheit schon sehr früh bekannt, man versuchte jedoch dieses nicht zu berechnen und zu beherrschen. Bis in die späte Antike hinein haben Menschen versucht das Risiko durch Gaben an die Götter zu beeinflussen. Durch Gaben milde gestimmte Götter sollten die Risiken im Leben von Menschen beeinflussen. Bei den Griechen gab es das Wort "eikos", welches mit "wahrscheinlich"gleichzusetzen ist. Es hatte eine ähnliche Bedeutung wie der heutige Risikobegriff. Sokrates definiert später "*eikos*äls " *Ähnlichkeit mit der Wahrheit*".

In der Neuzeit beschäftigte sich der Mathematiker Luca Paccioli in seinem Werk "*Summa de arithmetic, geometria et proportionalita*"(1494) mit Risikofragen zum Thema Glücksspiel [26].

Ab 1700 entwickelten sich Versicherungen für alle Lebensbereiche und somit auch

der moderne Risikobegriff. Von London aus verbreitet sich das Versicherungssystem und der Risikobegriff weltweit. Ebenfalls in diesem Zeitraum hegte Daniel Bernoulli (1700 -1782) einen interessanten Gedanken: Menschen bewerten Risiko unterschiedlich.

Ein sehr wichtiger Beitrag kam ebenfalls in dieser Zeit von Johann Carl Friedrich Gauß (1777 – 1855). Während seinen Landvermessungen entdeckte er, dass sich Messfehler normalverteilt verhalten und führte diese Normalverteilung (auch unter Gauß- oder Glockenkurve bekannt) näher aus. Er beeinflusste damit nicht nur das Risikomanagement sondern auch die Statistik und Wahrscheinlichkeitsrechnung.

Bis ins 20. Jahrhundert wurde Risiko meist mit dem Versicherungswesen gleichgesetzt. Mit Ausbruch des ersten Weltkriegs änderte sich diese Sichtweise und auch die klassische Ökonomie wurde nicht mehr als risikofrei angesehen [26].

Linguistisch lässt sich der Ursprung des Wortes "Risikoäuf das arabische *"risq"* oder lateinische "*riscum*" zurückführen. Das lateinische "*riscum*"bezieht seine Ursprünge aus der Seefahrt [27].

Mathematisch ist das Risiko definiert als:

$$R = p(E) * C \tag{1.1}$$

wobei *p(E)* die Eintrittswahrscheinlichkeit des Ereignisses und C die Kosten zur Behandlung des Risikos bezeichnen.

Die Berechnung von tatsächlichen Risikokosten ist in der Praxis jedoch nicht immer eine triviale Aufgabe. Als Beispiel werden hier mögliche Garantie- und Haftungskosten für ein verkauftes Produkt herangezogen.

Beispiel: Für Produkte, die ein Unternehmen bereits über einen längeren Zeitraum

hergestellt hat oder Produkte, die in großen Mengen produziert werden, liegen einem Unternehmen üblicherweise bereits historische Daten zu Garantiekosten und Wahrscheinlichkeiten vor. Dies verhält sich ähnlich einem Würfelwurf. Würfelt man z.B. 1.000-mal wird die Summe aller gewürfelten Punkte zwischen 3.000-4.000 liegen. Würfelt man jedoch nur einmalig ist jede Zahl zwischen 1 und 6 gleich wahrscheinlich. Aufgrund von historischen Daten und den daraus ableitbaren Wahrscheinlichkeiten kann somit der Erwartungswert für eine mögliche Schadenssumme errechnet werden.

Angenommen, es wurden 10.000 Stück Autos produziert. Von diesen 10.000 Stück sind 100 ein Garantiefall (1%). Das Schadensausmaß beträgt 15.000€. Das Risiko bzw. die zugehörigen Risikokosten berechnen sich daher wie folgt:

$$C = 15.000 * 1 \tag{1.2}$$

Die Risikokosten sind bei der Beachtung der obigen Formel daher 150€.

ISO/FDIS 31000:2009 definiert Risiko als "*effect of uncertainty on objectives*", wobei der genannte Effekt sowohl positiv als auch negativ gesehen wird.

Ähnliche Definitionen finden sich in fast allen Ansätzen des Risikomanagements, so zum Beispiel in der Cert/Octave-Methode [1], einer von der Japanischen Nationalbank entwickelten, sehr verbreiteten Methode [3], sowie auch im BCI-Handbuch "*Business Continuity in an Uncertain World*"[4].

1.2 Zielsetzung

Im ersten Kapitel dieser Arbeit werden die grundlegenden Mechaniken der Risikoanalyse behandelt. Dabei wird insbesondere auf das Risk Assessment eingegangen.

Des Weiteren wird BCP/BCM literarisch aufgearbeitet und die geläufigsten Standards erläutert.

Im zweiten Teil dieses Kapitels wird aus diesen beiden beleuchteten Themengebieten das triggerbasierte BCM näher ausgeführt und dessen Vorteile dargelegt. Als Fallbeispiel wird die Bank of Japan benutzt.

Das dritte Kapitel erläutert den Themenbereich Maturity Modells und stellt derzeit aktuelle Modell vor. Der Hauptpunkt dieses Kapitels bildet die Erstellung eines eigenen Maturity Modells.

Im nächsten Kapitel wird eine Case Study eines typischen österreichischen Klein- und Mittelbetriebs erstellt. Dazu wird die aktuelle Infrastruktur visuell dargestellt und mit Hilfe der vorgestellten und entwickelten Methoden ein BCM-Szenario angewandt.

Abschließend folgen eine Ergebnisdiskussion sowie eine Conclusio.

2 Grundlagen

Dieses Kapitel gibt eine Einführung in Business Continuity Management und Risk Assessment. Die behandelten Themen umfassen Definitionen, Standards und Anwendungsszenarien.

2.1 Risk Assessment

In einem Unternehmen oder der IT wird als Risikomanagement die Gesamtheit aller Maßnahmen, die zum definierten Umgang mit Risiken führen, bezeichnet. Das Risikomanagement soll spezifische Risiken einer Organisation identifizieren und für diese Risiken angemessene Reaktionen definieren. [27] definiert das Risikomanagement als einen formalen Prozess der die Identifikation, Beurteilung und Behandlung von Risiken ermöglicht.

Der ISO/FDIS Standard 31000:2009 teilt innerhalb des sogenannten Risikomanagementprozesses das Risikomanagement in insgesamt 7 Phasen - 5 aktive Phasen und 2 Meta-Phasen. Abbildung 2.1 stellt diese grafisch dar. [25]

Eine deutsche Übersetzung des Begriffes Risk Assessment fällt schwer. Gängige Wörterbücher übersetzen assessment etwa mit Prüfung, Bewertung, Beurteilung oder Analyse. “Risikoanalyse” kann nicht als Übersetzung für risk assessment herangezogen werden, da die risk analysis ein Teilbereich dieser ist. Ebenso ist Bewertung eine 1-zu-1 Übersetzung für die risk evaluation. Auch die Beurteilung ist keine geeignete Übersetzung, da, um etwas beurteilen zu können, bereits eine Beurteilungsgegenstand vorhanden sein muss (=Risiken), welche erst in der Teilphase risk

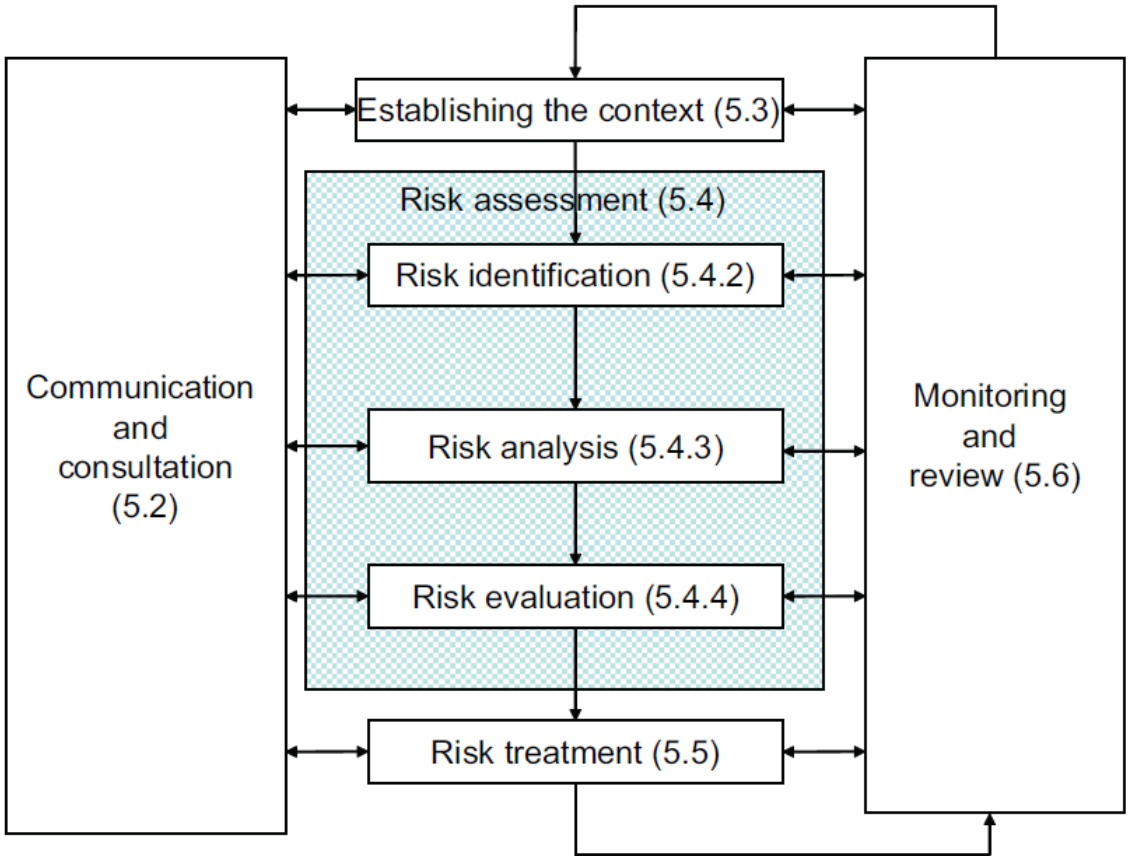

Abbildung 2.1: ISO 31000 Übersicht Phasen [25]

identification identifiziert werden. Daher wird folglich in dieser Arbeit als deutsche Übersetzung für risk assessment das Wort **Risikoprüfung** herangezogen.

Im Folgenden werden die drei Teilphasen näher erörtert.

2.1.1 (a) risk identification (Risikoidentifizierung):

Die Identifikation der Risiken umfasst eine möglichst vollständige Erfassung und Dokumentation aller Gefahrenquellen und Störpotentiale eines Unternehmens zu einem bestimmten Zeitpunkt [4]. Ergebnis dieses Schrittes ist eine umfangreiche und, wenn möglich, taxative Liste aller möglichen Risiken des betroffenen Bereiches. Dies ist wichtig, da in diesem Schritt nicht identifizierte Risiken, in weiteren Phasen des Risikomanagements nicht weiter behandelt und berücksichtigt werden.

ISO/FDIS 31000:2009 definiert die Risikoidentifikation als den Prozess zum Auffinden, Erkennen und Beschreiben von Risiken. Dabei sollen Risikoquellen, betroffene Risikobereiche, Risikoereignisse sowie deren Folgen und Konsequenzen erkannt werden. Die Folgen und Konsequenzen sind als Szenarios zu verstehen, welche einen Vorausblick und eine Abschätzung liefern sollen, wie die Auswirkungen eines Eintritts eins Risikos aussehen könnte.

Die Risikoidentifizierung erfolgt auf Basis von internen und externen Informationen. Diese können sowohl auf historische Daten, theoretischen Analysen, Expertenmeinungen, Brainstorming, Arbeitsgruppen oder den Interessen der Stakeholder basieren.

In Bezug auf Business Continuity Planning sind insbesondere Risiken aus den Bereichen Naturkatastrophen, Stromversorgung und Ressourcen verstärkt zu betrachten. Weniger relevant sind hingegen Finanzrisiken oder Marktrisiken.

2.1.2 (b) risk analysis (Risikoanalyse):

ISO/FDIS 31000:2009 definiert die Risikoidentifikation als den Prozess um den Typ des Risikos und dessen Level zu erfassen. Als Risikolevel ist das Risikoausmaß zu

verstehen, welches wiederum die Kombination der Konsequenzen (Kosten) und der Eintrittswahrscheinlichkeit ist.

Die Risikoanalyse bildet schlussendlich nicht nur die Basis für die Risikoevaluation, sondern auch die Entscheidungsbasis dafür, wie Risiken behandelt werden.

2.1.3 (c) risk evaluation (Risikoevaluierung):

In der Risikoevaluierung werden die Ergebnisse der Risikoanalyse mit den Risikokriterien verglichen und daraus abgeleitet, inwiefern ein Risiko behandelt werden muss (iaW. Signifikanz des Risikos feststellen). Des Weiteren wird für die Implementierung eine Prioritätsliste erstellt [25]. Bei dem Vergleich wird insbesondere das Risikolevel mit den Risikokriterien verglichen.

Es soll angemerkt werden, dass ein Risiko nicht unbedingt im engeren Sinn "behandelt"werden muss. Eine Behandlung im weiteren Sinn kann auch die Akzeptanz oder gar die Ignoranz eines Risikos (aus Gründen der Marginalität) sein. Jedoch kann das Ergebnis der Risikoevaluierung zu einem Risiko auch sein, dass eine tiefergehende Betrachtung nötig ist.

Risikokriterien müssen von der Organisation selbst definiert werden und können auf deren strategischen Zielen basieren oder auch von Standards, Gesetzen oder Policies abgeleitet werden.

Es wird empfohlen, dass die Risikokriterien bereits zu Beginn der Etablierung des Risikomanagementprozesses festgelegt sowie kontinuierlich überprüft werden. Bei der Definition dieser Kriterien sollten folgende Faktoren mit einfließen:

- Welchen Typen von Risiken werden betrachtet (z.B. Natur, menschlich, technisch etc.)?

- Welche Arten von Konsequenzen können sich ergeben und wie werden diese gemessen (Ruf, Geld, etc.)?

- Wie hoch wird die Eintrittswahrscheinlichkeit definiert?
- Welche Risikolevel sind vorhanden (1-5, etc.)?
- Wie wird der Level eines Risikos bestimmt?
- Ab wann ist ein Risiko akzeptierbar?

Diese grundsätzliche Vorgangsweise für die Behandlung von Risiken ist im Rahmen dieser Masterarbeit von fundamentaler Bedeutung und wird als Basis für die Risikobehandlung verwendet.

2.2 Business Continuity (BCP/BCM)

Die Fähigkeit den laufenden Betrieb in heutigen Unternehmen aufrecht zu erhalten wird von vielen Faktoren beeinflusst (eine genaue Darstellung von Business Continuity Planning findet sich z.B. in [35]). Neben eher in unseren Breiten unrealistischen Szenarien wie Terrorismus oder Tsunamis, sind doch Gefahren gegeben. Das Jahrhunderthochwasser in Österreich 2002 hatte massive Auswirkungen auf Unternehmen in Bereichen von Flüssen wie der Donau, Ybbs oder Enns. So musste die Firma Engel in Oberösterreich ihren Betrieb für mehrere Tage vollständig einstellen.

Um die Existenz eines Unternehmens sicherzustellen, ist es möglich sich auf potenzielle Bedrohungen, Schäden und Folgen vorzubereiten. Dieser Prozess wird unter dem Begriff Business Continuity Management zusammengefasst. [1]

Ähnlich wie viele Prozesse, ist BCM nicht mehr als klassischer Prozess, sondern als Lifecycle zu verstehen. [4] gibt hierbei in seinem Good Practice Guide einen allgemein gültigen und leicht verständlichen Lifecycle vor. Dieser ist Abbildung 2.3 zu sehen.

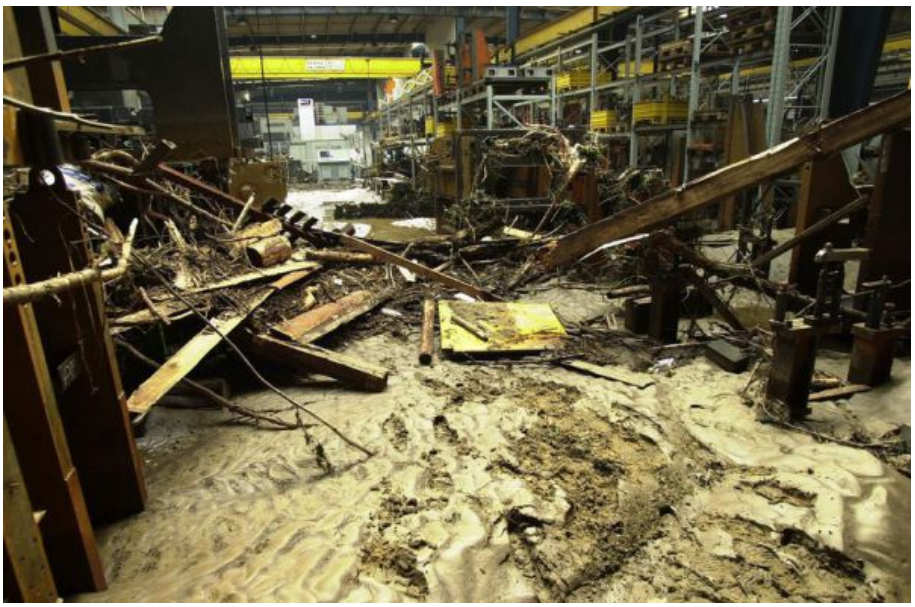

Abbildung 2.2: Zerstörungen bei der Fa. Engel/Schwerberg nach dem Hochwasser 2002 (C by Wassermann)

Ähnlich dem ISO 27001 Lifecycle PDCA (Plan-Do-Check-Act), ist hier ein kontinuierliches Review sowie das Einfließen der Review-Ergebnisse in die Verbesserung Herzstück des Prozesses.

Dieser Lifecycle bzw. Prozessansatz wird auch von der ENISA unterstützt und gelebt. Als Standardvorgehensweise werden hierbei folgende Schritte empfohlen [17]:

- Definition eines BCM Frameworks
- Durchführen einer Risikoanalyse
- Entwickeln eines BCM-Ansatzes
- Ausrollen des BCP-Plans
- Testen der BCP-Maßnahmen
- Erhalten und Verbessern des BCM

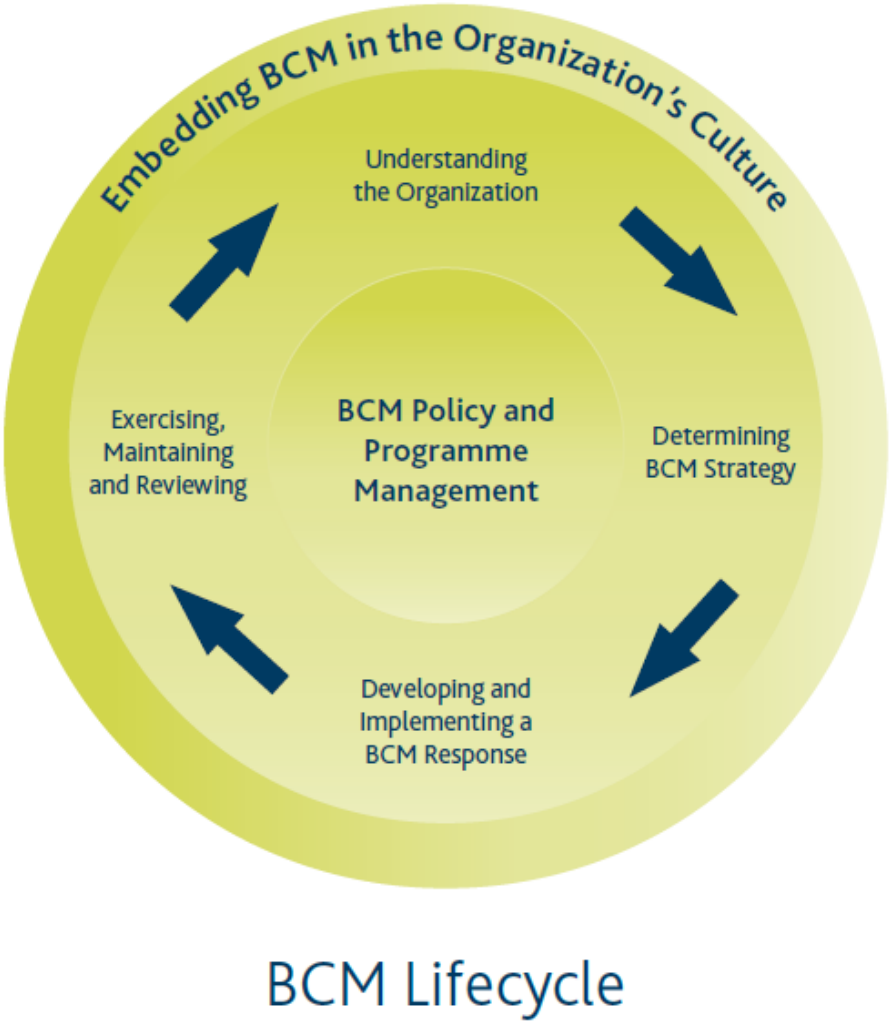

Abbildung 2.3: BCM Lifecycle nach BCI [4]

Dieser Lifecycle-Prozess ist ähnlich durch die Organisationen BCI (Business Continuity Institute), London First und die britische NaCTSO (National Counter Terrorism Security Office) definiert [5]. Dieser Prozess ist in Abbildung 2.4 dargestellt. Die verschiedenen Phasen bauen darauf auf eine Checkliste zur Verfügung zu stellen, um Unternehmen die Planung von BCM zu erleichtern. Dabei wird auch die Risikoevaluierung miteinbezogen. Jedes negative Ereignis, dass auf ein Unternehmen wirkt kann zu Problemen wie Auftragsverluste an die Konkurrenz, Rufschädigung, höhere Versicherungsprämien oder Schwierigkeiten im Supply-Chain-Management führen.

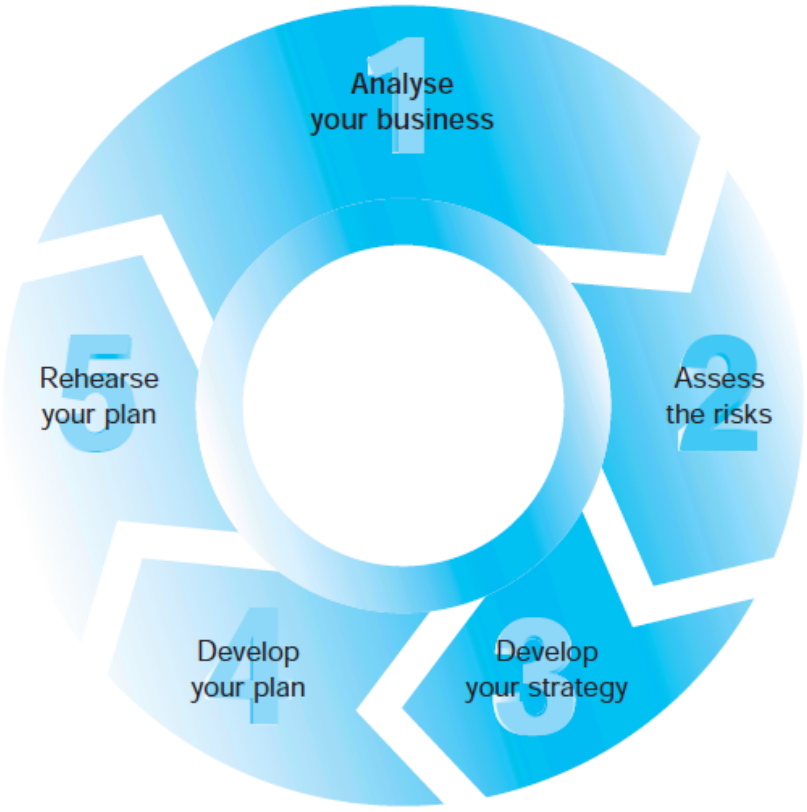

Abbildung 2.4: BCM-Prozess nach BCI/London First/NaCTSO [5]

Es ist an dieser Stelle jedoch anzumerken, dass BCM nicht nur Katastrophenmanagement im Fokus hat. BCM muss als Geschäftsprozess angesehen werden und ein breites Spektrum von Managementprozessen integrieren. Dazu zählen neben dem klassischen Katastrophenmanagement u.a. Risikomanagement, Gebäudemanagement, Krisenmanagement, Human Resources, Sicherheit oder auch PR. Insbesondere sollte der Fokus nicht ausschließlich auf IT-Belange fallen, da ansonsten wichtige andere Bereiche zu wenig Aufmerksamkeit erhalten.

Im Bereich BCP/BCM sind mittlerweile sehr viele Standards und Vorgaben publiziert:

- **BCI Good Practice Guide 2008**: Diese Richtlinie wurde zur Ergänzung des BS 25999 entwickelt. [6]

- **BS 25999**: Der britische Standard beschreibt ein Code of Practice für das BCM. Es ist möglich ein im Unternehmen etabliertes Business Continuity Management System nach diesem Standard zertifizieren zu lassen. [12]

- **BSI 100-2**: Das deutsche Werk beschreibt wie die IT-Grundschutz Methode implementiert werden kann. Der Hauptteil beschäftigt sich wie relevante Daten gesammelt werden können und das Informationssystem geschützt werden kann. Diese Information kann als Input für ein BC Programm dienen. [9]

- **ISO/IEC 24762:2008** (Guidelines for information and communications technology disaster recovery services): Der internationale Standard gibt Richtlinien zur Bereitstellung von IKT-Disaster-Recovery-Diensten vor. Es werden Anforderungen an die Implementierung, Betrieb, Monitoring und Aufrechterhalten dieser Dienste spezifiziert. Des Weiteren werden die Themen Auswahl einer Backup-Einrichtung sowie der kontinuierliche Dienst-Verbesserung behandelt. [24]

- **FEMA 141**: Dieser Standard beschäftigt sich vorwiegend mit der Entwicklung eines Incident-Response-Plans. Es werden daher keine eigentlichen BCP Aufgaben behandelt, jedoch ist ein gutes Incident-Handling Voraussetzung für ein funktionierendes BCM. [18]

- **CObIT**(Control Objectives for Information and related Technology): Der in der Wirtschaftsprüfung relevante Standard ist eine Sammlung von Best Practices für das Management der IT. Es werden Maßnahmen, Indikatoren und Prozesse geliefert, um die IT effizient zu gestalten. Zwar ist CObIT nicht ein spezifischer BCM Standard, jedoch ist die Abhandlung innerhalb von CObIT, insbesondere in Hinsicht auf das Reifegradmodell, des BCM weit verbreitet. [22]

- **FSA BC** (The Financial Services Authority Business Continuity Management Guide): Diese britische Vorgabe zielt auf Unternehmen aus dem Finanzsektor ab und erklärt u.a. Zeitpläne für das Recovery nach BCM-relevanten Vorfällen. [19]

- **HB 292-2006**: Das australische Handbuch beschreibt sehr genau alle Phasen und Elemente eines BCP. Auch liefert es Beispiele und Vorlagen. [34]

- **NFPA 1600** (Standard on Disaster/Emergency Management and Business Continuity Programs): Der Standard behandelt zwar alle Elemente des BCP, hat jedoch einen starken Focus auf das Disaster-Management sowie auf Kollaboration bei verteilten Unternehmensstandorten. [28]

- **NIST 800-34:2006** (Contingency Planning Guide for Federal Information Systems): NIST 800-34 ist ein Regelwerk, welches zur Entwicklung eines BCP herangezogen werden kann. Der Fokus liegt jedoch primär auf der Weiterführung und Aufrechterhaltung von einzelnen Services, nicht auf die eines gesamten IT-Systems. [29]

- **Pas 77**: (IT Service Continuity Management). Die öffentliche Spezifikation Pas 77 beinhaltet Elemente des BCP. In Kombination mit klassischen BCP Methoden können damit zuverlässige BCM-Pläne erstellt werden. [11]

Es ist durchaus vertretbar zu behaupten, ein Business Continuity Plan - je nach Unternehmensgröße - ist in einer Minimalform essenziell. Der Plan ist als Informationsgrundlage mit Handlungsanweisungen im Notfall zu betrachten.

Ein weiterer Teil eines solchen Plans können sogenannte Szenariotests sein. Innerhalb des Plans werden verschiedene mögliche Outcomes (Szenarien) erarbeitet und die notwendigen Reaktionen darauf einerseits definiert und andererseits auch für den Ernstfall getestet. Realistisch kann natürlich nicht für jede einzelne Möglichkeit ein eigenes Szenario erstellt werden. Daher ist auf eine möglichst breite Abdeckung an Szenarien sowie eine allgemeinere Anwendbarkeit dieser zu achten. Diese allgemeine Anwendbarkeit oder Ganzheitlichkeit ist ein wichtiger Faktor für den Erfolg eines BCM-Plans.

2.3 Risk Assessment als Ausgangspunkt für BCP/BCM

Nach der Klärung der theoretischen Bereiche und Fragenstellung der beiden Thematiken Risk Assessment und BCP/BCM sollen diese nun im folgenden Kapitel zueinander abgestimmt werden. Dazu werden die Bereiche des Risk Assessment für das BCP/BCM detailliert betrachtet und Beispiele entwickelt.

Dieser Schritt ist auch für das BCP/BCM essenziell, da nur dadurch die nötigen Maßnahmen und Strategien entwickelt werden können, um den (IT-)Betrieb aufrecht zu erhalten bzw. wiederherzustellen.

Als in den Risikokriterien festgelegte Risikotypen werden nach dem BSI Gefährdungskatalog [10] folgende betrachtet:

- G1 - Höhere Gewalt
- G2 - Organisatorische Mängel
- G3 - Menschliche Versagen
- G4 - Technisches Versagen
- G5 - Vorsätzliche Handlungen

2.3.1 (a) risk identification (Risikoidentifizierung)

Unabhängig vom Risikotyp ist für jedes Risiko auch die Risikoquelle zu identifizieren. Das können u.a. sein:

- Geographischer Ort

- Interne Bedrohung (Zugangsbestimmung, Sicherheitsbestimmungen etc.)
- Externe Bedrohungen (Nachbareinrichtungen)
- Nähe zu Einsatzkräften

Mögliche Risiken sind in Abbildung 2.5 aufgeführt.

Abbildung 2.5: Mögliche Risiken nach BSI-Level (Eigener Entwurf)

Eine Studie [14] des Storagespezialisten CNT ergabt, dass die Risiken bzw. Ursachen für konkrete Ausfälle durchaus sehr heterogen sind. Aus einer Analyse von 582 Vorfällen wurden 16 verschiedene Quellen festgelegt, wobei Stromausfälle mit 16% den größten Anteil der Ursachen ausmachten. Abbildung 2.6 stellt die Ursachenverteilung der Studie grafisch dar.

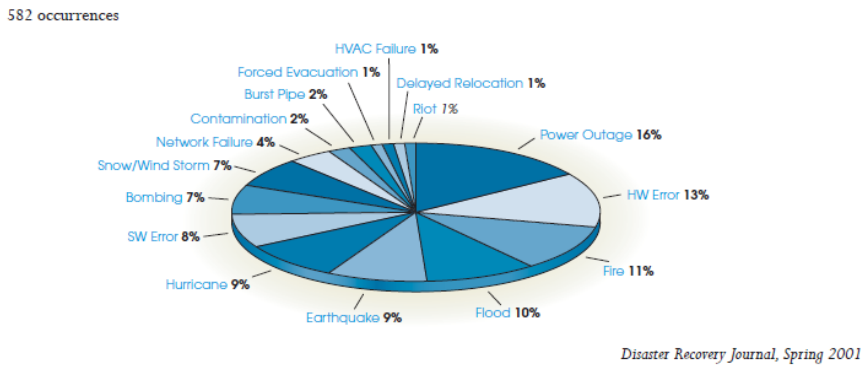

Abbildung 2.6: Verteilung der Ursachen für Ausfälle [14]

2.3.2 (b) risk analysis (Risikoanalyse)

Zur Risikoanalyse sind eine Eintrittswahrscheinlichkeit sowie die Risikokonsequenzen zu bewerten. Empfehlenswert ist dazu eine Risikomatrix (vgl. Abbildung 2.7).

	Schaden/Auswirkung			
Wahrscheinlichkeit	**Niedrig**	**Mittel**	**Hoch**	**Sehr hoch**
Sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
Wahrscheinlich	gering	mittel	hoch	hoch
Möglich	gering	gering	mittel	mittel
Unwahrscheinlich	gering	gering	gering	gering

Abbildung 2.7: Risikomatrix (Eigener Entwurf)

Die Risiken werden klassifiziert und einem Level zugewiesen. Diese Level (bei BSI Grundschutz heißen diese Schutzbedarf) können sein:

- **Gering**: Die Schadensauswirkungen sind minimal.
- **Normal**: Die Schadensauswirkungen sind begrenzt unüberschaubar.
- **Hoch**: Die Schadensauswirkungen können beträchtlich sein.

- **Sehr hoch**: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

2.3.3 (c) risk evaluation (Risikoevaluierung)

Die Ergebnisse der Risikoanalyse werden in diesem Schritt nun in dem Sinne evaluiert, inwiefern wie mit dem Risiko weiter zu verfahren ist. Es ist die Signifikanz der Risiken zu ermitteln. Daraus ist eine Prioritätenliste zu erstellen.

Sobald das Risk Assessment abgeschlossen ist, sollte nicht für jede einzelne Bedrohung bzw. Risiko eine Business Continuity Vorgangsweise entworfen werden, sondern diese nach Auslösern gegliedert werden. Diese Idee basiert darauf, dass es eine bestimmte Anzahl an Ereignisse gibt, auf welche auf eine bestimmte Art reagiert werden kann. Somit ist eine endliche Abdeckung möglich. Auch ist denkbar, dass durch ein Risiko oder eine Bedrohung mehrere Auslöser betroffen sind.

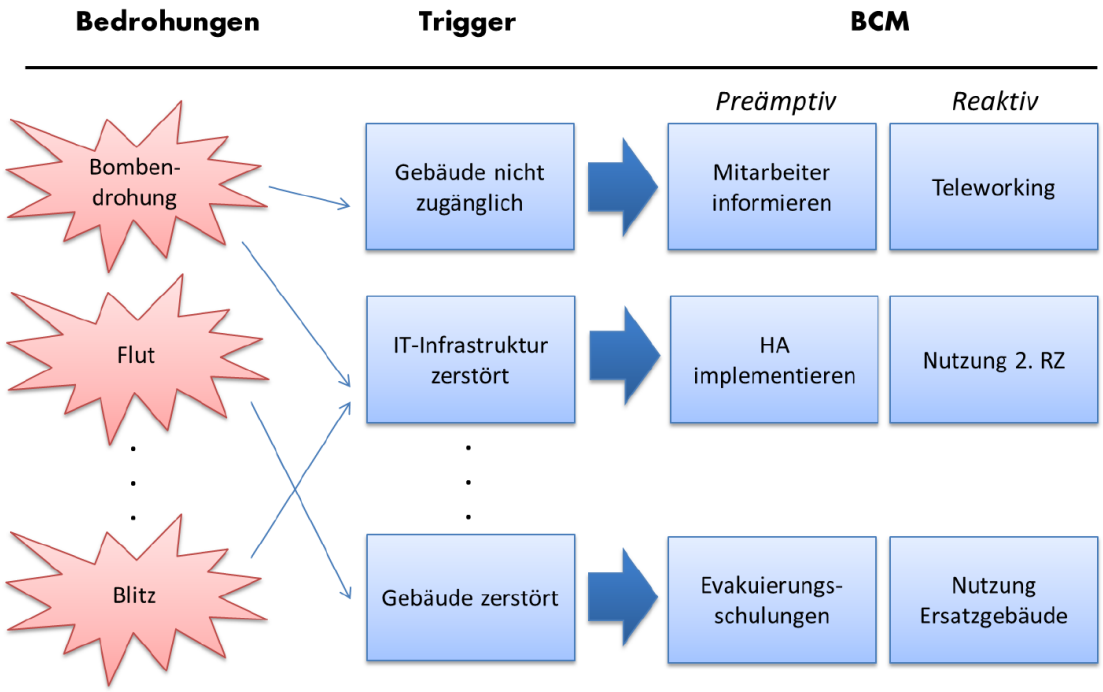

Abbildung 2.8: Trigger-basiertes BCP (Eigener Entwurf)

Weiterführend kann dieser Ansatz durch die Abkehr des klassischen Risk Assess-

ments gesehen werden. Die Problematik entsteht durch die Schwierigkeit der Erstellung eines Risk Assessment. Zwei Problematiken ergeben sich zum Risk Assessment:

- Selbst nach Abdeckung und genauer Betrachtung möglicher Risiken, ist es denkbar, dass ein Risiko eintritt, dass nicht betrachtet wurde

- Wenn das Risk Assessment zu detailliert ausgeführt wird, verwandelt sich die Analyse schnell in eine Sammlung unrealistischer Szenarien

Ein Ausgehen von den oben angesprochenen Triggern ist daher die zu empfehlende Strategie. Weitere solche Trigger können sein:

- Gebäude nicht zugänglich

- Gebäude zerstört

- Hardware oder Software Fehler

- Stromausfall

- Etc.

Im Folgenden wird ein Beispiel zur Unabhängigkeit vom Fehlerfall näher beschrieben: Das Szenario „Gebäude nicht zugänglich“ ist eingetreten, da das zentrale Schlüssel- und Sperrsystem fehlerhaft arbeitet. Somit können Mitarbeiter nicht zum Arbeitsplatz gelangen. Abhilfe dafür würden Telearbeitsplätze schaffen, da die Infrastruktur virtuell zugänglich ist. In dem Fall eines Chemieunfalles in der Nähe des Unternehmens ist ebenfalls das Szenario ”Gebäude nicht zugänglichänwendbar: Hardware, Software und IT-Infrastruktur sind zwar benutzbar, jedoch können die Mitarbeiter nicht zum Arbeitsplatz gelangen.

Die ENISA sieht in ihrer Publikation [17] ebenfalls einen direkten Konnex zwischen Risk Assessment und Business Continuity Planning. Abbildung 2.9 zeigt eine exemplarische Darstellung der Zusammenhänge zwischen den verschiedenen Dis-

ziplinen. Eingebettet in die Corporate Governance (GC) hat das BCM nicht nur starke Überschneidungen mit dem Risk Management (somit dem Risk Assessment), sondern auch mit dem IT-Risikomanagement sowie der zuständigen Stelle für Services.

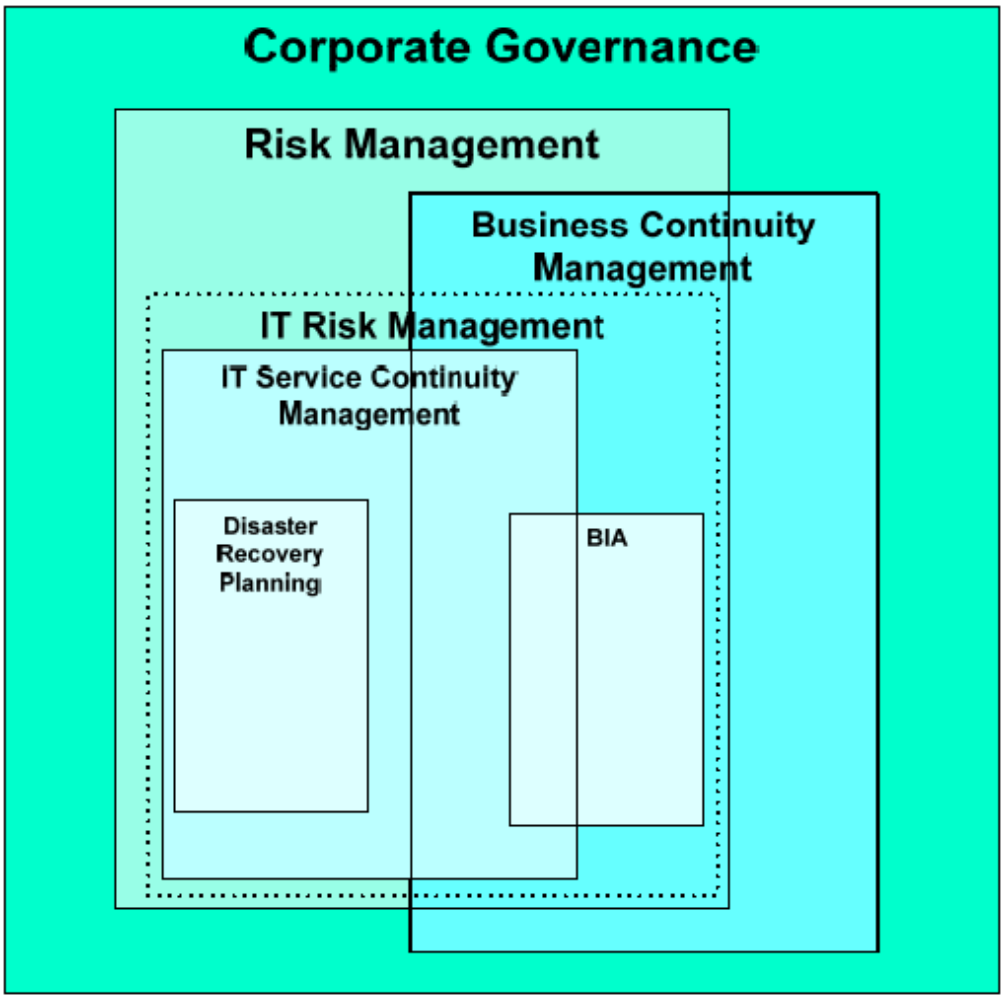

Abbildung 2.9: Verzahnung BCP und Risk Management [17]

Das behandelte Beispiel zeigt klar auf, dass eine gewissenhafte und vorbereitete Strategie zur Evaluierung und Bewertung von Risiken nötig ist, da ansonsten schnell der Umfang zu einer Herausforderung für das gesamte Business Continuity Management wird. Auch ist klar, dass ein Risk Assessment unumgänglich ist.

2.4 Fallbeispiel: BCP am Beispiel Bank of Japan

Die "Bank of Japan"[3] ist eine der wichtigsten Banken Japans. Nach den Terroranschlägen von New York von 2001 hat die Bank sich um ein Business Continuity Programm bemüht. Dabei konzentriert sich das Unternehmen einerseits auf die Minimierung der Auswirkungen einer Katastrophe und andererseits auf die höchst mögliche Continuity, um ihre Aufgaben auch im Katastrophenfall ausführen zu können.

Es soll hier aufgezeigt werden, dass die Bank einen Trigger-basierten Ansatz verfolgt und damit die Aufwände für das BCP im Rahmen halten kann.

Die "Bank of Japan"hat 3 Risikotypen definiert (ähnlich BSI Katalog):

- Naturkatastrophen
- Von Menschen verursachte Ausfälle (Auch Terroranschläge)
- Technische Ausfälle (Strom, Equipment etc.)

Daraus wurden im Weiteren 3 Szenarios abgeleitet, welche als Trigger dienen:

- Hauptstandort in Tokio ist voll funktionsfähig, aber das Hauptrechenzentrum ist nicht mehr einsatzfähig
- Hauptstandort in Tokio nicht mehr betriebsfähig, aber Hauptrechenzentrum voll funktionstüchtig
- Hauptstadtort und Hauptrechenzentrum in Tokio sind nicht einsatzfähig

Diese Szenarios sind unabhängig vom Auslöser immer mit einer vorgegeben Abhandlungsweise zu behandeln.

Um diese BCP zu ermöglichen, wurden folgende Maßnahmen getroffen. Diese betreffen sowohl den organisatorischen, personellen als auch den infrastrukturellen Be-

reich:

- **Disaster Management Team**: Dieses etablierte Team ist ein Kernstück des Konzepts der Bank of Japan. Es beansprucht die zentrale Verantwortung, Monitoring und Behandlung sämtlicher Belange der Business Continuity. Ebenfalls ist das Team für die Kommunikation mit internen als auch externen Stakeholdern zuständig.

- **Personal**: Im Bereich Personal wurden Maßnahmen getroffen, um im Katastrophenfall Ansprechpersonen zur Verfügung zu haben. Dies betrifft beispielsweise Bereitschaftsdienste während Nacht- oder Urlaubszeiten.

- **Kommunikation**: Um die physische Kommunikationsstruktur des Headquarters in Tokyo aufrecht erhalten zu können, wurden Standleitungen, Telefon- und Faxgeräte für den Notfall und ein drahtloses Netzwerk (ausschließlich für den Notfall) eingerichtet. Als weiteres Standbein zur Informationsverteilung werden Webseiten genutzt.

- **Zweitstandort**: Ein Backup-Rechenzentrum wird räumlich getrennt vom Hauptstadtort betrieben.

Da die Bank of Japan sich als zentrale Bank in Japan sieht, hängt von einer Aufrechterhaltung des Betriebs, nicht nur der Unternehmenserfolg ab, sondern auch politische und nationale Folgen spielen hier eine Rolle. Daher wurden gesellschaftsrelevante Operationen definiert, welche selbst in einem sehr schwerwiegenden Fall – Headquarter und Hauptrechenzentrum in Tokyo sind abgekapselt – betrieben werden sollen.

Dies betrifft für Tokyo:

- Bargeldausgabe

- Beobachtung des Zahlungsmarktes

- Finanzielle Notfallmaßnahmen in der betroffenen Region

Dies betrifft für Osaka:

- Geschäftsbetriebsverlagerung nach Osaka
- Betrieb des BOJ-NET (Bank of Japan Financial Network System)
- Durchführung von erfassten Transaktionen sowie wenn nötig eine Erweiterung der Kreditrahmen
- Informationsmanagement mit ausländischen Institutionen und Märkten

Essenziell für den IT-Betrieb ist das BOJ-NET. Dieses ist ein Computersystem, welches alle Standorte des Unternehmens verbindet und zur Verarbeitung sämtlicher Geschäftstransaktionen, insbesondere für die japanischen Regierungsgeschäfte, zuständig ist. Es handelt sich hier also um ein hoch kritisches System.

Der Business Continuity Plan der Bank of Japan ist ein etabliertes Werk und wird in der Literatur als Standardwerk angesehen. ([8], [2])

2.5 Fallbeispiel: Lernen aus der Vergangenheit - 11. September 2001

Die New York Times schrieb am 29. Januar 2002 in einem Artikel zur Thematik, dass mehrere Unternehmen an der Wall Street beschlossen die Arbeitsplätze mehrerer tausend Mitarbeiter in Vororte von New York zu verlegen: „*Nie wieder möchten diese globalen Unternehmen erleben, dass sie wegen einem einzigen katastrophalen Ereignis für Stunden, Tage oder Wochen den Betrieb einstellen müssen.*“

Die Terroranschläge von 11. September 2001 waren der ultimative Business Continuity Management Test der ansässigen Unternehmen. Die Qualität des BCM-Plans und die damit verbundene Wiederaufnahme der Betriebstätigkeit entschied über Millionenverluste und über den Unternehmensfortbestand mancher Firmen.

Natürlich ist ein solches Terrorereignis deutlich seltener als ein Brand im Rechenzentrum oder ein Ausfall von Hardware. Trotzdem wurde den Verantwortlichen durch die Terroranschläge ins Bewusstsein gerufen, dass es nicht völlig auszuschließen ist.

Das Unternehmen Deloitte-Touche-Tohmatsu war eines der betroffenen Unternehmen. Die Firma beschäftigte knapp 3.000 Mitarbeiter direkt gegenüber dem World Trade Center. Neben der Umschaltung des Datenzentrums auf Backup-Standorte mussten für die Mitarbeiter - zumindest temporär - Ersatzarbeitsplätze zur Verfügung gestellt werden. Deloitte-Touche-Tohmatsu veröffentlichte die wichtigsten Erkenntnisse aus den Ereignissen des 11. September für die Allgemeinheit [15]. Dazu zählen insbesondere:

- **Menschen sind nicht ersetzbar:** Während man Backup-Rechenzentren relativ einfach im Vorab organisieren kann, gibt es nur wenig Spielraum Backup-Mitarbeiter zu planen. Mehrere Unternehmen haben deshalb beschlossen, Büros außerhalb von großen Städten dauerhaft anzumieten. Diese Büros sollen Schlüsselfiguren im Notfall dazu dienen, den Betrieb aufrecht zu erhalten. Diese sind im vollen Umfang ausgestattet und jederzeit bezugsbereit. Dabei ist zu beachten, dass insbesondere bei Terroranschlägen Mitarbeiter persönlich betroffen sein können und aus psychischen Gründen nicht zur Arbeit erscheinen können.

- **Geographische Agglomeration ist ein Risiko:** Unternehmen die im Falle des 11. Septembers sämtliche ihrer Räumlichkeiten in Lower Manhattan hatten, waren am meisten betroffen. Daher wird empfohlen die Unternehmensstandorte - insbesondere in Städten - geografisch weiter zu trennen.

- **Computerarbeitsplätze sind essenziell:** Zwar wurde in vielen Unternehmen ein BCM-Plan für Rechenzentren erstellt, die konkrete Einrichtung für die Arbeitsplätze von Mitarbeitern fehlte allerdings. So konnte der Betrieb nicht weitergeführt werden, weil PCs oder Netzwerkeinrichtung nicht vorhanden bzw. nicht einsatzbereit waren. Abbildung 2.10 stellt die BCM-Investition in die verschiedenen Bereiche sowie die tatsächlichen Auswirkungen dieser bei den Anschlägen vom 11. September 2001 gegenüber. Es ist auch hier klar zu erkennen, dass Rechenzentren zwar stark bedacht wurden, die Bereiche rund um die Mitarbeiter und deren täglichen Arbeitsabläufe jedoch eindeutig zu wenig Beachtung fanden.

- **Verkehrssysteme sind nicht unverwundbar**: In den meisten BCM-Plänen vor dem 11. September ging man davon aus, dass das öffentliche Verkehrssystem dauerhaft verfügbar sei. So wurde beispielsweise in Plänen vorgeschlagen, dass Mitarbeiter per Flugzeug zu Backup-Einrichtungen gebracht werden sollten. Die Realität sah jedoch anders aus: Als Reaktion auf die Anschläge wurde der gesamte Luftraum in den USA für mehrere Tage gesperrt. Unter Androhung eines Abschusses wurden alle noch in der Luft befindlichen Flugzeuge aufgefordert, den nächstmöglichen Flughafen anzusteuern. Kein ziviles Flugzeug durfte mehr starten. Des Weiteren wurden alle Brücken und Tunnel nach Manhattan geschlossen.

- **Kommunikation ist eingeschränkt:** Eine Umsetzung der BCM-Pläne wird erschwert durch die Einschränkung der Kommunikationsmöglichkeiten. Durch das Ausmaß des Ereignisses waren einerseits wichtige Knotenpunkte zur Telekommunikation zerstört und andererseits die Verbliebenen durch den Informationsdrang der Bürger überlastet.

- **Testen ist wichtig:** Ein BCM-Plan kann noch so gut formuliert und durchdacht sein. Ist er in der Praxis nicht ausgetestet ist er quasi wertlos.

Dazu können Fragen wie *Was ist, wenn Mitarbeiter nicht zu ihrem Arbeitsplatz gelangen können?, Wie und wie schnell können wir alle Mitarbeiter erreichen?, Wie können Entscheidungen getroffen werden, wenn die Kommunikation eingeschränkt ist?* oder *Existieren BCM-Pläne für alle Bereiche und werden diese regelmäßig getestet?* gestellt werden.

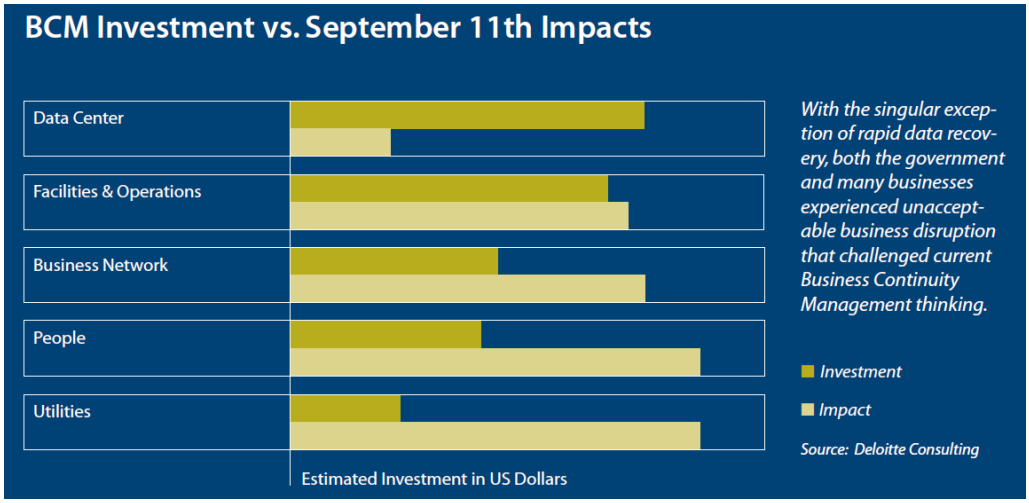

Abbildung 2.10: Gegenüberstellung der Investitionen und Auswirkungen [15]

Zwar ist die Eintrittswahrscheinlichkeit eines Terroranschlages gering, jedoch ist spätestens seit dem 11. September klar, dass es nicht völlig unrealistisch ist. Auch Europa ist in den vergangenen Jahren immer wieder mit Terroranschlägen unterschiedlichen Ausmaßes konfrontiert worden. Es sollten daher die bestehenden BCM-Pläne überdacht werden und insbesondere Bereiche neben Backup-Rechenzentren stärker fokussiert werden.

2.6 Fallbeispiel: BSI Datenschutzkonzept

2.6.1 Beschreibung

Die Sicherheit der eigenen Daten ist für die meisten Unternehmen und Behörden essenziell und wird laufend wichtiger. Die Bedeutung von Datensicherheit und die möglicherweise fatalen Auswirkungen von schlechter oder fehlender Datensicherheit

wird sowohl Führungskräften als auch Mitarbeitern immer mehr bewusst, nicht zuletzt, weil Skandale im Bereich Datensicherheit immer häufiger den Weg in die Medien finden.

Durch moderne und geeignete Datensicherungsmaßnahmen lassen sich die Risiken des Datenverlusts oder des unerlaubten Zugriffs auf Daten jedoch deutlich reduzieren. Eine funktionierende Datensicherung gewährleistet, dass durch einen redundanten Datenbestand auch bei Datenverlust der Betrieb kurzfristig wieder aufgenommen werden kann.

2.6.2 Notfallvorsorgekonzept

Standard-Maßnahmen
Bei der Umsetzung einer funktionierenden Datensicherung muss von der Erhebung der Einflussfaktoren auf die Datensicherung ausgegangen werden und eine Verfahrensweise für die Datensicherung entwickelt werden. Dabei muss unter anderem die Art der Datensicherung, die Häufigkeit und die Zeitpunkte der Datensicherung und der Lebenszyklus des Datensicherungssystems definiert werden. Die Basis dafür ist das Datensicherungskonzept, dass du Beginn erstellt werden muss.

Datensicherungskonzept
Vom Fachverantwortlichen oder vom Leiter der IT eines Unternehmens muss ein Datensicherungskonzept erstellt werden, dass aktualisierbar und erweiterbar niedergelegt werden muss. Das Konzept muss im ersten Teil den aktuellen Ist-Stand und die Motivation analysieren. Das beinhaltet Informationen zum vorhandenen und erwarteten Datenvolumen, den verwendeten IT-Systemen, der Änderungsfrequenz der Daten und der Verfügbarkeitsanforderungen. Im zweiten Teil muss das Konzept ein Lösungskonzept für die Datensicherung und Datenwiederherstellung beinhalten. Das Lösungskonzept muss aus technischer und wirtschaftlicher Sicht vertretbar sein. Außerdem müssen möglicherweise geltende rechtliche Einflussfaktoren, z. B. Datenschutzgesetze oder die verpflichtende Aufbewahrungsdauer von bestimmten Daten im Konzept beachtet werden.

Mögliche Inhaltliche Schwerpunkte im Konzept sind Definitionen zu Anwendungsdaten, Systemdaten, Software und Protokollierung, die Gefährdung Grundlage und Motivation hinter der Datensicherung und mögliche Einflussfaktoren des IT-Systems. Der Datensicherungsplan muss unter anderem die Art und Häufigkeit der Datensicherung, die Anzahl der gespeicherten Generationen, das verwendete Datensicherungsmedium und den Aufbewahrungsort für die Backup-Datenträger beinhalten. Außerdem müssen Verantwortlichkeiten, Transportmodalitäten, Wiederherstellungszeiten, mögliche Randbedingungen und weitere Anforderungen an die Datensicherung festgelegt werden.

Sollte ein umfassendes Datensicherungskonzept nicht umsetzbar sein, sollte zumindest ein Minimum Datensicherungskonzept erstellt werden. Dieses Konzept sollte zumindest Informationen zur verwendeten Software, zu Systemdaten, Anwendungsdaten, Protokolldaten und zur Durchführung der Datensicherung beinhalten.

Folgende Maßnahmen für die Erstellung und Umsetzung des Konzepts entsprechen dem aktuellen Stand der Technik und den Empfehlungen des BSI.

Personal
Mitarbeiter werden zum Thema Datensicherung geschult. Jeder Mitarbeiter ist über die Regeln der Datensicherung informiert und soll dadurch selbstständig auf Unzulänglichkeiten bei der Datensicherung hinweisen können. Zeitraum, in dem Daten gesichert werden muss auch an die Mitarbeiter weitergegeben werden, damit die wissen in welchem Zeitraum bzw. Wie lange Daten wiederhergestellt werden.

Datensicherung
Eine funktionierende und verlässliche Datensicherung Software muss neben der allgemeinen Leistungsfähigkeit mehrere Anforderungen erfüllen:

- Die Software muss mit bestehenden Systemen zusammenarbeiten können.
- Automatische Datensicherung muss zu definierten Zeitpunkten oder Intervallen möglich sein.
- Es muss definierbar sein welche Daten gesichert werden sollen und welche

nicht, die Informationen sollte in Form von Profilen speicherbar und wiederverwendbar sein.

- Vollständige und inkrementelle Kopien der Daten müssen von der Software umgesetzt werden können.

- Die Software sollte Daten miteinander vergleichen können. Die Funktion dient einerseits dazu Änderungen an gespeicherten Daten erkennen zu können und andererseits, um nach der Wiederherstellung von Daten die rekonstruierten Daten mit den gespeicherten Datensätzen vergleichen zu können.

- Bei der Wiederherstellung von Daten muss der Zielort der Wiederherstellung gewählt werden können. Die Software muss den Benutzer fragen, was mit Dateien passiert, die am Zielort bereits existieren, insbesondere wenn Dateien den gleichen Namen haben wie die zu rekonstruierende Dateien.

- Die gesicherten Daten müssen passwortgeschützt gespeichert werden können.

- Eine Durchsuchbarkeit der gesicherten Daten muss möglich sein, insbesondere nach Erstellungs- oder Modifikation Zeitpunkten.

- Eine Sicherung der Daten muss auf Netzwerk Trägern und online möglich sein.

- Falsche oder beschädigte Datenträger müssen von der Software erkannt werden.

- Änderungen und Status Updates müssen protokolliert werden und berechtigten Benutzern zugänglich sein.

Bei der Wahl der Software für die Datensicherheit soll auf professionelle und komfortable Datensicherung Wert gelegt werden. Sollte keine solche Software vorhanden sein, soll zumindest die, in den meisten Betriebssystemen vorhandene, Software zur Datensicherung verwendet werden.

Online-Sicherung

Daten werden über das Internet vom lokalen Rechner auf ein Online Speichersystem übertragen. Daten können ausschließlich über das Online Speichersystem abgesichert werden oder, in einer hybriden Variante sowohl lokal als auch online gesichert werden. Der Zugriff auf die Daten muss gesichert und nur für autorisierte Benutzer möglich sein.

Bei Online-Sicherung muss besonders auf die gesetzlichen Anforderungen bezüglich Datenschutzes und anderen möglicherweise vorhandenen gesetzlichen Verpflichtungen geachtet werden. Serviceanbieter für Online Datensicherungssysteme arbeiten laufend an der Sicherheit ihrer Systeme und bieten in den meisten Fällen zusätzliche Leistungen wie zb. Verschlüsselung an.

Softwaresicherung
Betriebssysteme und Anwendungen werden als Sicherungskopie gespeichert, um im Notfall möglichst schnell neu installiert werden zu können. Lizenznummern werden bei kostenpflichtiger Software mitgesichert. Alle Änderungen werden dokumentiert.

Physische Lagerung der Datenträger
Zugriff auf die Datenträger darf nur für autorisierte Personen erlaubt sein und muss im Notfall zeitnah möglich sein. Die Räumliche Bedingungen müssen für die langfristige Lagerung geeignet sein, was unter anderem Raumtemperatur und Luftfeuchtigkeit betrifft. Die Daten müssen physisch außerdem räumlich von den IT-Systemen getrennt sein.

Wartung und Qualitätssicherung
Die Wiederherstellbarkeit und die Verfügbarkeit der Daten müssen laufend getestet werden, damit sichergestellt ist, dass die Systeme im Bedarfsfall auch wirklich funktionieren. Es muss außerdem laufend getestet werden, ob die Datensicherung wie erwartet funktioniert.

Alte Soft- und Hardware kann dazu führen, dass die Wiederherstellbarkeit und Verfügbarkeit der Daten beeinträchtigt ist. Laufende Wartung ist daher notwendig, um die Systeme software- und hardwareseitig auf einem aktuellen Stand zu halten. Nach jeder Aktualisierung muss geprüft werden, ob die Systeme weiterhin

wie erwartet funktionieren.

Gefundene Fehler müssen so zeitnah wie möglich repariert werden, um die Sicherheit der Daten zu gewährleisten.

Erweiterte Maßnahmen
Erweiterte Schutzmaßnahmen werden nur bei erhöhtem Schutzbedarf verwendet und umfassen unter anderem Kryptokonzepte. Bei der Kryptografie werden die gesicherten Daten verschlüsselt versichert, dafür wird im Bedarfsfall ein eigenes Kryptokonzept erstellt.

2.7 Fallbeispiel: NIST

2.7.1 Beschreibung

NIST steht für National Institute of Standards and Technology und ist eine Bundesbehörde der Vereinigten Staaten von Amerika, zu deren Aufgaben die Entwicklung von Standardisierungsprozessen in der Technik gehört. Im Bereich Datensicherung und Datensicherheit hat das NIST umfassende Standards, Frameworks, Pläne und Guidelines erstellt.

2.7.2 Special Publications

NIST hat mehrere Publikationen zu Computer Security (SP 800), zu Cybersecurity Practice Guides (SP 1800) und zu Information Technology (SP 500), die im Folgenden beispielhaft beschrieben werden.

SP800 - Computer Security

Die SP 800 Publication Series beschäftigt sich mit Computer Security und umfasst zum aktuellen Zeitpunkt 178 Publikationen, die laufend erweitert werden [32].

Im Folgenden soll eine Publikation aus SP 800, der von NIST entwickelte Plan "Contingency Planning Guide for Federal Information Systems", wie beschrieben in der NIST Special Publication 800-23 Rev.1, genauer vorgestellt werden.

Beschreibung
Der Guide beschreibt praktische Guidelines für Unternehmen um eine durchgehende Funktionalität der IT-Systeme ohne größere Unterbrechungen zu gewährleisten. Diese Guidelines sind so formuliert, dass sie für die meisten Unternehmen sinnvoll umsetzbar sind, es kann je nach speziellen Anforderungen eines Unternehmens aber notwendig sein, dass noch zusätzliche Maßnahmen getroffen werden müssen, um die Anforderungen an Sicherheit zu gewährleisten.

Es werden spezifische Contingency Planning Empfehlungen für Client/Server Systeme, Telekommunikationssysteme und Mainframe Systeme beschrieben.

Contingency Pläne
NIST definiert mehrere Pläne, die sich alle mit der durchgehenden Funktionalität von IT Systemen beschäftigen und unterschiedliche Schwerpunkte haben:

- Business Continuity Plan (BCP)
- Continuity of Operations Plan (COOP)
- Crisis Communication Plan
- Critical Infrastructure Protection Plan (CIP)
- Cyber Incident Response Plan

- Disaster Recovery Plan (DRP)

- Information System Contingency Plan (ISCP) und

- Occupant Emergency Plan (OEP)

Beispiel: COOP
Der Contingency Plan COOP (Continuity of Operations Plan) fokussiert sich auf die essenziellen Aufgaben, die ein System zu erfüllen hat. Durch Umsetzung dieses Plans soll sichergestellt werden, dass essenzielle Aufgaben auch in Notfällen oder bei Ausfall des Systems bis zu 30 Tage über eine alternative Position erreichbar und funktional sind.

Der Plan beschäftigt sich unter anderen mit Plänen und Prozessen, die in solchen Notfällen angewendet werden, mit Risikomanagement, Budgetierung, dem Umgang mit essenziellen Funktionen, Verantwortlichkeiten, Personal und Tests.

Für manche Organisationen in den Vereinigten Staaten ist die Einhaltung von COOP verpflichtend.

Planung und Umsetzung der Contingency Pläne
Für alle oben genannten Pläne werden Prozesse und Strategien vorgestellt, die für die Planung und Umsetzung der Pläne im eigenen Unternehmen genutzt werden können und sollen. Die Guidelines berücksichtigen dabei technische Anforderungen und Lösungen, wirtschaftliche Faktoren, personelle Anforderungen, Qualitätssicherung und Wartung.

Templates
Die Guidelines beinhalten für die eigene Umsetzung nutzbare Templates für Low-Impact Systeme, Moderate-Impact Systeme und High-Impact Systeme.

SP 500 - Information Technology

Die in SP 500 veröffentlichten Publikationen beschäftigen sich mit Themen rund um Information Technology und Cybersecurity und beinhaltet zum aktuellen Zeitpunkt 5 Publikationen. Die Publikationen befassen sich mit IT Security Training Requirements, Fog Computation Conceptual Models, Workshops zum Thema Software Measures and Metrics to Reduce Security Vulnerabilities, Conformance Testing Methodology Frameworks und Cloud Computing Security Reference Architecture. [31]

SP 1800 - Cybersecurity Practice Guides

Die in SP 1800 veröffentlichten Publikationen beschäftigen sich mit Themen rund um Cybersecurity und beinhaltet zum aktuellen Zeitpunkt 21 Publikationen. Darin enthalten sind Guides für so vielfältige Themen wie Mobile Device Security, Energy Sector Asset Management und Multifactor Authentication for E-Commerce. [30]

3 Maturity Model

3.1 Entwicklung eines Maturity Models

Ursprünglich stammen Reifegradmodelle aus dem Qualitätsmanagement. Sie werden jedoch heute sehr oft im modernen Prozessmanagement eingesetzt. Sie helfen den aktuellen Status eines Prozesses im Unternehmen zu bewerten und zielen darauf ab, Entscheidungsträgern eine Hilfe bei der Weiterentwicklung der Firma zu sein.

Die Idee des Reifegradmodells ist es, dass jeder Prozess eine unterschiedliche Entwicklungsstufe haben kann. Diese Entwicklungsstufen werden auch Reifestufen genannt.

Ist ein Prozess einer gewissen Reife konform, spricht man auch vom Erreichen eines Reifegrades. Jede dieser Reifestufen hat bestimmte Kriterien. Um eine Reifestufe zu erreichen, muss ein Prozess all diese Kriterien sowie die in der darunterliegenden Stufe erfüllen.

Die beiden bekanntesten Modelle sind das CMMI (Capability Maturity Model Integration) und das SPICE (Software Process Improvement and Capability Determination). Die beiden Modelle werden in Folge kurz vorgestellt.

3.1.1 CMMI als mögliche Ausgangsbasis

Das CMMI (Capability Maturity Model Integration) [1] wurde 2002 auf Basis des früheren Reifegradmodells CMM (Capability Maturity Model) zur Beurteilung eines Status eines Prozesses entwickelt.

CMMI beurteilt die Reife eines Prozessteils durch sogenannte "*capability levels*"(zu Deutsch etwa: Fähigkeitsgrade). Diese lauten wie folgt:

- 0 - Incomplete
- 1 - Performed
- 2 - Managed
- 3 - Defined

Daneben sind für komplette Prozessgebiete "*maturity levels*"(zu Deutsch etwa: Reifegradphasen) festgelegt.

3.1.2 SPICE als mögliche Ausgangsbasis

Der internationale Standard ISO/IEC 15504 dient zur Bewertung von Unternehmensprozessen. Besser bekannt ist der Standard unter dem Namen SPICE (Software Process Improvement and Capability Determination). Primär wird er für Prüfungen im Bereich der Softwareentwicklung eingesetzt [23].

Der Standard definiert insgesamt 6 Reifegradstufen in seinem Maturity Modell. Diese sind in Abbildung 3.2 dargestellt.

Jeder dieser Reifegrade hat neun Prozessattribute zugeordnet, welche der Beurteilung des Prozesses dienen. Die Bewertung eines jeden solchen Prozessattributs

[1] http://www.sei.cmu.edu/cmmi/

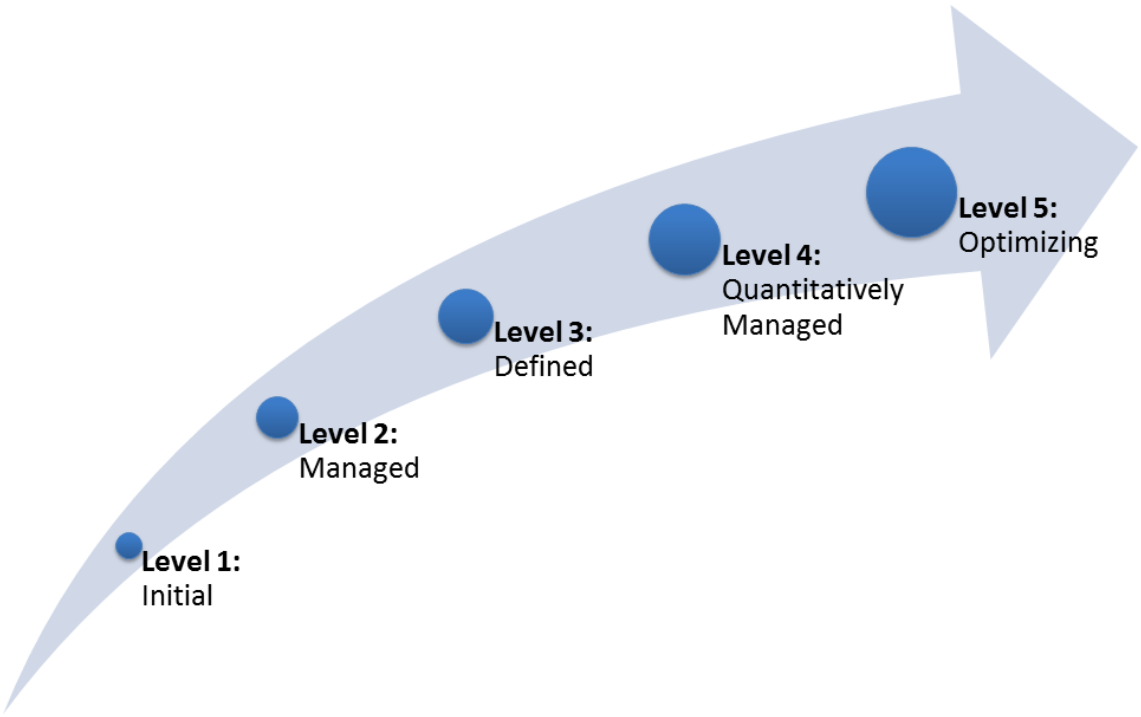

Abbildung 3.1: Maturity levels von CMMI (Eigener Entwurf)

erfolgt mit Hilfe einer vier stufen Skala:

- "nicht erfüllt": 0% - 15%
- "teilweise erfüllt": >15% - 50%
- "weitgehend erfüllt": >50% - 85%
- "vollständig erfüllt": >85% - 100%

Diese Reifegrademodelle sind für die diese Masterarbeit sowie insbesondere die Entwicklung eines eigenen Modells die theoretische Grundlage.

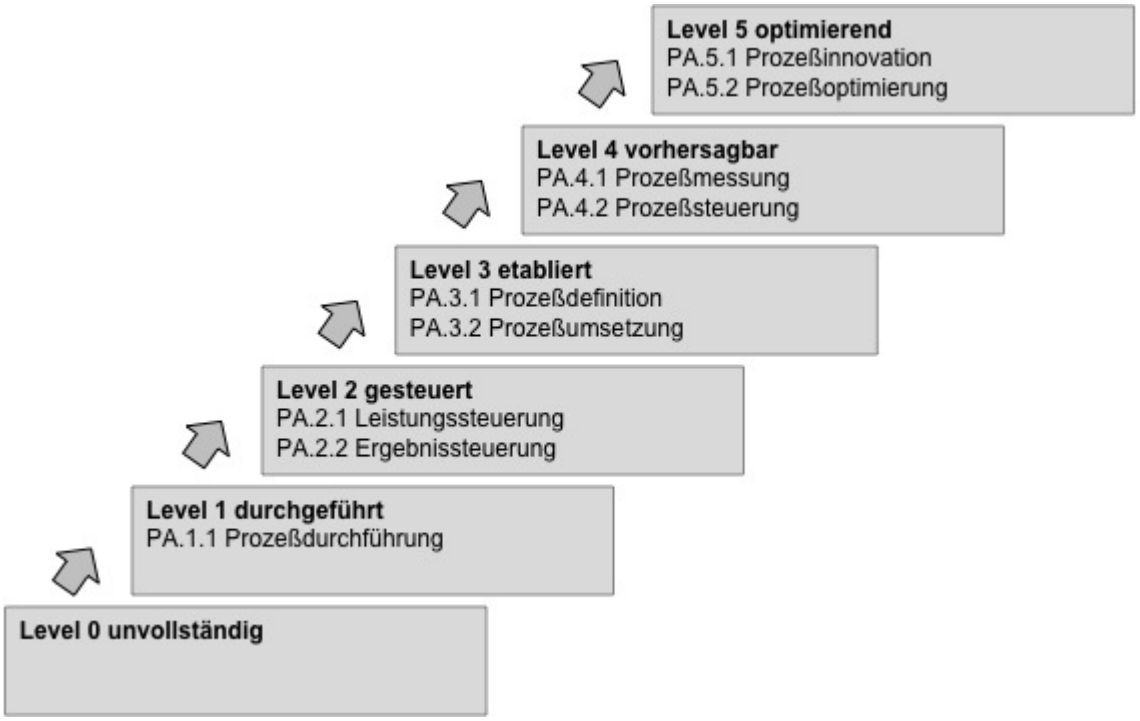

Abbildung 3.2: Reifegradstufen von SPICE (Wikimedia Commons / Dr.auth)

3.2 CobIT

CobIT (*Control Objectives for Information and Related Technology*) ist das Standardframework für die IT-Governance. Es wurde von der internationale IT-Prüfer-Verband ISACA (Information System Audit and Control Association) entwickelt.

Die erste Version CobIT 1 aus dem Jahre 1996 fokussierte sich rein auf Aspekte des IT-Audits. Über die Jahre hinweg wurde erstmals 2005 mit der Version 4.0 ein ganzheitliches IT Governance Framework veröffentlicht. Der nächste Evolutionsschritt war mit CobIT 5 (2012) [26] die Ablöse des Begriffes IT-Governance durch "*Governance of Enterprise IT*"(GEIT). Diese können wie folgt unterschieden werden:

- IT-Governance (CobIT 4): Die IT soll steuern.
- Governance of Enterprise IT (Cobit 5): Die IT soll gesteuert werden.

Die Entwicklung des Modells ist schematisch in Abbildung 3.3 dargestellt.

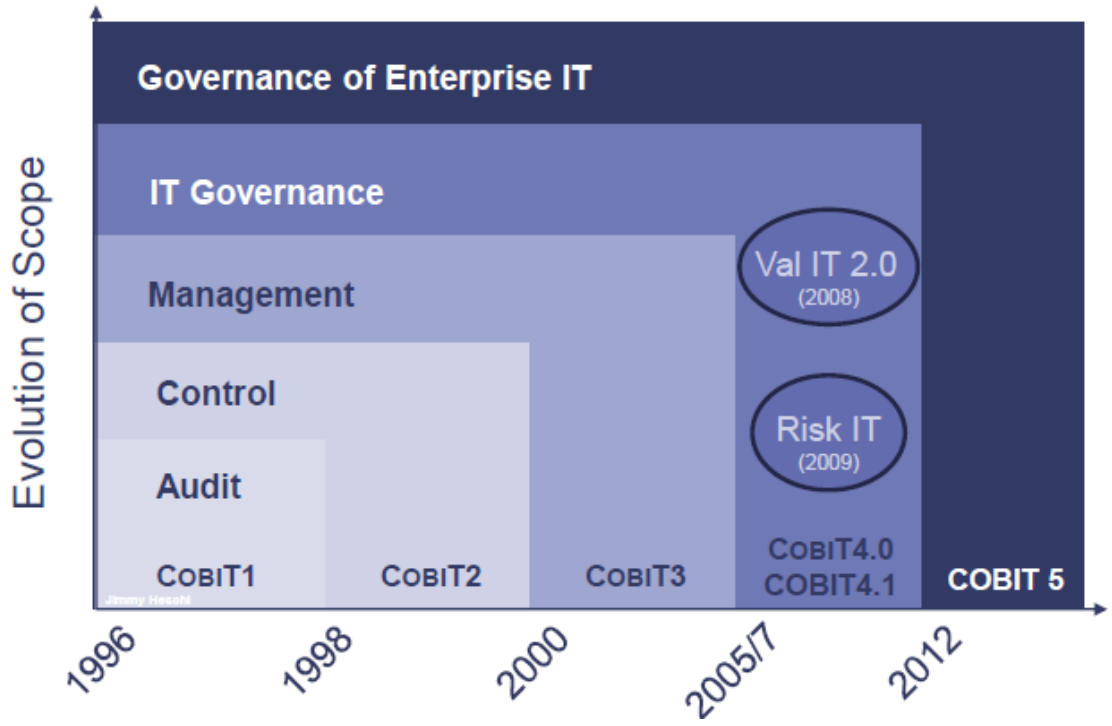

Abbildung 3.3: Entwicklung von COBIT [20]

Im Folgenden wird in dieser Masterarbeit nur noch der Begriff „Governance of Enterprise IT“ (GEIT) verwendet. Governance ist insbesondere seit CobIT 4.0 ein viel diskutierter Terminus. Im Zusammenhang damit werden oft Termini wie „Business Alignment“, SLAs, effiziente und effektive Prozesse, Verteilung von Entscheidungsrechten, Priorisierung von Projekten oder Kapazitäts- und Ressourcenplanung genannt. In dieser Masterarbeit wurde jedoch eine etwas andere, wenn auch möglicherweise ebenfalls umstrittene Definition, gewählt:

> GOVERNANCE OF ENTERPRISE IT: Doing the right things right.
> (Die richtigen Dinge richtig machen.)

Unter richtige „Ding“ kann hier beispielsweise eine Priorisierung von Projekten gesehen werden.

Als absolut essential und als Neuheitsfaktor in CobIT 5 zählen die 5 Prinzipien des Frameworks. Diese sind in Abbildung 3.4 grafisch dargestellt.

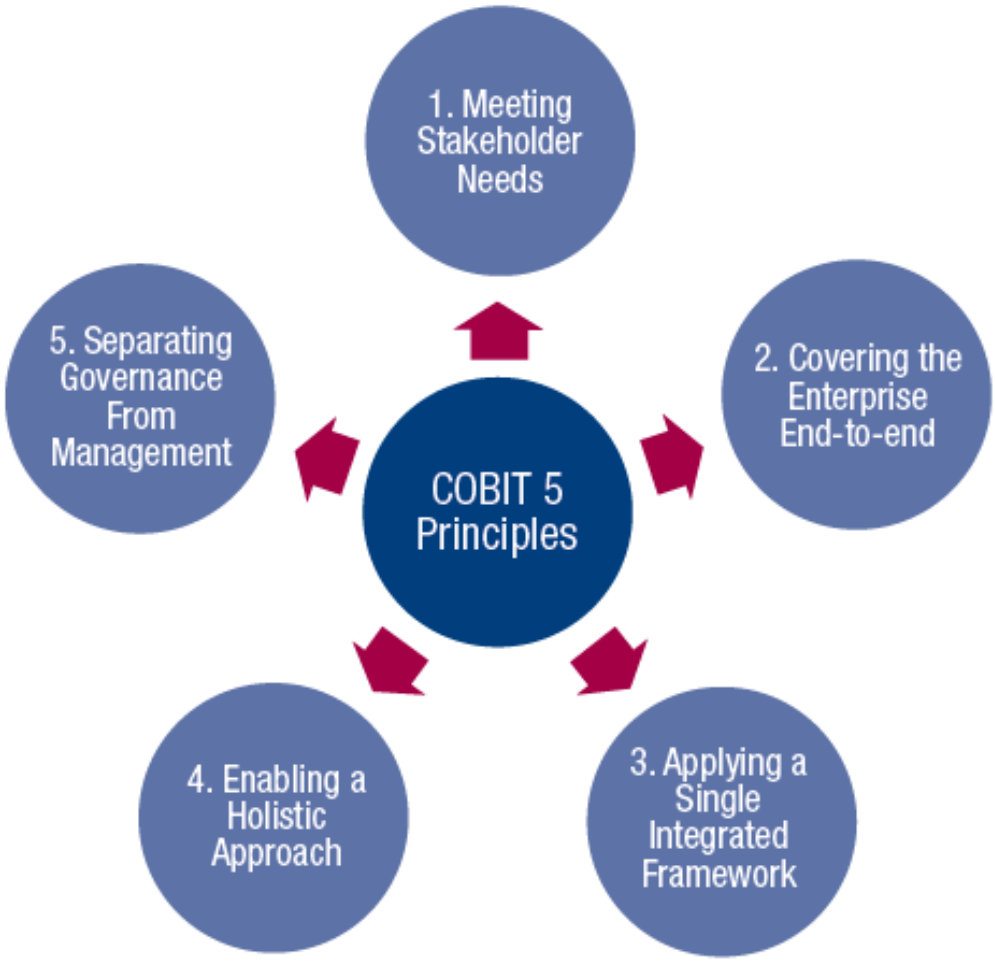

Abbildung 3.4: Die 5 Prinzipien von CobIT 5 [21]

Die 5 Prinzipien umfassen [22]:

1. **Anforderungen der Stakeholder**: Für die Stakeholder des Unternehmens soll eine Balance zwischen der Erzeugung von Profiten und Vorteilen sowie einer Optimierung der Risiken und Ressourcenplanung geschaffen werden.

2. **Abdeckung des gesamten Unternehmens**: Die Integration der Governance of Enterprise IT soll mit der unternehmensweiten IT soll im Zielfokus liegen.

3. **Anwendung eines einheitlichen Frameworks**: Es soll ein einziges Rah-

menwerk zur Abdeckung sämtlicher Prozesse und Vorgänge im Unternehmen gewählt werden.

4. **Ermöglichen eines ganzheitlichen Ansatzes**: Ein ganzheitlicher Ansatz mit Rücksichtnahme auf sogenannte Enabler ist zu wählen. Als Enabler sind Richtlinien/Prinzipien/Rahmenwerke, Prozesse, Organisationsstrukturen, Kultur/Ethik/Verhalten, Information, Services/Infrastruktur/Anwendungen und Mitarbeiter/Fähigkeiten/Kompetenzen zu verstehen.

5. **Unterscheiden zwischen Governance und Management**: Das IT-Management ist klar von GEIT abzugrenzen.

Essenziell ist in CobIT 5 die Unterscheidung zwischen Management und Governance. Auf die vorherige Definition von GEIT angelehnt kann diese Unterscheidung wie folgt gesehen werden:

> GOVERNANCE: Effektivität ergibt sich durch die Auswahl der richtigen Dinge.
>
> MANAGEMENT: Effizienz ergibt sich durch die korrekte Durchführung der zuvor richtigen Dinge

Die Governance ist daher als ein Mittel des Managements zu sehen, mit der Aufgabe diese Rahmenwerke, Tools und Möglichkeiten zu liefern, effizient zu handeln. Dieses Handeln wiederrum ist ein Planen, Entscheiden und Steuern um die Unternehmensziele zu erreichen.

Diese Prinzipien werden, durch die insgesamt im Framework 37 definierten Prozesse integriert und umgesetzt. Um die Qualität und den Umsetzungsgrad dieser Prozesse zu veranschaulichen und messen zu können werden, wie bereits zu Beginn des Kapitels beschrieben, Reifegradmodelle eingesetzt.

3.2.1 KPI

Um innerhalb eines Modells den Fortschritt oder Status überhaupt messen zu können sind Bewertungskriterien nötig. Als etabliert gelten hierbei die sogenannten Key Performance Indicator (KPI). Sie sind eine Leistungskennzahl, um Leistungen im Unternehmen zu messen. Insbesondere sollen damit kritische Erfolgsfaktoren ermittelt und bewertet werden.

KPIs können in verschiedenen Dimensionen auftreten:

- Zeit
- Prozent
- Auslastung

Für viele Bereiche gibt es vordefinierte Standard-KPIs aus Praxis und Literatur. Beispielsweise ist ein wichtiger Standard-KPI für Onlineshops die Abbruchrate im Bestellprozess. Für Produktionsbetriebe interessant ist oft die Auslastung einer Maschine (Overall Equipment Effectiveness) ein wichtiger KPI. .

Um KPIs zu implementieren müssen diese zuerst ermittelt und bestimmt werden. Dazu ist es ratsam zuerst den Prozess, für den KPIs erstellt werden sollen, detailiert zu untersuchen. Welche Prozessschritte sind besonders kritisch? In welchen Teilen kann ein monetärer Wert gemessen werden? Welche Faktoren sind für die Messung relevant?

Ziel der Verwendung von KPIs ist dem Management eine Bewertungsgrundlage zur Steuerung und Führung des Unternehmens zu liefern.

3.3 Evaluierung existierender Modelle

Aktuell existieren bereits einige BCM-spezifische Reifegradmodelle in der Literatur. Diese werden in diesem Abschnitt kurz vorgestellt und analysiert.

3.3.1 BCMM

Das BCMM wurde von der Virtual Coperation Inc. in 2004 als Tool entwickelt. Es dient dazu regelmäßig und kontinuierlich die "disaster preparedness"des Unternehmens zu messen.

Das Modell unterscheidet wie in Abbildung 3.5 ersichtlich, 6 verschiedene Maturity Level. Erst die Level 3-6 beschreiben den evolutionären Charakter des Modells.

The Business Continuity Maturity Model®

Increasing Business Continuity Competency Maturity

Maturity Model Levels	Level 1 Self Governed	Level 2 Departmental	Level 3 Cooperative	Level 4 Standards Compliant	Level 5 Integrated	Level 6 Synergistic
Athlete Analogy	Able to Crawl	Able to Walk	Able to Run	"Fit" Runner	Competitive Runner	Olympic Runner
Comparative Model	Organization "At Risk"		"Competent" Performer		"Best of Breed"	
Corporate Competencies	**Attributes of an Organization at Each Maturity Level**					
Leadership	VL	L	M	H	H	H
Employee Awareness	VL	L		M	H	H
BC Program Structure	VL	L		M	H	H
Program Pervasiveness	VL	VL	L	L	M	H
Metrics	VL	L	M	M	H	H
Resource Commitment	VL	L	M	H	H	H
External Coordination	VL	L	L	M	H	H
BC Program Content	**Attributes of Each BC Discipline at Each Maturity level**					
Incident Management	VL	L	M	H	H	H
Technology Recovery	VL	L	M	H	H	H
Business Recovery	VL	L	M	H	H	H
Security Management	VL	L	M	H	H	H

BCMM Graph

Abbildung 3.5: Modell nach BCMM (Quelle: Virtual Corp Webpräsenz)

Das Problem an diesem Modell ist, dass es primär als Tool zur Evaluierung (z.B. Internal Audit) entwickelt wurde. Des Weiteren basiert dieses Modell nicht auf einem

allgemein akzeptierten Best-Practice Methode und eine Eingliederung in ein bereits etabliertes Prozesssystem, gestaltet sich es daher als schwierig.

3.3.2 Modell nach Smit

Das 2005 vorgeschlagene Maturity Model [33] unterscheidet neben der klassischen Prozessreife auch noch die Dimension des BCM-Scopes. Die sich daraus ergebenen Quadrate werden SPQS (scope process quality stages) genannt.

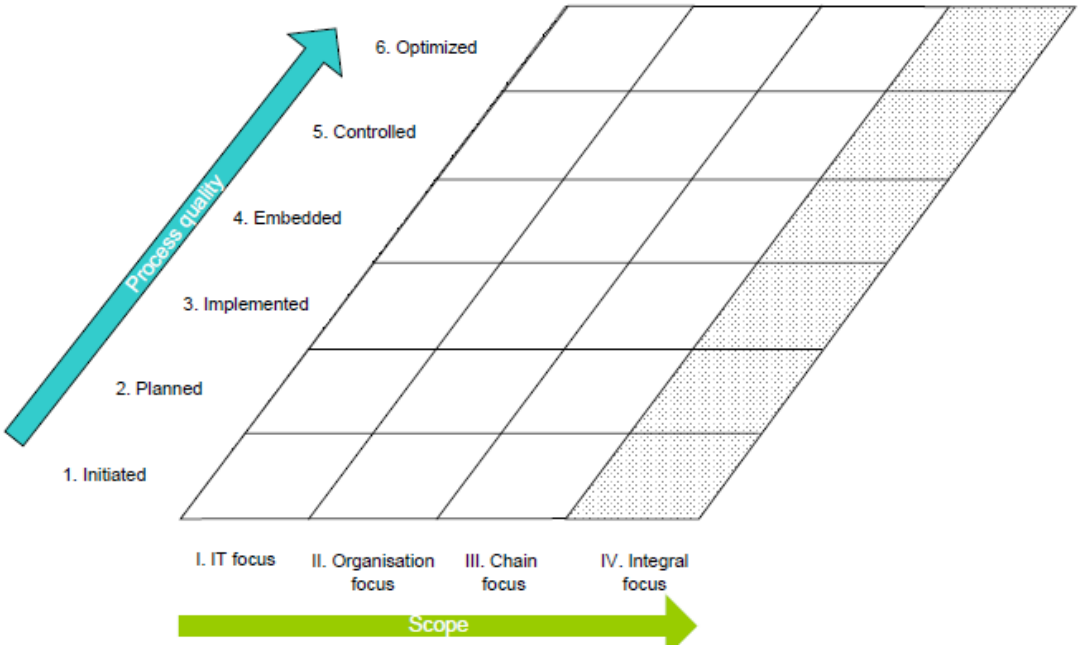

Abbildung 3.6: Modellübersicht Smit [33]

Weiterführend ist jeder dieser SPQS durch "Characteristics"beschrieben. Jede dieser weiter durch Objectives definiert. Diese sind wiederum in "Requirements"geteilt. Diese Requirements sind spezifisch und messbar.

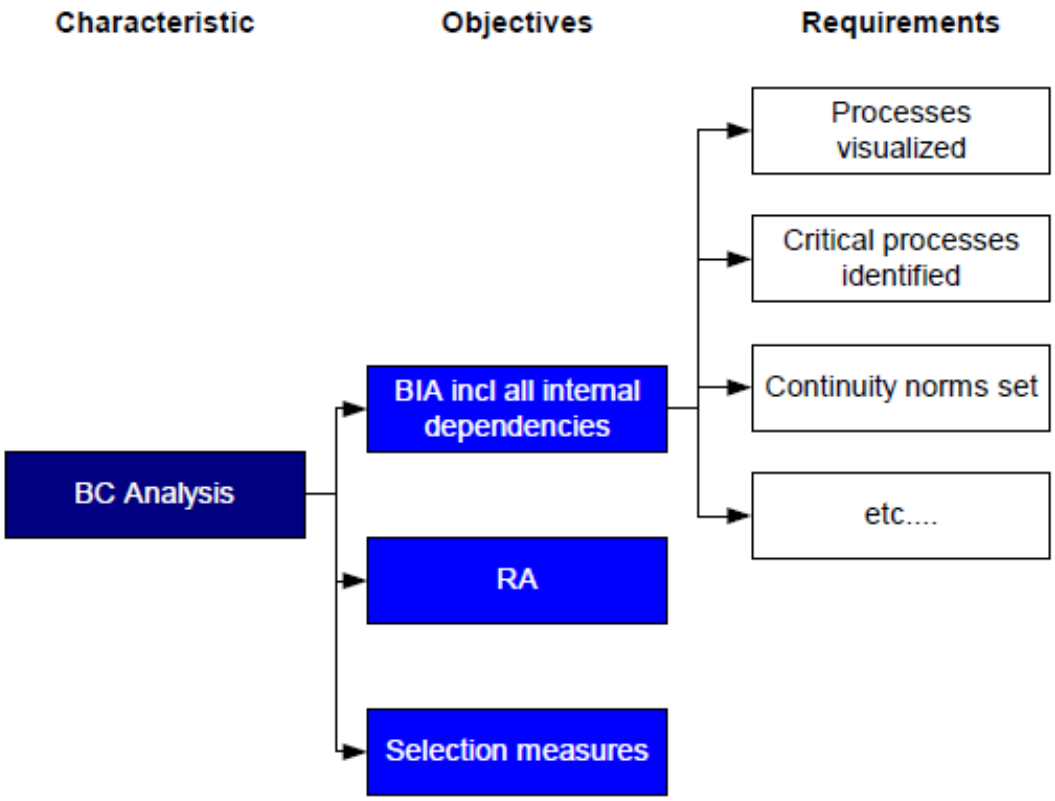

Abbildung 3.7: Modelldetails Smit [33]

3.4 Anforderungen an ein BCM Maturity Model

Bevor ein Maturity Model entwickelt wird, soll festgelegt werden welchen Anforderungen dieses Model gerecht werden muss.

Folgende Anforderungen werden als essenziell betrachtet [13]:

- **Anerkannte Methoden:** Das Rad soll nicht neu erfunden werden, sondern nur angepasst an die speziellen Bedürfnisse des BCM-Prozesses. Das Modell soll auf anerkannten Industriestandards basieren.

- **Ist-Zustandsaussage:** Das Modell soll fähig sein den aktuellen Ist-Zustand des BCM-Prozesses zu jedem Zeitpunkt darzulegen.

- **Level-basiert:** Das Modell soll auf Maturity-Level basieren, wobei die neuesten Entwicklungen von CobIT 5 (insbesondere im Betracht auf Level 0) in Betracht zu ziehen sind.

- **Ergebnis**: Das Modell soll Empfehlungen geben, inwiefern der BCM-Prozess zu verbessern ist.

- **Verständlichkeit**: Das Modell muss einfach gehalten sein, damit es innerhalb des Unternehmens oder der Organisation auch transportiert und verstanden werden kann.

Diese Anforderungen leiten sich aus der Evaluierung der bestehenden Modelle ab und sind als Mindestanforderung an das neue Modell gelten.

3.5 Modellentwicklung

Das auf CMMI basierend unter COBIT eingesetzte Prozessmodell ist eines der bekanntesten und weitesten verbreiteten Modellen. Aus diesem Grund wird dieses auch die Basis für das entwickelte Modell dienen.

Ein Hauptaugenmerk bei der Entwicklung des Modells wird auf den in Kapitel 2 vorgestellten Trigger basierenden Ansatz gelegt. Dieser empfiehlt bei der Umsetzung eines BCM-Ansatzes nicht nach Bedrohungen oder Risiken vorzugehen, sondern zuerst Trigger heraus zu kristallenen und für diese Maßnahmen zu entwickeln.

Das entwickelte Reifegradmodell schlägt insofern von der Norm ab, dass es nicht einzelne Prozessschritte bei der Entwicklung eines BCM-Plans bewertet. Diese Vorgehensweise ist aus mehreren Gründen negativ zu bewerten. Zum Ersten ist sie abhängig vom gewählten Framework und der Vorgehensweise und eine Vergleichbarkeit mit anderen Organisationen eventuell nicht immer möglich. Zum Zweiten ist eine praktikable Implementierung fraglich. Ein Framework könnte z.B. vereinfacht die Prozessschritte Initialisierung, Risk Assessment, Auswahl von Maßnahmen, Erarbeitung eines Plans, Implementierung und kontinuierliche Überprüfung

sein. Insbesondere beim BCM ist die Gewichtung auf diese verschiedenen Schritte sehr ungleich. Das Kernstück zu einer Qualitätsmessung im BCM-Bereich sind nicht etablierte Prozesse - dies kann innerhalb des klassischen Prozessmanagements oder der IT-Governance erfolgen - sondern die Beachtung und Umsetzung der identifizierten Trigger.

Daher wird die Qualität des BCM nicht an der Qualität der einzelnen BCM-Prozesse, sondern am Level der identifizierten Trigger gemessen. Diese wiederum erfolgt natürlich nicht an der Bewertung eines Triggers selbst, sondern an der Messung der Prozessgüte der dazugehörigen Maßnahmen.

Zur Bewertung eines Zustandes werden in Reifegradmodellen meist Levels (oder: capabilities) herangezogen. Analog zu COBIT 5 sind im entwickelten Modell folgende Level definiert:

- **Level 0**: Die Maßnahme wurde nicht implementiert oder verfehlt seinen Zweck. Auf dieser Stufe gibt es kaum oder gar keine Hinweise auf eine systematische Erfüllung des Maßnahmenzweckes.

- **Level 1**: Die implementierte Maßnahme erfüllt seinen Zweck.

- **Level 2**: Die zuvor beschriebene, durchgeführte Maßnahme wird jetzt in einer gemanagten Art und Weise implementiert (geplant, überwacht und angepasst).

- **Level 3**: Die zuvor beschriebene, gemanagte Maßnahme wird jetzt anhand eines definierten Prozesses implementiert, mit dem die Prozessergebnisse erreicht werden können.

- **Level 4**: Die zuvor beschriebene, etablierte Maßnahme wird jetzt innerhalb festgelegter Grenzen angewendet, um die Prozessergebnisse zu erreichen.

- **Level 5**: Die zuvor beschriebene, vorhersehbare Maßnahme wird kontinuierlich verbessert, um relevante aktuelle und künftige Unternehmensziele zu erreichen.

Nach der Bewertung jeder einzelnen Maßnahme, erfolgt die Bewertung des gesamten

Triggers. Je nach benötigter Stärke kann dies entweder immer der niedrigste Wert aller Maßnahmen sein, ein arithmetisches oder gewichtetes Mittel. Wichtig dabei ist, dass ein Trigger immer nur ein Level einnehmen kann. Das Erreichen eines höheren Levels ist nur durch vorheriges Erreichen allen niedrigeren Levels möglich.

Abbildung 3.8 zeigt diesen Messungs- und Bewertungsvorgang grafisch.

Trigger X	Gesamt	*Maßnahme 1*	....	*Maßnahme N*
	0	z.B. Level 0	...	z.B. Level 1

Trigger Y	Gesamt	*Maßnahme 1*	....	*Maßnahme N*
	2	z.B. Level 2	...	z.B. Level 3

Trigger Z	Gesamt	*Maßnahme 1*	....	*Maßnahme N*
	1	z.B. Level 1	...	z.B. Level 1

Abbildung 3.8: Entwickeltes Modell (Eigener Entwurf)

Damit ist eine präzise Bewertung gegeben, die trotz des Detaillierungsgrades eine Übersicht ermöglicht.

3.5.1 KPI für BCM

Um den BCM-Prozess zu bewerten sind spezielle KPIs erforderlich. Das können beispielsweise sein:

- Anzahl für den BCM-Prozess im Unternehmen ausgebildete Mitarbeiter
- Anzahl der durchgeführten BCM-Tests und Simulationen
- Einhaltungsgrad der regelmäßigen Aktualisierung und Überarbeitung der BCM-Dokumente

Mit solchen KPIs kann nun der aktuelle Stand des BCM erhoben werden und somit gegen den Optimalzustand verglichen werden. Der aus der GAP-Analyse Resultat ist das Verbesserungspotential für den BCM-Prozess.

3.5.2 Vorfallsbehandlung

Zur konkreten Behandlung von BCM relevanten Incidents (Vorfällen) soll nach einem vorgegebenen Schema gehandelt werden. Dies dient dazu, um in einem eingetretenen Notfall keine Maßnahmen und Schritte zu missachten sowie ein strukturiertes Vorgehen zu garantieren. Das vorgeschlagene Schema ist in Abbildung 3.9 dargestellt. Die in den beiden Prozessschritten (Sofortmaßnahmen umsetzen) und (Weitere Maßnahmen durchführen) angesprochenen Maßnahmen sind innerhalb eines Notfallhandbuches für alle Trigger zu definieren.

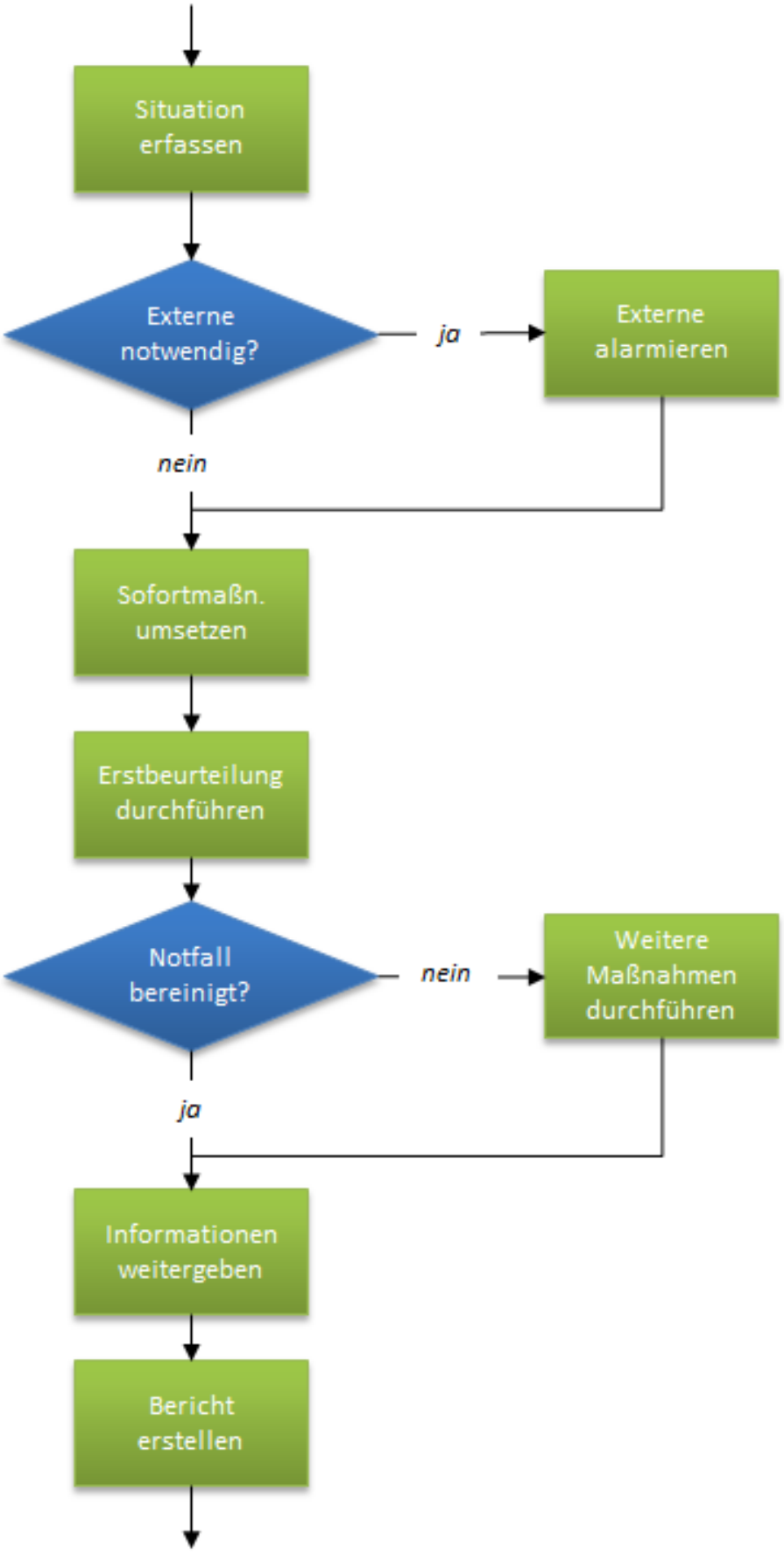

Abbildung 3.9: Schema zur Notfallbehandlung (Eigener Entwurf)

4 Case Study

4.1 Situationsbeschreibung

Österreich ist ein Land der Klein- und Mittelbetriebe (KMUs). 2011 arbeiteten 60.2% aller Erwerbstätigen in einem solchen Unternehmen [7]. Gerade jedoch bei dieser Betriebsgröße liegt oft der Fokus in der Leistungserstellung durch die Kernprozesse des Unternehmens. Themenbereich wie Informationssicherheit oder eben auch Business Continuity erhalten wenig bis kaum Beachtung. Aus diesem Grund behandelt diese Case Study exemplarisch einen Klein- und Mittelbetrieb.

4.2 Unternehmensbeschreibung

Das gewählte Unternehmen ist in der Druck- und Grafikbranche tätig. Die Firma entwirft selbst Designs für Banner, Prospekte, Folder, Einladungen, Postwurfsendungen und ähnlichem. Neben dem Entwurf ist das zweite Standbein das Bedrucken von Papier, Textilien und Plastikoberflächen. Ebenfalls können Spezialanforderungen bearbeitet werden (z.B. Entwurf und Druck eines Brettspiels, Bedrucken von Energydrink Dosen).

Im Jahresschnitt werden ca. 40 Mitarbeiter beschäftigt. Die Rechtsform des Unternehmens ist eine Gesellschaft mit beschränkter Haftung. Als Gesellschafter fungieren jeweils zu 50% gleichberechtigt zwei Personen. Das Unternehmen besteht seit 10 Jahren. Der Zielkundenkreis liegt im regionalen und lokalen Markt und basiert auf mündlicher Propaganda.

Das Unternehmen erwirtschaftet einen jährlichen Gesamtumsatz von ca. 20 Millionen Euro mit einem Gewinnanteil von 400.000 Euro.

4.2.1 Organisatorische Situation

Die organisatorische Gliederung des Unternehmens ist Abbildung 4.1 zu entnehmen.

Die Geschäftsführung sowie die vier Hauptabteilungen des Unternehmens befinden sich am selben Standort. Der Standort umfasst Büroräumlichkeiten für die Mitarbeiter, einen Empfangs- und Ausstellungsbereich, eine Lagerhalle für Drucksorten, einen Produktionsbereich sowie einen Serverraum.

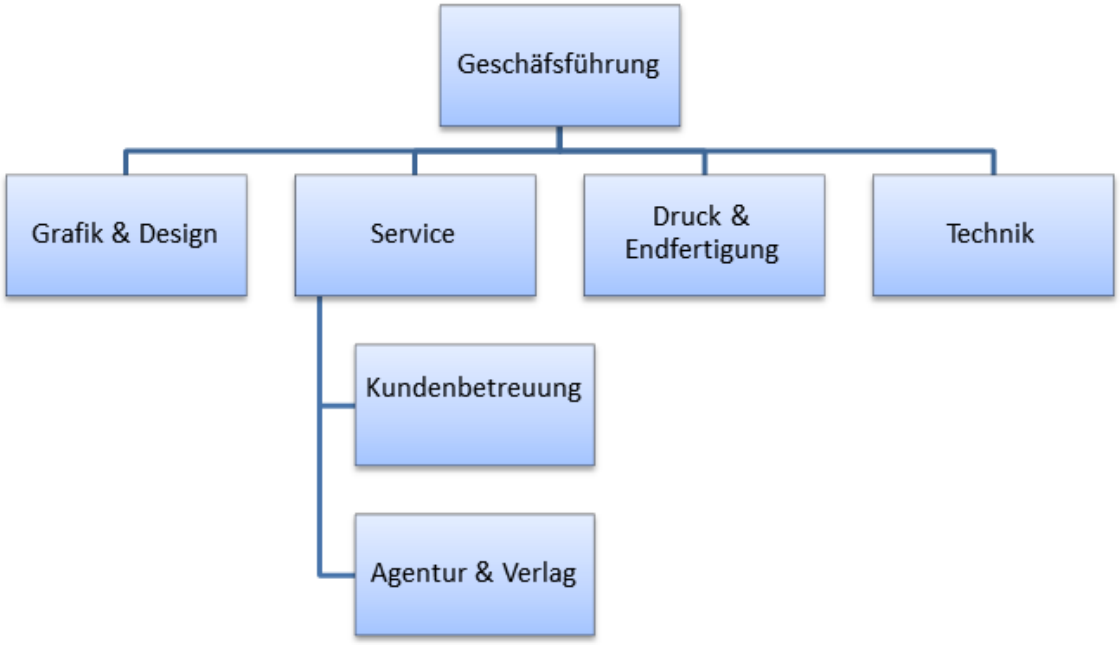

Abbildung 4.1: Organigramm des Unternehmens (Eigener Entwurf)

Die Abteilung Grafik und Design ist zuständig für die Erstellung von Produkten in einer Grafiksuite. Es werden beispielsweise Flyer, Plakate oder Zeitungen in den jeweiligen Programmen erstellt. Druck und Endfertigung beschäftigt Mitarbeiter die sowohl für die Einstellung und Bedienung sämtlicher Druckmaschinen als auch für

die Kommunikation und Übertragung der digitalen Rohprodukte zu den Druckmaschinen zuständig sind. Die Abteilung Service ist für sämtliche Kommunikation zu Partnern und Endkunden verantwortlich. Dort ist auch das Sekretariat ansässig. Die Abteilung Technik ist sowohl für Aspekte des Facility Managements als auch der IT zuständig. Hier ist hervorzuheben, dass diese Abteilung nur aus 2 Personen besteht. Dies spiegelt den niedrigen Stellenwert der IT innerhalb des Unternehmens bzw. die Fokussierung auf die Kernprozesse des Unternehmens wider.

Derzeit beschäftigt das Unternehmen 44 Mitarbeiter.

4.2.2 Technische Situation

Die derzeitige IT-Aufbau des Unternehmens ist in Grafik 4.2 schematisch dargestellt.

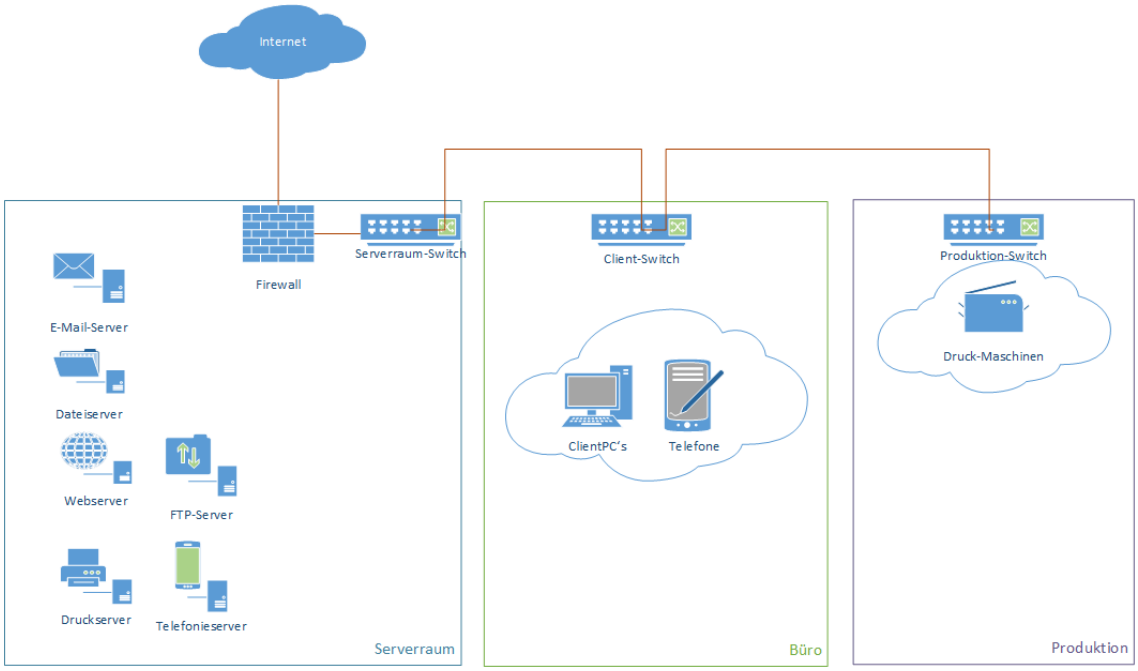

Abbildung 4.2: Netzwerksituation vor BCM-Maßnahmen (Eigener Entwurf)

Am Hauptstandort ist der Eintrittspunkt von außen über eine zentral verwaltete Firewall. Diese ist über einen DSL-Anschluss an das Internet angebunden. An diese

zentrale Firewall sind drei Switches angeschlossen, welche Zugriff zu einem jeweiligen weiteren Teilnetzwerk erlauben.

Serverraum-Netz
Dieses Netzwerk umfasst alle Server welche sich im physikalischen, zusammenhängenden Serverraum neben der Betriebsküche des Unternehmens befindet. Dabei sind alle Server-Funktionalitäten - E-Mail, Dateiablage, Web, FTP, Druck, Domäne, Datenbank sowie Telefonie - auf einem eigenen physikalischen Gerät implementiert. Der Webserver dient zur Darstellung der Unternehmenswebseite sowie des darauf aufsetzenden Produktkatalogs und Bestellservices.

Client-Netz
Der Hauptstandort verfügt über ein zentral verwaltetes Windows-Netzwerk mit insgesamt 46 Arbeitsplätzen. Diese verfügen über unterschiedliche Softwareinstallation (Textverarbeitung, Grafikdesign, Tabellenkalkulation, Präsentation, Fotobearbeitung, Drucksatz), welche dem jeweiligen Nutzer angepasst sind.

Produktions-Netz
Das Produktionsnetzwerk bündelt die Druckmaschinen. Dabei stehen dem Unternehmen primär Offsetdruckmaschinen, jedoch auch Tief- und Siebdruckgeräte, zur Verfügung.

4.2.3 Situation aus Sicht der Compliance

Das Unternehmen unterliegt wegen seiner Größe und Branche aus Sicht der Informationstechnik keinen relevanten Complianceanforderungen. Daher existieren zum Status Quo auch keine Richtlinien, Policies oder Dienstanweisungen zur Informationssicherheit, IT-Sicherheit oder Business Continuity.

4.3 Cloud

Onlinebasierte Datensicherung mittels Cloudservice: Neben der lokalen Datensicherung auf eigenen Servern wurde die Option einer onlinebasierten Datensicherung mittels Cloudservice besprochen. Vorteile einer Datensicherung in der Cloud sind in erster Linie, dass die Wartung und Sicherung der Systeme und Daten zum größten Teil an externe Firmen ausgelagert werden kann, was die Anforderungen an das eigene Team und Kosten reduziert. Im Rahmen der Analyse wurden die Vor- und Nachteile von online Datensicherung diskutiert und die Services und Preise bekannter Anbieter verglichen. Einer der größten Nachteile einer cloudbasierten Speicherung ist, dass immer eine Internetverbindung vorhanden sein muss, um Daten in die Cloud senden zu können. Auch ist eine hohe Datenübertragungsrate notwendig, um die Daten effizient in der Cloud speichern zu können. Ein weiterer Faktor, der bei der Analyse beachtet wurde, ist die Einhaltung der Datenschutzbestimmungen in Österreich. Gerade bei personenbezogenen Daten muss auf besonderen Schutz der Daten geachtet werden. Die am 25. Mai 2018 in Kraft getretene DSGVO setzt hier Anforderungen voraus, die von Unternehmen außerhalb der EU eventuell nicht erfüllt werden. Auch die verschlüsselte Datenübertragung mittels End-to-End Verschlüsselung sollte gewährleistet sein. Als weitere Nachteile wurde festgehalten, dass gerade bekannte Cloud-Anbieter trotz hoher Sicherheitsvorkehrungen immer wieder Ziel von Hacker-Angriffen sind. Für die Geschäftsführung war es ein wichtiges Anliegen komplette Kontrolle über die Daten zu haben, da die Weitergabe von Daten bei externen nicht so kontrolliert werden kann wie im eigenen Team. Ein weiteres Ziel war entsprechendes Knowhow bezüglich IT-Infrastruktur und Datensicherheit direkt in der Firma aufzubauen. Grundsatz der Geschäftsführung war, dass die Verantwortung und die Sicherheit der eigenen Daten vom eigenen Team übernommen und erfüllt werden sollen. Die höheren initialen Kosten wurden von der Geschäftsführung als sinnvolle Investition ins eigene Team und in die laufende Sicherheit betrachtet. Trotz der Vorteile und Einfachheit von onlinebasierter Datenspeicherung hat sich die Geschäftsführung wegen oben genannten Bedenken für ein selbst verwaltetes Datensicherungssystem entschieden.

4.4 Einführung eines BCM

Im Zuge einer nahestehenden Betriebsumsiedlung beschloss die Geschäftsführung vor dem Umzug die aktuelle Ist-Situation der IT-Landschaft zu erheben und daraus eventuelle Verbesserungsmaßnahmen abzuleiten. Diese Verbesserungsmaßnahmen bzw. aufgedeckten Problemfelder sollen direkt als Ausgangsbasis für ein KMU ökonomisch sinnvolles BCM bieten. Dieses BCM wird triggerbasiert aufgebaut und die Maßnahmen unterliegen dem in Kapitel 3 vorgestelltem Maturity Model.

4.4.1 Projekt IT-Neustrukturierung

Um die IT im Zuge des Umzugs neu zu strukturieren sowie ein BCM im Unternehmen zu etablieren, wird neben den eigenen Mitarbeitern ein IT-Berater aus dem Bereich Infrastruktur für die Umsetzung beigezogen. Für das zeitlich begrenzte Projekt *IT-Neustrukturierung und BCM-Gestaltung* wurden folgende Projektziele definiert:

- **A.** Feststellung des Stellenwerts der IT und Bedeutung des BCM für das Unternehmen
- **B.** Definition des Sicherheitsniveaus
- **C.** Einführung einer triggerbasierten BCM-Richtlinie

A. Feststellung des Stellenwerts der IT und Bedeutung eines BCM für das Unternehmen
Der Erfolg des Unternehmens ist abhängig von konsistenten Informationen in Bezug auf Kunden, Aufträge, Lieferanten und Partnerfirmen. Die Herstellung der Produkte für die Kunden ist ohne ein aufrechtes, funktionstüchtiges Produktionsnetzwerk nicht möglich, da alle Produktionsmaschinen IT-gesteuert arbeiten. Druckaufträge können nur von den jeweiligen Office-Stationen gestartet werden. Die IT ist daher ein wichtiger, unterstützender Teil des Unternehmens. Eine einsatzfähige IT ist die wesentliche Voraussetzung für die Erreichung des Geschäftsziele. Daher hat sich

die Geschäftsführung entschlossen ein BCM-Programm zu etablieren, um in Notsituation die Aufrechterhaltung der IT gewährleisten zu können. Die Aktualität und Angemessenheit des Programms sollen zumindest jährlich überprüft werden.

B. Sicherheitsniveau und Ziele
Nach Abwägungen über mögliche Bedrohungen sowie die möglichen Risiken und Werte der zu schützenden Güter strebt das Unternehmen ein mittleres Sicherheitsniveau und somit mittleres BCM-Niveau an. Dies entspricht dem branchenüblichen angepeilten Sicherheitsniveau in Betrieben mit vergleichbarer Mitarbeiteranzahl (vgl. [16]).

C. Einführung einer triggerbasierten BCM-Richtlinie
Das in Kapitel 2 vorgestellte Modell zur Entwicklung eines Business Continuity Managements soll in diesem Kapitel praktisch angewendet werden. Dabei werden ausgehend von den ermittelten Assets (IT-Systeme, Personal, Anlagevermögen) Bedrohungen nach den BSI-Gefahrenkatalogen ermittelt. Diese werden im nächsten Schritt zu verschiedenen Triggern gebündelt. Im letzten Schritt werden mögliche Maßnahmen präemptiv und reaktiv schematisch dargestellt. Eine taxative Ausarbeitung sämtlicher Maßnahmen für alle Trigger ist nicht angedacht, weil dazu eine engere und längere Zusammenarbeit mit dem Beispielunternehmen nötig wäre.

4.4.2 Erhebung der Assets

Die Erhebung der Assets ist für die, die Erstellung eines BCM die absolut notwendige Ausgangsbasis. Nur wer seine zu schützenswerten Güter identifizieren kann, ist fähig die möglichen Bedrohungen dafür zu erkennen und zu bewerten. Da die Firma Güter produziert ist im Unterschied zu reinen Dienstleistungsunternehmen auch das Anlagevermögen im Fokus der Asseterhebung. Das Anlagevermögen besteht im Unternehmen aus 85% Gebäude und Maschinen. Nur 15% fallen dabei auf die Hardware der IT-Systeme. Neben diesen ist auch das Personal ein wichtiges Asset für die Unternehmensausführung. Zu den essenziellen Assetgruppen zählen:

- Bürogebäude

- Produktionsgebäude
- IT-Netzwerk
- IT-Serverlandschaft
- Telefonielandschaft
- Druckmaschinen

Die detaillierte Auflistung der Server und Netzwerkkomponenten ist Grafik 4.3 zu entnehmen.

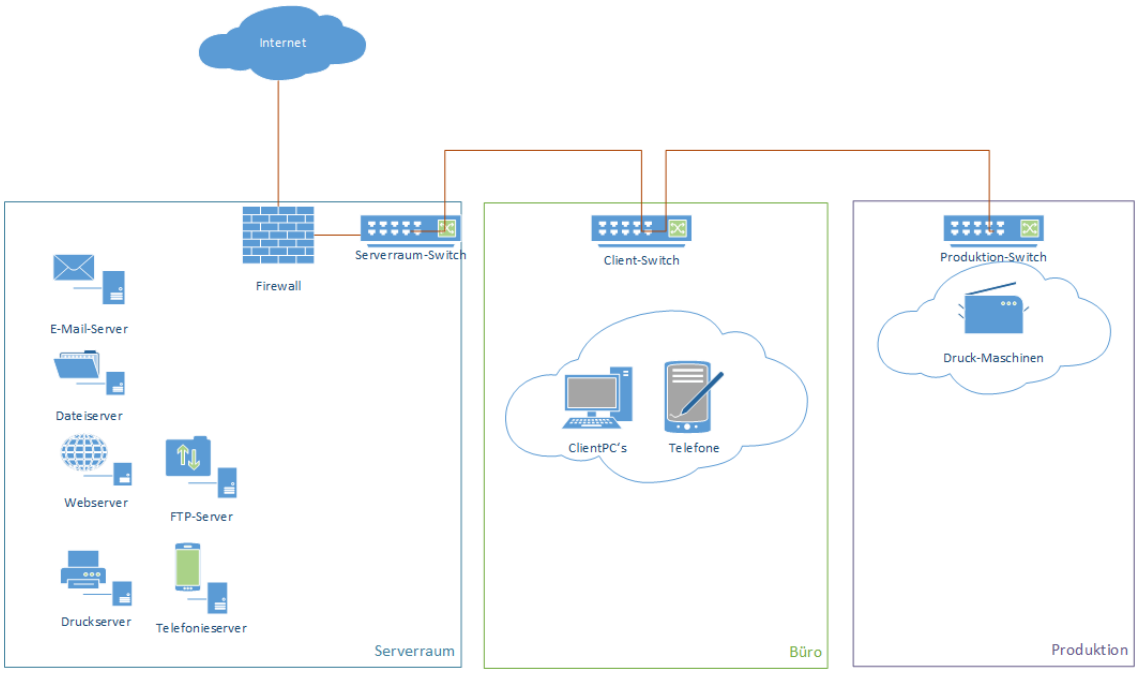

Abbildung 4.3: Netzwerksituation vor BCM-Maßnahmen (Eigener Entwurf)

Vor der Umstrukturierung sind folgende IT-Systeme im Einsatz:

- Webshopsoftware
- Finanzbuchhaltung & Personaldatenverwaltung

- Auftrags- und Kundenverwaltung
- Benutzerauthentifizierung Teleworker
- Email, Terminmanagement
- Zentrale Dokumentenverwaltung
- Design- & Grafiksoftware

4.4.3 Umbau der IT-Infrastruktur im Rahmen des Betriebsumzuges

Im Zuge des Umstiegs von Mieträumlichkeiten zu Betriebsgebäuden in Eigenbesitz wurde von seitens der Geschäftsführung das bereits erwähnte Projekt *IT-Neustrukturierung und BCM-Gestaltung* gestartet. Da die IT als essenzieller Baustein für den Erfolg des Unternehmens angesehen wird, wurde im Zuge des Umzugs beim Neuaufbau der IT-Infrastruktur insbesondere auf sicherheitstechnische Aspekte Rücksicht genommen. Durch den Umzug hat sich der Aufbau der Infrastruktur wie in Abbildung 4.4 dargestellt verändert.

Bei der Neugestaltung wurden in erster Linie Redundanzen auf verschiedenen Ebenen eingeführt, um Ausfällen entgegen wirken zu können. Physisch getrennt sind folgende Netze:

- **Serverraum 1:** Der primäre Serverraum befindet sich im Kellerbereich des Hauptstandortes.
- **Serverraum 2:** Der sekundäre Serverraum befindet sich ca. 50 Meter entfernt im Kellerbereich eines benachbarten Unternehmens. Die beiden Serverräume sind unterirdisch mit einer 10Gbit Leitung verbunden.
- **Büro:** Die Büroräumlichkeiten für die Mitarbeiter befinden sich im Erdge-

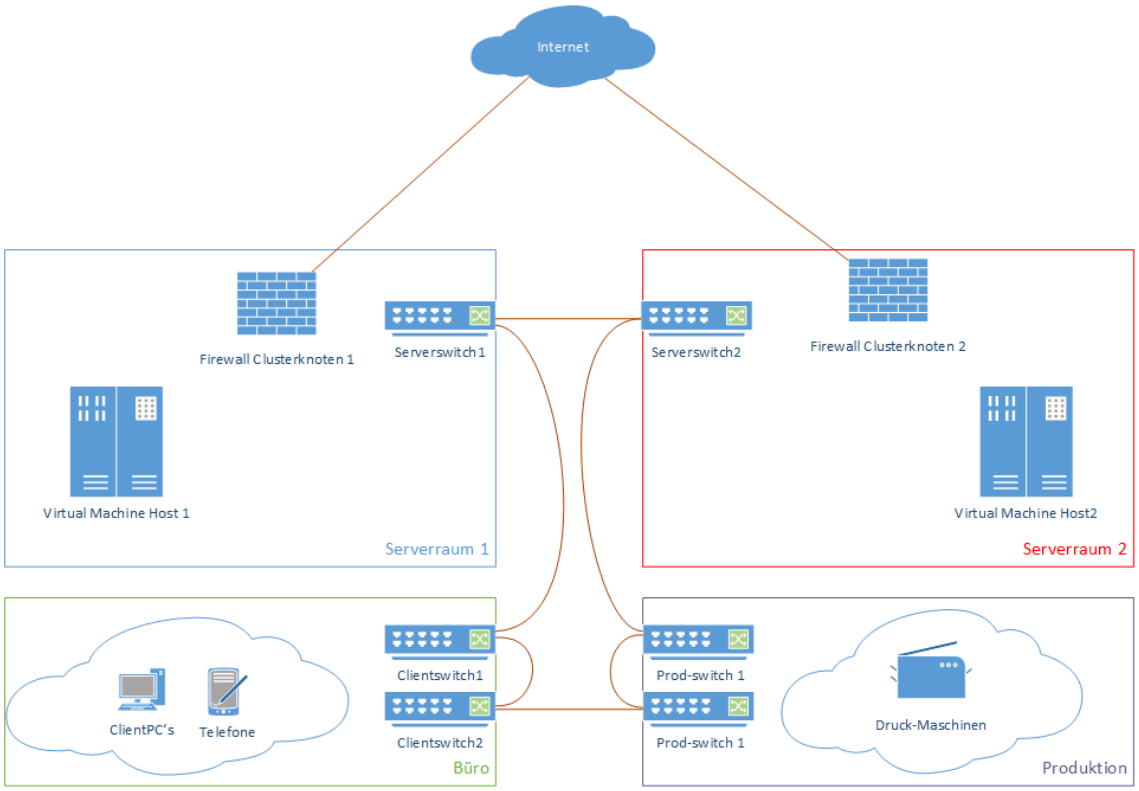

Abbildung 4.4: Netzwerksituation nach BCM-Maßnahmen (Eigener Entwurf)

schoss sowie 1. Stock des Hauptstandortes.

- **Produktion:** Die Produktionshalle des Unternehmens ist in einem eigenen Brandschutzabschnitt und Gebäudezubau des Hauptstandortes.

Durch die räumliche Trennung konnten bereits vier verschiedene Brandschutzabschnitte erstellt werden. Die Einführung eines zweiten Serverraumes ermöglicht die Aufrechterhaltung des Betriebs bei Ausfall von Servern oder des gesamten Serverraum 1. Ein Ausfall könnte nur einen Firewallcluster, einen Serverswitch, einen Server oder ein virtuelles Serversegment betreffen. In jedem Fall würde die entsprechende Komponente aus Serverraum 2 den Betrieb übernehmen.

Das Büro- und Produktionsnetzwerk ist ebenfalls über zwei Clientswitches angeschlossen. Jeder Client ist hierbei an jeden dieser beiden Switches angeschlossen. Auf eine doppelte Anbindung der Druckmaschinen wurde aus Kostengründen für das KMU verzichtet. Jedoch können bei einem Ausfall eines Clientswitches die notwen-

digen Druckmaschinen händisch auf den zweiten, funktionstüchtigen Clientswitch umgesteckt werden.

Der Umstieg von mehreren physischen Servern auf einen zentralen Server, der die verschiedenen Serverelemente in virtuellen Umgebungen anbietet, ermöglicht nicht nur eine massive Kosteneinsparung, sondern auch eine einfache Verwaltung der oben beschriebenen angestrebten Redundanz. Ebenfalls ist durch den Umbau nun eine zweite Internetanbindung über einen zweiten Provider eingeplant worden.

Logisch wurde das Netzwerk durch die Einführung unterschiedlicher VLANs abgesichert. VLANs bieten eine sehr kostengünstige Variante zur Einrichtung mehrerer physikalisch getrennter Netze. Zusätzlich eröffnen VLANs eine einfache Wartbarkeit und weiter Umstrukturierungen und Änderungen sind relativ einfach durchzuführen. Neben diesen Aspekten bieten VLANs aus sicherheitstechnischer Sicht auch einen Schutz gegen diverse dolose Attacken wie z.B. MAC-Spoofing. Die fünf eingerichteten VLANs decken dabei den Bereich Produktion, Telefonie, Clients, Server und DMZ (Demilitarized Zone) getrennt ab.

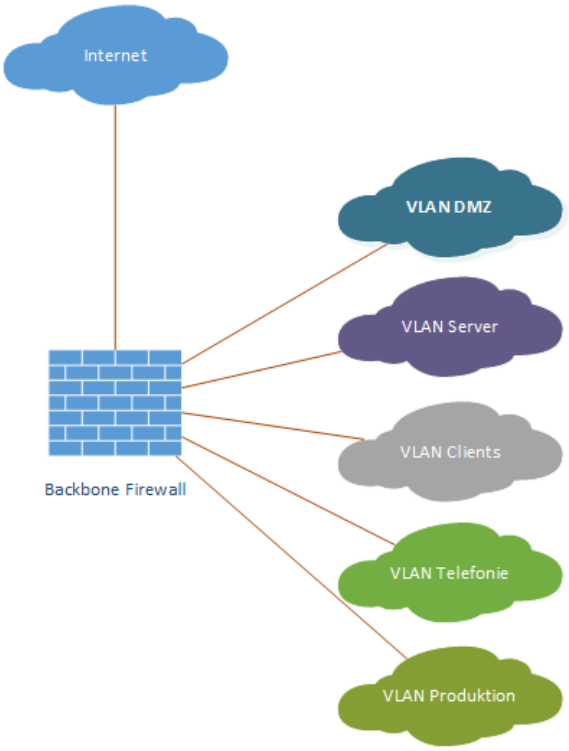

Abbildung 4.5: Defintion VLANs im Netzwerk (Eigener Entwurf)

Auf Seite der Software wurde erhoben für welche Services durch eine Verschiebung in die Cloud es sowohl zu einer Kostenersparnis als auch zu einer erhöhten Verfügbarkeit kommen könnten. Der Fokus lag dabei ganz klar auf SaaS – Software as a Service. Folgende Ideen wurden dabei behandelt:

- **Authentisierungsservices für Teleworker:** Zukünftig soll Teleworking für die Mitarbeiter unterstützt werden. Dafür wird ein geeignetes Authentisierungsservice insbesondere für den 2. Faktor benötigt. Klassische Zwei-Faktor-Systeme stützen sich auf den RSA SecurID Token mit einem internen Server zur Prüfung der Authentisierung. Für das Unternehmen kommt nach reichlicher Evaluierung das Cloudservice Duo Security mit ihrem Konzept zur One-Tap-Authentication für Teleworker in Frage.

- **Adobe Creative Cloud Suite:** Also Design- und Grafikunternehmen stützt sich die Firma auf die Produkte der Firma Adobe. Diese werden auch als Cloudvariante angeboten. Zwar sind klare Vorteile im Bereich von Sicherheit durch Updates erkennbar, jedoch sind die Produkte bei einem Internetausfall nicht nutzbar. Daher verzichtet die Geschäftsführung auf die Nutzung der Adobe Creative Cloud Suite.

- **Dokumentenverwaltung mit mobiler Unterstützung:** Es wurde evaluiert, ob eine Dokumentenverwaltung in der Cloud für die Unterstützung der Mobilität Vorteile brächte. Die Kosten der angebotenen Produkte wie z.B. der Firma Brainloop überschreiten jedoch deutlich das Budget eines KMUs.

Sämtliche Services zur Finanzbuchhaltung und Personendatenvearbeitung wurden aus Verfügbarkeitsgründen (Internetausfall dgl.) sowie des Datenschutzes (personenbezogen Daten, geschäftsrelevante Daten) von der Geschäftsführung abgelehnt.

4.4.4 Einführung eines Triggerbasierten BCM

Das entwickelte BCM-System stützt sich neben der Ermittlung der Assets des Unternehmens auf den Bedrohungskatalog des BSI sowie die bereits umgesetzten Maßnah-

men aus der Neustrukturierung der IT-Infrastruktur. Exemplarisch wurden sieben Trigger mit den gebündelten Bedrohungen und zugehörigen Maßnahmen ausgearbeitet. Da BCM-Systeme immer einen sehr unternehmensspezifischen Charakter aufweisen, besteht hierbei kein Anrecht auf Vollständigkeit. Während der Erstellung der Case Study wurde ebenfalls festgestellt, dass eine Bewertung und Festlegung der aktuellen Maturity Level erst im Lauf des *Lebens* des BCM-Systems vorgenommen werden kann. Erst durch die Erprobung und Arbeiten mit den Maßnahmen durch das Fachpersonal ist eine detaillierte Bewertung möglich. Daher wurde in diesem Schritt darauf verzichtet. Die Tabellen am Ende dieses Kapitels beinhalten die sieben Trigger sowie die zugehörigen Maßnahmen.

Im folgenden Abschnitt werden noch, die beiden technischen Maßnahmen, die noch nicht im obigen im Rahmen der Umstrukturierung erläutert wurden, detailliert beschrieben. Dabei handelt es sich um die Einführung des Yubikeys zur Verringerung der Passwörter im Unternehmen und die der One-Tap-Authentication von Duo Security für Teleworker.

M-24: Yubikey
Die schwedische Firma Yubico ist, wie RSA, ein Hersteller eines Hardware-Security-Tokens (Yubikey). Die Yubikey-Hardware wird in den Varianten Standard, Nano (Mini Variante) und NEO (Standard+NFC) angeboten. Das Unternehmen wurde 2007 gegründet und hat Niederlassungen in Schweden, England und Kalifornien.

Yubikey ist ein kleiner Token mit USB-Anschluss, der für einen Login in den USB-Schacht geschoben werden muss. Bei Berührung auf einen kapazitiven Schalter generiert Yubikey OTPs (one-time passwords) zur Authentisierung von Benutzern und kann somit als 2. Faktor eingesetzt werden. Da der Yubikey als Standardtastatur erkannt wird, wird er von den gängigen Betriebssystemen Windows, Mac und Linux unterstützt. Es sind dazu keine weiteren Treiber notwendig.

Yubikey kann als OTP (HOTP), Challenge-Response (TOTP) oder statisches Passwort eingesetzt werden. Die erzeugten OTPs können entweder von Yubicos Cloudservice oder einem selbst betrieben Yubikey Validation Server verifiziert werden. Yubikey OTPs werden standardmäßig gegen das YubiCloud Validation Service authentifiziert.

Abbildung 4.6: Yubikey NEO (Quelle: Yubico Webpräsenz)

M-25: One-Tap-Authentication

Die One-Tap-Authentication ist eine App am SmartPhone, die einem bei einem Login-Versuch eine Benachrichtigung darüber übermittelt. Ist der Login-Versuch gewünscht kann per *Fingertip (Tap)* auf das SmartPhone-Display der Zugriff gestatten oder andernfalls abgelehnt werden. Dadurch fällt das Abtippen des Codes wie bei einem Hardwaregebunden RSA SecurID Tokens weg. Anbieter davon sind beispielsweise Duo Security und Toopher.

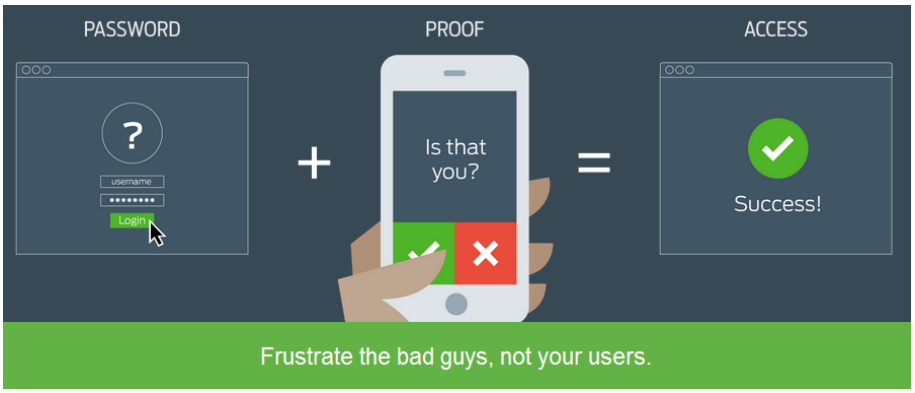

Abbildung 4.7: Funktionsweise One-Tap-Authentication (Quelle Duo Webpräsenz)

Durch den Einsatz eines App-Tokens ergeben sich weitere Vorteile: Die Wahrscheinlichkeit des Bemerkens eines SmartPhone Diebstahls oder Verlusts fällt dem Nutzer wesentlich schneller auf, als der eines klassischen Hardware-Tokens.

4.4.5 Fazit

Die praktische Case Study dieses Masterarbeit zeigt klar auf, dass auch für Klein- und Mittelbetriebe ein BCM-Plan durchaus sinnvoll vor allem auch trotz beschränkter Ressourcen erstell- und durchführbar ist.

Das dazu in dieser Arbeit erarbeitete trigger-basierte Modell eignet sich besonders für diese Zwecke, da es einen sehr praktikablen und praxisnahen Ansatz hat. Das trigger-basierte BCM-Planungs-System hat den weiteren Vorteil, dass die Trigger auch über die Zeit ausformuliert werden können und so die Ressourcenbelastung verteilt werden kann. Dafür sollte eine initiale Klassifizierung nach Priorität der verschiedenen Trigger vorgenommen werden.

Da oft in Klein- und Mittelbetriebe organisatorische Strukturen schwächer ausgeprägt sind und auch insbesondere die IT-Dokumentation nicht immer vorhanden ist, ist die Erstellung eines BCM-Plans auch mit weiteren Vorteilen behaftet. So können beispielsweise die Outputs wie die Dokumentation der IT-Systeme nicht nur im Katastrophenfall genutzt werden, sondern auch die Kommunikation im täglichen Betrieb verbessern. Auch ergibt sich ein neuer Blick auf den Wert und Relevanz der IT. Zukünftige Investition können besser geplant und geschätzt werden. Der Stellenwert der IT rückt näher in den Fokus und es erfolgte ein Bewusstmachen über deren Notwendigkeit.

Insbesondere der Zeitpunkt einer Betriebsumsiedlung wie im Falle dieser Case Study eignet sich hervorragend für die Erstellung eines BCM-Plans, da etwaige Änderungen und Anpassungen an der IT-Infrastruktur sehr einfach und auch deutlich kostengünstiger durchgeführt werden können.

Klar ist jedoch auch, dass insbesondere in Falle von Klein- und Mittelbetrieben auf jeden Fall zumindest für die initiale Beratung ein Experte herangezogen werden sollte. Die Aneignung des spezifischen BCM-Planungs-Wissens ist durchaus zeitintensiv und gerade im Falle einer Betriebsumsiedlung ist die Arbeitsbelastung für alle Mitarbeiter ohnehin bereits erhöht.

4.5 Laufendes System

Der Umsetzungszeitraum der Umstrukturierung hat angefangen von den ersten Überlegungen bis zur vollständigen Umsetzung 11 Monate gedauert. Die Konzeption der Lösung hat 2 Monate in Anspruch genommen, die Umsetzung selbst mehrere Wochen. Durch den Umzug und andere Aufgaben, die in der Firma vom Team erledigt werden mussten, erhöhte sich der Umsetzungszeitraum dadurch auf fast ein Jahr. Das System ist seit der Fertigstellung im laufenden Betrieb und wird vom Team selbst gewartet und kontrolliert. Das initiale Setup wurde gemeinsam mit dem externen Berater durchgeführt und validiert. Für den laufenden Betrieb wurden Prozesse erarbeitet, die eine laufende Kontrolle und Validierung der Datensicherungssysteme und Datensicherheit sicherstellen. Diese Prozesse werden vom Team selbst verwaltet und durchgeführt. Änderungen und Ergebnisse der Tests werden vom Team protokolliert. Das laufende System funktioniert wie erwartet und die höhere Datensicherheit wurde wie erhofft durch die Umsetzung erfüllt. Das Team hat während der Umsetzung und auch im laufenden Betrieb durch die an sie gestellten Herausforderungen wertvolles Knowhow erarbeitet und die Priorität von Datensicherheit und Datenschutz an das Team kommunizieren können. Das gesamte Team wurde zum Thema Datensicherheit geschult und weiß über die grundlegenden Prozesse Bescheid. Seit der Einführung des Systems kam es noch zu keinem Notfall, der eine Wiederherstellung der Daten notwendig gemacht hat. Durch regelmäßige Tests konnte aber sichergestellt werden, dass die Wiederherstellung der Daten im Notfall zeitnah funktioniert.

Bedrohung				Trigger				Maßnahme			
ID	Name	Beschreibung	BSI-Katalog	ID	Name	Beschreibung	Level	ID	Name	Art	Level
B-1	Bombendrohung (Umgebung etc.)	Durch eine Bombendrohung sind Zufahrtsmöglichkeiten nicht verfügbar.	-	T-1	Gebäude nicht zugänglich	Das Gebäude ist aus Sicherheitsgründen für das Personal nicht zugänglich oder ist nicht erreichbar.	-	M-1	Mitarbeiter vorab über Bedrohungen informieren	P	-
B-2	Blitz	Blitzeinschläge können direkte oder indirekte Schäden am Gebäude verursachen.	G 1.3					M-2	Evakueirungschulungen	P	-
B-3	Feuer	Durch einen beispielsweise begrenzten Feuerausbruch kann ein Teil des Gebäudes nicht zugänglich sein.	G 1.4					M-3	Bereitstellung eines Erstatzgebäudes für Kundenbesuche	P	-
B-4	Wasser	Eintritt von Waser, verursacht z.B. durch Regen, undichte Leitungen, Störung in der Wasserversorgung, defekte Sprinkleranlagen, etc. kann den Zutritt zu Gebäuden oder das Gebäude selbst beeinträchtigten.	G 1.5					M-4	Teleworking für Mitarbeiter	R	-
B-5	Sturm	Stürme oder Orkane können die Außenreichtungen eines Gebäudes oder die Zufahrtsmöglichkeiten stark einschränken.	G 1.13					M-5	Information der Mitarbeiter per Telefon	R	-
B-6	Infrastrukturausfall	Durch den Ausfall umliegender Infrastruktur wie z.B. öffentliche Verkehrsmittel oder gesperrte Zufahrtswege können Mitarbeiter nicht zu ihrem Arbeitsplatz anreisen.	-								

Bedrohung				Trigger				Maßnahme			
ID	Name	Beschreibung	BSI-Katalog	ID	Name	Beschreibung	Level	ID	Name	Art	Level
-	Blitz	Siehe B-2	-	T-2	Arbeiten im Office Bereich ist durch eine zerstörte IT-Infrastruktur nicht mehr möglich	Essentielle Teile der IT-Infrastruktur sind zerstört. Die IT als Ganzes ist somit nicht nutzbar.	-	M-6	Bereitstellung eines 2. Serverraums	P	-
-	Wasser	Siehe B-4	-					M-7	USV-Anlage um für zentrale Server zumindest kurfristige Stromausfälle ausgleichen zu können	P	-
-	Feuer	Siehe B-3	-					M-8	Information der Mitarbeiter per Telefon	R	-
B-7	Staub, Verschmutzung	Durch Staub oder Verschmutzung kommt es zu einem Gebrechen einer technischen Komponente.	G 1.8					M-9	Redundante Internatanbindung	P	-
B-8	Fahrlässige Zerstörung von Geräten	-	G 3.2					M-10	Teleworking der Mitarbeiter	R	
B-9	Kabelbrand	-	G 1.6								
-	Ausfall der Stromversorgung	siehe B-17	-								
B-10	Technisches Gebrechen	Ein fehlerhafter Bauteil führt zum Ausfall der TK-Einrichtungen.	-	T-3	Telefonische oder Emailkommunikation mit Kunden nicht möglich / Keine Möglichkeit Aufträge anzunehmen	Durch den Ausfall eines essentiellen Komponenten ist die Kommunikationsmethode nicht nutzbar. Dadurch können Aufträge oder Supportanfragen nicht beantwortet werden.	-	M-11	Redundante Auslegung des E-Mail Servers	P	-
B-11	Konfigurations- und Bedienungsfehler	Durch eine falsche Konfiguration ist eine Kommunikation nicht mehr möglich.	G 3.38					M-12	Redundante Auslegung der IT-Infrastruktur	P	-
B-12	Software-Schwachstellen oder Fehler	-	G 4.22					M-13	Abschließen eines SLAs	P	-
B-13	Ausfall oder Störung von Netzkomponenten	Der Teilbereich Email/Telefon etc. ist durch den Ausfall von Netzkomponenten betroffen.	G 4.31					M-14	Anlegen eines Manuals zur Fehleridentifizierung	P	-
B-14	Ausfall eines Weitverkehrsnetzes	-	G 1.10					M-15	Abarbeiten des Manuals zur Fehleridentifizierung	R	-

Bedrohung				Trigger				Maßnahme			
ID	Name	Beschreibung	BSI-Katalog	ID	Name	Beschreibung	Level	ID	Name	Art	Level
-	Ausfall eines Weitverkehrsnetzes	Siehe B-14	-	T-4	Aufträge im Webshop können nicht angenommen werden	Der Webshop ist für Kunden nicht erreichbar.	-	M-16	Redundante Internetanbindung	P	-
-	Technisches Gebrechen	Siehe B-10	-					M-17	Doppelte Auslegung Server durch Virtualisierung	P	-
-	Ausfall durch Fehlbedienung	Siehe B-11	-					M-18	Schulung Mitarbeiter für spezifische Webserver Probleme	P	-
-	Ausfall der Stromversorgung	Siehe B-17						M-19	Patchprozess etablieren	P	
-	Software-Schwachstellen oder Fehler	Siehe B-12	-					M-20	Kunden per Newsletterverteiler informieren	R	-
B-15	Personalausfall	Personal mit notwendigen Fachtkenntnissen steht nicht zur Verfügung.	G 1.1	T-5	Produktionsbetrieb kann nicht aufrecht erhalten werden	Die Produktionsmaschinen können keine Zwischen- oder Endprodukte fertigstellen	-	M-21	Schulung unterschiedlicher Mitarbeiter auf denselben Maschinen	P	-
B-16	Ausfall von IT-Systemen	Druck durch IT Probleme nicht möglich (Netzwerk, Server, Daten..)	G 1.2					M-22	Redundante Auslegung der IT-Infrastruktur	P	-
B-17	Ausfall der Stromversorgung	Durch externe oder interne Probleme ist keine ausreichende Stromversorgung möglich.	G 4.1					M-23	Teleworking	R	-
B-18	Ungeeigneter Umgang mit Passwörtern	-	G 3.43	T-6	Externer Zugriff auf IT-Systeme aus logischen Gründen nicht möglich	Der VPN-Zugriff für Telearbeiter ist nicht möglich.	-	M-24	Einführung eines Tokens zum Passwortersatz	P	-
B-19	Fehlverhalten bei der Nutzung von VPN-Diensten	-	G 3.41					M-25	Einführung einer One-Tap-Authentication zur Vereinfachung der Authentifizierung	P	-
-	Ausfall durch Fehlbedienung	Siehe B-11	G 3.9					M-26	Prozess zur Passworterneuerung und Rücksetzung definieren	P	-

Bedrohung				Trigger				Maßnahme			
ID	Name	Beschreibung	BSI-Katalog	ID	Name	Beschreibung	Level	ID	Name	Art	Level
B-20	Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten	-	G 3.1	T-7	Dateneverlust von unternehmenskritischen Informationen zu Kunden, Produkten oder Design	Aufträge können wegen fehlender Daten nicht ausgeführt werden	-	M-27	Redundante DB-Server Auslegung durch Virtual Ressources	P	-
B-21	Verlust von Daten einer Datenbank	-	G 4.28					M-28	Tägliches Backup	P	-
B-22	Defekte Datenträger	Durch einen Datenträger kommt es zum Datenverlust.	G 4.7					M-29	Mitarbeiterschulung	P	-
B-23	Verlust der Datenbankintegrität/-konsistenz	Durch den Verlust der Datenbank kommt es zu einem großflächigem Datenverlust.	G 4.30					M-30	Etablierung eines Prozesses zur Fehlerbehebung	P	-
B-24	Ausfall einer Datenbank	Durch den Verlust der Datenbank kommt es zu einem großflächigem Datenverlust.	G 4.26					M-31	vgl. M-24	P	-
-	Ungeeigneter Umgang mit Passwörtern	Siehe B-18	-								

5 Conclusio

Ziel dieser Arbeit war es ausgehend zu den gewonnen theoretischen Erkenntnissen aus den Themenbereichen Risk Assessment und Business Continuity Management eine praktische Case Study auszuarbeiten. Zu diesem Zweck wurde ein triggerbasiertes Modell zur Kontinuitätsplanung sowie ein einfaches, zugehöriges Maturity Model entwickelt. Das Maturity Model stützt sich dabei auf die bereits bekannten Vorgehensmodelle CMMI, SPICE und CobIT.

Das angesprochen triggerbasierte Modell basiert auf der Bündelung der identifizierten Bedrohungen auf die festgelegten Assets des Unternehmens aus. Diese Bedrohungen wurden im Risk Assessment ermittelt. Durch die Bündelung wird erreicht, dass das Übersehen möglicher Risiken keine gravierenden Auswirkungen hat, da der Ausgangspunkt für Maßnahmen immer der Trigger selbst und nicht die mögliche Bedrohung bzw. Risiko ist. Des Weiteren nimmt ein triggerbasiertes Modell Komplexität durch Bündelung und Vereinfachung aus dem BCM-System. Dies eignet sich insbesondere für Klein- und Mittelbetriebe.

Im Fallbeispiel hat sich gezeigt, dass Trigger als Ausgangspunkt für die Erstellung von Business Continuity Plänen einfach und praxisnahe eingesetzt werden können. Dabei ergab sich, dass der BCM/BCP-Prozess sich effektiv umsetzen lies. Andererseits musste auch festgestellt werden, dass ein BCM-System nur durch die umfassende Beteiligung des Fachpersonals erstellt werden kann. Ebenfalls ist ein bereits abgebildetes Prozessmanagementsystem von Vorteil.

5.1 Lessons Learned

Durch der Entwicklung des triggerbasierten BCM-Systems und der Recherche bereits vorhandener Systeme sowie der Dokumentation des praktischen Anwendungsbeispieles sind folgende Lessons Learned festzuhalten:

- Die praktische Case Study dieses Masterarbeit zeigt klar auf, dass auch für Klein- und Mittelbetriebe ein BCM-Plan durchaus sinnvoll vor allem auch trotz beschränkter Ressourcen erstell- und durchführbar ist.

- Die Umsetzung des triggerbasiertes BCM-Systems gestaltete sich einfach und eignet sich daher für KMUs, die keine hohen Ansprüche an das Detaillevel haben und maximal ein mittleres Sicherheitsniveau erreichen möchten.

- Für KMUs eignet sich zur Auslegung einer redundanten Infrastruktur die Servervirtualisierung und die Auslagerung von Softwarediensten in die Cloud.

- Da oft in Klein- und Mittelbetriebe organisatorische Strukturen schwächer ausgeprägt sind und auch insbesondere die IT-Dokumentation nicht immer vorhanden ist, ist die Erstellung eines BCM-Plans auch mit weiteren Vorteilen behaftet. So können beispielsweise die Outputs wie die Dokumentation der IT-Systeme nicht nur im Katastrophenfall genutzt werden, sondern auch die Kommunikation im täglichen Betrieb verbessern.

- Als Authentisierungsservices für Teleworker hat sich das One-Tap-Authentication-System als für KMUs geeignet heraus kristallisiert. Es ist einerseits für die User einfach zu verstehen und bietet andererseits ein ausreichend hohes Sicherheitsniveau.

- Die Bewertung eines Maturity Levels ist nicht trivial. So konnte zwar ein initiales Modell entwickelt werden, ohne direkten Firmenbezug und Zusammenarbeit mit den entsprechenden Fachabteilungen ist eine Bewertung der Prozesse zum aktuellen Ist-Stand jedoch nicht möglich.

Abschließend ist zu sagen, dass in jeglichem Fall - unabhängig von der Unternehmensgröße auf jeden Fall ein Experte für das Business Contiuity Planning herangezogen werden sollte. Da in Klein - und Mittelbetrieben die finanziellen Mittel dafür oft knapp sind, ist dies zumindest für die initiale Planung zu erwägen. Der Bereich BCP/BCM ist durch die verschiedenen Methoden, Ansätze und Standards derart komplex, dass ein Unternehmen von der Erfahrung eines Experten mehr profitieren kann als die Kosten zu Buche schlagen.

5.2 Reflexion und Ergebnisse

Abschließend ist zu sagen, dass die Etablierung eines triggerbasierten BCM-Systems insbesondere für KMUs mit wenigen Personal- und Ressourcenmitteln ein geeignetes, kostengünstiges Mittel zur Einführung eines grundlegenden Business Continuity Managements sein kann. Die Bewertung der Maturity Level ist jedoch erst eine Entwicklung die während der Laufzeit eines BCM-Systems vorgenommen werden sollte.

Es ist an dieser Stelle wichtig anzumerken, dass BCM nicht nur Katastrophenmanagement im Fokus hat. BCM muss als Geschäftsprozess angesehen werden und ein breites Spektrum von Managementprozessen integrieren. Dazu zählen neben dem klassischen Katastrophenmanagement u.A. Risikomanagement, Gebäudemanagement, Krisenmanagement, Human Resources, Sicherheit oder auch PR. Insbesondere sollte der Fokus nicht ausschließlich auf IT-Belange fallen, da ansonsten wichtige andere Bereiche zu wenig Aufmerksamkeit erhalten.

5.3 Outlook

Die Anschläge vom 11. September und der letzten 15 Jahre haben der IT-Welt aufgezeigt, dass einerseits nichts unvorstellbar ist und andererseits die Vorbereitung bereits die halbe Miete ist. Gezieltes und praxisnahes Business Continuity Planning ist in Zukunft wohl nicht nur für Großunternehmen aus dem Dienstleistungs- und

Finanzsektor ein Thema, sondern insbesondere auch für weniger IT-affinen Industrieunternehmen und Klein- Und Mittelbetriebe.

Es wird insbesondere auch immer wichtiger das eigene Personal im Bereich BCP/BCM zu schulen, da die Komplexität des Themas deutlich steigt. Bei der konkreten Implementierung ist darauf hinzuweisen, dass auf jeden Fall internationale Standards miteinbezogen und gefolgt werden sollte. Die Fallbeispiele und Literaturrecherche haben auch gezeigt, dass momentan noch ein zu großer Fokus der monetären Mittel auf den Schutz bzw. Ausfallsicherheit der Rechenzentren liegt. Dies wird und sollte sich mehr auf der Absicherung, Redundanz und Wiederverstellbarkeit der Organisationsabläufe und Personalressourcen fokussieren.

Seit CobiT im April 2012 veröffentlicht wurde, wird dieser Framework auch im Business Continuity Planning ein immer größere Rolle spielen. BCP/BCM wird in Zukunft immer weniger eine eigene Disziplin bleiben, sondern sich mehr und mehr mit anderen Themenbereichen des Managements und IT-Managements, wie beispielsweise Informationssicherheitsmanagement, interne Revision, internes Kontrollsystem, Prozessmanagement oder Servicemanagement, verzahnen und vernetzen.

Literaturverzeichnis

[1] CERT/Octave Methode. www.cert.org/octave/.

[2] Arduini, F. Business continuity and the banking industry. Communications of the ACM 53, 3 (March 2010), 121–125.

[3] Bank of Japan. Business Continuity Planning at the Bank of Japan. Tech. rep., September 2003.

[4] BCI. Expecting the unexpected - Business continuity in an uncertain world. www.thebci.org.

[5] BCI, London First, N. Expecting the unexpected - Business continuity in an uncertain world. Tech. rep., 2003.

[6] BCI (Business Contuinty Institute). BCI GPG (Good Practices Guide), 2008.

[7] bmwfj (Bundesministerium für Wirtschaft, F. u. J. Mittelstandsbericht 2012: Bericht über die Situation der kleinen und mittleren Unternehmen der gewerblichen Wirtschaft, Juli 2012.

[8] Boerse, J.-H. Business Continuity Management bei Pandemien. GRIN –Verlag für akademische Texte, 2007.

[9] BSI 100-2: BSI (Bundesamt für Sicherheit in der Informationstechnologie). It-grundschutz vorgangsweise, 2008.

[10] BSI 100-2: BSI (Bundesamt für Sicherheit in der Informationstechnologie). It-grundschutzgrundschutzkataloge, 2013.

[11] BSI (British Standards Institution). Pas 77 (IT Service Continuity Management), 2006.

[12] BSI (British Standards Institution). Bs 25999 business continuity management, 2007.

[13] Carbonel, J.-C. Assessing IT Security Governance through a MaturityModel and the Definition of a Governance Profile. ISACA, 2008.

[14] CNT - Computer Network Technology. The IT Infrastructure of Business Continuity. Tech. rep., Januar 2002.

[15] Deloitte Touche Tohmatsu. A New Paradigm for Business Continuity Management - Lessons from September 11th. Tech. rep., 2002.

[16] Deutsches Bundesministeriums für Wirtschaft und Technologie. IT-Sicherheitsniveau in kleinen und mittleren Unternehmen, September 2012.

[17] ENISA (European Network and Information Security Agency). Business and IT Continuity - Overview and Implementation Principles. Tech. rep., Februar 2008.

[18] Federal Emergency Management Agency. Fema 141 (emergency management guide for business and industry), 1993.

[19] FSA (Financial Services Authority). Fsa bc (the financial services authority business continuity management guide), 2006.

[20] Heschl, J. Von it-governance bis cobit), 2012.

[21] Information Systems Audit and Control Association (ISACA). CobIT (Control Objectives for Information and related Technology) 5 Framework Overview, 2012.

[22] Information Systems Audit and Control Association (ISACA). CobIT (Control Objectives for Information and related Technology) 5.0, 2012.

[23] International Organization for Standardization. Iso/iec 15504 (spice: Software process improvement and capability determination), 2008.

[24] International Organization for Standardization. Iso/iec 24762:2008 (guidelines for information and communications technology disaster recovery services), 2008.

[25] International Organization for Standardization. Iso 31000:2009, 2009.

[26] Lehecka, G. Kurze Geschichte von Risiko und Risikomanagement.

[27] Merna, T., and Al-Thani, F. Corporate Risk Management. John Wiley & Sons, 2008.

[28] NFPA (National Fire Protection Association). NFPA 1600 (Standard on Disaster/Emergency Management and Business Continuity Programs), 2007.

[29] NIST (National Institute of Standards and Technology). NIST 800-34 (Contingency Planning Guide for Federal Information Systems), 2010.

[30] NIST (National Institute of Standards and Technology). SP 1800 - Cybersecurity Practice Guides, 2020.

[31] NIST (National Institute of Standards and Technology). SP 500 - Information Technology, 2020.

[32] NIST (National Institute of Standards and Technology). SP800 - Computer Security, 2020.

[33] Smit, N. Business Continuity Management - A Maturity Modell. Erasmus University Rotterdam, 2005.

[34] Standards Australia. Hb 292-2006 (a practitioners guide to business continuity management), 2006.

[35] Whitman, M., and Mattord, H. Management of Information Security. Thomson Course Technology, Stamford, CT, USA, 2010.

Zusammenfassung

In Unternehmen, insbesondere aus dem Finanzbereich, ist eine nahezu 100%ige Verfügbarkeit aller Services und Dienstleistungen fast eine Selbstverständlichkeit aus Kundensicht. Diese kann jedoch in der heutigen globalen und vernetzten Welt, welche eine Unzahl an Risiken birgt, oft nur durch viel Glück erreicht werden. Nur ausgereifte und durchdachte Pläne im Hintergrund können eine Hochverfügbarkeit garantieren und somit den Unternehmensfortbestand sichern.

Solche Pläne sind Teil des Business Continuity Managements (BCM) und werden Business Continuity Plan (BCP) genannt. Der Grundstein eines jeden BCP ist eine Ermittlung von Risiken. Diese werden nach modernen Vorgehensschemata mit Hilfe einer Risikoanalyse ermittelt. Dazu wird in dieser Arbeit eine Übersicht ausgewählter Ansätze zu solchen Risikoanalysen und Assessments gegeben. Von den Risiken ausgehend werden innerhalb eines BCM Maßnahmen ermittelt um einen Betrieb weiterzuführen und aufrecht zu erhalten.

Anschließend wird gezeigt, wie Ergebnisse des Risk Assessment in Form von Triggern als Ausgangspunkt für die Erstellung von Business Continuity Plänen eingesetzt werden können. Diese wird am Beispiel des Business Continuity Plannings (BCP) der Bank of Japan (BoJ) untermauert.

Um auch den BCM/BCP-Prozess zu beobachten und verbessern zu können, wird für diesen Zweck ein zugeschnittenes Maturity Modell entwickelt.

Die Erkenntnisse werden auch innerhalb einer Case Study für ein SME angewandt.

Abstract

From a customer perspective we nowadays expect a 100% availability from companies, particularly when it comes to financial services. However, in today's global and interconnected world, which involves a myriad of risk, this can often only achieved through luck. Only mature and well-thought-out plans in the background can guarantee high availability and therefore ensure a company's continued existence.

Such plans are part of the Business Continuity Management (BCM) and are called Busines Contuinuty Plan (BCP). The foundation of every BCP is the identification of the respective risks. In accordance with modern practices these risks are mostly determined within a risk analysis. Therefore this Master's Thesis gives an overview of selected approaches to such risk analyzes and assessments. Based on the risks further measures are determined to continue to operate and maintain in a BCM.

Afterwards it will be shown that the result of the risk assessment can be used as starting point for the creating of the Business Continuity Plans. These starting points will be given in form of triggers. This approach will be supported by a case study.

For the purpose of being able to monitor and improve the BCM/BCP process a tailored maturity model will be developed.

The findings will be be applied within a case study.