FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Vergleich unterschiedlicher Ansätze zur Implementierung eines Business Continuity Management

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Bernhard Tinkl
Matrikelnummer 0426773

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer: Privatdoz. Dipl.-Ing. Mag. Dr.techn. Edgar Weippl
Mitwirkung: Dipl. Ing. Stefan Jakoubi & Dipl. Ing. Simon Tjoa

Wien, 13.07.2011

(Unterschrift Verfasser) (Unterschrift Betreuer)

Erklärung zur Verfassung der Arbeit

Bernhard Tinkl
Höberthgasse 15, 3003 Gablitz, Österreich

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 15.07.2011

_____

(Bernhard Tinkl)

Abstract

Business Continuity Management (BCM) is one of the most essential management-strategies with a promising future.

Since 11th September, 2011 only a few big enterprises remain, which are without any kind of Continuity Management. With time, also smaller enterprises became aware of the importance of this strategy. Small companies started to realize, they are as vulnerable as there bigger brothers to business interruption or operational breakdowns. Those can endanger the consistency of the company, no matter the size of the enterprise.

Experts, who have to implement BCM, are able to choose from a wide variety of different standards. For a prevailing overview of the standards, one has to calculate some amount of expenses. Comparing the methods and standards with each other will require even more time and money to be spent on the subject. Fatal for success are the implementation of some criteria, which allow the expert to compare the unmanageable amount of standards.

These criteria were chosen in a prior stage. Since the standards can change over time, the aim of this work should not only be a comparison of standards, but also create a system capable of comparing standards to each other over the next years without any need for new criteria. Nevertheless, the primary goal was to be able to compare the standards which are chosen in this work in the best possible way.

Out of each area, only the most important standards nowadays were chosen to be compared in this work. They are described individually and were evaluated with every criterion in advance. Later a table was created, which shows a quick overview of the most important criteria for each standard. This allows comparing the standards to each other with the most critical characteristics. This overview should provide a good source of information, so Business Continuity Managers can pick a suitable method which fits their enterprises profile easily.

In conclusion it can be said that, it is initial to create criteria to compare the standards in between. Those will help Business Continuity Managers to operate on a more effective level.

Kurzfassung

Business Continuity Management (BCM) ist eine der zentralen und zukunftsträchtigsten Managementstrategien. Spätestens seit den Ereignissen vom 11. September 2001 gibt es wenig große Unternehmen, die nicht die eine oder andere Art von betrieblichem Kontinuitätsmanagement in Ihrem Unternehmen implementiert haben. Auch bei kleinen Unternehmen wird dieses Thema aktueller, da diese von Katastrophen heimgesucht werden können und unter Umständen noch anfälliger für einen längeren Betriebsausfall sind. Eine solche längere Unterbrechung kann möglicherweise auch eine Gefährdung für den Fortbestand des Unternehmens bedeuten.

Das Problem welches sich Experten stellt, die ein BCM in ihr Unternehmen einführen wollen ist, dass es dafür eine unüberschaubar große Anzahl an verschiedenen Standards gibt. Um hier den Überblick alleine über die Standards zu behalten, bedarf es eines großen Aufwandes. Um auch noch die Vor- und Nachteile der einzelnen Standards zu kennen, sind nochmals mehr Zeit und Wissen notwendig. Darüber hinaus sind Kriterien zu erarbeiten, welche einen Vergleich der einzelnen Standards ermöglichen.

Diese Kriterien wurden in einer Vorstufe erstellt. Da sich die Standards mit der Zeit ändern, soll es neben dem eigentlichen Vergleich der Standards zusätzlich als Ziel dieser Arbeit gesehen werden, neue Standards mit einem in der gegeben Arbeit zu vergleichen. Hierzu eignet sich das oben bereits erwähnte Set an Kriterien. Diese Kriterien sind so ausgewählt, dass sie auch in den nächsten Jahren einen Großteil der Bedürfnisse abdecken und damit auch einen Vergleich von neuen Standards vereinfachen. Primär wurden sie so gewählt, dass sie die vorliegenden Guidelines optimal bewertbar machen.

In dieser Arbeit werden einige der derzeit wichtigsten Standards ausgewählt. Diese Auswahl wurde vom Autor so getroffen, dass eine möglichst breite Auswahl verfügbar ist. Zusätzlich wurden in jedem der Bereiche die wichtigsten Standards ausgewählt. Anschließend wurden diese miteinander verglichen, sodass ein schneller Überblick über die wichtigsten Eigenschaften dieser Werke ermöglicht wird. Dafür werden zuerst diese Standards allgemein beschrieben, daran anschließend werden die erwähnten Kriterien herangezogen. Auf Grundlage dieser Kriterien wird die Gegenüberstellung der Werke durchgeführt. Dieser Vergleich wird jeweils mit allen zehn vorgestellten Guidelines durchgeführt. Zuerst werden die Werke einzeln bewertet, im Anschluss daran werden sie in den zentralen Punkten miteinander verglichen. Damit wird entweder eine kompletter Überblick über die Werke gewährleistet oder der Nutzer kann die für sich selber relevanten Kriterien entnehmen.

Als abschließendes Resultat wird eine Übersicht präsentiert, in welcher auf einen Blick die für die ausgewählten Kriterien passendsten Standards gezeigt werden. Mit diesem Überblick soll es BCM-Managern noch weiter vereinfacht werden, eine erste Vorauswahl für den geeigneten Standard für ihr Unternehmen zu finden.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

In den letzten Jahren ist es immer wichtiger geworden, nach Unterbrechungen der Arbeitstätigkeit den Betrieb eines Unternehmens möglichst schnell wieder herzustellen. Die Konkurrenz wird aufgrund der Globalisierung immer härter, Betriebsausfälle führen rascher zu ernsthaften Schäden und gefährden damit den Fortbestand des Unternehmens. Daher versuchen viele Unternehmen ihren Fortbestand trotz Risiken mit hohem Schadensausmaß zu sichern, ohne dabei auf die ökonomische Nachhaltigkeit zu übersehen.

Aus diesem Ansatz heraus lässt sich auch der immer größer werdende Erfolg des Business Continuity Managements erklären. Unternehmen suchen nach einem Weg, kostengünstig und effizient einerseits ihre Risiken zu kontrollieren und andererseits für den Katastrophenfall gewappnet zu sein.

Business Continuity Management (BCM) ist ein sehr allgemein gefasster, weitgehend abstrakter Begriff. Unter diesem Begriff finden sich unzählige Implementierungen verschiedenster Autoren. Viele dieser Standards werden von großen, auf dieses Themenfeld spezialisierten Organisationen erstellt. Andere wiederum werden von Unternehmen genau auf ihre eigenen Bedürfnisse angepasst. Wieder andere werden von Branchenvertretern auf exakt eine Branche angepasst. Und nicht zuletzt gibt es auch staatliche Stellen, welche wiederum andere BCM-Standards herausgeben. Aus all diesen Quellen entsteht eine große Anzahl an unterschiedlichen BCM-Werken. Zusätzlich sind diese Werke alle in ihrer Natur sehr unterschiedlich. Dadurch wird es Personen, welche sich (noch) nicht ausführlich mit der Materie beschäftigt haben, schwer gemacht, sich einen Überblick zu verschaffen und für eine mögliche Umsetzung in einem Unternehmen den richtigen Standard zu finden.

Ziel dieser Arbeit soll es zusätzlich auch sein, einen Überblick über einige der wichtigsten Standards zu schaffen. Die Begriffe Standard, Guide und Guideline werden in dieser Arbeit synonym verwendet. Ein Vergleich ist dann sinnvoll, in denen die Anzahl der Werke gering gehalten wird. Aufgrund der großen Anzahl an unterschiedlichen Standards ist es nicht einfach, eine aussagekräftige Auswahl an Standards auszuwählen. Daher wurden einige wichtige Kriterien aufgestellt und nach diesen eine Auswahl getroffen. Die Standards sollen verschiedene Bereiche abdecken und jeweils zu den wichtigsten in ihrem Bereichen gehören. Schlussendlich wurden zehn unterschiedliche Standards ausgewählt, die den Auswahlkriterien am besten entsprechen.

Um den Vergleich der zehn Standards aussagekräftig durchführen zu können, soll außerdem ein Katalog mit Kriterien erstellt werden, nach welchen ein BCM-Verantwortlicher selbst einen BCM-Standard bewerten kann. Diese Kriterien sollen ein möglichst allgemeingültiges Bild der Standards vermitteln können. Sie sollen die wesentlichen Bereiche der Standards abdecken und auf alle Standards anwendbar sein. Somit soll es BCM-Zuständigen ermöglicht werden, einen nicht in dieser Arbeit aufgeführten Standard nach diesen Kriterien zu bewerten und mit einem Referenzwerk (zum Beispiel aus dieser Arbeit) zu vergleichen.

Bei den verglichenen Standards sollen folgende Aspekte herausgearbeitet werden. Einerseits sollen die einzelnen Standards unabhängig voneinander nach den vorher ausgearbeiteten objektiven Kriterien bewertet werden. Andererseits soll speziell auf Stärken und Schwächen

der einzelnen Werke im Vergleich zueinander geachtet werden. Dabei soll ermittelt werden, in welchen Bereichen die Standards den anderen voraus sind beziehungsweise wo im Vergleich zu den anderen Standards noch Nachholbedarf besteht.

Abschließend wird der aktuelle Stand der Forschung ermittelt. Zusammenfassend soll dargestellt werden, in welchen Bereichen die Forschung welche Fortschritte zeigt. Dazu wird BCM nicht als Ganzes gesehen, sondern es werden auch die einzelnen Unterbereiche, wie Risikomanagement, Business Impact Analyse, die Erstellung eines Notfallhandbuches oder die Umsetzung eines Notfallplans betrachtet.

1.1 Struktur der Arbeit

Zur besseren Übersichtlichkeit der Arbeit ist diese in drei Blöcke gegliedert welche die grundsätzliche Struktur der Arbeit festlegen.

Der erste umfangreiche Block beschäftigt sich mit der Auswahl der einzelnen Standards und Kriterien. Hier werden alle Standards, die verglichen werden, auch beschrieben. Ebenso werden alle zum Vergleich verwendeten Kriterien dargestellt.

Der zweite Themenbereich ist die Anwendung der einzelnen Kriterien auf die verschiedenen Standards. Hier wird ein detaillierter Vergleich aller Standards durchgeführt. Aus dieser umfangreichen, detaillierten Aufstellung wird dann abschließend eine Conclusio gezogen, in der die wichtigsten Ergebnisse dieses Vergleiches übersichtlich dargestellt werden.

Der dritte Block befasst sich mit den theoretischen und wissenschaftlichen Bereichen des Themas. Dazu zählen vor allem die theoretische Einführung in das Thema sowie die Beleuchtung der aktuellen wissenschaftlichen Forschungen.

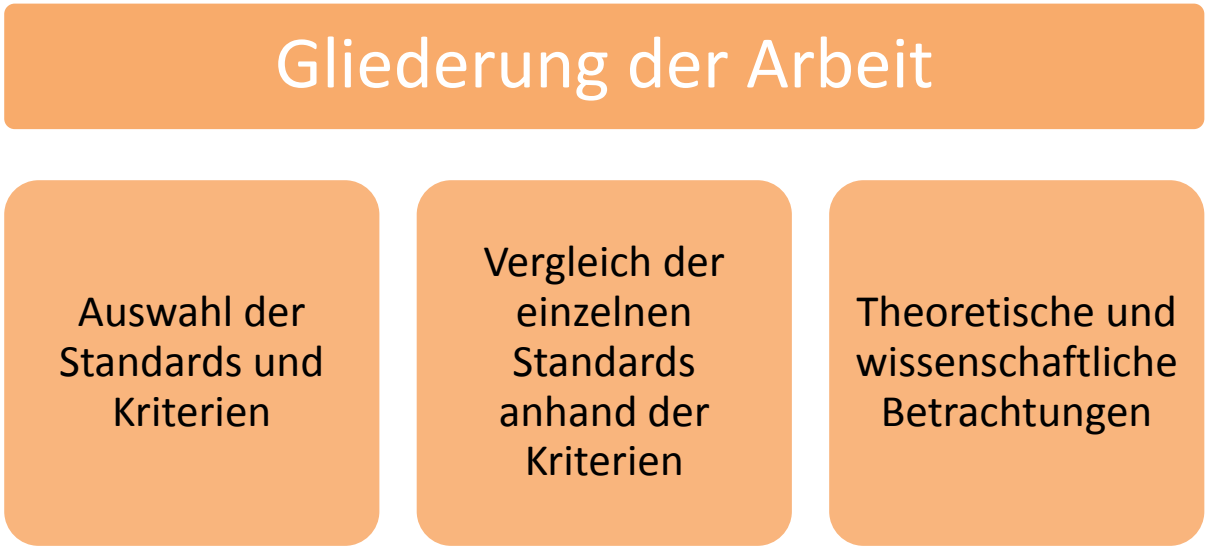

Abbildung 1 - Gliederung der Arbeit

2 Allgemeine Definition von Business Continuity Management

2.2 Was ist Business Continuity Management (BCM)?

Business Continuity Management (zu Deutsch oft auch „Betriebliches Kontinuitätsmanagement“) ist ein ganzheitlicher Managementprozess mit dem Ziel, potentiell gravierende Risiken, die das Überleben eines Unternehmens gefährden, frühzeitig zu erkennen, zu bewerten und Maßnahmen dagegen zu ergreifen (BS25999-1 Code of Practice, 2006 S. 2) (BSI-Standard 100-4, 2008 S. 1). Dies soll erreicht werden, indem rechtzeitig verschiedenste Notfallsituationen sowie die Fähigkeit des Unternehmens, darauf zu reagieren, bewertet und gegebenenfalls verbessert werden. Dadurch wird einerseits eine Umgebung geschaffen, welche die Ausfallssicherheit der Unternehmensprozesse erhöht. Andererseits wird durch ein organisiertes Handeln in Notfallsituationen die Reaktion auf unvorhergesehene Ereignisse verbessert. Da es weder möglich ist, auf alle Ereignisse optimal vorbereitet zu sein, noch alle kritische Prozesse ausfallsicher zu gestalten, muss es das Ziel des BCM sein, die Störung unternehmenskritischer Prozesse so kurz wie möglich zu halten um die Existenz des Unternehmens sicherzustellen. Solche Störungen können entweder menschlichen Ursprunges (zum Beispiel terroristische Angriffe) oder natürlichen Ursprunges sein. Zu letzterer Gruppe sind beispielsweise Erbeben oder Hochwasser zu zählen (BSI-Standard 100-4, 2008 S. 1).

BC ist eine Managementstrategie, welche nicht erst zum Zeitpunkt eines Notfalles implementiert wird. Es müssen bereits im Vorhinein relevante Aktivitäten durchgeführt werden, um beim Auftreten eines Notfalles vorbereitet zu sein. Zu solchen Vorbereitungen gehören einerseits das Erstellen schriftlicher Dokumente wie Notfallpläne oder Leitfäden für das Verhalten bestimmter Personen. Andererseits sind auch Prozeduren wie Backups oder die Bereitstellung alternativer Arbeitsplätze dazuzurechnen (BSI-Standard 100-4, 2008 S. 1).

Auf der anderen Seite ist BC auch keine Managementstrategie welche im Moment des Notfalles endet. Die BC-Strategie legt fest, was nach einer Unterbrechung des Normalbetriebes in einem Unternehmen zu geschehen hat. Dieses Disaster Recovery („Notfallwiederherstellung“) soll dafür sorgen, dass der Normbetrieb möglichst schnell wieder hergestellt werden kann, oder zumindest so rasch, dass das Unternehmen weiter überleben kann.

Jede Organisation hat Aufgaben und Ziele. Diese sind in verschieden kurz-, mittel- und langfristigen Plänen definiert. BCM spricht alle Bereiche des Unternehmens an, ganz besonders aber solche, die im Falle einer Störung das Fortbestehen des Unternehmens gefährden können. Da das Unternehmen vom Management genauso abhängig ist wie von seinen Mitarbeitern, von bestimmten Technologien oder von Standorten, kann sich diese Ausfallssicherheit über alle Bereich der Institution erstrecken. Daher muss dieser Prozess ganzheitlich in ein Unternehmen integriert werden. Erste Aufgabe des Business Continuity Managements ist es, die wichtigsten Bereiche zu identifizieren. Es besteht ferner die Notwendigkeit, dass das obere Management diesen Prozess ernst nimmt und voll inhaltlich wie ablauftechnisch unterstützt (BCI GPG, 2010 S. 5).

2.3 Für wen ist BCM relevant?

Viele Unternehmen fühlen sich gegenüber unternehmenskritischen Risiken unverwundbar. Argumente wie „Wir sind zu groß für solche Probleme“ oder „Bei uns gibt es keine terroristischen Anschläge“ sind oft zu hören. Business Continuity richtet sich explizit an alle Unternehmen, unabhängig von Branche, Unternehmensgröße oder Sitz des Unternehmens. Es gibt verschiedene Ansätze, die sich auf verschiedene Unternehmensarten spezialisieren. Diese sind sowohl branchenspezifische Anleitungen als auch Guidelines, die sich auf bestimmte Unternehmensgrößen spezialisieren. Diese Guides können jedem Unternehmen helfen, das Bestmögliche aus dem Business Continuity Management herauszuholen. Während die genauen Prozesse von Größe, Art und Struktur des Unternehmens abhängen, bleiben die grundsätzlichen Prinzipien des BCM bei allen Organisationen gleich, egal ob sich diese im öffentlichen oder privaten Sektor befinden und große, mittlere oder kleine Unternehmen sind.

Die meisten Katastrophen sind nicht in den Medien zu sehen. Einzelne Bombenanschläge oder Flutkatastrophen schaden vergleichsweise wenigen Unternehmen. Hingegen sind die Katastrophen, welche selten groß bekannt werden oft viel gefährlicher. Oftmals reichen schon kleine Störungen, um die Kernaktivitäten eines Unternehmens zu gefährden. Der Ausfall eines Lieferanten, eines EDV-Systems oder ein Feuer in einem Kernbereich des Unternehmens können unter Umständen bereits die Kernprozesse des Unternehmens stilllegen und dadurch das Fortbestehen eines Unternehmens ernsthaft gefährden (BCI GPG, 2010 S. 5-6).

2.4 Warum BCM?

Der Sinn des Business Continuity Management liegt primär darin, dass ein Unternehmen einen Reaktionsplan auf unvorhergesehene, größere Betriebsunterbrechungen hat. Dadurch kann in Notfällen rasch und effektiv reagiert sowie größerer Schaden vermieden werden. Während dies für die meisten Unternehmen als Grund bereits genug sein müsste, gibt es noch weitere Gründe.

Der offensichtlichste Grund für die Implementierung eines BCM in einem Unternehmen ist eine gesetzliche Vorschrift. Gewisse Branchen oder Unternehmen sind verpflichtet, ein solches Managementsystem umzusetzen. Ein gutes Beispiel hierfür sind verschiedene Bankenverbände, die ihren Banken dieses vorschreiben (BCI GPG, 2010 S. 6).

Ein weiterer Beweggrund für die Umsetzung von BC kann der bessere Ruf gegenüber Kunden, Auftragnehmern und Stakeholdern sein. Wissen diese, dass das Unternehmen ein solides BC umgesetzt hat, erteilen sie diesem Unternehmen leichter Aufträge da das Risiko in vielen Bereichen deutlich sinkt. Somit kann sich das Unternehmen unter Umständen einen kompetitiven Marktvorteil dadurch erarbeiten, dass seine eigenen Risiken minimiert werden. Dies kann zu einem doppelten Vorteil führen und die durch BCM entstehenden Kosten leicht aufwiegen. Unter Umständen kann es auch seine Margen erhöhen, indem BC als „customer care“ dargestellt wird (BSI-Standard 100-4, 2008 S. 1).

Da zu Beginn des Business Continuity Managements eine genaue Analyse des Unternehmens durchführt wird und auch im weiteren Verlauf immer wieder Reviews der vorhandenen Strukturen macht, kann BC sozusagen als Nebenprodukt dabei helfen, die Effizienz eines

Unternehmens zu steigern, indem es Schwachstellen aufdeckt. Solche Schwachstellen könnten sonst unter Umständen unentdeckt bleiben.

Sollte trotz Business Continuity Management eine Unterbrechung des Normbetriebes eintreten, kann ein Unternehmen, welches ohne diese Managementstrategie in dieser Situation vielleicht nicht überleben würde, gestärkt aus dieser Lage hervorgehen. Durch das erfolgreiche Meistern einer solchen Situation kann das Unternehmen schnell den Ruf eines krisensicheren, reaktionsschnellen Betriebes erlangen, auf den Kunden auch in schwierigen Lagen vertrauen können (BCI GPG, 2010 S. 5).

3 Auswahl und Beschreibung der verschiedenen BC-Standards

3.1 Allgemeine Kriterien zur Auswahl der einzelnen Standards

Aufgrund der Relevanz des Themas liegt eine Vielzahl von verschiedenen Werken zu dem weit gefassten Thema Business Continuity vor. Diese reichen von unverbindlichen Guides bis hin zu Standards mit umfangreichen Zertifizierungen. Auch sonst unterscheiden sich diese Werke. Eine beträchtliche geografische Diversität ist dadurch erkennbar, dass Werke aus praktisch allen wichtigen Industrieländern verfügbar sind. Ferner sind zu den wichtigsten Wirtschaftszweigen jeweils eigene Werke verfügbar. Auch Standards, die nicht auf bestimmte Branchen fixiert sind, sind verfügbar. Manche Werke finden international große Verbreitung, während andere lediglich von einzelnen Unternehmen verwendet werden.

Die Auswahl der Standards gestaltete sich daher schwierig. Der Autor hat versucht, die in der Industrie gängigsten Standards auszuwählen. Aufgrund der sprachlichen Einschränkungen wurden ausschließlich Standards welche in deutscher oder englischer Sprache verfügbar sind, in Erwägung gezogen. Des Weiteren wurden Standards von größeren, wichtigeren Organisationen verwendet. Es wurden Werke gewählt, welche entweder frei verfügbar oder deren Beschaffung mit geringen Kosten verbunden war. Ansonsten wurde auf eine möglichst große Bandbreite an verschiedenen Guidelines wertgelegt. So sind Standards aus verschiedenen Erdteilen (Europa, USA, Ozeanien), für verschiedene Branchen (Finanzwesen, Telekommunikation, regierungsnahe Organisationen), für Personen mit unterschiedlichen Vorkenntnissen im Bereich BCM oder für Organisationen mit unterschiedlicher Größe in der Auswahl vorhanden.

3.2 Good Practice Guidelines (Business Continuity Institute)

Der GPG wurde erstmals 2002 vom Business Continuity Institute publiziert. Diese in 85 Ländern tätige und mit über 4000 Mitgliedern erfahrene Organisation versucht seit Jahren, einen hohen Standard und Kompetenz im Bereich des Business Continuity Management zu setzen. Als Sammlung von Best Practices beeinflusste der GPG maßgeblich die Entwicklung des PAS 56, des Britischen Standards für BCM in dieser Zeit. 2005 wurde der Standard von Grund auf überarbeitet und lehnt sich seit damals im Aufbau stark an den BS25999 Standard an. Inhaltlich beeinflussen jedoch auch die wichtigsten internationalen Standards den GPG. Die letzte Überarbeitung fand 2008 statt.

Ziel des GPG ist es, einen Überblick über die wichtigsten BCM-Techniken zu geben sowie, wie bereits der Name schon sagt, gute Praktiken in diesem Bereich zu sammeln und zu publizieren. Dem BCI ist es dabei wichtig, den gesamten BCM-LifeCycle von der Konzeption bis hin zur andauernden Pflege des Business Continuity Managements anzusprechen. Die Besonderheit dieser Guideline liegt darin, dass sie eine der wenigen ist, die eine wirklich praktische Hilfe zur Umsetzung eins Business Continuity Managements bietet.

Erstellt wurde der GPG von Mitgliedern des BCI. Diese haben langjährige Erfahrung in der praktischen Umsetzung von BCM-Maßnahmen. Daher sieht sich der GPG als eine praxisnahe Sammlung von Maßnahmen zur Umsetzung eine BCM-Strategie. Überall dort, wo theoretische Standards wie der BS 25999 nach einem Prozess verlangen, will der GPG eine

genauere Methodik bieten. Darüber hinaus sollen noch weitere nützliche Schritte gesetzt werden, die den BCM-Prozess verbessern und die Umsetzung erleichtern (BCI GPG, 2010 S. 2-3).

3.3 BSI 100-4

Der vierte Teil des Standards des Bundesamts für Sicherheit und Informationstechnik, Notfallmanagement, wurde im November 2008 erstmals herausgegeben. Das Ziel des BSI 100-4 ist es, die durch steigende Risiken verursachten Gefahren zu managen und minimieren. Das sogenannte Notfallmanagement soll Risiken erkennen, analysieren und Maßnahmen dagegen ergreifen können. Der Standard 100-4 soll eine Methodik vorstellen, die zur Einführung und Erhaltung eines Notfallmanagements beitragen. Damit soll die Kontinuität des Geschäftsbetriebs erhöht und gesichert werden. Der BSI 100-4 basiert auf den hauseigenen BSI 100-1 (Managementsysteme für Informationssicherheit) und BSI 100-2 (IT-Grundschutz-Vorgehensweise) Standards. Jedoch zeichnet den neuen BSI 100-4 ein ganzheitlicher Ansatz aus, der nicht mehr auf rein technische Maßnahmen beschränkt ist (BSI-Standard 100-4, 2008 S. 1).

Das BSI ist ein Bundesamt und dem Ministerium für Inneres unterstellt. Der BSI 100-4 ist der einzige gebräuchliche, deutschsprachige Standard zu diesem Thema. Da er von einer staatlichen Organisation herausgegeben wird, beinhaltet er eine Standardisierung, die bei den meisten Behörden in Deutschland umgesetzt wird. Aber auch eine Vielzahl von Unternehmen greift auf diesen Standard zurück. Durch seine Staatsnähe kann auch eine große Rechtssicherheit und ein genaues Eingehen auf die lokalen Gegebenheiten sichergestellt werden.

Auch dieser Standard versucht nicht ausschließlich abstrakte Anleitungen zur Implementierung von BCM zu bieten, sondern auch, wo immer es möglich ist, praxisnahe Hinweise zu liefern. Dabei wird auf über 120 Seiten mit zahlreichen Beispielen versucht, zu erklären, wie die Umsetzung und Weiterführung des BCM am besten und effizientesten zu bewerkstelligen ist.

3.4 BS 25999

Die British Standards Institution, kurz BSI, gilt als die älteste und einer der größten Stellen zur Erstellung von Standards. Mit über 27000 Standards und 6000 Personen aus 1800 Organisationen die sich an der Erstellung dieser beteiligen, verfügt diese Organisation über umfangreiche Ressourcen und große Erfahrung.

Erforderlich wurde ein neuer Standard in Großbritannien im Jahre 2006 durch den UK Companies Act, der gesetzlich festlegte, dass Manager bei der Führung eines Unternehmens besondere Sorgfalt walten lassen müssen. Der BS2599 besteht aus zwei Teilen, dem „Code of Practice“ (BS25999-1) und der „Specification“ (BS25999-2). Der erste Teil sieht sich als praxisnaher Leitfaden mit zahlreichen Ratschlägen. Dieser ist größtenteils aus dem Vorgänger PAS 56 hervorgegangen. Hier werden vor allem Best Practices angeführt (BS25999-1 Code of Practice, 2006 S. 1). Der zweite Teil ist in der Folge der eigentliche Standard. Dieser spezifiziert die Anforderungen, die von der britischen Standardisierungsbehörde an eine Organisation gestellt werden, wenn diese ein effektives Business Continuity Management

implementieren will. (BS25999-2 Specification, 2007 S. ii) In diesem Teil wird besonders auf einen generischen Ansatz geachtet. Es soll allen Organisationsformen, allen Unternehmensgrößen sowie verschiedensten Managementsystemen ermöglicht werden, sich diesem Leitfaden anzupassen. Dabei soll besonders darauf geachtet werden, dass nicht eine Uniformität in allen Unternehmen eintritt, sondern dass jede Organisation besonders ihre Stärken betonen kann und ihre Schwächen möglichst verringert werden (BS25999-2 Specification, 2007 S. 4).

3.5 Financial Service Authority BCM Practice Guide

Im Jahre 2005 hat die Financial Service Authority (FSA) gemeinsam mit der Bank of England (Zentralbank Großbritanniens) und der HM Treasury (britisches Finanzministerium) ein größeres Projekt durchgeführt (Financial Services Authority, 2005), das darauf abzielte, die Belastbarkeit und Fähigkeit zur Erholung der britischen Finanzbranche im Falle einer größeren operationalen Unterbrechung wie einer Naturkatastrophe oder eines terroristischen Anschlags zu ermitteln. In Rahmen dieses Projektes wurden über 60 Unternehmen mehr als 1000 Fragen zum Thema BCM gestellt (FSA BCM, 2006 S. 1).

Aus den Ergebnissen dieser Studie wurde dann eine Guideline zu den Best Practices des BCM erstellt. Diese beruht ausschließlich auf den Ergebnissen der durchgeführten Studie. Hierzu wurden in dem Guide zwei verschiedene Practices eingeführt: Einerseits die „Observed standard practice“, andererseits die „Observed leading practice“. Erstere sind solche Methoden, die von dem Großteil der 60 Teilnehmer gemacht wurden. Hierbei wird sozusagen der allgemeingültige Standard beschrieben. Der zweite Ansatz hingegen beschreibt den Ansatz, den die am höchsten punktenden 20 % aller Teilnehmer verwendeten (FSA BCM, 2006 S. 2-3). Oftmals sind in beiden Kategorien die Ergebnisse gleich, manchmal sind Ergänzungen in den Leading Practices zu finden, manchmal werden auch gänzlich andere Ansätze verfolgt.

Der FSA BCM Practice Guide richtet sich klarerweise primär an die Finanzbranche. Auch soll er weder ein Anfängerleitfaden noch eine Hilfe zur Einführung eines Business Continuity Management sein. Es soll eher Unternehmen mit schon bestehenden BCM Denkanstöße geben, mögliche Schwachstellen zu finden und Verbesserungen durchzuführen. Auch sollte keiner der gegebenen Punkte die unverrückbare und einzige Lösung darstellen, sondern mehr ein Rahmen sein, in dem man seine eigenen Methoden entwickeln kann (FSA BCM, 2006 S. 3-4).

3.6 ISO/PAS 22399

Die International Organization for Standardization ist weltweit die wohl wichtigste Standardisierungsorganisation. Mitglieder sind zurzeit 161 nationale Standardisierungsorganisationen. Trotzdem ist es eine Non-governmental Organization. Sie will eine Verbindung zwischen staatlichen und privaten Organisationen bilden.

ISO 22399 wurde als “Publicly available specification” (PAS) veröffentlicht. Dies bedeutet, dass es keine ISO-Norm ist, sondern eine Übereinkunft zwischen den Verfassern (International Organization for Standardization, 2009). Diese muss nach spätestens drei Jahren reviewt werden, um zu entscheiden, was mit dem Dokument geschehen soll. Nach

spätestens sechs Jahren muss es entweder in einen internationalen Standard umgewandelt oder zurückgezogen werden (ISO 22399, 2007 S. iv).

ISO/PAS 22399 bietet eine allgemeine Anleitung für eine Organisation, um eigenständige Performance-Kriterien für Notfallmanagement und Fortführung von Kernprozessen zu finden. Dabei wird nicht der Ausdruck „BCM-LifeCycle“ verwendet, sondern „IPOCM LifeCycle“. Dies steht für “**i**ncident **p**repardness and **o**perational (business) **c**ontinuity **m**anagement”. Damit soll besonders die Zuständigkeit für alle Organisationsformen, und zwar sowohl im privaten als auch im öffentlichen Sektor, betont werden. Der vom technischen ISO-Komitee TC 223 herausgegebene Standard betont besonders den holistischen Ansatz des IPOCM-LifeCycle. Es soll ein ganzheitlicher Ansatz geschaffen werden, welcher auch in einem geeigneten Management eingebunden werden soll. Explizit ausgeschlossen aus ISO/PAS 22399 werden Notfallmaßnahmen, die nach einer Katastrophe zu folgen haben (ISO 22399, 2007 S. v-vii).

3.7 ASIS SPC.1-2009

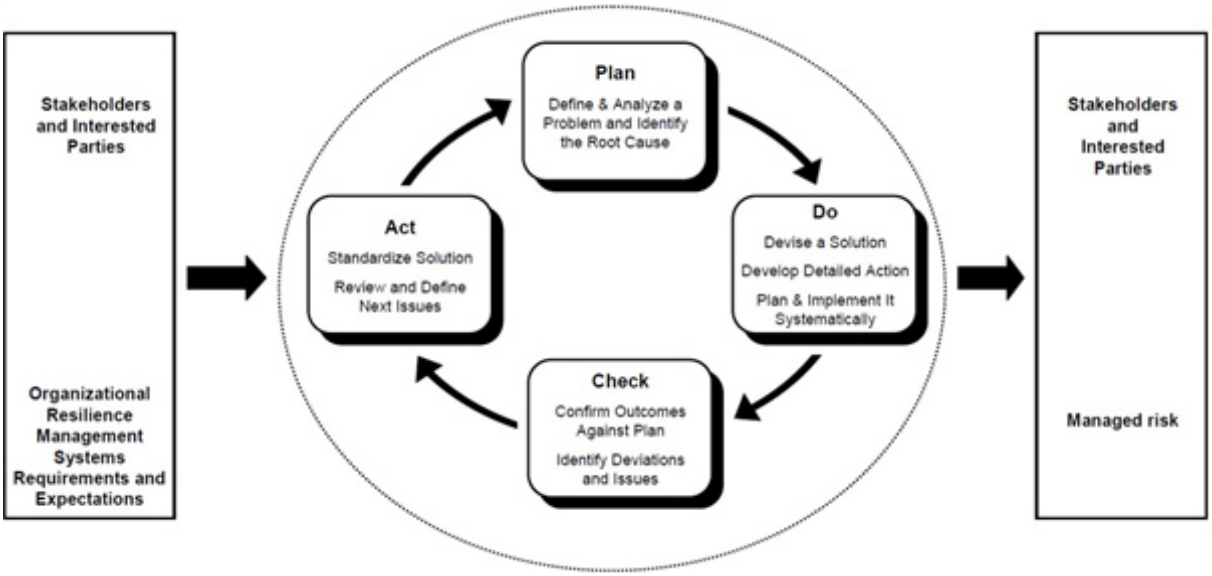

Abbildung 2 (ANAO-Building resilience in public sector entities, 2009)

Die American Society for Industrial Security (ASIS) erstellte diesen Standard mit speziellem Schwerpunkt auf die organisatorischen Aspekte des Business Continuity Managements. Die Guideline verwendet einen prozeduralen Ansatz, um den BC-Prozess zu implementieren, etablieren, operieren, überwachen, reviewen, erhalten und verbessern. Um den BC-Prozess zu strukturieren wird das „Plan-Do-Check-Act“ Modell benutzt (ASIS SPC.1-2009, 2009 S. vii-viii).

Wie Abbildung 2 zeigt, wird als Erstes der Input gesammelt. Dieser besteht aus den Interessen und Bedingungen der verschiedenen beteiligten Personen und Stakeholder. Mit diesen Informationen werden folglich die eigentlichen Schritte durchgeführt. Der Schritt „Plan“ erstellt die verschiedenen Policys, Prozesse, Ziele und Prozeduren, welche für Risikomanagement, Notfallvorsorge und das Reagieren kurz- und längerfristig nach einem Notfall zuständig sind. Diese müssen mit den allgemeinen Zielen und Policys des Unternehmens kompatibel sein. Der nächste Schritt „Do“ implementiert die in dem Punkte „Plan“ erarbeiteten Prozesse, Prozeduren, Schritte, Kontrollen und Policys. „Check“ ist für die Überprüfung der Leistung zuständig. Es wird die Performance der Prozesse gegen die

Policy, die Ziele und die praktische Erfahrung des Unternehmens gemessen. Anschließend werden die erarbeiteten Ergebnisse an das Management zum Review weitergeleitet. Im vierten Schritt, „ACT“, werden korrigierende und präventive Maßnahmen ergriffen. Diese Maßnahmen sollen basierend auf den Resultaten der internen Reviews und Audits erfolgen. Ziel dieser Schritte soll eine kontinuierliche Verbesserung des Managementsystems sein. Der Kreislauf dieser vier Schritte soll fortlaufend wiederholt werden und somit eine immer weitere Verbesserung erreichen. Wichtig ist, dass der Output ein Risikomanagement ist, welches den Anforderungen der Stakeholder und sonstigen interessierten Personen entspricht (ASIS SPC.1-2009, 2009 S. vii-viii).

Ein weiterer Schwerpunkt liegt auch auf der vollen Kompatibilität zu diversen ISO-Standards. Dies bewirkt, dass die Befolgung des Standard durch einen Auditprozess überprüft werden kann, welcher auch mit diversen ISO-Standards kompatibel ist (zum Beispiel ISO 9001:2000) (ASIS SPC.1-2009, 2009 S. ix).

3.8 NIST SP800-34

Die vom National Institute of Standards and Technology (NIST) herausgegebene NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems ist ein BC-Standard, welcher sich speziell auf IT-Fragen konzentriert. Es werden Maßnahmen besprochen, um die IT-Dienste nach einem Notfall oder einer Systemstörung möglichst schnell wieder herzustellen. Dabei sieht sich der SP800-34 als Teil eines generell für ein Unternehmen gültigen Business Continuity Prozesses. In diesen muss sich der IT-Plan eingliedern.

Die Guideline selbst richtet sich vor allem an die Regierungsorganisationen des Entstehungslandes USA. Diese sind dazu angehalten die Ratschläge dieses Standards einzuhalten. Allerdings sind die meisten der Tipps auch für Privatunternehmen, vor allem für solche, welche einen Starken IT-Bedarf haben, nutzbar.

Neben den üblichen Phasen des BCM werden in diesem Standard sieben verschiedene IT-Systeme genau besprochen, wobei jedes IT-System von zwei Seiten beleuchtet wird. Einerseits werden die Anforderungen an die Systeme besprochen, andererseits werden Lösungen zur technischen Umsetzung geboten. Einige Bereiche wie Backups, Redundanz der Systeme oder die Dokumentation werden bei allen IT-Bereichen besprochen. Die sieben Kategorien sind:

1. Desktop Computer und tragbare Systeme

Dabei sind alle normalen Arbeitsstationen gemeint die ein Unternehmen für seine Mitarbeiter betreibt, oder auch mobile Geräte wie Laptops oder Personal Digital Assistants (PDAs).

2. Server

Server sind Computer, die dazu verwendet werden, als Teil eines Netzwerkes zentralen Speicherplatz zu bieten oder zentrale Applikationen zu betreiben. Oftmals ist vor allem der komplette Datenbestand eines Unternehmens auf einem oder mehreren Servern zentral gespeichert.

3. Webseiten

Webseiten sind Informationsseiten die über das Internet oder Intranet betrieben werden. Diese Informationen sind auf einem zentralen Server (Webserver) gespeichert. Webseiten können unter Umständen geschäftskritisch für ein Unternehmen sein. Ein gutes Beispiel für eine unternehmenskritische Webseite ist ein eBusiness-Unternehmen welches sämtliche Geschäftsfelder über einen Webshop abwickelt.

4. Local Area Networks (LAN)

Ein LAN ist ein Netzwerk welches einem bestimmten Unternehmen gehört und mindestens zwei Computer über eine zentrale Stelle (Hub) miteinander verbindet. Die Größe eines solchen Netzwerkes ist unbegrenzt, es können auch viele hundert PC und mehrere Server miteinander verbunden werden.

5. Wide Area Network (WAN)

Ein Wide Area Network ist ein Netzwerk zur Datenkommunikation, welches aus zwei oder mehreren verschiedenen Lokal Area Networks (LAN) besteht, welche auf verschiedenen geografischen Orten verteilt sind. Das WAN ermöglicht den Zugriff von einem LAN auf ein anderes.

6. Verteilte Systeme

Verteilte Systeme sind verschiedene autonom arbeitende Systeme, welche miteinander verbunden sind. Auf den Anwender wirken sie daher als ein System und diese müssen sich nicht darum kümmern, welches der verschiedenen Systeme die gewünschte Aktion ausführt. Ein typisches Beispiel für ein solches System ist eine verteilte Datenbank, bei der die Daten auf verschiedene Datenbanken verteilt sind aber durch ein zentrales System miteinander verbunden sind. Daher ist es für den Benutzer nicht relevant, wo er nach welchen Daten suchen muss. Dies erledigt das System für ihn.

7. Mainframe Systeme

Ein Mainframe ist ein leistungsstarker Computer für viele Benutzer, der große Rechenleistungen übernehmen kann. Die Terminals, die auf dieses System zugreifen, müssen selbst keine Rechenleistung haben, es reicht wenn sie die Ergebnisse des Mainframes anzeigen. Außerdem sind alle Daten zentral an diesem Ort gespeichert.

Diesem aus dem Jahr 2002 stammenden Guide fehlt bei dieser Einteilung aus heutiger Sicht eindeutig der Bereich Wireless Local Area Networks (WLAN). Obwohl viele der Maßnahmen trotzdem für diesen Bereich gültig sind, fehlen hier eindeutige Ratschläge. Das Fehlen der ebenfalls nicht in diesem Standard behandelten Supercomputer (Computer mit extrem hoher Rechenleistung) wird hingegen für die wenigsten Unternehmen ein Problem sein (NIST 800-34, 2002 S. iv-v).

3.9 NFPA 1600

Der „Standard on Disaster/Emergency Management and Business Continuity Programs“ der National Fire Protection Association ist der kürzeste der verwendeten Standards. Er beschreibt in prägnanter Art die erforderlichen Schritte. Dieser seit 1991 immer wieder weiterentwickelte Standard ist weniger zur Umsetzung neuer BC-Methoden geeignet, sondern sollte eher als Checkliste verwendet werden, um bestehende Maßnahmen zu prüfen und verbessern. Diese Einschränkung ergibt sich aus der kurzen Formulierung, die zwar theoretisch dazu ausreicht, einen BC-Plan aufzustellen, praktisch dazu aber wenige Anhaltspunkte gibt und daher dafür wenig geeignet scheint.

3.10 NISCC Telecommunications Resilience

Das „National Infrastructure Security Co-Ordination Centre“ (NISCC) ist dafür zuständig, den Schutz von kritischer Infrastruktur vor elektronischen Angriffen in Großbritannien zu verbessern. Zu diesem Zweck erstellte es unter anderem den Standard zur Telecommunications Resilience. Wie der Name bereits sagt, spezialisiert sich dieser Standard auf BC-Maßnahmen im Bereich Telekom. Dieser Standard ist besonders für jene Unternehmen interessant, welche eine starke Abhängigkeit von der Telekommunikation haben. Mit einer Fokussierung auf die Infrastruktur in Großbritannien werden wichtige Zahlen, zum Beispiel aus dem Bereich der Verfügbarkeit eines Dienstes, ebenso aufgeführt wie Maßnahmen, die zur Sicherstellung der Aufrechterhaltung des Betriebes notwendig sind. Auch bestimmte Technologien, die zur Erhöhung der Ausfallssicherheit beitragen, werden besprochen. Interessant sind die im Anhang aufgeführten Fragebogen, mit denen das eigene Unternehmen ebenso auf verschiedene Telekommunikations-Probleme geprüft werden kann, wie der Anbieter der Telekommunikationsdienste (Telecommunications Resilience, 2006 S. 5-7).

3.11 ANAO - Business Continuity Management - Building resilience in public sector entities

Das Australien Nation Audit Office (ANAO) erstellte diese Guideline mit einem speziellen Schwerpunkt auf öffentliche Institutionen. Trotzdem ist dieser Standard auch für private Unternehmen gut nutzbar (ANAO-Building resilience in public sector entities, 2009 S. III). Er teilt sich in zwei Bereiche: Den eigentlichen Standard und ein sogenanntes Workbook in welchem sich Templates, Checklisten und Beispiele befinden. (ANAO-Building resilience in public sector entities, 2009 S. 1) Durch diese Teilung wird der Standard auch für Einsteiger gut verständlich. Beide Teile sind nach derselben Struktur aufgebaut, somit wird das Verstehen weiter erleichtert.

4 Kriterien zur Bewertung der Standards

4.1 Sprache

Es soll verglichen werden, in welcher Sprache die Standards zur Verfügung stehen. Je nach Unternehmen ist die richtige Sprache unter Umständen von großer Bedeutung. Bei einem multinationalen Großkonzern wird diese weniger ins Gewicht fallen, da dort die Ressourcen verfügbar sind, um die Guidelines in einer anderen Sprache zu verstehen beziehungsweise diese auch zu übersetzen. Bei Klein- und Mittelbetrieben allerdings, die in einem Land oder einer Region angeordnet sind, wird es schwieriger sein, Guidelines in fremden Sprachen umzusetzen, da möglicherweise die benötigten linguistischen Fähigkeiten nicht im Unternehmen vorhanden sind. Allerdings sollte generell davon ausgegangen werden, dass zumindest Englisch als Fremdsprache in jedem Unternehmen ausreichend gesprochen wird, um Standards in dieser Sprache zu verstehen und umsetzen zu können.

4.2 Ort der Entstehung

Verschiedene Länder haben verschiedene Sitten. Diese wirken sich auch auf wirtschaftliche Ansichten und Abläufe aus. Je nach Land oder zumindest Region sind damit verschiedene Ansätze zur Lösung eines Problems normal. Allerdings sind auch für die Implementierung von BCM-Maßnahmen regionale Unterschiede nicht zu übersehen. Möglicherweise sind Maßnahmen, die durch die Autoren eines BCM-Standards erdacht worden sind, für die Manager, die diese umsetzen sollen, aufgrund von kulturellen Unterschieden nicht akzeptabel. Daher soll aufgelistet werden, wo die Entstehung der verschiedenen Guidelines anzusiedeln ist.

4.3 Zeit der Entstehung

Business Continuity Management gilt als ein relativ junges Fachgebiet, welches Anfang der 90er Jahre anfing, sich als eigene Disziplin herauszubilden. Trotz allem, oder vielleicht gerade deshalb, hat sich in den letzten Jahren auf diesem Gebiet einiges weiterentwickelt. Es wurden neue Methoden implementiert und alte verfeinert, verbesserte Abläufe geschaffen sowie Zielsetzungen geändert. Aber vor allem wurden und werden auf die aktuellen geopolitischen und wirtschaftlichen Rahmenbedingungen Rücksicht genommen und die Guidelines dementsprechend angepasst. Somit kann es passieren, dass, wenn veraltete Standards herangezogen werden, suboptimale oder vielleicht sogar schlechte Resultate bei der Implementierung von BCM bekommt. Durch eine Auflistung der Entstehungsdaten soll solchen Problemen vorgebeugt werden.

Ein weitere Punkt, der hier beachtet werden soll, sind die Aktualisierungszyklen. Damit ist gemeint, dass ermittelt werden soll, wann die letzte Aktualisierung des Standards herausgegeben wurde, um die wievielte Version es sich handelt und ob dies schon eine Endversion oder noch ein Vorversion ist.

4.4 Verfügbarkeit

In diesem Kriterium ist zu klären, wie die Verfügbarkeit der untersuchten Standards ist. Manche dieser Standards sind kostenpflichtig, was vor allem für Klein- und Mittelbetriebe oft uninteressant ist, da die Ausgaben zu hoch im Vergleich zu dem Mehrgewinn gegenüber einem freien Standard sind. Ein größeres Unternehmen hingegen legt wahrscheinlich weniger Gewicht auf die Kosten als auf den Mehrgewinn, der bei einem großen Unternehmen dann diese um ein Vielfaches übersteigen kann. Es wird verglichen, welche Standards frei sind und welche nicht, und wenn möglich die Höhe der Kosten ermittelt.

4.5 Art

Im Aufbau unterscheiden sich die Guidelines zwischen solchen, die textuell und ausführlich beschrieben sind, und solchen, die wie eine Checkliste aufgebaut sind. Erstere geben im Normalfall eine umfangreiche Beschreibung der durchgeführten Tätigkeiten und Schritte. Diese soll es auch nicht so versierten Anwendern erleichtern, entsprechende Schritte umzusetzen. Oft sind dabei auch Verweise auf praktische Umsetzung von in der Guideline theoretisch besprochenen Vorgängen enthalten.

Im Gegensatz dazu sind Checklisten oder Guidelines, die eher listenartig aufgebaut sind, zumeist eine minimale Art, einen Vorgang zu beschreiben. Es werden daher die notwendigsten Punkte aufgelistet, ohne diese genauer zu beschreiben. Es bleibt dem Wissen und der Erfahrung des Anwenders überlassen, diese korrekt umzusetzen. Dadurch entsteht ein wesentlich kürzeres, effizienteres Dokument, welches allerdings auch weniger Hinweise zur korrekten Anwendung enthält.

4.6 Vorhandene Tools zur Unterstützung

Guidelines, wie sie hier verglichen werden, liegen im Normalfall im Papierformat oder maximal als PDF vor. Auf jeden Fall sind sie immer textuell. In manchem Fällen ist es von Vorteil, gewisse Vorgänge zu automatisieren beziehungsweise elektronisch durchzuführen. Manche Hersteller bieten Tools an, die speziell auf ihre Guidelines ausgerichtet sind. Es soll ermittelt werden, welche Guidelines solche passende Tools haben, was diese leisten und was sie gegebenenfalls kosten. Solche Tools können in allen Phasen des BCM eingesetzt werden. Ein Beispiel hierfür ist, dass ein Tool zur Berechnung verschiedenen Risiken in der Phase der Risikoanalyse zur Verfügung gestellt wird.

4.7 Allgemein/branchenspezifisch

Verfügbar sind BCM-Guidelines, die von großen BCM-Organisationen herausgegeben werden und allgemeine Ratschläge zum Thema BCM enthalten. Diese Guidelines sind dann zumeist grundsätzlich gehalten und geben Ratschläge, die unabhängig von dem Bereich sind, in dem sie angewendet werden. Bei solchen Guides bleibt es dem Anwender überlassen, aus den allgemeinen Ratschlägen sich die für seine Situation angepasste, praktische Umsetzung zu erarbeiten. Solch allgemein gehaltenen Guides sind im Idealfall auf jede Branche und jedes Unternehmen anwendbar. Folglich gibt es auch bei den allgemeinen Guidelines solche, die sich eher an große Unternehmen richten und solche, die mehr auf Klein- und Mittelbetriebe ausgerichtet sind. Generell sollten allgemeine Guidelines relativ unabhängig von konkreten

Situationen auf alle Unternehmen umgesetzt werden. Der Nachteil bei solchen Guidelines ist, dass durch die oben genannten Kriterien kaum mehr konkrete Ratschläge gegeben werden, sondern im Normalfall eher allgemeingültige Schritte empfohlen werden. Dadurch bleibt viele praktische Umsetzungen von verschiedenen Prozessen der Erfahrung und dem Können des Anwenders überlassen. Der Vorteil dabei ist, dass selbst für Branchen, in denen BCM noch nicht üblich ist beziehungsweise für die es noch keine konkreten BCM-Guides gibt, BCM einfacher umgesetzt werden kann.

Als Gegenstück dazu liegen Guidelines vor die von Firmen oder Organisationen publiziert werden und deren intern entwickelten BCM-Maßnahmen dokumentieren. Diese sind auf das Unternehmen ausgerichtet, von dem sie erstellt wurden. Dadurch wird deutlich, welche Maßnahmen das Unternehmen ergreift, um BCM zu implementieren. Diese sind nur in den seltensten Fällen für das eigene Unternehmen umsetzbar, allerdings bieten sie eine gute Orientierungshilfe. Unter anderem sollten neben der Branche auch noch Kriterien wie Unternehmensgröße, Ausrichtung der Produkte, des Unternehmens und vieles anderes berücksichtiget werden. Das Vorhandensein von branchennahen Guidelines bedingt aber nicht unbedingt, dass das Umsetzen von BCM-Maßnahmen einfacher gemacht wird.

4.8 Unternehmensgröße

Die Unternehmensgröße hat einen nicht unwesentlichen Einfluss auf die Implementierung eines BCM. Je größer ein Unternehmen ist, desto größer sollte zwar der Bedarf an BCM sein, desto schwieriger ist es jedoch, dieses auch zu installieren. Bei großen Unternehmen oder Organisationen sind andere Kriterien wichtig als bei Klein- und Mittelbetrieben. Einige Aspekte die dieses Kriterium ausmachen, wie zum Beispiel der Umsetzungsaufwand oder die Kosten, werden schon durch andere Kriterien abgedeckt. So ist ein hoher Kostenpunkt für Großbetriebe weniger wichtig als für kleine. Hingegen wird eine ausführliche Beschreibung aller Schritte für ein größeres Unternehmen weniger wichtig sein, da es Experten mit dem nötigen Know-how einsetzen kann. Eine kleine Unternehmung hingegen wird eher auf ein günstiges und effizientes Verfahren setzen wollen, welches sich ohne zusätzliches Wissen anwenden lässt.

4.9 Art der Verfügbarkeit

In der heutigen Zeit hat sich als Publikationsweg neben den klassischen Medien Buch und Zeitschrift noch ein weiteres, neues Medium etabliert: der digitale Weg. Normalerweise als PDF-File (plattformübergreifendes Dateiformat für Dokumente, von der Firma Adobe Systems entwickelt) oder auf einer Webseite als HTML-Text verteilt, löst dieses oft das klassische Medium ab. Auch bei einer hohen Anzahl von Guidelines ist dies inzwischen der Fall. Der Vorteil liegt auf der Hand: eine billigere, einfachere Verbreitung. Viele Guides greifen darauf zurück. Manche wählen den Mittelweg und publizieren beides. Auf der anderen Seite will mancher Klient lediglich einen der beiden genannten Wege. Daher soll ermittelt werden, auf welchen Weg die Guidelines zu beziehen sind.

4.10 Möglichkeiten zur Zertifizierung

International setzt es sich immer weiter durch, verschiedene Maßnahmen durch unabhängige Institutionen zertifizieren zu lassen, um dadurch die Qualität der erbrachten Leistungen

sicherzustellen. Oft wird dies von Vertragspartnern oder Kunden gewünscht beziehungsweise gefordert. Ähnlich ist dies auch, wenn die Manager eines Unternehmens BCM-Maßnahmen umsetzen. Manche große BCM-Organisationen bieten verschiedene Arten von Zertifizierungen an. Diese werden zwar nicht für alle Unternehmen, die diese Maßnahmen umsetzen, von Relevanz sein, allerdings benötigen manche Firmen aufgrund der oben genannten Verpflichtungen die eine oder andere Art von Qualitätsüberprüfung, welche sich am leichtesten und besten mit einer Zertifizierung durch eine unabhängige BCM-Organisation erreichen lässt. Sollten verschiedene Arten von Zertifikationen vorhanden sein, soll ermittelt werden, welche Teilbereiche diese umfassen und welche Bereiche nicht berücksichtigt werden. Ebenso soll verglichen werden, wer zertifiziert werden kann, ob dies für ganze Unternehmen möglich ist beziehungsweise für Einzelpersonen (BCM-Verantwortlicher) oder für beide Möglichkeiten.

4.11 Rechtliche Begrenzungen

Durch die lokale Entstehung der Guidelines kann es in gewissen Fällen zu einer Anwendung von lokalen Gesetzen und zur Annahme von rechtlichen Rahmenbedingungen kommen. Durch die lokale Begrenzung von Gesetzen, die vor allem in Europa durch die einzelnen Nationalstaaten häufig der Fall ist, kann es zu verschiedenen Gesetzeslagen in gleichen Situationen kommen. Dies muss berücksichtigt werden, wenn es zu rechtlichen Betrachtungen und Entscheidungen kommt. Sind in einem Guide verschiedene regionale Gesetze aufgeführt und angewendet, wird es bei einer Umsetzung in einer anderen Region zu Problemen kommen. Sind rechtliche Ratschläge hingegen eher allgemein gehalten, kann dies einigen Problemen vorbeugen, auch wenn trotz allem zur korrekten Anwendung das nötige Know-how vorhanden sein muss.

4.12 Flexibilität

Die Guidelines für BCM geben bestimmte Maßnahmen vor, die umgesetzt werden müssen um erfolgreich zu sein. Nicht immer ist es möglich, alle diese Maßnahmen umzusetzen. Es kann verschiedene Gründe geben, warum dies nicht möglich ist. Manchmal sind beispielsweise gewisse Technologien für ein Unternehmen verpflichtend, auch wenn diese laut BCM nicht als ideal anzusehen sind, weil sie beispielsweise ein hohes Risiko bergen. Auch sind manchmal durch gewisse regionale Gegebenheiten Eingriffe in Teile, sei es organisatorisch oder technisch, des Unternehmens nicht möglich. Dadurch müssen die Personen, die BCM umsetzen, flexibler arbeiten.

Es soll bewertet werden, wie ein BCM-Ansatz mit solchen Problemen umgeht. Wie werden solche Probleme in den Ansatz mit einbezogen? Gibt es alternative Wege, solche Technologien trotzdem sinnvoll zu bewerten oder wird starr auf dem vorgegebenen Weg weitergegangen?

4.13 Organisatorisch/kulturell

Um ein BCM durchzuführen, sind stets auch organisatorische Maßnahmen zu ergreifen. Diese Maßnahmen setzen eine gewisse organisatorische Flexibilität voraus. Je nach Ist-Situation und Soll-Situation können diese Änderungen auch umfangreicher sein. Vor der Umsetzung des BCM muss sichergestellt werden, dass solche organisatorische Änderungen möglich sind.

Bei diesem Kriterium ist auch zu berücksichtigen, wie umfangreich die organisatorischen Maßnahmen sein müssen, um andere Punkte des BCM umzusetzen. Ebenso fällt in diesen Bereich der Ablauf eines BCM. Müssen zusätzliche Maßnahmen ergriffen werden, um es durchzuführen? Welche Rahmenbedingungen sind notwendig, um den BCM-Ansatz durchzuführen?

Dieses Kriterium soll die benötigte Tiefe des Eingriffs in ein organisatorisches System vergleichen. Somit soll bewertet werden, ob und in wieweit die Organisation in einem Unternehmen davon berührt wird. Es ist nicht gesagt, dass eine Änderung in der Struktur eines Unternehmens schlecht ist. Es soll ausschließlich die benötigte Tiefe des Eingriffes festgestellt werden, ohne diese positiv oder negativ zu beurteilen.

4.14 Welche Organisation steht dahinter?

Guidelines in dieser Größenordnung werden meist von Organisationen oder Unternehmen publiziert. Dies können spezialisierte Organisationen sein, aber auch Unternehmen, welche ihren Standard publik machen. Eine weitere Möglichkeit ist, dass die Guides und Richtlinien von einem Staat oder einer staatlichen Organisation herausgegeben werden. Jede dieser Organisationen hat ihre Vor- und Nachteile So kann eine staatliche Organisation auf eine breite Infrastruktur zugreifen, hat dafür wahrscheinlich wenig Spitzenmanager in diesem Bereich. Ein Großunternehmen mag zwar mehr Know-How haben, allerdings wird es diesem im Normalfall schwerer fallen, seine Standards durchzusetzen. Spezialisierte Organisationen können am besten auf Know-how zugreifen, da sie sich von jedem Unternehmen und jeder stattlichen Organisation diese holen können. Im Gegenzug dazu werden sie mit finanziellen Mitteln am knappsten bestückt sein, da sie auf Lizenzen und Spenden angewiesen sind.

4.15 Vorlage/Querverbindung zwischen Guidelines

Obwohl das Business Continuity Management eine relativ junge Disziplin ist, gibt es schon eine Vielzahl an Standards, Guidelines und Umsetzungen davon. Doch kaum ein Standard versucht, das Rad neu zu erfinden und sich komplett unabhängig von allen anderen Standards weg zu entwickeln. Die meisten Guides werden andere Werke als Vorlage nehmen oder sich an anderen Guidelines zumindest orientieren. Ziel ist es, die Querverbindungen innerhalb der Guidelines herauszufinden. Möglicherweise können damit Parallelen und Unterschiede gefunden werden.

4.16 Zielgruppe

In diesem Kriterium soll die Zielgruppe des jeweiligen Standards bestimmt werden. Manche Guidelines richten sich an das obere Management und sind daher eher übersichtsmäßig gestaltet. Andere wiederum richten sich an die BCM-Verantwortlichen selbst. Eine weitere Zielgruppe, sind die Techniker, welche dann mit der geänderten Struktur arbeiten. Je nach Zielgruppe haben die Guidelines unterschiedliche Schwerpunkte.

4.17 Gegebene Templates

Zur Durchführung der im BCM empfohlenen Maßnahmen sind Checklisten, Formulare, Fragebögen und Ähnliches notwendig. Diese zu erarbeiten, kann viel Arbeit sein, die nicht

oder nur begrenzt notwendig ist, da sie in vielen Punkten bei allen Unternehmen gleich sind. Mitgelieferte Templates können viel Arbeit ersparen. Eine Anpassung an das eigene Unternehmen ist einfacher zu vollziehen als eine Neuerstellung. Außerdem reduziert sich das Risiko, etwas zu übersehen, da der Anwender der Standards auf die gesammelte Erfahrung von vielen BCM-Verantwortlichen zurückgreifen kann. Auch beispielgebende Vorlagen erleichtern die Umsetzung von Maßnahmen. Ebenfalls damit sichergestellt wird eine Risikominimierung, da die Autoren der Guides im Normalfall die für ihre Methoden geeignetsten Hilfsmittel kennen und somit den Anwendern die besten Tipps geben können. Sollte dies nicht der Fall sein und der Anwender findet ein aus seiner Sicht besseres Mittel, so ist immerhin einen inhaltliche Führung durch die Vorgabe gegeben. Es soll einerseits angegeben werden, welche Templates dem Guide beiliegen, andererseits aber auch bewertet werden, ob die angefügten Hilfsmittel den Zweck erfüllen oder ob es bessere Alternativen gibt.

4.18 Benötigte Ressourcen

Finanzielle Mittel spielen bei der Einführung eines neuen Managementsystems immer eine entscheidende Rolle. Oft werden Projekte aufgrund eines zu großen finanziellen Aufwandes vom Management nicht genehmigt. Doch nicht der finanzielle Aufwand alleine entscheidet. Zusätzlich sind ebenso personelle und organisatorische Umstellungen und die damit verbundenen Aufwände zu berücksichtigen. Mögliche organisatorische Umschichtungen können auf lange Zeit teurer werden als kurzfristige Investitionen. Nicht zuletzt dürfen auch die technischen Umstellungen nicht außer Acht gelassen werden. Eine Umstellung der technischen Ausrüstung, die durch die Einführung des BCM notwendig werden kann, kann einschneidende Auswirkungen auf alle Bereiche des Unternehmens haben. Daher darf auch hier der finanzielle Aufwand nicht unterschätzt werden.

Bei dem Vergleich soll ermittelt werden, mit welchem finanziellen Aufwand bei der Einführung zu rechnen ist. Es soll dabei weniger auf die Anschaffungskosten als auf die Auswirkungen bei der Einführung eines solchen Systems Wert gelegt werden. Demgegenüber kann es nicht bei jedem Unternehmen zu gleichen Kosten kommen, doch soll eine allgemeine Aufwandsabschätzung erstell werden.

Anmerkung: Dieser Punkt wurde später weggelassen, da er nicht bewertbar war.

4.19 Integration von Organisationsprozessen

Es soll untersucht werden, welche Schnittstellen eine Guideline zu Organisationsprozessen zulässt, beziehungsweise welche sie unterstützt. Die meisten Guidelines werden bereits von Anfang an so konzipiert, dass sie gewisse interne Managementprozesse unterstützen. Dazu zählen beispielsweise allgemeine Begriffe wie Records Management (Schriftgutverwaltung) oder Change Management, aber auch konkrete Implementationen davon, wie zum Beispiel ITIL oder gewisse ISO-Standards.

4.20 Benötigte Vorkenntnisse

Vor allem Klein- und Mittelbetriebe werden es sich selten leisten können, einen bereits voll ausgebildeten BCM-Verantwortlichen mit Erfahrung einzustellen. Im Normalfall wird ein

Manager der bereits in dem Unternehmen beschäftigt ist, für diese Aufgabe abgestellt. Dieser kann im Normallfall keine Erfahrung mit BCM haben. Normalerweise wird dieser Manager in einem der Teilgebiete des BCM, beispielsweise im Risikomanagement oder in der Business Impact Analyse, schon Erfahrungen haben und dieses einbringen können. Um ein komplettes BCM-Management erstellen zu können, sind auch andere Fähigkeiten zu erwerben. Je kleiner ein Unternehmen, desto weniger Ressourcen hat es vermutlich zur Verfügung. Es soll ermittelt werden, ob es möglich ist, den Standard ohne intensivere Schulungen adäquat umzusetzen, oder ob es aufgrund von fehlenden Informationen oder komplizierten Vorgängen nötig ist, ein fundiertes Hintergrundwissen zum Thema BCM zu haben.

4.21 Methoden

Für viele Schritte im BCM werden Methoden zur aktiven Bestimmung von Daten benötigt. Beispielsweise wird im Teil „Understanding the Organisation“ im Good Practice Guide des BCI eine Business Impact Analyse durchgeführt. In diesem Teil des Vergleiches soll ermittelt werden, wie die Anforderungen an solche praktische Schritte gestellt werden. Werden die Schritte ausführlich erklärt und wird genaue Anleitung gegeben? Sind unterstützende Unterlagen zu allen Teilen der praktischen Arbeiten im Guide enthalten? Auf der anderen Seite ist es möglich, dass eine Guideline nur einen allgemeinen Hinweis auf das gibt, was zu tun ist. Im oben genannten Beispiel ist dies dann „Führen Sie eine Business Impact Analyse durch.“. Es werden hiermit keine Begrenzungen zur Anwendung gebracht, aber auch keine Erleichterungen in Hinsicht auf die am besten anzuwendenden Methoden gegeben.

4.22 Ausschließlich Maßnahmen zur Einführung von BCM oder auch Überprüfung und Weiterführung

Da ein typischer BCM-Standard aus mehreren Phasen besteht, soll hier überprüft werden, ob die Einführung eines BCP in der Guideline angedacht ist, oder ob auch BCP-Tests und das Erhalten, Weiterführen und Warten des BCP in diesem Werk angedacht ist. Damit soll sichergestellt werden, dass das BCM nicht nach der Einführung des Business Continuity Planes eingestellt wird und das BCM niemals ordentlich und komplett durchgeführt wird. Sollte dies gewünscht sein, soll auch die Testung und Weiterführung des BCM in dem Standard verfügbar sein.

4.23 Ergänzendes Material

Unter ergänzenden Materialen fallen jene Dinge die unter 4.17 „Templates“ sowie unter 4.6 „Vorhandene Tools zur Unterstützung“ nicht enthalten sind, aber den Guidelines trotzdem als Unterstützung beigelegt sind. Als Beispiele seien hier ergänzende Literatur oder Verweise auf wissenschaftliche Arbeiten genannt. Generell sollen diese Materialien dem Anwender, der sich mit BCM beschäftigt, einen genaueren Einblick in die Materie geben. Es sollen hier, ähnlich wie in einer wissenschaftlichen Arbeit, Quellen genannt, Referenzen erzeugt und Hintergründe erläutert werden. Nicht nur der Umfang der Materialien ist ausschlaggebend, sondern auch deren Qualität und Relevanz.

Hier soll auch untersucht werden, wie es mit der Präsenz der jeweiligen Standards im Internet aussieht. Es soll geklärt werden, ob und wie viele Erwähnungen, Kritiken, Hilfen und

Ähnliches im Internet verfügbar sind. Dazu soll eine Analyse von verschiedenen Suchmaschinen wie Google, Yahoo sowie andere relevante Treffer herangezogen werden.

4.24 Phasen

Jedes BCM-Programm gliedert sich in Unterteile beziehungsweise Phasen. Jede dieser Phasen arbeitet einen bestimmten Teil des BCM ab. Diese Phasen unterscheiden sich je nach BCM-Standard. Es soll ermittelt werden, in welche Phasen sich welcher Standard gliedert. Wenn möglich sollen die einzelnen Phasen verglichen werden. Ebenfalls soll beurteilt werden, welche Phasen bei bestimmten Guidelines einmalig sind, welche fehlen und welche bei allen gleich sind. Doch vor allem sollen die Unterschiede in den verschiedenen Guidelines herausgearbeitet werden. Damit soll erreicht werden, dass die Standards untereinander besser vergleichbar sind. Möglicherweise sind dadurch auch gewisse Stärken oder Schwächen von bestimmten Guides herauszusehen.

4.25 Beratung & Support

Je nach der Organisation, die hinter einem Standard steht, bietet diese Beratung und Support bei der Einführung eines BC-Managements an. Vor allem bei staatlichen Organisationen besteht diese Möglichkeit öfters. Die Beratung soll vor allem die Umsetzung eines korrekten Standards sicherstellen. Support bezieht sich hier weniger auf das aktive Unterstützen der Unternehmen als auf das Zur Verfügung stellen von Know-how und Hilfestellungen. Es soll verglichen werden, welche Art von Support zu Verfügung gestellt wird.

4.26 Befolgung der Richtlinien der Aufsichtsbehörden

Es gibt Richtlinien von Behörden, welche eine gewisse Kontrolle über kritische Prozesse fordern. Beispielsweise muss eine Aktiengesellschaft andere, strengere Standards einhalten als ein Unternehmen in privater Hand. Es soll ermittelt werden, welche Richtlinien die Standards unterstützen beziehungsweise welche Kriterien sie nicht erfüllen.

4.27 Befolgung von internationalen IT-Standards

Mit Einführung eines BCM-Standards werden zum Teil auch andere Standards mit eingeführt. Dies entsteht dadurch, dass sich Standards in manchen Bereichen überschneiden beziehungsweise auch einen anderen Standard als Vorlage nehmen. Dadurch kann zum Teil mit Einführung einer Guideline ein Teil einer anderen erfüllt werden. Dies kann dabei helfen, einen bereits bestehenden Standard einfacher in einen neuen über zu führen. Es soll ermittelt werden, welcher Standard welchen anderen unterstützt.

5 Vergleich der einzelnen Standards

5.1 GPG/BCI

5.1.1 Sprache

Der Good Practice Guide (GPG) des Business Continuity Institute (BCI) ist in seiner neuesten Version auf Englisch erhältlich. Dies erklärt sich durch seine Entstehung im englischen Sprachraum. Zu dem Volltext ist auch noch eine Art Folder erhältlich, der sich „The Pocket Sized Good Practice Guidelines“ nennt und eine zweiseitige Kurzzusammenfassung des GPG ist.

Die aktuelle Version (2008-2) ist in keiner anderen Sprache erhältlich. Jedoch ist die Version 2005 (die in den Grundzügen mit der aktuellen Version weitgehend übereinstimmt) ebenfalls in italienischer und deutscher Sprache erhältlich. Zusätzlich ist der Folder in den Sprachen Deutsch und Koreanisch zum Download verfügbar.

5.1.2 Ort der Entstehung

Der Sitz des Business Continuity Institute befindet sich in Caversham, einer Kleinstadt westlich von London, England. Das 1994 gegründete Institut hat heute mehr als 4000 Mitglieder aus über 85 Ländern. Auch an der Erstellung des GPG haben Mitglieder aus verschiedenen Ländern mitgewirkt. Dadurch entstehen in dem Good Practice Guide keine starken regionalen Besonderheiten. Einzig die deutliche Anlehnung an den BS 25999 kann in manchen Fällen möglicherweise zu regionalen Beschränkungen führen, doch wird versucht, in der Guideline des BCI möglichst allgemein zu bleiben und nicht zu sehr auf regionale Gepflogenheiten einzugehen.

5.1.3 Zeit der Entstehung

Das BCI hat ihren ersten Good Practice Guide im Jahre 2002 publiziert. Dieses Dokument hatte damals großen Einfluss und diente vielen anderen Standards als Vorlage, beispielsweise dem PAS56. Im Jahre 2005 wurde der alte Standard komplett überarbeitet. Er wurde an den neuesten Stand der BCM-Praktiken angepasst und strukturell neu gestaltet. Nach der Herausgabe des britischen Standards BS 25999 im November 2006 wurde der GPG adaptiert, um dem neuen Standard zu entsprechen. Dieser Standard wird regelmäßig reviewt und den aktuellen Gegebenheiten angepasst. Hierbei passieren meist kleine Änderungen, Struktur und Grundinhalt bleiben gleich. Die zur Zeit der Erstellung dieser Arbeit aktuelle, und daher auch verwendete, Version ist 2008-2. Im Jahr 2009 wird ein grundlegendes Review des GPG durchgeführt, um dann im Jahr 2010 einen neuen GPG 2010 herauszugeben. Dieser soll dann auf dem neuesten Stand sein sowie Änderungen in Inhalt und Umfang haben (BCI GPG, 2010 S. 3).

5.1.4 Verfügbarkeit

Der Good Practice Guide steht auf der Homepage des Business Continuity Institute gratis zum Downloaden zur Verfügung. Da es keine kostenpflichtige Version gibt, steht der Guide allen Usern kostenfrei zur Verfügung.

5.1.5 Art

Der Good Practice Guide ist ein textuelles Dokument, welches in den meisten Vorgängen ausführlich beschrieben ist. Auf sechs Kapitel aufgespalten, hat jeder Teil zwischen 16 und 38 Seiten. Es soll auch Anfängern im Bereich BCM ermöglichen, einen Einblick in dieses Thema zu bekommen. Die Guideline ist zwar generell in ganzen Sätzen mit ausführlicher Beschreibung erstellt, wo notwendig werden auch Listen zu Aufzählung verwendet (BCI GPG, 2010 S. 4).

5.1.6 Vorhandene Tools zur Unterstützung

Zur Unterstützung der Anwender des Good Practice Guide gibt es auf der Homepage des Business Continuity Institute eine eigene Sektion mit entsprechenden Tools. Diese Sektion ist allerdings Mitgliedern dieser Organisation vorbehalten. Nicht-Mitglieder haben auf diese Unterstützung keinen Zugriff, können daher auch keine einzelnen Tools kaufen. Die Tools selbst wurden von Mitgliedern des BCI entwickelt und dort zu Verfügung gestellt. Diese reichen von Score Cards und Templates bis hin zu BCM-Programmen, mit denen digital und automatisiert Benchmarks erstellen werden können.

5.1.7 Allgemein/branchenspezifisch

Der GPG ist nicht an eine bestimmte Branche gekoppelt. Er wurde mit der Absicht erstellt, alle Branchen in gleichem Maße zu unterstützen. Daher ist dieser Standard allgemein genug gehalten, um für alle möglichen Branchen zu gelten. Es ergeben sich manchmal Praktiken, die nicht für alle durchführbar oder zielführend sind, aber im Allgemeinen wird darauf geachtet, keine zu spezifischen Empfehlungen zu geben.

Der Vorteil dieses Standards ist, dass er von BCM-Managern aus verschiedensten Ländern und verschiedensten Branchen erstellt wurde. Dadurch entsteht mehr oder weniger eine Mischung aus verschiedenen Best Practices die in unterschiedlichen Bereichen angewendet werden. Durch die umfangreiche Erfahrung der Manager, die diese Guideline erstellt haben, ergibt sich eine gute Kombination aus praktischer Erfahrung und theoretischem Wissen (BCI GPG, 2010 S. 8).

5.1.8 Unternehmensgröße

Auch hier gilt Ähnliches wie bei dem Kriterium zum Thema branchenspezifisch. Die Guideline wurde mit spezieller Ausrichtung auf Unabhängigkeit der Unternehmensgröße erstellt. Es soll ermöglicht werden, dass alle Unternehmen diese Guideline verwenden können, von solchen mit einer einzelnen Niederlassung bis hin zu global agierenden Unternehmen (BCI GPG, 2010 S. 6-8).

5.1.9 Art der Verfügbarkeit

Der Guide ist downloadbar, das Dateiformat ist das allgemein übliche Adobe PDF. Er ist unterteilt in sechs Teile, entsprechend des Aufbaues der Guideline. Auch die Übersetzungen in andere Sprachen (siehe →5.1.1) sind auf derselben Homepage verfügbar. Alte Standards (beispielsweise GPG 2005) sind auf der Homepage schwer oder gar nicht zu finden, wenn sie

ersichtlich sind, allerdings auch gratis erhältlich. Der Standard ist in keiner anderen Form verfügbar.

5.1.10 Möglichkeiten zur Zertifizierung

Das Business Continuity Institute bietet eine Zertifizierung für Einzelpersonen an. Diese Organisation hat einen Benchmark entwickelt, um die Best Practices bewerten zu können. Dieser wird CBCI genannt und kann an verschiedensten Orten abgelegt werden. Basierend auf den international anerkannten „Certification Standards for Business Continuity professionals“, wurden ursprünglich zehn Themenbereiche entwickelt, die die wichtigsten Skills eines BCM-Managers umschreiben. Um sich an den aktuellen Aufbau des Good Practice Guide anzupassen, wurden diese zehn Bereiche auf die sechs aktuellen Kapiteln umgelegt. Somit gibt es für jeden Bereich eine Zusammenfassung (BCI-Membership Criteria) der wichtigsten Kompetenzen, die ein BCM-Manager können muss, um die Zertifizierung zu bekommen.

Das BCI bietet zusätzlich verschiedene Mitgliedschaften an. Diese spiegeln auch in gewisser Weise eine Art Zertifizierung wieder. Die entsteht dadurch, dass die verschiedenen Mitgliederstufen (Fellow, Member, Specialist, Associate Member, Affiliate, Student) unterschiedliche Vorbedingungen haben, welche auf den Grad der Erfahrung mit dem Thema BCM haben. Beispielsweise muss man, um Mitglied zu werden, zur Zeit der Aufnahme im Bereich Business Continuity Management arbeiten, die oben genannte CBCI mit Auszeichnung bestehen und mindestens drei Jahre mit allen sechs Teilen des GPG gearbeitet haben. Erst dann kann man sich um diesen Titel (auch MBCI genannt) bewerben (BCI-Membership Criteria). Hieraus wird ersichtlich, dass in dieser Organisation ein hoher Anspruch, auch an praktische Fähigkeiten gestellt wird. Interessierte müssen aber nicht Mitglied werden, um eine Zertifizierung des BCI zu bekommen.

Eine Zertifizierung für Organisationen wird hingegen nicht angeboten. Dies entsteht dadurch, dass das Business Continuity Institute ein Zusammenschluss von aktiven BCM-Managern ist und keine Mitarbeiter hat, welche in ein Unternehmen gehen, um dort die Umsetzung der BCM-Maßnahmen zu überprüfen.

5.1.11 Rechtliche Begrenzungen

Der GPG wurde von Personen aus verschiedenen Ländern entwickelt. Es kann damit auch nicht von einer regionalen Entstehung geredet werden. Ebenso war es den Autoren wichtig, ein allgemeingültiges Werk zu schaffen, welches möglichst wenigen Beschränkungen unterliegt. Durch diese beiden Kriterien kann der Anwender auch keine rechtlichen Begrenzungen feststellen. Trotz der allgemeinen Art des Standards darauf geachtet werden, dass keine regionalen Gesetze verletzt werden, denn es kann nie ausgeschlossen werden, dass die Guideline geltendem Recht widerspricht (BCI GPG, 2010 S. 8).

5.1.12 Flexibilität

Der GPG ist zwar von der Struktur her starr, allerdings ist er inhaltlich durchaus als flexibel zu betrachten. Dies ist sicher eine Folgeerscheinung der allgemeingültigen Formulierung. Dadurch dass keine branchenspezifischen Ratschläge gegeben werden, kann es hier nicht zu

Problemen kommen. Schwierigkeiten kann es allerdings bei der Ausführung der Methoden geben. Da diese relativ genau spezifiziert sind, kann es bei Problemen in der Ausführung der Methoden zu Problemen in der weiteren Vorgehensweise kommen.

5.1.13 Organisatorisch/kulturell

Es können keine Eingriffe in die Unternehmenskultur oder Struktur festgestellt werden. Dadurch dass versucht wurde, den Standard möglichst allgemein zu halten, werden keine besonderen Einschnitte gemacht. Auch auf branchenspezifische Details wird dadurch nicht eingegangen.

5.1.14 Welche Organisation steht dahinter?

Der Good Practice Guideline wurde vom Business Continuity Institute verfasst. Diese Organisation ist in der Nähe von London, Großbritannien beheimatet und wurde 1994 gegründet. Zurzeit besteht sie aus über 4000 Mitgliedern aus mehr als 85 Ländern verteilt über die ganze Welt. Der Schwerpunkt liegt zwar im Anglo-Amerikanischen Raum, trotzdem ist der Einfluss auch aus anderen Ländern bedeutend. Das Motto „Promoting the art and science of business continuity management worldwide" (BCI-About) sagt viel über die Arbeit der Organisation aus. BCM wird nicht nur als einfache wissenschaftliche Disziplin gesehen, sondern auch als Kunst. Wichtig ist den Mitgliedern, darüber hinaus der ethische Standard. Eigene ethische Richtlinien (BCI - Code of Ethics) müssen von allen Mitgliedern akzeptiert und praktiziert werden.

5.1.15 Vorlage/Querverbindungen zwischen den Guides

Der Good Practice Guide war ursprünglich die Vorlage des PAS 56. Als aus diesem in der Folge der BS 25999 hervorging, wurde auch der GPG neu strukturiert. Er orientiert sich in der derzeit aktuellen Fassung stark an den BS 25999 Standard. Die Struktur wurde vom BS 25999:1 übernommen. Wo immer es möglich ist, wurde ein Verweis auf die entsprechende Stelle im BS 25999 gesetzt. Dies ist vor allem durch die enge Vernetzung von BCI und BSI (=Organisation, welche hinter dem BS 25999 steht) zu erklären. Allerdings ist der GPG (im Gegensatz zum BS 25999) nicht ein rein britischer Standard, sondern wurde von Mitgliedern aus der ganzen Welt entwickelt. Er will die Good Practices weltweit zusammenfassen. Dadurch ergibt sich auch eine Querverbindung zu anderen Standards. Der GPG ist daher so geschrieben, dass er auch die wichtigsten Bereiche des NFPA1600 (Vereinigte Staaten von Amerika und Kanada), des HB221 und des APS 232 (beide Australien) sowie des FSA (Großbritannien) abdeckt. Auf keinen Fall aber soll der GPG als Ersatz für einen der oben genannten Standards gebraucht werden. Vielmehr soll er die Good Practices aus allen diesen Standards zusammenfassen. Der GPG gibt keine Garantie für eine volle Kompatibilität mit den genannten Guidelines, allerdings kann davon ausgegangen werden, dass in den grundlegenden Punkten ein hoher Übereinstimmungsgrad vorhanden ist (BCI GPG, 2010 S. 6-8, 10).

5.1.16 Zielgruppe

Die Zielgruppe des Good Practice-Guide ist relativ breit gefächert. Einerseits eignet er sich gut als Einführung für BCM-Anfänger, die sich mit diesem Thema vertraut machen wollen.

Er legt ausführlich die Methoden und Prozesse dar, beschreibt kontinuierlich den Zweck eines Vorganges und definiert Resultate der durchgeführten Vorgänge. Dadurch eignet er sich ebenfalls für Manager, die nicht direkt mit dem Business Continuity Management zu tun haben, sondern dessen Auswirkungen auf das Unternehmen auf die eine oder andere Art berücksichtigen müssen.

Andererseits eignet sich der GPG auch für fortgeschrittene Anwender. Er stellt prägnant die Kernpunkte des BCM dar. Wie der Name schon sagt, werden vor allem Good Practices, also praktische Anwendungsratschläge, gegeben, die sich bei vielen anderen Unternehmen beziehungsweise den Managern dieser Unternehmen schon als brauchbar herausgestellt haben (BCI GPG, 2010 S. 2).

5.1.17 Gegebene Templates

Der GPG hat selbst keine Templates welche die Erstellung von Dokumenten erleichtern. Es gibt allerdings (wie bereits unter 5.1.6 erwähnt) eine große Anzahl von Mitgliedern des BCI erstellten Templates. Diese sind allerdings ausschließlich von Mitgliedern zugänglich und daher kostenpflichtig.

5.1.18 Benötigte Ressourcen

Werden im GPG nicht berücksichtigt.

5.1.19 Integration von Organisationsprozessen

Der GPG bezieht Standards aus verschiedenen Ländern mit ein. Es werden daher die wichtigsten Punkte des NFPA 1600, des HB221, des APS232 und des FSA BCM Guide berücksichtigt. Ebenso werden Referenzen auf Record Management (Schriftgutverwaltung, ISO 15489) (BCI GPG, 2010 S. 14)] und Change Management (ITIL) gesetzt. Generell kann man sagen, dass der Good Practice-Guide versucht, so viele Prozesse wie möglich zu integrieren. Dass dabei nicht auf alle Aspekte geachtet werden kann, ist verständlich.

5.1.20 Benötigte Vorkenntnisse

Obwohl sich der Good Practice-Guide nicht als Werk für Anfänger im Bereich BCM sieht, kann er doch dafür herangezogen werden. Damit gelingt es Anfänger-Usern im Bereich BCM einen guten Überblick zu geben.

5.1.21 Methoden

Die Methoden im GPG sind weitgehend exakt beschrieben. Es werden zu jeder Methode durch den fixen Aufbau (siehe →5.1.24) eine Einleitung, die Vorbedingungen, der Sinn der Methode, die der Methode zugrundeliegenden Konzepte und Annahmen, der Prozesse, die Methode und dazugehörenden Techniken, den Output sowie eine Review Strategie dargelegt. Möglicherweise wird der User sich aufgrund der fehlenden Templates beziehungsweise fehlenden Beispielen bei manchen Methoden noch Unterstützung aus anderen Quellen suchen müssen. Allerdings gibt der GPG so die Informationen, dass gut mit ihm als alleiniges Instrument gearbeitet werden kann.

Durch den oben dargelegten Aufbau werden nicht nur die eigentlichen Methoden beschrieben, sondern auch die Vor- und Nachbedingungen, Auswirkungen und Begleiterscheinungen. Damit wird es dem Leser einfacher gemacht, sich die Einbettung der unter Umständen neuen Methoden in die Unternehmenslandschaft vorzustellen und die Integration des Business Continuity Managements in das Unternehmen besser durchzuführen.

5.1.22 Ausschließlich Maßnahmen zur Einführung von BCM oder auch Überprüfung und Weiterführung

Der GPG deckt alle Teile des Business Continuity Management Cycles ab. Es beginnt mit der BCM-Policy, dem Verstehen des Unternehmens, geht über BCM-Strategie und Implementierung bis hin zu Übungen und Einbettung in die Unternehmenskultur. Somit deckt dieser Standard alle gängigen Bereiche des BCM ab.

5.1.23 Ergänzendes Material

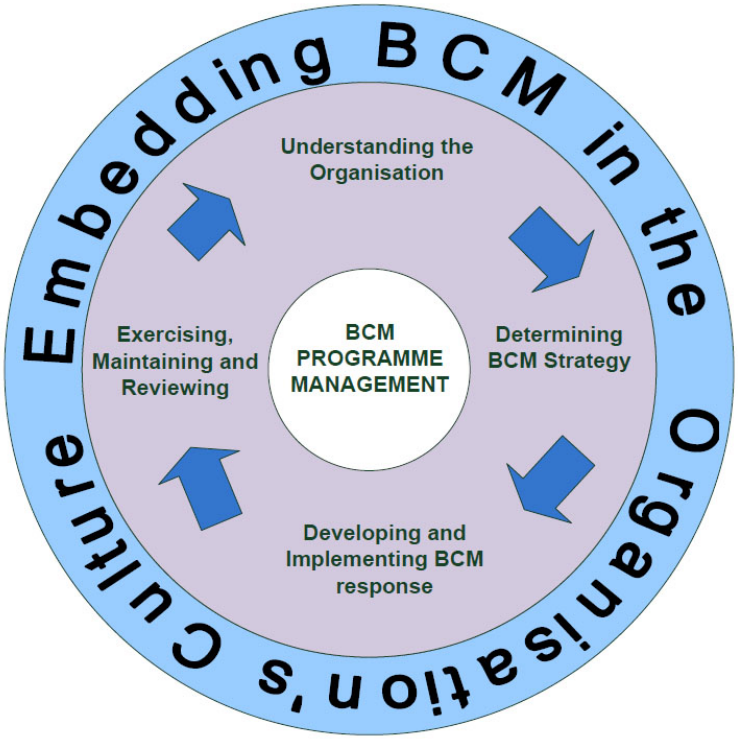

Abbildung 3 - (BCI GPG, 2010)

Das Business Continuity Institute bietet ein umfangreiches Angebot an zusätzlichen Materialien, die das Thema BCM behandeln. Sämtliche anschließend aufgeführten Teile sind kostenpflichtig. Einzige frei verfügbar ist ein Glossar (BCI - Glossary), in dem die am meisten relevanten Begriffe erklärt werden.

Einerseits gibt es einen eigenen Online-bookstore (BCI-Bookstore), in dem ausschließlich Bücher zu diesem Thema vorliegen.

Des Weiteren wird eine hohe Anzahl an verschiedenen Kursen, Trainings und Schulungen angeboten. Diese sind in unterschiedlichen Längen und zu verschiedenen Themen im Bereich BCM verfügbar. Diese Kurse sind weltweit verteilt, sodass regelmäßig ein Kurs zumindest

auf seinem eigenen Kontinent angeboten wird. Das BCI organisiert auch regelmäßige Symposien, an denen Teilnehmer der Organisation teilnehmen können um ihre Erfahrungen auszutauschen und neue Erkenntnisse zu gewinnen.

Ein umfangreicher E-Learning- Kurs (BCI - E-Learning) bietet zu allen sechs Kapiteln eine Lerneinheit an. Dieser ist auch darauf ausgelegt, eine Vorbereitung auf das BCI-Zertifikat zu sein. Dank Fragen in jeder Lerneinheit kann das eigene Wissen überprüfen werden. Ein einzelnes Kapitel kostet zurzeit EUR 178,-, alle sechs Kapiteln insgesamt EUR 570,- (BCI-E-Learning).

Im Shop des BCI werden Filme, DVDs und anderes visuelles Material zu angeboten, welches sich zur Weiterbildung im Bereich BCM einsetzen lässt. Die Homepage des BCI (BCI-Bookstore) gibt über alle Materialien einen brauchbaren Überblick und führt auch weitere Bücher und andere Informationen an, welche zu Themen im Bereich BCM sinnvoll sind.

5.1.24 Phasen

Der Good Practice-Guide besteht aus sechs Teilen, welche sich eng an den BS 25999 anlehnen. Jeder Hauptteil in einem Kapitel folgt demselben Aufbau. Als erstes steht eine Einleitung, in welcher der folgende Teil im Überblick beschrieben wird. Danach folgen die benötigten Vorbedingungen, und als dritter Punkt der Grund für diesen Schritt. Anschließend werden die Annahmen die getroffen werden müssen um den Schritt umzusetzen beschrieben. Im fünften Teil wird der Prozess selbst beschrieben. In der Folge werden die Methoden festgelegt, welche angewandt werden sollen, um diesen Schritt auszuführen. In Teil sieben wird besprochen, was der Output aus dem durchgeführten Schritt sein soll. Als letzter Punkt wird noch erörtert, wie ein Review der durchgeführten Aktivität auszusehen hat (zum Beispiel (BCI GPG, 2010 S. 5-9)).

Die sechs Teile, nach denen der GPG aufgebaut ist, sind (BCI GPG, 2010 S. 4):

<u>BCM Policy& Programme Management</u>

Dieser Teil beinhaltet eine Einleitung zum Thema Business Continuity Management. Darin wird erläutert, was BCM ist, wozu es dient, warum Unternehmen es benötigen und wie es mit anderen Disziplinen im Unternehmen zusammenhängt. Anschließend wird erklärt, wie der Guide aufgebaut ist und wie er angewendet werden soll. Abschließend folgen die beiden Punkte „BCM-Policy“ und „Programme Management“.

BCM Policy& Programme Management stellt die Grundlage dar, auf dem alle weiteren Teile aufgebaut sind. Es definiert die Grundlagen und ermöglicht dadurch einen sinnvollen Einsatz des weiteren Guides.

<u>Understanding the Organisation</u>

Dieser Teil beschäftigt sich mit dem grundlegen Verständnis des eigenen Unternehmens sowie der Erfassung der Eigenschaften des Unternehmens in weiter bearbeitbare Werte.

Zu diesem Zwecke wird zuerst die Business Impact Analysis durchgeführt. Dies ist ein Prozess, der die Auswirkung einer Betriebsunterbrechung über eine gewisse Zeit hinaus

berechnet. Danach wird die Continuity Recovery Requirements Analysis durchgeführt, die abschätzen soll, welche Ressourcen jede Aktivität bei der Wiederaufnahme benötigt. Abschließend soll ein Risk Assessment durchgeführt werden. In diesem Zuge soll die Wahrscheinlichkeit und die Auswirkungen von bekannten Gefahren berechnet werden.

Determining Business Continuity Strategy

In diesem Kapitel wird beschrieben, wie aufbauend auf der in den ersten beiden Kapiteln durchgeführten Analyse eine BC-Strategie festgelegt wird. Es soll eine entsprechende Strategie gewählt werden, sodass die Ziele, Verpflichtungen und Aufgabenbereiche kosteneffizient unterstützt werden. In diesem Kapitel soll darauf geachtet werden, mögliche Probleme im Vorhinein zu eliminieren oder zumindest deren Wahrscheinlichkeit zu verringern.

Dieses Kapitel besteht aus drei Teilen. Im ersten Kapitel wird eine high-level BC-Strategie festgelegt, um die Produkt- und Servicelieferfähigkeit zu erhalten. Im zweiten Teil wird die genaue Strategie für jede Aktivität beziehungsweise jeden Prozess bestimmt. Im letzten Schritt dieses Kapitels werden zu den erstellten BC-Aktivitäten die jeweiligen benötigten Ressourcen zugeordnet und ermittelt, wo diese herkommen und wie sie verwendet werden.

Developing & Implementing a BCM Response

Im vierten Teil des GPG werden die detaillierten Aktionen geplant, die als Antwort auf eine Unterbrechung der Geschäftsprozesse gesetzt werden müssen. Hier wird vor allem eine klare Vorgehensweise (Prozedur) festgelegt, weiters die Kommunikation mit den Stakeholdern gesucht sowie die genauen Pläne, um unterbrochene Aktivitäten wiederaufzunehmen, festgelegt. Da jede Störung andersartig ist, sind flexible Pläne zu erstellt. In jeden Fall ist es wichtig, dass sich diese Pläne an die Unternehmenskultur anpassen.

Das Kapitel Developing & Implementing a BCM Response gliedert sich in vier Teile: Zuerst soll eine Struktur erstellt werden, wer wann auf welche Probleme wie reagiert. Damit soll zwischen strategischen, taktischen und operativen Maßnahmen unterschieden werden und festgelegt werden, in welchem Zeitraum welche dieser Maßnahmen getroffen werden muss. Im zweiten Teil wird ein Incident Management Plan erstellt. Dabei handelt es sich um grundlegende Pläne, um im Falle eines Problems möglichst rasch reagieren zu können. Auch die dafür zuständigen Personen sollen festgelegt werden. Anschließend wird der BC-Plan erstellt. Dieser Plan soll die Reaktion des gesamten Unternehmens auf eine Störung zusammenfassen. Die Stellen, die diesen Plan ausführen, sollen in der Lage sein, die Informationen, die sie über die Auswirkungen der Störung bekommen, zu analysieren und die geeigneten Strategien zu ergreifen. Inhalt und Bestandteile des Planes werden von Unternehmen zu Unternehmen verschieden sein.

Der letzte Teil bezieht sich vor allem auf mittlere und größere Unternehmen. Sollte der BC-Plan zu umfangreich und kompliziert werden, sollen die Maßnahmen auf der operativen Ebene ausgegliedert werden. Je nach Unternehmen können dabei ein oder mehrere Pläne erstellt werden.

Exercising, Maintaining & Reviewing BCM Arrangements

In diesem Kapitel soll sichergestellt werden, dass die zuvor festgelegten Strategien, Pläne und Verpflichtungen eingehalten werden. Dazu werden ein Übungsplan sowie Reviews und Aktualisierungspläne erstellt. Diese drei Punkte werden ausführlicher erläutert.

Als Erstes wird das Übungsprogramm erklärt, welches erstellt werden soll. Dieses soll von der Struktur her einfach beginnen und immer komplexer werden. Hier wird auch auf Probleme, die sich durch Outsourcing ergeben eingegangen. Dieses Programm soll möglichst alle Bereiche abdecken. Anschließend sollen die erarbeiteten Maßnahmen in praktische Übung umgesetzt werden. Damit wird sichergestellt, dass das Unternehmen jederzeit auf Eventualitäten vorbereitet ist. Um die Übungen effizient zu gestalten, sollen diese soweit wie möglich in die üblichen Unternehmensprozesse eingegliedert werden. Als weiterer Arbeitsschritt soll dann das Review erfolgen, wobei dieses wiederum aus internen und externen Audit sowie einer Selbsteinschätzung besteht. Bei diesen Audits soll die Ist-Situation im Unternehmen gegen vordefinierte Standards verglichen werden. Allerdings muss darauf geachtet werden, dass sich Standards entwickeln und es für den Erfolg nicht wesentlich ist, dass ein Standard korrekt umgesetzt wurde, sondern dass die Prozesse insgesamt ordnungsgemäß umgesetzt werden.

Embedding BCM in the Organisation’s Culture

Um Business Continuity Management erfolgreich durchführen zu können, muss dieses als selbstverständlich akzeptiert und als Teil der normalen Routine durchgeführt werden. Dadurch werden BC-Maßnahmen effizienter, das Vertrauen der Stakeholder in BCM wird größer und die Auswirkungen von Betriebsstörungen werden verringert. Dafür schlägt der GPG drei Schritte vor:

Als Erstes soll ermittelt werden, wie hoch das Bewusstsein für BCM in einem Unternehmen zurzeit ist. Ebenso soll in diesem Schritt ermittelt werden, wie hoch dieses Bewusstsein werden soll und wie dies gemessen werden kann. Danach soll das Bewusstsein für BCM geprägt werden. Dazu werden die drei Arten Training (in spezifischen BCM-Fähigkeiten), Erziehung (in allgemeine BCM-Fragen) und Bewusstsein (Wissen über spezielle BCM-Probleme) herangezogen. Als letzten Punkt führt der GPG noch an, dass dieser Wandel in der Unternehmenskultur überwacht werden muss. Des Weiteren soll diese Bewusstseinsschaffung auch nicht als einmalige Aufgabe verstanden werden, sondern als fortlaufende, periodische Angelegenheit, welche einen gewissen Aufwand benötigt, um erfolgreich zu sein.

5.1.25 Beratung & Support

Das Business Continuity Institute bietet keinen direkten Support an, sondern lediglich Schulungen und Trainings. Diese helfen nicht bei Problemen, die kurzfristig gelöst werden müssen, sondern bieten langfristige Informationen.

Beratung und Support im eigentlichen Sinn kann das BCI insofern auch schwer bieten, als dass es sich seine Experten und Trainer zumeist selbst aus der Privatwirtschaft rekrutiert, und diese daher der Organisation nicht immer zur Verfügung stehen.

5.1.26 Befolgung der Richtlinien der Aufsichtsbehörden

Der GPG befolgt keine Richtlinie von Aufsichtsbehörden jeglicher Art. Dies kann durch zwei Gründe erklärt werden:

Einerseits wurde der Standard von Experten aus der ganzen Welt erstellt und ist daher international. Da Aufsichtsbehörden im Normalfall regional eingeschränkt sind, ist es nicht möglich, Richtlinien einzuhalten. Es kann sein, dass gewisse Gesetze in gewissen Ländern mit diesem Standard erfüllt werden, aber der User sollte sich nicht darauf verlassen und jeweils die lokalen Gesetze überprüfen.

Der zweite Grund ist die Allgemeinheit des Standards. Dadurch dass keine Branche ausgeschlossen wird und der Standard allgemein gültig sein soll, können auch die Richtlinien der Aufsichtsbehörden von einzelnen Branchen nicht berücksichtigt werden. Eine solche Aufsichtsbehörde ist beispielsweise die Bankenaufsicht eines Landes.

5.1.27 Befolgung von internationalen IT-Standards

Der Good Practice-Guide ist nicht darauf ausgelegt internationalen IT-Standards zu folgen. Da der Standard praxisnahe ist und von Experten erstellt wurde, die in Unternehmen sich damit befassen, kann davon ausgegangen werden, dass er einigen IT-Standards entspricht. Es wird jedoch von den Autoren des Guides ausdrücklich darauf hingewiesen, dass es keine Garantie gibt, dass er einen dieser Standards voll inhaltlich und formal unterstützt (BCI GPG, 2010 S. 8).

5.2 BSI 100-4

5.2.1 Sprache

Der BSI 100-4 ist in deutscher Sprache erhältlich. Sowohl die Buchform als auch das freie PDF (siehe →5.2.4) sind in dieser Sprache verfügbar. Eine englische Übersetzung liegt inzwischen auch vor (BSI 100-4 english). Darüber hinaus sind keine weiteren Sprachen verfügbar.

5.2.2 Ort der Entstehung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist in Deutschland angesiedelt, mit dem Hauptsitz in Bonn. Daher besteht eine starke Affinität zu der Region Deutschland. Einerseits ist der BSI 100-4 der einzige weit verbreitete Standard in diesem Bereich im deutschen Sprachraum, andererseits ist die Organisation stark an deutsches Recht und an deutsche Gegebenheiten gebunden.

5.2.3 Zeit der Entstehung

Die aktuelle Version wurde im November 2008 fertiggestellt und im Februar 2009 in Buchform herausgegeben. Im Rahmen der CeBIT2009 (März 2009) erfolgte die offizielle Vorstellung, anschließend daran war auch die frei verfügbare Variante im PDF-Format auf der Homepage des BSI zu finden. Dies ist die erste Version dieses Standards (BSI-Standard 100-4, 2008 S. 1).

5.2.4 Verfügbarkeit

Der BSI 100-4 ist in Buchform sowie digitaler Form erhältlich. Die digitale Form wird gratis auf der Homepage des BSI zur Verfügung gestellt. (BSI-IT-Grundschutz-Standards). Die Buchform ist im allgemeinen Buchhandel erhältlich und kostet EUR 39,80 (Online Buchhändler Amazon.de, Stand: 8. Juni 2009).

5.2.5 Art

Der BSI 100-4 ist ausführlich und textuell beschrieben. Auf 123 Seiten werden sämtliche Vorgänge ausführlich beschrieben. Zahlreiche Tabellen, Bilder und Diagramme helfen zum leichteren Verständnis. Die Vorgänge sind ausführlich und leicht verständlich beschrieben.

5.2.6 Vorhandene Tools zur Unterstützung

Der BSI 100-4 hat zwar keine Tools, welche die Umsetzung des Standards erleichtern, doch ist dem Thema ein eigenes Kapitel gewidmet. In diesem wird beschrieben, was die Tools können müssen. Es werden die Eigenschaften von guten Tools erläutert, ohne spezielle Tools zu erwähnen. Damit kann sich jedes Unternehmen die Tools, die am besten passen zusammenstellen und hat dennoch eine Anleitung (BSI-Standard 100-4, 2008 S. 98-99).

5.2.7 Allgemein/branchenspezifisch

Der BSI-Standard ist unabhängig von allen Branchen erstellt worden, und lässt sich damit allgemein anwenden. Dies erklärt sich vor allem dadurch, dass er von einer staatlichen Organisation erstellt wurde (BSI-Standard 100-4, 2008 S. 2).

5.2.8 Unternehmensgröße

Prinzipiell ist der Standard so geschrieben, dass er von Unternehmen beliebiger Größe verwendet werden kann. Es wird jedoch explizit darauf hingewiesen, dass einige der Maßnahmen ausschließlich für große Unternehmen sinnvoll sind. Bei Klein- und Mittelbetrieben können manche der Maßnahmen weggelassen werden, was das einzelne Unternehmen für sich entscheiden muss (BSI-Standard 100-4, 2008 S. 2).

5.2.9 Art der Verfügbarkeit

Der BSI 100-4 wird in zwei Versionen angeboten: Einerseits wird er im Fachbuchhandel als Buch vertrieben. Der vollständige Name lautet „Notfallmanagement: BSI-Standard 100-4 zur Business Continuity (Broschiert)“, der Verlag ist „Bundesanzeiger“, ISBN-10 3898176932 beziehungsweise ISBN-13 978-3898176934. Der Preis beträgt EUR 39,80 (Online Buchhändler Amazon.de, Stand: 8. Juni 2009).

Ebenfalls verfügbar ist der BSI 100-4 im Internet, und zwar auf der Homepage des BSI im Dateiformat PDF.

5.2.10 Möglichkeiten zur Zertifizierung

Beim BSI kann ein Unternehmen sich nach dem ISO Standard ISO 27001 zertifizieren lassen. Zu diesem Vorgang wird nicht nur der BSI 100-4 herangezogen, sondern auch alle anderen Teile der BSI 100 Reihe (BSI-Zertifizierungsstandard). Damit wird allgemein die IT eines Unternehmens zertifiziert. Auch eine Zertifizierung einer Person ist möglich, diese ist dann berechtigt selbst das Zertifizierungsverfahren für ein Unternehmen durchzuführen. Eine eigene BSI-Zertifizierung für BSI 100-4 konnte aufgrund der Recherche nicht gefunden werden.

Der Zertifizierungsprozess für ein Unternehmen ist in drei Teile gegliedert. Jeder dieser Schritte beinhaltet bestimmte Kriterien, die ein Unternehmen erfüllen muss. Als Grundlage für alle weiteren Schritte dient die Einstiegsstufe. Hier können Unternehmen bereits ihren Willen demonstrieren und ihren Kunden zeigen, dass sie auf dem Weg zu einem ISO-Standard sind. Danach folgt die Aufbaustufe, welche einen weiteren Schritt in Richtung Zertifizierung zeigt. Der nächste Schritt ist dann die vollkommene ISO-Zertifizierung. Einzelne Schritte können ausgelassen werden, doch stellt das Absolvieren dieser drei Schritte den einfachsten Weg zur Zertifizierung dar.

5.2.11 Rechtliche Begrenzungen

Durch die allgemein und branchenunabhängige Formulierung im BSI 100-4 können keine rechtlichen Begrenzungen festgestellt werden. Auch die Fokussierung auf Deutschland zeigt keine rechtlichen Einschränkungen. Es wird allerdings auf andere Gesetze verwiesen, welche für die Umsetzung relevant sein könnten. Trotz allem muss darauf geachtet werden, dass kein geltendes Recht verletzt wird, da die Autoren darauf hinweisen, dass es immer zu rechtlichen Problemen kommen kann (BSI-Standard 100-4, 2008 S. 16).

5.2.12 Flexibilität

Prinzipiell kann der BSI 100-4 als flexibel bezeichnet werden. Er gibt in zahlreichen Bereichen Methoden vor. Zumeist ist es möglich, diese an das Unternehmen anzupassen oder auch gewisse Teile wegzulassen. Daneben gibt es Bereiche, in denen der Standard ein starres, verpflichtendes Schema vorgibt, welches einzuhalten ist. Alternative Wege werden zwar nicht angegeben, es wird jedoch darauf hingewiesen, dass der beschriebene Weg oft nicht der einzig Richtige ist.

5.2.13 Organisatorisch/kulturell

Es konnten keine Eingriffe in die Unternehmenskultur festgestellt werden welche über das normale Maß der Veränderung bei der Implementierung eines neuen Managementsystems hinausgehen. Auch wenn die Änderungen von Unternehmen zu Unternehmen verschieden sind, kann generell gesagt werden, dass die Eingriffe nicht tiefgehend sind.

5.2.14 Welche Organisation steht dahinter?

Das im Januar 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der zentrale IT-Sicherheitsdienstleister des Bundes in Deutschland (BSI-Leitbild). Es ist ein dem Ministerium für Inneres unterstelltes Bundesamt, welches sich primär mit IT-

Sicherheitsfragen beschäftigt. Es hat zum Ziel, die Informations- und Kommunikationstechnik sicher zu machen. Seine Aufgabe gliedert sich in vier Bereiche: 1) Information, 2) Beratung, 3) Entwicklung und 4) Zertifizierung. Mit etwa 500 Mitarbeitern aus den Bereichen Informatik, Physik, Mathematik und auch anderen Wissenssparten verfügt das in Bonn ansässige Amt über umfangreiche Ressourcen.

5.2.15 Vorlage/Querverbindungen zwischen den Guides

Der BSI 100-4 baut hauptsächlich auf seinen Vorgängern 100 -1, 100-2 und 100-3 auf, welche ihm als Grundlage dienen. Allerdings beschreibt er jeweils ein eigenständiges Managementsystem für die Geschäftsfortführung und die Notfallbewältigung.

Der BSI zitiert zahlreiche andere Standards aus der ganzen Welt. Da der der erste deutschsprachige Standard ist, nimmt er sich Standards aus anderen Ländern als Vorbild. Dazu zählen unter anderem die britischen Standards BS 25999 und GPG, der australische HB221, die amerikanischen Standards NFPA1600 und PAS77 sowie diverse ISO-Standards wie ISO 22399 und ISO 27001 (BSI-Standard 100-4, 2008 S. 4-9).

5.2.16 Zielgruppe

Der BSI richtet sich an alle Notfall- bzw. Business Continuity Manager, Krisenstabsmitglieder, Sicherheitsverantwortliche, -beauftragte, -experten und -berater, die mit dem Management von Notfällen und Krisen technischen und nicht-technischen Ursprungs betraut sind. Alle die den BSI 100-4 anwenden wollen, sollten mit den Grundlagen der BSI-Standards 100-1, 100-2 und 100-3 vertraut sein. (BSI-Standard 100-4, 2008 S. 2)

5.2.17 Gegebene Templates

Im Anhang des BSO 100-4 sind zwei Templates gegeben. Einerseits ist ein Leitfaden zur Erstellung eines Notfallhandbuchs verfasst (BSI-Standard 100-4, 2008 S. 113-114). Andererseits wird gezeigt wie ein Geschäftsfortführungsplan aussehen kann (BSI-Standard 100-4, 2008 S. 115-116). Beide Pläne sind als Gliederung gegeben und stellen beispielhafte Inhaltsverzeichnisse dar, die an das jeweilige Unternehmen angepasst werden müssen.

5.2.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.2.19 Integration von Organisationsprozessen

Der BSI 100-4 Standard orientiert sich allgemein an seinen Vorgängern mehr als an anderen Organisationsprozessen. So werden vor allem Prozesse unterstützt, die im BSI 100-2 Standard definiert werden. Der Anwender findet einzelne Hinweise auf andere Prozesse, wie Organisational Risk Management oder Configuration Management, allerdings sind diese Hinweise am Rand erwähnt und garantieren keine Sicherheit zur Kompatibilität (BSI-Standard 100-2, 2008).

5.2.20 Benötigte Vorkenntnisse

Um den vollen Umfang des BSI 100-4 verstehen zu können ist es empfehlenswert, zumindest den BSI Standard 100-2 erarbeitet zu haben. Dies erklärt sich vor allem durch die starke Abhängigkeit der beiden Werke. Der BSI 100-4 Standard ist ohne ein Unternehmen, welches ein Managementsystem nach BSI 100-2 hat nicht einführbar. Sollte das Unternehmen bereits nach diesem Standard ausgerichtet sein, fällt es umso leichter, den BSI 100-4 Standard einzuführen, da gewisse Synergieeffekte erreicht werden können. Eine nähere Beschäftigung mit den beiden anderen verwandten BSI-Standards (BSI 100-1 und 100-3) ist empfehlenswert, aber nicht unbedingt erforderlich (BSI-Standard 100-4, 2008 S. 2,4).

Abseits der Kenntnis dieses Standards ist kein weiteres Vorwissen erforderlich. Aufgrund der ausführlichen Beschreibung der Methoden (siehe →5.2.21) ist kein Wissen zu den verschiedenen angewandten Methoden notwendig.

5.2.21 Methoden

Die Methoden im BSI 100-4 Standard sind ausführlich beschrieben. Zu jedem erforderlichen Schritt ist eine ausführliche textuelle Beschreibung mit Informationen, Vorgehensweisen, Ratschlägen und Hintergrundinformationen vorhanden. Zusätzlich werden Vorgänge mit grafischen Hilfsmitteln, wie Diagrammen und Bildern, unterstützt. Oft gibt es auch beispielhafte Darstellungen von Ergebnissen. Hiermit soll dem Anwender die Darstellung der Ergebnisse erleichtert beziehungsweise ihm eine Hilfestellung bei der Durchführung der Operation gegeben werden. Diese sind zumeist tabellarisch und zeigen mögliche Kategorien oder Ergebnisse.

5.2.22 Ausschließlich Maßnahmen zur Einführung von BCM oder auch Überprüfung und Weiterführung

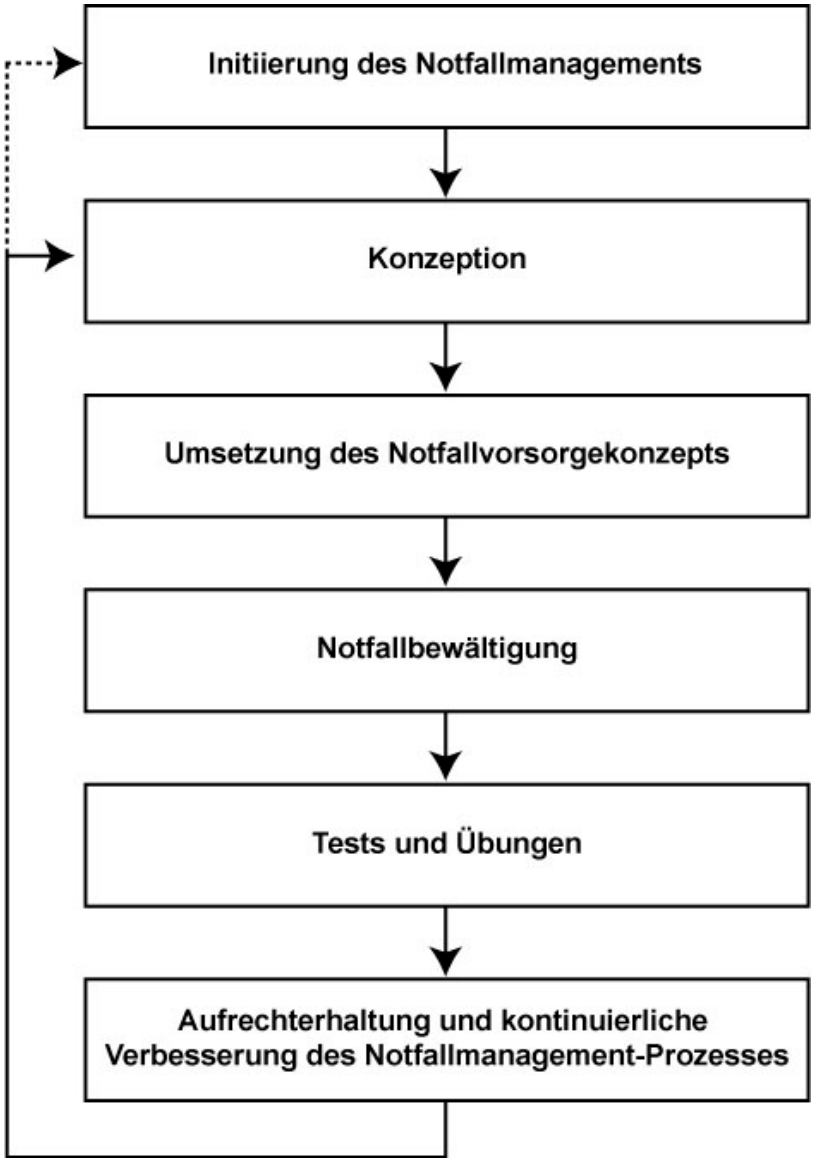

Abbildung 4 - (BSI-Standard 100-4, 2008)

Der BSI 100-4 Standards deckt sämtliche üblichen Teile des BCM-Cycles ab. Er beginnt mit einer allgemeinen Erklärung und Einführung zum Thema BCM, geht weiter von der Initialisierung des Prozesses über die Durchführung bis hin zur stetigen Überprüfung der Umsetzung. Auch das Training der Maßnahmen wird miteinbezogen.

5.2.23 Ergänzendes Material

Da der BSI 100-4 zurzeit ein neuer Standard ist, ist noch wenig zusätzliches Material verfügbar. Das Bundesamt für Sicherheit in der Informationstechnik selber gibt kein zusätzliches Material heraus welches sich direkt und ausschließlich auf diesen Standard konzentriert. Einzig die vorangegangenen Standards BSI 100-1, 100-2 und 100-3 stehen als Material zur Ergänzung zur Verfügung. In diesem Rahmen muss vor allem der BSI 100-2

besonders hervorgehoben werden, da dieser eine Voraussetzung zum Verständnis des BSI 100-4 ist (BSI-Standard 100-1, 2008) (BSI-Standard 100-2, 2008) (BSI-Standard 100-3, 2008).

5.2.24 Phasen

Der BSI 100-4 Standard ist in zwölf Kapitel gegliedert, wobei jedes dieser Kapitel einen Schritt in der Einführung eine Business Continuity Managements in einem Unternehmen beschreibt. Der fortlaufende Text wird durch Grafiken und Tabellen aufgelockert. Die Unterkapitel sind zumeist kurz und die Überschriften beschreiben bereits anschaulich worin es im Folgenden geht.

Kapitel 1 ist die Einleitung. Hier wird Allgemeines wie Literaturverzeichnis, Anwendungshinweise oder Adressatenkreis besprochen. Das darauf folgende zweite Kapitel beschreibt die fachbezogenen, allgemeinen Elemente des Standards. Dazu gehören unter anderem eine Begriffserklärung und die Auflistung anderer relevanter Standards. Im dritten Kapitel wird schließlich der Aufbau des BCM in diesem Dokument erläutert und ein Überblick über die folgenden Kapiteln gegeben. Darüber hinaus werden die empfohlene Dokumentation sowie der Schutz dieser Dokumentation erläutert.

In Kapitel vier wird der eigentliche BCM-Prozess gestartet beziehungsweise der Notfallmanagementprozess initiiert. Dies geschieht vorerst durch die Bestimmung eines Verantwortlichen. Danach wird der komplette Prozess konzeptioniert und geplant werden, wozu unter anderem das Festlegen der Zielsetzung und Anforderungen sowie des Geltungsbereiches zählen. Danach müssen die organisatorischen Voraussetzungen geschaffen werden. Dabei werden vor allem Rollen verteilt, aber auch die Kommunikationswege festgelegt. Nun wird eine Leitlinie erstellt und bekannt gemacht, in der alle diese Maßnahmen festgehalten werden. Nun müssen die benötigten Ressourcen freigemacht werden. Abschließend sind alle Mitarbeiter einzubinden, damit ein Bewusstsein für Notfallmaßnahmen geschaffen werden kann.

Im anschließenden fünften Kapitel wird das Konzept und daher als aller Erstels eine Business Impact-Analyse erstellt. Dies wird ausführlich mit Grafiken und Tabellen sowie einigen Beispielen erläutert. Der nächste Schritt, die Risikoanalyse, ist optional, da sie in mehreren Fällen schon durch andere Maßnahmen abgedeckt ist. Nun kann basierend auf der Business Impact-Analyse der Ist-Zustand erfasst werden. Ist dies geschehen, können Kontinuitätsstrategien erarbeitet werden, wozu eine Kosten-Nutzen-Analyse ausgeführt wird. Als Grundlage für die weiteren Schritte wird nun aus den gewonnenen Daten ein Notfallvorsorgekonzept erstellt, und daher vor allem das Vorgehensmodell und die Vorsorgemaßnahmen definiert.

Im sechsten Kapitel wird das Notfallvorsorgekonzept möglichst effizient geplant, durchgeführt, begleitet und überwacht. Als Erstes wird eine Kosten- und Aufwandschätzung vorgenommen, danach wird entschieden in welcher Reihenfolge die Maßnahmen umgesetzt werden. Gleichzeitig wird zusätzlich die Verantwortung der einzelnen Aufgaben festgelegt. Schlussendlich werden dann noch realisierungsbegleitende Maßnahmen definiert.

Im umfangreichen siebten Kapitel wird das Thema Notfallbewältigung und Krisenmanagement behandelt. Hier wird erklärt, welche Maßnahmen zu setzen sind, wenn trotz aller Vorsichtsmaßnahmen ein Notfall eintritt. Es wird ein allgemeiner Ablauf, von der Meldung des Notfalles über Sofortmaßnahmen, Kompetenzverteilung, Wiederanlauf, Nacharbeiten bis hin zu nachträglicher Analyse und Dokumentation, erklärt. Nach einer kurzen psychologischen Analyse von Arbeiten in Krisen wird auf den Punkt Kommunikation eingegangen. Sowohl für die interne als auch für die externe Kommunikation werden Ratschläge gegeben. Das Kapitel abschließend wird das Notfallhandbuch erklärt. Sowohl sein Zweck wie auch der benötigte Inhalt werden ausgeführt.

Das achte Kapitel beschäftigt sich mit Tests und Übungen. Damit soll sichergestellt werden, dass ein Unternehmen nicht nur ein perfektes theoretisches Konzept hat, sondern dieses auch praktisch umsetzen kann. Damit soll Routine geschaffen und der in Krisensituationen immer auftretende Stress damit reduziert werden. Es werden zuerst verschiedene Arten beschrieben, wie geübt werden kann. Anschließend wird festgelegt, welche Dokumente, sowohl Planungsdokumente als auch Pläne für den Notfall, benötigt werden. Abschließend wird erklärt, wie diese Übungen und Tests am besten realisiert werden..

Kapitel neun beschäftigt sich mit der Aufrechterhaltung und kontinuierlichen Verbesserung von Notfallmaßnahmen. Zuerst wird die Aufrechterhaltung der vorhandenen Maßnahmen besprochen. Kriterien werden festgelegt, nach denen ein gutes BCM auf längere Zeit hin gemessen werden kann, wozu verschiedene Überprüfungen vorgestellt werden. Abschließend wird das wichtige Kapitel Informationsfluss und Managementbewertung behandelt. Dies dient vor allem dazu, das Management permanent einzubinden und am aktuellen Stand zu halten.

Das zehnte Kapitel behandelt den Zusammenhang von Outsourcing und Notfallmanagement. Eingegangen wird einerseits auf die rechtlichen Aspekte, auf das Abschließen von Verträgen, andererseits auch auf das interne Planen von Maßnahmen im Falle eines Notfalls bei Inanspruchnahme von externen Betrieben.

Kapitel elf behandelt das Thema Tools, indem erläutert wird, wie verschiedene, vor allem elektronische, Werkzeuge zur effizienteren Planung und Umsetzung von Maßnahmen genutzt werden können. Dabei werden zwar keine definitiven Tools genannt, doch werden eine Reihe von Kriterien aufgelistet die ein gutes Tool ausmachen (siehe Kapitel 5.2.6).

Das zwölfte Kapitel ist ein Glossar, in welchen die wichtigsten Begriffe zu diesem Thema erklärt werden.

Im Anschluss stehen vier Anhänge zur Verfügung. Im ersten werden Strategieoptionen erläutert, verschiedene Ressourcen werden genannt und die dazugehörige optimale Nutzung. Anhang B listet präventive Maßnahmen auf, die ein Unternehmen ergreifen kann. Anhang C beschreibt eine beispielhafte Gliederung eines Notfallhandbuches, während der letzte Anhang die Gliederung eines Geschäftsfortführungsplans vorstellt (BSI-Standard 100-4, 2008).

5.2.25 Beratung& Support

Das Bundesamt für Sicherheit in der Informationstechnik bietet als Herausgeber keinen Support an. Lediglich private Anbieter welche Experten auf diesem Gebiet sind werden aufgeführt.

5.2.26 Befolgung der Richtlinien der Aufsichtsbehörden

Der Standard wurde vom deutschen Bundesamt für Sicherheit in der Informationstechnik erstellt, einer staatlichen Behörde. Daher kann davon ausgegangen werden, dass in Deutschland selbst sämtliche Richtlinien erfüllt werden. Darüber hinaus werden wenige Aspekte garantiert. Allerdings sollte im deutschsprachigen Raum davon ausgegangen werden können, dass die meisten Kriterien, die eine Aufsichtsbehörde stellt erfüllt werden. Trotzdem sollte weder in Deutschland noch in anderen Ländern sicher davon ausgegangen werden.

5.2.27 Befolgung von internationalen IT-Standards

Der BSI 100-4 entspricht dem hauseigenen BSI 100-1 (Managementsysteme für Informationssicherheit) und damit auch ISO 27001 und ISO 27002. Zusätzlich entspricht er dem ebenfalls im selben Amt erstellten IT-Sicherheitshandbuch. Dieses ist zwar auch auf Deutschland zentriert, kann aber durchaus mit ähnlichen Werken in anderen Ländern verglichen werden (BSI-Standard 100-4, 2008 S. 4-9).

5.3 BS 25999

5.3.1 Sprache

Der BS 25999-Standard ist in Englisch verfasst. Dies ergibt sich daher, dass die Organisation, welche ihn verfasst, eine britische Organisation ist. Weiters gibt es auch Übersetzungen für den deutschsprachigen sowie spanischsprachigen Raum (BSI-Shop).

5.3.2 Ort der Entstehung

Die British Standards Institution ist die Organisation, welche in Großbritannien die Standards festlegt. Auch wenn sich diese Organisation inzwischen auch international betätigt und Großbritannien in allen weltweiten Standardisierungsorganisationen vertritt, so ist sie immer auch ein Teil der britischen Administration und somit dort verantwortlich. Dadurch ist eine eindeutige Orientierung an Großbritannien vorhanden.

5.3.3 Zeit der Entstehung

Da der BS 25999 in zwei Teile geteilt ist, müssen zwei verschiedene Entwicklungszyklen betrachtet werden. Der erste Teil (BS 25999-1:2006) ist zeitlich früher entstanden und wurde im Dezember 2006 publiziert. Er ging aus dem PAS56, der von derselben Organisation verfasst wurde, hervor und ersetzte diesen. Der zweite Teil (BS 25999-2:2007) wurde dann ein Jahr später herausgegeben (November 2007). Beide Teile sind bis heute (Stand Juli 2009)

in ihrer ursprünglichen Fassung aktuell. Aktualisierungen wurden keine herausgegeben (BS25999-2 Specification, 2007 S. ii).

5.3.4 Verfügbarkeit

Der BS 25999 ist nicht frei verfügbar. Er kann zwar auf der Homepage des BSI heruntergeladen werden, allerdings gegen eine Gebühr. Jeder Teil kostet 100 Pfund (ca. EUR 115) und beide Teile können unabhängig voneinander gekauft werden. Eine Preisreduktion um 50 % ist für Mitglieder des BSI möglich. In diesem Fall kostet ein Teil 50 Pfund (ca. EUR 57, Stand Juli 2009).

5.3.5 Art

Der BS 25999 ist eher listenartig aufgebaut. Im Code of Practice (BS 25999-1) werden die einzelnen Punkte relativ ausführlich beschrieben. Oft sind auch Kommentare zu einzelnen Punkten verfügbar, welche zusätzliche Informationen oder Hilfestellungen bieten. Einige Grafiken und Tabellen sind zusätzlich vorhanden. Die Unterpunkte sind oft verschachtelt, sodass es bis zu vier Unterpunkte geben kann.

Der zweite Teil ist noch stärker listenartig aufgebaut und oft einzelne Punkte aneinander gereiht. Auch hier sind oft viele Punkte in einander verschachtelt. Interessant ist, dass am Anfang jedes größeren Teils eine Kurzbeschreibung mit dem Zweck dieses Teiles steht, was einen Überblick gibt.

5.3.6 Vorhandene Tools zur Unterstützung

Auf der Homepage des BSI stehen verschiedene Tools zur Verfügung. Diese sind allerdings nicht ausschließlich auf den BS 25999 beschränkt, sondern sind auch für andere Standards geeignet oder sogar gedacht. Besonders ist das BSI BS 25999-2 „Business Continuity Self-assessment online toolkit“ (BSI Self-assessment Online), mit welchem sich ein Unternehmen online bewerten kann. Dieser Toolkit beinhaltet verschiedenste Tools aus allen Bereichen, die bei der Umsetzung eine Business Continuity Managements nützlich sein können.

5.3.7 Allgemein/branchenspezifisch

Das BSI als britische Standardisierungsbehörde versucht ein allgemeines Standardisierungswerk zu schaffen. Es ist darauf ausgelegt für alle Branchen zu gelten. Daher sind keine speziellen Teile vorhanden die sich auf eine bestimmte Branche anwenden lassen (BS25999-1 Code of Practice, 2006 S. 1) (BS25999-2 Specification, 2007 S. ii).

5.3.8 Unternehmensgröße

Die Unternehmensgröße ist bei diesem Standard nicht näher spezifiziert. Alle Unternehmensgrößen, vom Kleinbetrieb bis zum multinationalen Konzern, sollen abgedeckt werden. Daher soll jedes Unternehmen, das einen Prozess ausführt und diesen absichern will, angesprochen werden (BS25999-1 Code of Practice, 2006 S. 1) (BS25999-2 Specification, 2007 S. ii).

5.3.9 Art der Verfügbarkeit

Der BS 25999 steht sowohl in Buchform als auch im digitalen Format PDF zur Verfügung. Die Kosten sind für beide Formate gleich (siehe 5.2.4). Jeder der beiden Teile des BS 25999 (Code of Practice und Specification) muss separat bezogen werden. Die beiden werden komplett unabhängig voneinander, sowohl in Buchform als auch im digitalen Format, angeboten.

5.3.10 Möglichkeiten zur Zertifizierung

Der BS 25999 besteht aus zwei Teilen. Der erste Teil, Code of Practice, beschreibt Ansätze, um ein erfolgreiches BCM durchführen zu können. Dabei werden auch auf allgemein übliche Praktiken eingegangen, wobei eine objektive Bewertung kaum zu finden ist. Dadurch kann für den ersten Teil des BS 25999 keine Zertifizierung angeboten werden.

Der zweite Teil, die Spezifikation, aber wurde von vornherein so konzipiert, dass er eine Zertifizierung zulässt. Dazu werden nur solche Teile aufgenommen, welche objektiv bewertet werden können. Dadurch wird ein kleinerer Bereich des BCM abgedeckt, dieser ist dann allerdings zertifizierbar.

Im zweiten Teil können ausschließlich Organisationen zertifiziert werden (BS25999-Zertifizierung). Eine Zertifizierung für Einzelpersonen ist nicht vorgesehen (BS25999-2 Specification, 2007 S. ii).

5.3.11 Rechtliche Begrenzungen

Der Code of Practice (Teil 1) gibt lediglich allgemeine Ratschläge und Hilfen zur Vorgehensweise. Daher sind in diesem Teil keine rechtliche Begrenzungen oder Einschränkungen zu finden.

In der Spezifikation sind die Hinweise in Bezug auf die Standardisierung und Zertifizierung wesentlich genauer. Allerdings sind trotzdem keine Einschränkungen hinsichtlich gesetzlicher Grenzen zu finden. Dies erklärt sich sicher auch durch die allgemein gehaltene Form der Guideline.

5.3.12 Flexibilität

Beide Teile des BS 25999 folgen einem starren Aufbau. Auch der Ablauf der Aktionen ist eher starr. Vor allem im zweiten Teil (Spezifikation) wird ein fester Ablauf vorgeschrieben. Flexibilität ist hier eher nicht vorhanden. Manche Bereiche aus dem ersten Teil sind hier etwas flexibler und können zum Teil weggelassen und zum Teil verändert werden. Im zweiten Teil aber ist, wie bei einer Spezifikation eher üblich, ein minimales, dafür aber starres Grundgerüst erstellt worden.

5.3.13 Organisatorisch/kulturell

In keinem der beiden Teile des BS 25999 Standards können besondere Anforderungen an die Strukturänderung eines Unternehmens gefunden werden. Die Änderungen, die vorgenommen werden sollen, erscheinen weder unmäßig noch für ein normales Unternehmen nicht

durchführbar. Dass es in einzelnen Fällen zu Problemen kommen kann, ist zwar deswegen nicht auszuschließen, aber im Normalfall sollte alles den Ansprüchen genügen.

5.3.14 Welche Organisation steht dahinter?

Die British Standards Institution (BSI) wurde 1901 gegründet und ist seit 1938 die Organisation in Großbritannien die Standards festlegt. Auch wenn sich diese Organisation inzwischen international betätigt und Großbritannien in allen weltweiten Standardisierungsorganisationen vertritt, so ist sie immer noch ein Teil der britischen Administration und somit dort auch verantwortlich.

5.3.15 Vorlage/Querverbindungen zwischen den Guides

Der BS 2599 orientiert sich in erster Linie stark an verschiedenen ISO-Standards. So sind hier folgende ISO-Standards zu nennen: ISO 9000,ISO 9001, ISO 14001, ISO 17799, ISO 20000, ISO 27001; ISO 13335, ISO/IEC Guide 62, ISO Guide 73. Weitere Standards sind in der offiziellen Quellenliste nicht zu finden (BS25999-1 Code of Practice, 2006 S. 42) (BS25999-2 Specification, 2007 S. 21-23).

5.3.16 Zielgruppe

Der erste Teil der BS 25999 eignet sich für alle Manager und Personen, die sich in der einen oder anderen Art mit BCM beschäftigen müssen. Obwohl umfangreicher als der zweite Teil, enthält er allgemeine und praktische Punkte, die für das Ausführen des BCM benötigt werden.

Der zweite Teil hingegen ist für Personen relevant, die die genaue Durchführung des BCM überwachen und die Zertifizierung durchführen. Genaue Regeln werden festgelegt, diese sind im Normalfall nicht für alle relevant, sondern für einige wenige die sich intensiv mit dem Business Continuity Management beschäftigen (BS25999-2 Specification, 2007 S. ii).

5.3.17 Gegebene Templates

In keinem der beiden Teile des BS 25999 sind Templates gegeben.

5.3.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.3.19 Integration von Organisationsprozessen

In erster Linie besteht eine enge Verbindung zu ISO 27001 und eine Zertifizierung nach diesem Standard ist möglich. Auch die ISO-Standards ISO 9001 und ISO 14001 sind mit diesem Standard kompatibel. Zu diesen drei Standards gibt es am Ende des jeweiligen Teiles des BS 25999 auch eine Tabelle, in der die wichtigsten Inhaltsteile auf diese Standards umgelegt werden. Des Weiteren kann eine enge Verwandtschaft zum ebenfalls vom BSI entwickelten PAS 77:2006 (IT Service Continuity Management) festgestellt werden. Diese beiden Standards decken sich in den meisten Bereichen (BS25999-2 Specification, 2007 S. 21-22).

5.3.20 Benötigte Vorkenntnisse

Auch hier ist zwischen den beiden Teilen zu differenzieren. Der erste Teil (BS 25999-1) ist einsteigerfreundlich und ohne große Vorkenntnisse zu erfassen. Die oft hinzugefügten Kommentare erleichtern das Verständnis.

Beim zweiten Teil hingegen sollte ein fundiertes Vorwissen in mehreren Bereichen vorhanden sein. In erster Linie ist die Kenntnis des Bereiches BCM notwendig. Ebenso sollte der Anwender sich im Bereich der Betriebswirtschaft auskennen, hier vor allem in den Unternehmensstrukturen und der Personalführung.

5.3.21 Methoden

Auch hier muss zwischen den beiden Teilen unterschieden werden. Im ersten Teil (Code of Practice) werden die Methoden relativ genau beschrieben. Die Schritte werden einzeln aufgeschlüsselt. Allerdings kommt der Standard ohne Beispiele aus, auch die Erklärungen sind eher dürftig. Daher werden die Schritte zwar genau aufgehführt, allerdings ohne Erklärung. Somit ist eine Durchführung der Methoden zwar genau vorgegeben, aber ohne Erfahrung oder zumindest weitere Nachforschungen nicht einfach durchzuführen.

Im zweiten Teil werden in der Spezifikation keine Methoden erwähnt. Hier wird gesagt, was in einer Methode verpflichtend ist. Alles andere bleibt dem Anwender überlassen. Der Anwender muss auch nicht alle Schritte aus dem ersten Teil erfüllen. Somit kann man sagen dass im zweiten Teil keine Methoden beschrieben werden.

5.3.22 Ausschließlich Maßnahmen zur Einführung von BCM oder auch Überprüfung und Weiterführung

Im BS 25999 werden alle Teile des Business Continuity Managements abgedeckt, und zwar von der Planung bis hin zur Überprüfung der Maßnahmen (BS25999-2 Specification, 2007 S. 2).

5.3.23 Ergänzendes Material

Da der BS 25999:2 in Großbritannien einer der geläufigsten Standards ist, nach dem eine Zertifizierung möglich ist, erhält er dort auch einige Unterstützung. Hier sind voerst Whitepapers zu nennen, die von unabhängigen Dritten verfasst werden. Diese sollen dabei helfen, den Standard besser nachzuvollziehen und diesen in einem Unternehmen leichter umsetzen zu können.

Kurse und Schulungen werden aufgeführt, welche von diversen Privatorganisationen angeboten werden. Diese haben ähnlich wie die Whitepapers die Aufgabe das Verständnis für den Standard zu verbessern und die Einführung zu erleichtern. Die Schulungen stehen für Personen zur Verfügung, auch wenn die Zertifizierung nach BS 25999-2 für ein Unternehmen ist (How to Deploy BS 25999, 2008).

5.3.24 Phasen

Die beiden Teile des BS 25999 folgen einem ähnlichen, jedoch nicht gleichen Aufbau, daher werden hier beide Teile einzeln aufgelistet. Die zwei ersten Teile haben die gleichen ersten Punkte. Zuerst wird das Ziel der jeweiligen Teile beschrieben. Danach folgt eine Begriffserklärung, in welcher die wichtigsten Begriffe zum Verständnis des Standards beschrieben werden.

1.BS 25999-1

Im ersten Teil folgt eine Übersicht zum Thema Business Continuity Management. Der Begriff wird erklärt, Strategien zur Umsetzung werden gebracht und Vergleiche mit anderen Disziplinen erörtert. Des Weiteren werden Gründe genannt, aus welchem ASpekt BCM sinnvoll ist. Abschließend werden die Elemente des BCM-LifeCycle und deren Zusammenhang erklärt.

Im Anschluss daran folgt eine Sektion zum Thema BCM-Policy, worin Kontext und Inhalt dieses Dokumentes beschrieben werden. Weiters werden auch Ratschläge zur einfacheren und besseren Entwicklung der Policy gegeben.

Punkt fünf des ersten Teils beschreibt das BCM-Programm Management, welches laut diesem Standard der zentrale Teil des BCM ist. Nach einer kurzen Übersicht werden die Verantwortlichkeiten verteilt. Nun soll das BCM im Unternehmen implementiert werden. Anschließend wird auf das kontinuierliche Management eingegangen. Abschließend wird die Dokumentation des BCM-Vorganges beschrieben.

Das sechste Kapitel beschäftigt sich mit dem Verstehen der Organisation. Anfänglich wird eine Business Impact-Analyse durchgeführt. Danach werden die kritischen Aktivitäten und die Anforderungen für eine Wiederaufnahme der Aktivitäten ermittelt. Anschließend wird ein Risk Assassement durchgeführt. Auf Basis dieser Bewertung sowie der BIA sollen dann die Maßnahmen ermittelt werden, welche im Rahmen des BCM umgesetzt werden.

Im siebenten Kapitel wird die BC-Strategie festgelegt. Hierzu müssen verschiedene Faktoren wie zum Beispiel Menschen, Technologien, Informationen oder Stakeholder beachtet werden. All diese Faktoren werden beschrieben.

Kapitel acht beschäftigt sich mit dem Entwickeln, dem Planen und Implementieren von Notfallmaßnahmen. Darin wird beschrieben, welchen Inhalt und welche Struktur die Pläne haben müssen. Dabei werden folgende Pläne besprochen: Zuerst der Incident Management Plan, der beschreibt wie ein Unternehmen im unmittelbaren Katastrophenfall zu reagieren hat. Danach folgt der Business Continuity-Plan, der mittelfristig dafür zuständig ist, die kritischen Kernprozesse wiederherzustellen.

Kapitel neun behandelt das Thema der laufenden BCM. Hierzu zählen diverse Trainingsprogramme, welche durchgeführt werden müssen, um das Programm im Unternehmen zu etablieren. Anschließend wird beschrieben, wie die BCM-Maßnahmen auf Dauer reviewed werden müssen.

Das zehnte Kapitel beschäftigt sich mit dem Integrieren der BCM-Maßnahmen in die Unternehmenskultur. Hier geht es einerseits um die Bewusstseinsbildung, andererseits um das Antrainieren von verschiedenen Skills.

2. BS 25999-2

Nach den beiden einleitenden Teilen folgt eine Beschreibung der Planungsphase des BCM-Systems. Dies inkludiert auch die BCM-Policy, das Einführen in die Unternehmenskultur und die komplette Dokumentation.

Anschließend werden die wesentlichen Punkte zum Thema Einführung und Ausführung des BCM besprochen. In diesem Kapitel befinden sich die Business Impact-Analyse und das Risk Assessement. Ferner werden hier die Auswahl der Strategien und die Auswahl der Strategien bei akuten Notfällen besprochen. Abschließend werden in der Folge die Übungs- und Trainingsprogramme erwähnt.

Das fünfte Kapitel beschäftigt sich mit dem Monitoring und der Überwachung der laufenden Maßnahmen. Zuerst werden interne Audit-Maßnahmen besprochen. Als zweiter Punkt wird das Management-Review erläutert.

Das sechste und letzte Kapitel befasst sich mit der Erhaltung und Verbesserung eines laufenden Systems. Diese Maßnahmen werden in zwei Teile unterteilt. Einerseits korrektive beziehungsweise präventive Maßnahmen, andererseits kontinuierliche Verbesserung.

Als Anhang folgt eine Vergleichstabelle zu den ISO-Standards ISO 9001, ISO 14001 und ISO27001. Dabei werden die einzelnen Kapitel auf die Kapitel der jeweiligen ISO-Standards umgelegt (BS25999-2 Specification, 2007).

5.3.25 Beratung & Support

Das BSI bietet wenig Support an. Einzig Trainingskurse, die es den Mitarbeitern erleichtern sollen, den Standard zu verstehen, werden angeboten. Support für ein einzelnes Unternehmen ist nicht vorgesehen.

5.3.26 Befolgung der Richtlinien der Aufsichtsbehörden

Da das BSI die britische Standardisierungsbehörde ist, kann davon ausgegangen werden, dass ein Großteil der Richtlinien von allen Aufsichtsbehörden eingehalten wird. Allerdings weist der Standard BS 25999 dezidiert darauf hin, dass eine Einhaltung dieses Standards nicht automatisch eine Übereinstimmung mit den Richtlinien bedeutet (BS25999-2 Specification, 2007 S. ii).

5.3.27 Befolgung von internationalen IT-Standards

Durch die Einführung des BS 25999 werden eine Reihe weiterer Standards unterstützt. So wird mit Einführung der Business Impact Analysis auch ein Teil von PAS 77 erfüllt. Durch die Nähe zu diversen ISO-Standards werden einige Teile von diversen ISO-Richtlinien erfüllt. Allen voran wird ISO/IEC 27001 erfüllt. Auch kann eine grundlegende Übereinstimmung mit großen Teilen von ITIL und CoBIT festgestellt werden. Allerdings muss diese in konkreten

Fällen überprüft werden um sicher zu gehen, dass eine volle Kompatibilität hergestellt ist (BS25999-2 Specification, 2007 S. 21-22).

5.4 FSA

5.4.1 Sprache

Der Business Continuity Management Practice Guide der Financial Services Authority ist ausschließlich in englischer Sprache verfügbar. Andere Sprachen konnten nicht gefunden werden.

5.4.2 Ort der Entstehung

Das FSA ist eine Nicht-Regierungsorganisation mit Sitz in England (FSA - About). Das Dokument wurde ausschließlich in England erstellt. Dadurch, dass die Organisation, die diese Guideline erstellt hat, dem englischen Finanzministerium meldepflichtig ist, ist eine starke Bindung an britische Normen gegeben.

5.4.3 Zeit der Entstehung

Die zurzeit aktuelle Version wurde im November 2007 publiziert. Dies war die erste und bisher auch einzige Version dieses Dokuments. Davor gab es eine Fassung (Financial Services Authority, 2005) aus dem Jahr 2005, welche die wichtigsten Erkenntnisse des Resilience Benchmarking Project zusammenfasste. Aus diesem entstand dann wiederum der Business Continuity Management Practice Guide, der hier behandelt wird. Im Jahr 2008 wurde die Diskussion darüber neu aufgenommen und eine neue Diskussionsgrundlage (Financial Services Authority, 2008) erstellt.

5.4.4 Verfügbarkeit

Der FSA-BCM-Standard ist frei und auf der Homepage des FSA frei zum Downloaden (FSA BCM, 2006) verfügbar.

5.4.5 Art

Der Aufbau der Business Continuity Guideline der Financial Services Authority ist rein listenartig. Es werden einzelne Punkte der Reihe nach abgearbeitet. Auf circa 30 Seiten werden im Querformat mehrere Tabellen angeführt, auf denen einzeln die verschiedenen Schritte angeführt werden. Sechs Kapiteln, die in mehrere Teile unterteilt wurden, sind in der Guideline enthalten.

5.4.6 Vorhandene Tools zur Unterstützung

Ein umfangreiches Tool liegt vor, welches die Selbsteinschätzung der Unternehmen erleichtern soll (FSA-Tool). Dieses Tool war schon vor der Guideline verfügbar. Die ursprüngliche Version dieses Tools diente der Erstellung des Standards (siehe 5.4.15). Die

jetzt verfügbare Fassung ist eine verkleinerte Version des ursprünglichen Fragebogens, auf dem diese Guide basiert.

5.4.7 Allgemein/branchenspezifisch

Der FSA-BCM-Standard ist auf die Finanzbranche ausgerichtet. Die Ratschläge und Tipps sind auf Banken und Finanzinstitute ausgerichtet. Obwohl auch andere Unternehmen davon profitieren können, sind diese nicht direkt angesprochen (FSA BCM, 2006 S. 1-2).

5.4.8 Unternehmensgröße

Da der Guide auf Finanzinstitute und Banken ausgerichtet ist, ist auch die Unternehmensgröße begrenzt. Die Ratschläge, die dieser Standard gibt, sind auf große Unternehmen ausgerichtet. Dies erklärt sich vor allem daraus, dass fast alle Banken und Finanzunternehmen mittelgroße oder große Unternehmen sind. Daher würde es wenig Sinn machen, die Ratschläge auf Kleinbetriebe auszurichten. (FSA BCM, 2006 S. 1-2)

5.4.9 Art der Verfügbarkeit

Wie heute zumeist üblich, verwendet das FSA das Internet als Publikationsweg. Daher ist der Standard auf der Homepage der Financial Services Authority zu finden. Die Homepage ist eher unübersichtlich und die Guideline schwer zu finden. Zu finden ist der Standard am ehesten über die Suchfunktion.

5.4.10 Möglichkeiten zur Zertifizierung

Derzeit besteht keine Möglichkeit, sich nach dem FSA-BCM zu zertifizieren. Dies hat den Grund, dass das FSA diese Guideline nicht als echten Standard sondern als Empfehlung und Denkanregung sieht. Verpflichtende Maßnahmen sind nicht vorgeschrieben. Alle Maßnahmen werden als Ideen beziehungsweise als aus der Umfrage ermittelte Best Practices gesehen. Daher wäre eine Zertifizierung gegen die eigentliche Idee dieser Guideline (FSA BCM, 2006 S. 1-2, 4).

5.4.11 Rechtliche Begrenzungen

Bei diesem Standard kann insofern nicht von rechtlichen Begrenzungen gesprochen werden, als dass er keinen verpflichtenden Teil enthält. Somit wird jede rechtliche Grenze irrelevant (FSA BCM, 2006 S. 4).

5.4.12 Flexibilität

Der Standard ist ausgeprochen flexibel gestaltet. Dadurch dass es keine Vorschriften gibt, sind sämtliche vorgeschlagenen Maßnahmen optional. Der Guide soll keine Checkliste darstellen, in der ein Punkt nach dem anderen abgearbeitet wird und ein Punkt einen anderen voraussetzt. Vielmehr soll er ein flexibles Werkzeug sein, welches ein Framework zum Planen darstellt und das Denken anregt.

5.4.13 Organisatorisch/kulturell

Dadurch dass keine Einführung des BCM in ein Unternehmen in diesem Standard enthalten ist, ist es nicht möglich den notwendigen Eingriff in ein Unternehmen zu bewerten. Da Banken, auf die sich diese Guideline ausrichtet, schon ein BCM haben müssen, kann auch nicht von umfassenden Eingriffen gesprochen werden. Daraus folgt, dass die Auswirkungen dieses Guides auf ein Unternehmen eher gering sind.

5.4.14 Welche Organisation steht dahinter?

Die Financial Services Authority (FSA) ist eine Privatorganisation, die von staatlicher Seite kontrolliert wird. Sie wird von den Firmen finanziert, die sie auch kontrolliert. Das Finanzierungsmodell funktioniert so, dass alle Firmen die Aktivitäten ausführen, die von der FSA überwacht werden, mit einer Gebühr belegt werden. Diese Konstruktion löste in den 90er-Jahren die auf viele Stellen verteilte Kontrolle der Finanzindustrie ab. Somit wird einerseits eine staatliche Überwachung der Banken garantiert, andererseits besteht eine unmittelbare Nähe zu der kontrollierten Branche. Ebenfalls ist eine zentrale Stelle zur Überwachung dieser Branche vorhanden. Die Direktion wird vom Finanzministerium bestimmt. Diese ist lediglich für strategische Entscheidungen zuständig. Die täglichen Operationen werden von dafür definierten Personen durchgeführt. Besonderen Wert legt die FSA auf die Tatsache, dass sie so transparent wie möglich arbeitet und lediglich dem Finanzministerium und dadurch dem britischen Parlament rechenschaftspflichtig ist (FSA - About).

5.4.15 Vorlage/Querverbindungen zwischen den Guides

Verbindungen zu anderen Guidelines bestehen nicht, auch diente kein anderer Standard als Vorlage für dieses Werk.

Dies erklärt sich aus der Tatsache, dass dieser Guide aus einer eigens dafür angefertigten Studie entstanden ist. Drei große Organisationen (das FSA, die Bank of England und das britische Finanzministerium) führten dabei gemeinsam ein großes Projekt durch, um den britischen Finanzsektor auf eine bedeutende operative Störung wie beispielsweise einen Terroranschlag zu bewerten. Dazu wurden ungefähr 60 der wichtigsten britischen Finanzunternehmen auf freiwilliger Basis jeweils in etwa 1.000 Fragen gestellt. Die Resultate wurden anschließend ausgewertet und als Endprodukt der hier behandelte FSA-BCM-Standard geschaffen. Ungewöhnlich dabei war, dass sich fast alle großen Unternehmen in diesem Sektor mit außergewöhnlichem Einsatz und hoher Akzeptanz diesem Projekt widmeten. Dies lässt sich, so die Studienautoren, damit erklären, dass sich die Finanzinstitute ein gutes Feedback und eine gute Bewertung der eigenen Stellung im Vergleich zu anderen Unternehmen erwarteten. Es wurde somit ein Standard geschaffen, der nicht die Idealziele vorgibt, sondern die zurzeit realisierten Standards wiederspiegelt und somit einen Vergleich innerhalb der Branche ermöglicht. (FSA BCM, 2006 S. 1) (Resilience Benchmarking Project, 2005)

5.4.16 Zielgruppe

Der FSA-BCM-Standard ist vor allem für jene relevant, die strategische Maßnahmen in einem Unternehmen bestimmen oder für die BCM-Maßnahmen in einem Unternehmen zuständig sind. Daher richtet sich das Dokument an das höhere Management und an die BCM-Verantwortlichen. Nicht gedacht ist dieses Dokument für einfache Mitarbeiter, die im BCM eine ausführende und keine planende Rolle spielen. (FSA BCM, 2006 S. 1-2)

5.4.17 Gegebene Templates

Im FSA-BCM-Standard sind keine Templates gegeben. Dies resultiert daraus, dass dies kein eigentlicher Standard, sondern eher eine Sammlung an Best Practices ist. Ebenfalls ein Grund ist, dass es auf einer Studie und nicht auf akademischer Forschung beruht. Da die Grundlage der Studie ein Fragebogen war, war es nicht möglich, Templates in das Dokument zu integrieren, da dies im Fragebogen nicht vorgesehen war.

5.4.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.4.19 Integration von Organisationsprozessen

Aufgrund der Entstehung des Standards (siehe 5.4.15) gibt es auch keine Sicherheit zur Integration von anderen Organisationsprozessen in Unternehmen. Es kann zwar davon ausgegangen werden, dass manche andere Prozesse voll unterstützt werden, aber dies kann nicht sichergestellt werden. Daher wird kein Organisationsprozess voll unterstützt.

5.4.20 Benötigte Vorkenntnisse

Um den BCM-Standard der Financial Services Authority verwenden zu können, bedarf es einiger Vorkenntnisse, vor allem im Bereich BCM. Da keine Erklärungen oder Beschreibungen vorhanden sind, erschwert es ein fehlendes Vorwissen, die vorgeschlagenen Maßnahmen sinnvoll umzusetzen.

5.4.21 Methoden

Sämtliche Methoden in diesem Dokument sind allgemein gehalten. Keine Methode ist genauer beschrieben.

5.4.22 Nur Einführung oder Überprüfung und Weiterführung

Aufgrund der ungewöhnlichen Entstehung der BCM-Richtlinie der FSA (siehe 5.4.15) ist in diesem Fall sowohl die Überprüfung als auch die Weiterführung eines BCM-Standards enthalten, nicht aber die Einführung. Dies ist leicht dadurch erklärbar, dass die Banken, auf die dieses Dokument zugeschnitten ist, verpflichtet sind, über ein gewissen Maß an Business Continuity im Unternehmen zu verfügen. Daraus folgt, dass es wenig Sinn machen würde, die Einführung eines BCM in ein Unternehmen zu beschreiben. Prinzipiell ist eine Einteilung in die bei anderen Standards üblichen Phasen mit diesem Standard schwer möglich. Die

Einteilung ist nicht nach Zeit, sondern nach Unternehmensbereichen gegliedert. Dadurch ist ein Vergleich mit anderen Standards schwer möglich.

5.4.23 Ergänzendes Material

Zu dem Guide sind wenig zusätzliche Materialien vorhanden. Das Einzige was hilft, dieses Werk zu verstehen, ist eine genaue Beschreibung der Studie, die dem Guide zu Grunde liegt. Dies hilft, die grundlegenden Aspekte dieses Werkes nachzuvollziehen (Resilience Benchmarking Project, 2005).

5.4.24 Phasen

Die erste Phase ist die eigentliche BCM-Phase. Sie wird Corporate Continuity genannt und gliedert sich in fünf Unterphasen. Hier wird zuerst das BC geplant, danach wird der BC-Plan erstellt. Anschließend werden dem Plan die benötigten Ressourcen zugewiesen. Nach einem Planreview werden abschließend die Erholungszeiten für die kritischen Operationen festgelegt.

Im Teil B geht es um Krisenmanagement. In den Bereichen Kultur, Team und Kommunikation wird das Verhalten im Falle eines Notfalles festgelegt.

Der dritte Teil behandelt elektronische Systeme. In den beiden Unterpunkten IT und Telefon werden die wichtigsten Maßnahmen in diesem Bereich bei einem Notfall behandelt. Dieser Punkt ist der, in dem die Verhaltensweise und die Vorbedingungen in der IT festgelegt werden.

Teil D ist für die Verwaltung der Gebäude im Notfall zuständig. Hier wird darüber Auskunft gegeben, welche Bedingungen diverse Einrichtungen haben müssen um für Notfälle gerüstet zu sein.

Der letzte Teil schließlich behandelt alle Bereiche über Personen beziehungsweise Mitarbeiter. Zuerst wird erklärt, wie die Mitarbeiter hinsichtlich der BCM-Maßnahmen ausgebildet und trainiert werden sollen. Am Ende wird zusätzlich das Krisenmanagement hinsichtlich der Mitarbeiter angesprochen.

5.4.25 Beratung & Support

Aufgrund der Entstehungsgeschichte dieser Guideline ist verständlich, dass es keine Beratung beziehungsweise Support von dieser Stelle gibt. Da die meisten Banken ohnedies über ein professionelles BCM-Management verfügen, ist dies auch nicht zielführend. Auch ist der Guide so verfasst, dass ein entsprechender Support nicht notwendig ist.

5.4.26 Befolgung der Richtlinien der Aufsichtsbehörden

Da dieser Standard eine Sammlung von praktizierten BCM-Maßnahmen ist, ist es nicht möglich, dass alle in diesem Dokument besprochenen Richtlinien aktiv umgesetzt werden. Andererseits ist es auch unwahrscheinlich, dass die größten Unternehmen im Bereich der Finanzwirtschaft Richtlinien oder Gesetzte verletzten. Daher kann davon ausgegangen

werden, dass die wichtigsten Richtlinien beachtet werden, ohne darauf wirklich Wert zu legen.

5.4.27 Befolgung von internationalen IT-Standards

Auch hier muss davon ausgegangen werden, dass die Autoren dieser Guideline keinen Wert darauf legten, ob dieser internationale IT-Standards erfüllt oder nicht. Da jedoch die Praktiken der größten Finanzunternehmen zusammengefasst wurden, werden manche Standards zumindest zum Teil unterstützt. Zu nennen sind hier vor allem der PAS 77 und der ISO Standard ISO 27002, die zumindest zum Teil unterstützt werden.

5.5 ISO 22399

5.5.1 Sprache

Der Standard ISO 22399 ist wie die meisten Standards in englischer Sprache verfügbar. Dies erklärt sich vor allem aufgrund der Internationalität des Standards.

5.5.2 Ort der Entstehung

Die Entstehung des Standards erfolgt international, es kann von keinem Ort der Entstehung gesprochen werden. Wie bei ISO-Standards üblich, wurde der Standard von einem Komitee aus internationalen Mitgliedern erstellt. Zurzeit besteht das Komitee aus knapp 40 Mitgliedsländern, verteilt über die ganze Welt.

5.5.3 Zeit der Entstehung

Der Standard wurde nach ausführlicher Ausarbeitung am 15.November 2007 als internationaler Standard publiziert. Zuvor wurde das Dokument, wie bei der ISO üblich, von einem technischen Komitee erstellt. Danach wurde die Guideline an alle Mitglieder zur Begutachtung geschickt und in der Folge darüber abgestimmt. Um das Prädikat ISO/PAS (Publicly Available Specification) zu erhalten, muss mit einfacher qualifizierter Mehrheit dem Werk zugestimmt werden (ISO 22399, 2007 S. iv).

5.5.4 Verfügbarkeit

Der ISO/PAS 22399 ist kostenpflichtig zu kaufen. Die Kosten belaufen sich auf CHF 124 (~ EUR 86,-). Der Preis bleibt gleich, egal in welcher Form der Standard gekauft wird.

5.5.5 Art

Der Aufbau des ISO/PAS 22399 ist textuell, dennoch ist dem Standard eindeutig seine technische Seite anzumerken. Die Sprache ist präzise und kurz gefasst, kommt schnell zum Punkt und verwendet keinen Aufwand für rhetorische Mittel. Obwohl der Aufbau textuell ist, werden häufig Aufzählungen verwendet, was vom oben erwähnten „technischen“ Stil kommt.

5.5.6 Vorhandene Tools zur Unterstützung

Durch die weite Verbreitung und die hohe Anerkennung, die der ISO/PAS 22399 erfährt, gibt es unzählige private Firmen, die sich auf die Unterstützung zur Ausführung dieses Standards

spezialisiert haben. Bei diesem kommerziellen Support finden sich auch diverse Tools, die alle auf die ein oder andere Weise die Umsetzung des Standards unterstützen. Hier sind zum Beispiel große Tools wie „Crisis Commander“ (Crisis Commander) oder „Impact Aware“ (Impact Ware) zu nennen. Der Markt ist in diesem Bereich so groß, sodass nicht alle Tools hier genannt werden können.

5.5.7 Allgemein/branchenspezifisch

Der Standard ist allgemein gültig, keine Branche wird ausgeschlossen oder besonders angesprochen. Dies erklärt sich vor allem aus der Entstehung und der Organisation, die ihn erstellt hat. Die ISO erstellt allgemein gültige internationale Standards und besteht aus vielen Mitgliedsländern. Das Ziel dieses Standards war auch immer, allgemeingültig zu sein (ISO 22399, 2007 S. v-vi).

5.5.8 Unternehmensgröße

Der Standard soll für alle Unternehmensgrößen, vom Einzelbetrieb bis hin zum multinationalen Großunternehmen gültig sein (ISO 22399, 2007 S. v-vi).

5.5.9 Art der Verfügbarkeit

Der ISO/PAS liegt in zwei verschiedenen Formen vor, die sich voneinander wenig unterscheiden. Einerseits kann man ihn als PDF kaufen und direkt auf seinen PC laden. Andererseits ist auch eine gedruckte Version desselben Standards verfügbar.

5.5.10 Möglichkeiten zur Zertifizierung

Eine Zertifizierung nach ISO/PAS 22399 ist nicht möglich.

5.5.11 Rechtliche Begrenzungen

Durch die Internationalität der Guideline ist keine rechtliche Begrenzung festzustellen. Da der Standard von Personen aus verschiedenen Ländern verfasst und Standards aus unterschiedlichen Regionen verwendet wurden, können keine regionale Begrenzungen bewertet werden (ISO 22399, 2007 S. vii).

5.5.12 Flexibilität

Der ISO/PAS 22399 sieht sich selbst als ein flexibles Tool, welches auf verschiedenen Arten implementiert werden kann. Man kann den Standard durchaus seinen Bedürfnissen anpassen, allerdings innerhalb bestimmter Grenzen. Trotzdem kann der Standard eher flexibel verwendet werden (ISO 22399, 2007 S. vi).

5.5.13 Organisatorisch/kulturell

Laut dem Standard selbst verlangt die Einführung eines BCM in ein Unternehmen einen grundlegenden kulturellen Wechsel im Unternehmen. Dies ist bei dieser Guideline selber nicht deutlicher festzustellen als bei anderen Guides. Daher kann gesagt werden, dass wie bei

jeder Einführung eines neuen Systems Änderungen notwendig sind, diese jedoch nicht umfangreicher sind als bei anderen Systemen (ISO 22399, 2007).

5.5.14 Welche Organisation steht dahinter?

Die International Organization for Standardization gilt als die weltweit größte Organisation für die Entwicklung und Publikation von internationalen Standards. Die Organisation besteht aus einem Verbund von zurzeit 162 nationalen Standardisierungsbehörden. Dazu kommt eine große Anzahl an Mitgliedern aus der Privatwirtschaft. Da das ISO eine Non-Governmental Organisation (ein zivilgesellschaftlicher Interessensverband) ist, ist es ihr zentraler Auftrag, die öffentlichen und die privaten Organisationen zu verbinden beziehungsweise einen Konsens zwischen ihnen zu finden. Das zentrale Hauptquartier befindet sich in Genf in der Schweiz. Seit dem Jahr 1947 publiziert das ISO diverse Standards. Und zwar bisher über 17.500.

Der Name ISO leitet sich nicht, wie er vielleicht vermuten lässt, von den Anfangsbuchstaben des Namens ab, sondern vom lateinischen „isos“, auf Deutsch „gleich“. Daher ist die Abkürzung in allen Sprachen gleich.

Ein neuer Standard wird normalerweise von einem Industriesektor über ein nationales Komitee beantragt, welches dann einen Vorschlag in der internationalen ISO-Versammlung einbringt. Wird dieser Vorschlag angenommen, wird ein sogenanntes technisches Komitee gegründet, welches in der Folge den Standard selbst erarbeitet. Dieses besteht aus Experten aus dem jeweiligen Sachgebiet. Nach Erarbeitung des Standards muss dieser von mehr als 50% der Mitglieder genehmigt werden.

5.5.15 Vorlage/Querverbindungen zwischen den Guides

Der Standard wurde von Mitgliedern aus verschiedenen Ländern erarbeitet. Dabei wurden auch bereits bestehende Standards in die Arbeit mit einbezogen. Hier sind vor allem die folgenden Standards zu nennen: Der amerikanische NFPA 1600:2004, der britische BS 25999-1:2006, der australische HB 221:2004 und der israelische INS 24001:2007 sowie diverse japanische Industriestandards (ISO 22399, 2007 S. iv).

5.5.16 Zielgruppe

Da der ISO/PAS 22399 gewisse Vorkenntnisse verlangt, ist er nicht für jedes Unternehmen geeignet. Er bezieht sich auf Manger, besonders auf jene die mit der Einführung und Erhaltung von Business Continuity Management beschäftigt sind. Aber auch Manager, für die er Auswirkungen für ihre tägliche Arbeit hat, sind relevante Teile vorhanden (ISO 22399, 2007 S. v-vii).

5.5.17 Gegebene Templates

Im ISO 22399 sind keine Templates gegeben.

5.5.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.5.19 Integration von Organisationsprozessen

In diesem Standard werden mehrere Organisationsprozesse angesprochen, die in den Prozess integriert werden können. Hier sind zu nennen: Corporate Governance (ISO 22399, 2007 S. 30) und Operational Control (ISO 22399, 2007 S. 19-20) sowie mit Einschränkungen Records Management und Change Management.

5.5.20 Benötigte Vorkenntnisse

Um den Standard verstehen zu können, sind grundlegende Kenntnisse im Bereich BCM notwendig. Der Standard eignet sich nicht als Einführung in das Thema BCM. Obwohl zu Beginn eine kurze Einleitung und eine Begriffsdefinition vorhanden sind, müssen beim weiteren Bearbeiten doch bereits Vorkenntnisse vorhanden sein. Allerdings sind zum Verständnis Grundkenntnisse ausreichend. Für die Umsetzung dieses Werks hingegen müssen bereits mehr Erfahrungen in diesem Bereich gegeben sein, da ansonsten Methoden zu allgemein angeführt sind und manche Begriffe und Vorgänge nicht verständlich erscheinen.

5.5.21 Methoden

Die Methoden sind in dem Standard allgemein gehalten. Allerdings werden im Anhang verschiedene Methoden detaillierter besprochen. So beschreibt Anhang A (ISO 22399, 2007 S. 24-25) die Business Impact Analyse exakter. Anhang B (ISO 22399, 2007 S. 26-27) beschäftigt sich mit dem Notfallschutzprogramm. Anhang C (ISO 22399, 2007 S. 28-29) geht auf Details im Bereich Continuity Management ein. Letztlich wird noch angesprochen, wie im Unternehmen die Vorbereitung auf Zwischenfälle in die Unternehmenskultur eingeführt werden kann.

5.5.22 Nur Einführung oder Überprüfung und Weiterführung

Der ISO-22399-Standard deckt alle Bereiche von der Policy, über Planung und Einführung bis hin zu Überprüfung und Review ab. Auch Erhaltung und Weiterentwicklung werden besprochen (ISO 22399, 2007 S. 8).

5.5.23 Ergänzendes Material

Von der ISO-Organisation werden keine zusätzlichen Informationen zu dem Standard herausgegeben. Dies würde nicht dem Modell der ISO entsprechen. Allerdings werden von diversen anderen privaten Organisationen Hilfen und spezielles Material herausgegeben und vor allem verkauft. Dies muss aber immer mit Vorsicht in Bezug auf die Qualität der Unterlagen gesehen werden.

5.5.24 Phasen

Das ISO/PAS 22399-Dokument beginnt nach einem kurzen Vorwort, in dem die organisatorischen Aspekte der Entstehung angerissen werden, mit einer allgemeinen Einleitung. Hier wird eine allgemeine Einleitung mit einer Übersicht über die verschiedenen Phasen gegeben. Ferner werden Zielgruppe, Managementmodelle und allgemeine Ratschläge zur Anwendung genannt.

In den danach folgenden Kapiteln werden der Aufgabenbereich des Standards, eine Begriffsdefinition und ein Flow-Diagramm zu dem BCM-Modell aufgeführt.

Im fünften Kapitel beginnt die eigentliche BC-Definition mit der Erstellung einer Policy. Es wird erklärt, was eine Policy ist. Weiters werden der Rahmen sowie die Zuständigkeit geklärt. Anschließend werden die Weiterentwicklung und das Review behandelt. Abschließend in diesem Kapitel wird die Struktur des Projektteams, welches für BCM zuständig ist, definiert.

Das nächste Kapitel beschäftigt sich mit der Planungsphase. Nach einer allgemeinen Einleitung werden rechtliche Probleme behandelt. In den folgenden Schritten wird ein Risk Assessment und eine Impact-Analyse durchgeführt. Danach wird der umfangreiche Punkt der Erstellung eines BCM-Plans, oder wie es in dem Standard genannt wird, eines „Incident preparedness and operational continuity management programs“. Hier werden die genauen Schritte von der Prävention bis hin zum Recovery Management erläutert.

Teil sieben ist der Implementierung und Ausführung der Pläne gewidmet. Hier werden als Erstes die benötigten Ressourcen zugeordnet. Anschließend soll das BC im Unternehmen verankert werden. Die folgenden beiden Unterpunkte beschäftigen sich mit dem Training und der internen Kommunikation. Abschließend in diesem Punkt wird auf die Prozeduren im Bereich Finanz und Administration eingegangen.

Das achte Kapitel befasst sich mit der Überprüfung der Leistung der umgesetzten Maßnahmen. Zuerst wird die Leistung überprüft und beobachtet. Danach soll ein Trainingsprogramm erstellt werden. Nun werden korrektive sowie präventive Maßnahmen ergriffen. Zusätzlich sollten bestimmte Maßnahmen ergriffen werden, um die Programme aktuell zu halten. Abschließend werden in diesem Kapitel Ratschläge gegeben, wie interne Audits und Selbstüberprüfungen durchgeführt werden können.

Das letzte Kapitel schreibt dem Topmanagement vor, regelmäßige Reviews zu geplanten Intervallen durchzuführen, um sicherzugehen, dass noch bestimmte Parameter des BCM korrekt sind.

Am Ende der Guideline gibt es weiters vier Anhänge. Der erste beschäftigt sich eingehender mit dem Vorgang der Impact-Analyse. Der zweite Anhang ist dem Thema Erstellung eines Programms zur Reaktion im Notfall gewidmet. Der dritte Anhang präzisiert das BCM-Programm. Der abschließende letzte Teil des Anhangs befasst sich mit der Schaffung einer BCM-Kultur im Unternehmen, genauer gesagt mit der Corporate Governance (siehe auch 5.6.195.5.19).

5.5.25 Beratung & Support

Die International Standards Organisation bietet selbst keine Beratung oder Support an. Dies würde weder der Struktur noch der Aufgabe dieser Organisation entsprechen. Allerdings steht ein breiter kommerzieller Support von privaten Firmen zur Verfügung (siehe auch 5.5.6).

5.5.26 Befolgung der Richtlinien der Aufsichtsbehörden

Der ISO 22399 ist ein internationaler Standard der von Mitgliedern aus verschiedenen Ländern entwickelt wurde. Daher ist es nicht möglich dass die Richtlinien eines bestimmten

Landes erfüllt werden. Dennoch wird auf internationale Gepflogenheiten eingegangen, daher ist nicht anzunehmen, dass wichtige Richtlinien verletzt werden.

5.5.27 Befolgung von internationalen IT-Standards

Internationalen IT-Standards werden nicht aktiv unterstützt.

5.6 ASIS SPC.1-2009

5.6.1 Sprache

Der Standard ist ausschließlich in englischer Sprach verfügbar, was durch die Herkunft bedingt ist.

5.6.2 Ort der Entstehung

Der ASIS SPC1 ist lokal schwierig zuzuordnen, da der Standard in den USA von Experten ebenfalls erstellt wurde. Andererseits ist zu erkennen, dass einige Mitglieder aus anderen Ländern beteiligt sind und diese Mitglieder auf die Kompatibilität zu diesen Ländern achten. Dafür spricht die Kompatibilität zu diversen ISO-Standards (ASIS SPC.1-2009, 2009 S. iii, viii).

5.6.3 Zeit der Entstehung

Der Standard ist im März 2009 bestätigt worden. (ASIS SPC.1-2009, 2009 S. i) Eine ältere Version dieser Guideline liegt nicht vor. Allerdings gibt es einen ähnlichen Standard der gleichen Organisation, der als Vorgänger bezeichnet werden kann (Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery (ASIS International, 2004)).

5.6.4 Verfügbarkeit

Der Standard ist kostenpflichtig. Die Kosten belaufen sich auf USD 107,- (ca. EUR 75,-). Sowohl die Softcover-Variante als auch das PDF kosten denselben Betrag (ASIS-Shop).

5.6.5 Art

Der Aufbau des Guides ist textuell, wobei eine präzise Granularität eingehalten wird. Die einzelnen Punkte sind dabei kurz, dafür prägnant beschrieben. Oft werden Aufzählungen verwendet.

5.6.6 Vorhandene Tools zur Unterstützung

Tools, die speziell für diesen Standard erarbeitet wurden, konnten bei der Recherche nicht gefunden werden. Allgemeine, kommerzielle Tools zur Unterstützung können verwendet werden.

5.6.7 Allgemein/branchenspezifisch

Der Standard ist allgemein gehalten und enthält keine branchenspezifische Ratschläge. Im Standard selbst wird von einer Zuständigkeit für private-, Non-Profit- und Non-Gouvernement-Organisationen sowie öffentliche Institutionen als Zielgruppen gesprochen (ASIS SPC.1-2009, 2009 S. vii).

5.6.8 Unternehmensgröße

Die Guideline spezifiziert keine bestimmte Unternehmensgröße und ist daher für sämtliche Unternehmen geeignet (ASIS SPC.1-2009, 2009 S. vii).

5.6.9 Art der Verfügbarkeit

Der Guide ist in zwei verschiedenen Arten zu erhalten, und zwar einerseits als PDF auf der Homepage (ASIS - Download), andererseits in Buchform als Softcover, zu beziehen im ASIS-Bookstore (ASIS-Shop).

5.6.10 Möglichkeiten zur Zertifizierung

Das ASIS sieht es als eine seiner Hauptaufgaben an, Zertifizierungen anzubieten und durchzuführen. Daher werden ausschließlich Einzelpersonen zertifiziert. Allerdings werden verschiedene Stufen beziehungsweise Schwerpunkte angeboten. Die Kosten liegen zwischen USD 200,- und USD 400,-, je nach Art und Ort der Zertifizierung. Die Lizenz ist drei Jahr gültig, nach diesem Zeitraum muss die Zertifizierung erneuert werden. Derzeit liegen drei verschiedene Zertifizierungen des ASIS vor:

1. Der Certified Protection Professional (CPP). Dieser Titel ist eine allgemeine Zertifizierung zum Security Experten/Manager. Diese Zertifizierung fällt in den Bereich des Business Continuity Managements. Die Prüfung besteht aus 200 Multiple-Choice-Fragen aus acht verschiedenen Bereichen (Security Principles and Practices, Business Principles and Practices, Personnel Security, Physical Security, Information Security, Emergency Practices, Investigations, Legal Aspects). Mit dieser Bandbreite werden Themen aus allen relevanten Bereichen angesprochen. Diese Zertifizierung ist auch in Spanisch möglich.

2. Die zweite Möglichkeit ist der Professional Certified Investigator (PCI). Dieses Zertifikat gilt speziell für Ermittler. Die drei Themengebiete der Zertifizierung (Case Management, Evidence Collection, Case Presentation) zeigen eindeutig, für wen dieses Zertifikat gilt. Und zwar sollen Personen angesprochen werden, die mit Ermittlungen, Fallevaluationen und Bewertung von Managemententscheidungen zu tun haben. Dieses Zertifikat hat mit den besprochenen Standards nichts zu tun und fällt auch nicht in den Bereich BCM.

3. Das dritte Zertifikat, Physical Security Professional (PSP), beschäftigt sich, wie der Name schon sagt, mit der physischen Sicherheit. Personen die dieses Zertifikat bestehen, sollen den gesamten Vorgang der physischen Sicherheit - von der Risikoanalyse und Gefahrenbewertung über Entwurf und Einführung von verschiedenen Maßnahmen bis hin zur Kostenanalyse - durchführen können. Die Themengebiete der Prüfung sind „Physical Security Assessment“, „Application, Design, and Integration of Physical Security Systems“ und „Implementation of Physical Security Measures“ (ASIS - Certification).

5.6.11 Rechtliche Begrenzungen

Der Standard selbst schließt jegliche rechtliche Begrenzung aus und bemerkt explizit, dass geltendes Recht immer und ausnahmslos über allen in diesem Guide genannten Maßnahmen zu stehen haben. Da der Standard auch keinen absoluten Bedingungen stellt, ist dies möglich (ASIS SPC.1-2009, 2009 S. ii, iii).

5.6.12 Flexibilität

Der Standard ist flexibel. Dies zeigt sich besonders an der Möglichkeit, verschiedene andere Managementsysteme zu integrieren (siehe 5.6.19). Zusätzlich können Methoden erweitert, verändert oder sogar gestrichen werden. Der Standard sieht sich selbst als Übersicht und als eher allgemeine Ratgeber. Auch Genauigkeit und Umfang sollen je nach verschiedenen Faktoren, wie zum Beispiel Unternehmensgröße, angepasst werden.

5.6.13 Organisatorisch/kulturell

Ein besonderer Eingriff in das organisatorische System kann nicht festgestellt werden. Durch die hohe Flexibilität werden diverse Wege aufgezeigt, aber keine davon vorgeschrieben.

5.6.14 Welche Organisation steht dahinter?

Die American Society for Industrial Security (ASIS) wurde 1955 gegründet. Sie besteht heute aus mehr als 35.000 Mitgliedern weltweit. Ihre Aufgabe ist es, die Effektivität und Produktivität von für Security zuständigen Mitarbeitern zu verbessern. Dieses Ziel soll durch Lernprogramme und –Materialien, verschiedene Seminare und Veranstaltungen sowie mit der Publikation der Zeitschrift „Security Management“ (Security Management), erreicht werden. Die ursprünglich rein US-amerikanische Gesellschaft ist inzwischen weltweit tätig und hat Mitglieder überall auf der Welt. Seit 2002 ist der offizielle Name ASIS International. Es ist eine Non-Profit-Organisation die sich aus Mitgliedsbeiträgen und Zahlungen für diverse Dienstleistungen finanziert (ASIS-About).

5.6.15 Vorlage/Querverbindungen zwischen den Guides

Der ASIS-Standard hat eine starke Verbindung zu diversen ISO-Standards, aus denen in verschiedenen Bereichen Aspekte einfließen. Relevant für das Business Continuity Management sind hier vor allem der ISO/PAS 22399:2007 (Societal security - Guideline for incident preparedness and operational continuity management), aber auch der ISO/IEC 27001:2005 (Information technology - Security techniques - Information security management systems – Requirements) (ASIS SPC.1-2009, 2009 S. vii, ix, 41-43).

Abseits der ISO-Standards nimmt sich der Standard eine Vorlage, den hauseigenen Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery (siehe 5.6.3) (ASIS SPC.1-2009, 2009 S. iii).

5.6.16 Zielgruppe

Die Zielgruppe dieses Standards ist das Management, und hier besonders jede Gruppe, die sich aktiv mit dem BCM beschäftigt. Für die Personen, die in unteren Hierarchieebenen daran

beteiligt sind, bietet die Guideline geringe Informationen, da sie sich wenig mit praktischen Details beschäftigt (ASIS SPC.1-2009, 2009 S. vii, 1-2).

5.6.17 Gegebene Templates

Templates sind nicht gegeben.

5.6.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.6.19 Integration von Organisationsprozessen

Der Standard orientiert sich stark an diversen ISO-Standards. Hier sind der ISO 9001:2000 (Quality management systems - Requirements), der ISO 14001:2004 (Environmental management systems - Requirements with guidance for use) und der ISO/IEC 27001:2005 (Information technology- Security techniques - Information security management systems – Requirements) sowie ISO 28000:2007 (Specification for security management systems for the supply chain) zu nennen. All diese Normen sollen möglichst gleichzeitig unterstützt werden, sodass das Risiko in sämtlichen Bereichen möglichst klein gehalten werden kann. Als Beispiel wird aufgeführt, dass um ISO 14001 (Umweltschutz) zu implementieren, zusätzlich noch Umweltthemen in den ASIS-Standard eingeführt werden sollen. Beispielsweise sind hier bei der Risikoanalyse auch der Einfluss auf die Umwelt mit einzubeziehen.

Der ASIS-Standard ist daher in der Intension geschrieben worden, flexibel genug zu sein, um auch andere Managementprozesse in das System zu integrieren. Ein besonderer Schwerpunkt liegt dabei auf den genannten ISO-Standards, zu denen auch eine Vergleichstabelle vorhanden ist (ASIS SPC.1-2009, 2009 S. vii, ix, 41-43).

5.6.20 Benötigte Vorkenntnisse

Grundlegende Vorkenntnisse über Business Continuity sind notwendig. Da der Standard nicht alle Details erklärt, wäre es schwierig, den Standard nachzuvollziehen. Zusätzlich sind Kenntnisse über Unternehmensführung und –Planung von Vorteil, da viele Ausdrücke und Vorgänge verlangt werden, die ausschließlich mit solchen Vorkenntnissen nachvollziehbar sind (ASIS SPC.1-2009, 2009 S. 1-2).

5.6.21 Methoden

Die Methoden sind ausnahmslos allgemein gehalten. Genauere Beschreibungen zu einzelnen Vorgehensweisen sind nicht vorhanden und es wird ein allgemein strategischer Ansatz verfolgt.

5.6.22 Nur Einführung oder Überprüfung und Weiterführung

In der Guideline werden umfassend alle Schritte, von den Vorbedingungen über Implementierung bis hin zu Review und kontinuierlicher Verbesserung, besprochen (ASIS SPC.1-2009, 2009 S. vii-ix).

5.6.23 Ergänzendes Material

Auf der Homepage des ASIS finden sich verschiedene Informationen. Einerseits gibt es diverse Konferenzen und Schulungen die sowohl speziell auf diesen Standard, als auch allgemeiner auf relevante Themen, ausgerichtet sind. Zusätzlich gibt es eine digitale Bibliothek, in der informative Unterlagen bezogen werden können. Abschließend ist weiter eine E-learning-Plattform vorhanden, auf der verschiedene Lerninhalte verfügbar sind (ASIS-Education). Die meisten dieser Inhaltspunkte sind so aufgebaut, dass sie auf eine Zertifizierung abzielen.

Zusätzlich gibt es eine umfangreiche Liste mit Case Studies, Guidelines, Reports und White Papers zu dem Thema Informationssicherheit. Dieses beziehen sich nicht ausschließlich auf diesen Standard, sondern allgemein auf das Thema Security. Daneben sind auch Dokumente die für Informationssicherheit verfügbar (ASIS - Toolkit).

5.6.24 Phasen

Prinzipiell ist der Standard in zwei Teile geteilt: einerseits der eigentliche Standard (Organizational Resilience Management System Requirements, Kapitel 4) und andererseits der als Anhang A definierte Teil „Guidance On The Use Of The Standard“.

Der Standard beginnt mit einer allgemeinen Einleitung sowie der Definition des Zuständigkeitsbereiches. Danach folgen Referenzen und der Verweis auf die Begriffsdefinitionen in Anhang D.

Der Hauptteil gibt zu Beginn eine allgemeine Definition und eine Definition des Zuständigkeitsbereiches des Systems.

Anschließend wird die Management-Policy definiert, und zwar wird sowohl der Inhalt als auch die Rolle des Managements.

Des Weiteren folgt die Planungsphase, wobei zuerst ein Risiko-Assessment und eine Impact-Analyse ausgeführt werden. Rechtliche und sonstige Anforderungen werden ebenso geklärt wie die Ziele festgelegt werden.

In der Guideline folgt im Anschluss die Implementierung und Operation, wofür zuallererst Ressourcen, Rollen und Verantwortlichkeiten geklärt werden. Daran anschließend werden Trainingsmaßnahmen besprochen, um jeden Betroffenen optimal vorbereiten zu können. Die beiden nächsten Themen betreffen die Dokumentation sowie die Kontrolle der Dokumente. Nach einer kurzen Erklärung zum Thema operationale Kontrolle wird abschließend in diesem Kapitel behandelt, welche Maßnahmen gesetzt werden sollen um Vorfälle vorzubeugen beziehungsweise darauf vorbereitet zu sein.

Im nächsten Kapitel folgt der Themenblock Evaluation, wobei zuerst das Monitoring festgelegt wird. Danach sollen Übungen und Tests durchgeführt werden. Bei Problemen, sollen korrigierende Maßnahmen ergriffen werden. Der nächste Block behandelt die Kontrolle der Aufzeichnungen, welche durchgehend aufrechterhalten werden muss. Am Ende dieses Kapitels werden ergänzende Ratschläge zur Frage der internen Audits gegeben.

Das Thema Management-Review schließt den Hauptteil ab. Hier wird erklärt, welche Inputs und Outputs diese Reviews haben sollen. Auch der Pflege und Verbesserung dieser Reviews ist jeweils ein Punkt gewidmet.

Anhang A gibt, wie bereits einleitend erwähnt, zusätzliche Informationen und soll dabei helfen, die Anforderungen aus dem Hauptteil besser umzusetzen. Dabei sollen diese Ratschläge hauptsächlich informativer Natur sein, und an dem eigentlichen Standard dadurch nichts geändert werden. Daher sich der Benutzer im Zweifelsfall an den Standard halten und nicht an den Anhang. Der Aufbau des Anhangs A ist entsprechend dem Aufbau des Hauptteiles.

Anhang B beschreibt die Kompatibilität zu anderen Management-Systemen, speziell den ISO-Normen ISO 9001:2000, ISO 14001:2004, ISO/IEC 27001:2005 und ISO 28000:2007 (siehe 5.6.19). Eine Tabelle gibt an, wo die einzelnen Punkte des Aufbaus des ASIS-Standards auf die jeweiligen Inhalte in den genannten ISO-Standards umgelegt werden.

Anhang C beschreibt die Konventionen zu verschiedenen Ausdrücken, um eindeutige Klarheit zu schaffen.

Anhang D ist eine Begriffserklärung für alle Begriffe dieses Dokuments, die missverständlich verstanden werden können.

Anhang E beschreibt die Einschränkungen, aber auch Bedingungen zur Anwendung des Standards.

Der letzte Anhang schließlich betrifft das Literaturverzeichnis.

5.6.25 Beratung & Support

Durch seine Internationalität und seine große Mitgliederanzahl bietet das ASIS ein umfangreiches Networking an, allerdings keinen Support.

5.6.26 Befolgung der Richtlinien der Aufsichtsbehörden

Da das ASIS eine internationale Organisation ist (wenn auch mit Schwerpunkt auf den US-amerikanischen Markt), können keine Richtlinien von Aufsichtsbehörden befolgt werden. Es werden aber auch keine verpflichtenden Maßnahmen gesetzt, sondern die Vorgaben sind flexibel aufgebaut. Dadurch kommt es kaum zu Problemen mit diversen Richtlinien. Auch ist hier, ähnlich wie bei den legalen Aspekten (siehe 5.6.11) explizit erwähnt, dass Richtlinien und Gesetze jeweils über den zu implementierenden Maßnahmen stehen (ASIS SPC.1-2009, 2009 S. ii-iii).

5.6.27 Befolgung von internationalen IT-Standards

Durch die starke Verbindung zu diversen ISO-Standards wird vor allem der ISO 27001 Standard aktiv unterstützt. Andere IT-Standards werden nicht aktiv unterstützt, auch wenn eine Kompatibilität durch die hohe Flexibilität und die Kompatibilität zu diversen ISO-Normen nicht ausgeschlossen werden kann. (ASIS SPC.1-2009, 2009 S. vii, 41-43)

5.7 SP800-34

5.7.1 Sprache

Der Standard ist ausschließlich in englischer Sprache verfügbar.

5.7.2 Ort der Entstehung

Die Guideline ist in den Vereinigten Staaten von Amerika entstanden. Die dafür zuständige Behörde, das NIST (siehe 5.7.14), ist die US-Amerikanische Standardisierungsbehörde. (NIST 800-34, 2002 S. 1)

5.7.3 Zeit der Entstehung

Die erste und bislang einzige Version dieses Standards ist am 11. Juni 2002 publiziert worden. Seither ist an der Guideline keine Änderung mehr vorgenommen worden. Im Zuge der Recherche konnte auch nicht festgestellt werden, ob in nächster Zeit eine erneuerte Version geplant ist.

5.7.4 Verfügbarkeit

Der Standard ist frei verfügbar, ein Copyright besteht nicht.

5.7.5 Art

Der Aufbau des SP800-34 ist textuell. Auf über 100 Seiten werden die Themen ausführlich erklärt, Bilder und Tabellen lockern das Bild auf. Die Sprache des Standards ist für ein solches Dokument einfach und klar gehalten, das wird dadurch vereinfacht. Es wird mit vielen Beispielen gearbeitet, sodass das Verständnis auch von unbekannten Vokabeln relativ einfach ist. Dadurch fällt es auch nicht übermäßig ins Gewicht, dass das Glossar relativ dürftig ist.

5.7.6 Vorhandene Tools zur Unterstützung

Tools speziell für diesen Standard sind nicht vorhanden. Kommerzielle Produkte können verwendet werden, jedoch ist kein Tool ausschließlich auf dieses Werk zugeschnitten.

5.7.7 Allgemein/branchenspezifisch

Prinzipiell ist der Guide so geschrieben, dass er für alle Unternehmen in verschiedensten Branchen verwendbar ist, obwohl er speziell für öffentliche Institutionen gedacht ist. Hier im Besonderen für solche, die mit sensiblen Informationen arbeiten. Für diese Unternehmen ist er besonders ausgelegt. Der Standard ist zwar auch ein BC-Guide, jedoch wird in erster Linie die IT behandelt. Daher macht dieser Standard vor alle für jene Organisationen und Unternehmen Sinn, welche eine starke Abhängigkeit von allen Arten von Informationstechnologie haben (NIST 800-34, 2002 S. 1-3).

5.7.8 Unternehmensgröße

Begrenzungen bezüglich der Unternehmensgröße sind nicht existent. Dessen ungeachtet ist der Standard so entstanden, dass er auf öffentliche Institutionen ausgerichtet ist. Daher ist ein Schwerpunkt auf größere Organisationen beziehungsweise Unternehmen festzustellen, jedoch ist ein Großteil der Maßnahmen auf sämtliche Unternehmensgrößen anwendbar (NIST 800-34, 2002 S. 1-3).

5.7.9 Art der Verfügbarkeit

Der Standard ist ausschließlich im Format PDF auf der Homepage des NIST zu finden (NIST 800-34 - Download). Andere Vertriebswege sind nicht verfügbar.

5.7.10 Möglichkeiten zur Zertifizierung

Die Möglichkeit sich nach diesem Standard zertifizieren zu lassen besteht nicht. Weder Personen- noch Unternehmenszertifizierungen sind vorhanden.

5.7.11 Rechtliche Begrenzungen

Da dieser Standard besonders für US-amerikanische, öffentliche Institutionen ausgelegt ist, sind auch die rechtlichen Begrenzungen in dieser Richtung zu finden. Er ist kompatibel mit diversen US-Gesetzen und daher für diese Organisationen geeignet. Bei Anwendung dieses Standards aber außerhalb des Wirkungsbereiches dieser Gesetze (einerseits außerhalb der Landesgrenzen, andererseits in der Privatwirtschaft), sind diese Gesetze zu beachten, daher sind diese Beschränkungen in diesem Fall nicht gültig (NIST 800-34, 2002 S. 1).

5.7.12 Flexibilität

Der SP800-34 ist in gewissen Bereichen auffällig flexibel. Vor allem Kapitel fünf beschreibt Bereiche, die zwar nicht auf jedes Unternehmen zutreffen, aber je nach Bedarf verwendet werden können. Auch die sonstigen Punkte sind variabel an die jeweilige Situation adaptierbar.

5.7.13 Organisatorisch/kulturell

Ein besonderer Eingriff in die Organisation kann nicht festgestellt werden.

5.7.14 Welche Organisation steht dahinter?

Das National Institute of Standards and Technology (NIST) ist eine Bundesbehörde (federal agency) der USA und dem Handelsministerium (U.S. Department of Commerce) unterstellt. Sitz der Behörde ist in Gaithersburg, Maryland und Boulder, Colorado (jeweils USA). Sie hat ein Gesamtbudget von über 1,6 Milliarden US-Dollar und beschäftigt über 2900 Mitarbeiter sowie mehrere tausend Spezialisten und Akademiker.

Die Aufgaben des NIST gliedern sich in vier Teile: 1) Das Baldrige National Quality Program, welches sich mit der Förderung von Spitzenleistungen in US-amerikanischen Unternehmen befasst, 2) die Hollings Manufacturing Extension Partnership, welche ein US-

weites Netzwerk von Büros darstellt, die sich mit der technischen Unterstützung von kleineren Betrieben beschäftigt, 3) das Technology Innovation Program, welches Preise für besonders innovative Produkte in verschiedenen Bereichen vergibt und 4) verschiedene Forschungslabors, die helfen sollen die technische Infrastruktur in den USA zu verbessern. Zehn unterschiedliche Labors, wobei eines davon, das Information Technology Laboratory, für den SP800-34 Standard zuständig ist (NIST - About), stehen zur Verfügung.

5.7.15 Vorlage/Querverbindungen zwischen den Guides

Eine Querverbindung zu anderen Guidelines konnte nicht hergestellt werden. Dies erklärt sich einerseits vermutlich durch das vergleichsweise hohe Alter des Standards (siehe 5.7.3), andererseits durch die regionale Beschränkung auf die Vereinigten Staaten von Amerika. Auch die starke Fokussierung auf die IT-Branche mag dafür verantwortlich sein.

5.7.16 Zielgruppe

Als Zielgruppe können all jene Mitarbeiter gesehen werden, die sich mit dem Thema Business Continuity beschäftigen. Im Dokument selbst sind verschiedene Gruppen genannt: Manager, Systemadministratoren, Information System Security Officers, System-engineers and -architects, andere User und weiteres Personal, welches für verschiedene Aufgaben im Informationssystem zuständig sind. Grundsätzlich sind für all diese Gruppen verschiedene Teile relevant, der Standard ist besonders für die zuerst genannten Gruppen der Manager und Systemadministratoren relevant (NIST 800-34, 2002 S. 1,4).

5.7.17 Gegebene Templates

Zwei umfangreiche Templates sind im SP800-34 gegeben.

Anhang A zeigt ein Template für einen Notfallplan. Dieser umfangreiche Plan ist als Gerüst zur Erstellung eines eigenen Plans gedacht, wozu dieser nach Belieben erweitert beziehungsweise verändert werden. In diesem Template sind in kursiver Schrift immer wieder Erklärungen und Hinweise auf verschiedene Probleme angeführt. Das Template ist in sechs Teile geteilt: 1) Einleitung, 2) Konzept des laufenden Betriebs, 3) Alarmmeldung und Aktivierung des Planes, 4) Operationen zur Wiederherstellung des Betriebs, 5) Rückführung zum Normalbetrieb und 6) Anhänge an den Plan.

Anhang B ist eine beispielhafte Business Impact-Analyse sowie ein Template. Dieses Template kann kopiert und anschließend je nach Bedarf verändert und angepasst werden.

Zusätzlich zu diesen beiden umfangreichen Templates sind im Standard selbst einige kleinere Templates gegeben, die eine Mischung aus Template und Beispiel darstellen. Hier sind zu nennen: Recovery Strategy Budget Planning Template (Tabelle 3-2), Sample Record of Changes (Tabelle 3-3) und Contingency Strategies Summary (Tabelle 5-2).

5.7.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.7.19 Integration von Organisationsprozessen

Der Schwerpunkt dieses Standards liegt auf der IT-Continuity, die daher auch besonders unterstützt wird. Damit zusammenhängend werden auch verschiedene Softwareprozesse, wie Software-Entwicklungsprozesse und Release Management untersetzt. Zuletzt werden auch noch Verweise auf das Record-Management (Schriftgutverwaltung) angeführt.

5.7.20 Benötigte Vorkenntnisse

Dieser Guide ist so verfasst, dass er mit wenig oder keinen Vorkenntnissen zu verstehen ist. Falls trotzdem BCM-Wissen nötig ist, kann eine Vertiefung in den Wissensgebieten IT und Management vorgenommen werden.

5.7.21 Methoden

Die Methoden sind in dieser Guideline genau beschrieben, wobei Ratschläge gegeben und Vorgehensweisen besprochen werden. Ferner sind praktische Beispiele gegeben, welche das Verständnis des Besprochenen erleichtern. Oft sind außerdem Denkanstöße gegeben, welche das Erweitern von gegeben Methoden und das Erarbeiten von individuellen Vorgehensweisen erleichtern sollen.

5.7.22 Nur Einführung oder Überprüfung und Weiterführung

Sämtliche Phasen des Business Continuity Managements sind vorhanden, allerdings unterschiedlich ausführlich. Manche Phasen werden angerissen (zum Beispiel die Initialisierung des Prozesses), andere wiederum sind ausführlich beschrieben (beispielsweise die Business Impact-Analyse) (NIST 800-34, 2002 S. 4-5).

5.7.23 Ergänzendes Material

Zu dem SP800-34 sind keine direkten unterstützenden Materialien gegeben. Allerdings sind in der Datenbank des NIST weitere Standards vorhanden die möglicherweise in gewissen Bereichen weitere Informationen geben. Beispielsweise gibt es den Standard SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response), welcher sich speziell mit Forensik bei Zwischenfällen beschäftigt. Diese weiteren Informationen sind jedoch eher zur Spezialisierung als zur zusätzlichen Information.

5.7.24 Phasen

Der SP800-34 ist in fünf Teile unterteilt und beginnt mit einer allgemeinen Einleitung. In dieser werden neben der zuständigen Behörde auch der Zweck und der Gültigkeitsbereich sowie Zielgruppe und die Struktur des Dokuments besprochen.

Kapitel zwei enthält einen weiteren allgemeinen Teil in dem der Hintergrund des BC besprochen wird. Sowohl der Zusammenhang zwischen Risiko- und Notfallmanagement als auch die verschiedenen Arten von Plänen werden hier behandelt (Tabelle 2-1). Abschließend wird der Notfallplan (Contingency Plan) und dessen Life-Cycle genauer erklärt.

In Phase drei wird der eigentlich Business Continuity-Zyklus mit der Planungsphase begonnen. Dieses Kapitel beschreibt den Prozess zur Erstellung eines solchen Planes. Nach einer kurzen einleitenden Übersicht wird mit dem Entwurf der Policy begonnen. Daran anschließend folgt der umfangreiche Block der Business Impact-Analyse. Aus den gewonnenen Daten sollen nun Möglichkeiten gefunden werden, präventive Maßnahmen zu setzen um einen Notfall zu vermeiden, anstatt ihn im Nachhinein zu behandeln. Da sich nicht alle Zwischenfälle vermeiden lassen, müssen weitere Schritte bestimmt werden, um mit einem solchen Fall umgehen zu können. Hier werden IT-spezifische Maßnahmen wie Backups, alternative Standorte und Ausrüstung, aber auch allgemeine Dinge wie Verantwortlichkeiten und Kostenplanung besprochen. Ist ein solcher Plan zur Notfallreaktion nun erstellt, gilt es diesen einerseits zu überprüfen und zu üben, andererseits zu pflegen und kontinuierlich zu verbessern. Diesen beiden Themen sind die abschließenden beiden Punkte dieses Kapitels gewidmet.

Kapitel vier beschreibt die Struktur des Planes, dessen Entstehung im letzten Kapitel erfasst wurde. Dieser Plan ist in fünf Teile unterteilt. Der erste Teil nennt sich „Supporting Information“ und enthält eine allgemeine Einleitung, welche sich mit Zweck und Gültigkeitsbereich sowie Zielgruppe und die Verantwortlichkeiten beschäftigt. Der zweite Teil (Notification/Activation Phase) beschreibt die ersten Aktivitäten, welche nach Eintreten eines Notfalls zu ergreifen sind. Hier wird zuerst besprochen, wer wen zu informieren hat, anschließend wird der Schaden bewertet und abschließend der konkrete Plan aktiviert. Die nun folgende „Recovery Phase“ führt die im Notfallplan aufgelisteten Maßnahmen aus und endet, wenn dieser umgesetzt ist und die IT wieder, wie im Vorhinein festgelegt, funktioniert. Der vierte Teil des Planes beschreibt die Maßnahmen, die zu ergreifen sind, um nach einem Notfall wieder den Normalbetrieb herzustellen. Der Anhang des Dokuments soll zum Beispiel Wegbeschreibungen, BIA und Kontaktinformationen für zuständiges Personal enthalten. Ein Musterbeispiel für einen solchen Plan ist in Anhang A des SP800-34 enthalten.

Das abschließende fünfte Kapitel des SP800-34 beschäftigt sich mit ergänzenden Maßnahmen und Ratschlägen für IT-spezifische Angelegenheiten im Falle eines Notfalles. Diese Maßnahmen sollen dabei helfen, IT-Strukturen möglichst effizient für den Notfall vorzubereiten. Dabei werden folgende sieben Informations-technologische Bereiche beschrieben:

- Desktop Computer und tragbare Systeme (zum Beispiel Laptops)
- Server
- Webseiten
- Local area networks
- Wide area networks
- Verteilte Systeme
- Mainframe Systeme

Für jede dieser Plattformen werden zwei Ansätze diskutiert: Einerseits die Faktoren, die für die Umsetzung des Notfallplanes beachtet werden müssen (Contingency Considerations), andererseits Lösungsansätze für verschiedene Probleme, die mit diesen Systemen auftreten (Contingency Solutions). Hier sind beispielsweise die Häufigkeit der Backups oder die Redundanz der Systeme zu nennen.

Abschließend folgen acht Anhänge. Der erste ist ein Beispiel für den Aufbau eines Notfallplanes (siehe Kapitel vier). Anhang B ist ein Beispiel beziehungsweise ein Template für eine BIA (siehe Kapitel drei). Der dritte Anhang beschäftigt sich mit häufig gestellten Fragen zu dem Thema Notfallmanagement. Anhang D befasst sich im Überblick mit einem nicht-technischen Teil des Notfallplanes, nämlich mit dem Umgang mit den Angestellten im Notfall. Dies ist allerdings nicht der Schwerpunkt dieses Standards und wird daher in einer knappen Ausführung mit Verweis auf andere, genauere Quellen behandelt. Anhang E ist eine Worterklärung die sich mit den wesentlichen Begriffen beschäftigt. Anhang F zählt weitere Quellen zu diesem Thema auf, während Anhang G das Literaturverzeichnis enthält. Der Standard schließt mit einem Index.

5.7.25 Beratung & Support

Zu diesem Guide gibt es kommerziellen Support. Das NIST selbst bietet keinen Support und keine Beratung an, weder für Personen noch für Unternehmen.

5.7.26 Befolgung der Richtlinien der Aufsichtsbehörden

Der Standard befolgt die Richtlinien der US-Amerikanischen Gesetze. Hier wird zum Beispiel der Information Technology Management Reform Act (Clinger-CohenAct) behandelt. Sollte der Standard außerhalb von US-Amerikanischen Regierungsorganisationen verwendet werden, kann keine Garantie auf Kompatibilität mit diversen Aufsichtsbehörden gegeben werden (NIST 800-34, 2002 S. 1).

5.7.27 Befolgung von internationalen IT-Standards

Von dem Standard werden keine IT-Standards vollständig unterstützt. Demgegenüber ist durch die hohe Fokussierung auf die IT davon auszugehen, dass mehrere Standards zumindest teilweise unterstützt werden. Namentlich werden die zur Zeit der Entstehung des SP800-34 aktuellen Standards PAS 77 und ISO 1779 soweit unterstützt, dass der SP800-34 dabei hilft, diese zu implementieren. Daher kann auch davon ausgegangen werden, dass die jeweiligen Nachfolger dieser beiden Standards (PAS 77:2006 und ISO/IEC 27002) auch zumindest teilweise unterstützt werden.

5.8 NFPA 1600-2007

5.8.1 Sprache

Der Standard ist in Englisch und in Spanisch verfügbar.

5.8.2 Ort der Entstehung

Der Standard ist den Vereinigten Staaten von Amerika entstanden.

5.8.3 Zeit der Entstehung

Der Standard wurde erstmals im Jahr 1995 unter dem Titel "Recommended Practice for Disaster Management", damals noch als „recommended practice“, publiziert. Die darauffolgende Version aus dem Jahr 2000 war bereits ein Standard in dem Sinn, dass es

verpflichtende Bereiche gab. Hier wurde auch erstmals ein umfassender Ansatz zu dem Thema Notfallmanagement mit Elementen der Business Continuity verwendet. Die Version aus dem Jahre 2004 stand noch spürbar im Zeichen der Ereignisse vom 11.September 2001 in New York. Die amerikanische Regierung (namentlich der 9/11 Comission Report) empfahl (Comission on Terrorist Attacks) auch privaten Unternehmen, ein BCM zu implementieren und nannte dafür den eigens dafür adaptierten NFPA 1600. Die zurzeit aktuelle Version aus dem Jahre 2007 wurde vor allem um die Prävention erweitert (NIST 800-34, 2002 S. 1). Zurzeit ist die nächste Revision im Gange.

5.8.4 Verfügbarkeit

Die englischsprachige Version ist im Format PDF gratis herunterzuladen (NFPA 1600, 2007). Die spanischsprachige Version, alle Buchformen und sämtliche älteren Versionen sind kostenpflichtig und kosten USD 39,50 pro Stück.

5.8.5 Art

Der Aufbau des NFPA 1600 ist größtenteils listenförmig, wobei jeder Listenpunkt aus einer kompakten Anweisung besteht. Erst im Anhang, der dann auch als erklärendes Material bezeichnet wird, sind grundlegende Informationen ausführlicher erklärt.

5.8.6 Vorhandene Tools zur Unterstützung

Abseits der allgemeinen, kommerziellen Tools sind zu diesem Standard keine spezifischen Tools verfügbar.

5.8.7 Allgemein/branchenspezifisch

Der Standard ist allgemein gehalten und lässt keine Ausrichtung auf eine bestimmte Branche erkennen. Der Standard ist bewusst allgemein gehalten, sodass keine Begrenzungen auftreten.

5.8.8 Unternehmensgröße

Bei der Überprüfung kann keine Begrenzung auf eine bestimmte Unternehmensgröße festgestellt werden. Der Standard soll für alle Organisationen jeder Größe valid sein.

5.8.9 Art der Verfügbarkeit

Der Standard ist als PDF und als Buch verfügbar. Im Shop des NFPA (NFPA-Shop) sind auch ältere Versionen (2000,2004) verfügbar.

5.8.10 Möglichkeiten zur Zertifizierung

Derzeit besteht keine Möglichkeit zur Zertifizierung, weder für Personen noch für Organisationen. Allerdings kann eine Befolgung in den Vereinigten Staaten von Amerika insofern beachtenswert sein, als dass eine Befolgung dieser Richtlinien im Falle eines Rechtsstreits nach einem Vorfall als entlastend gilt.

Im Anhang D des Dokuments wird eine ganze Liste an Organisationen aufgelistet, welche Akkreditierungs- und Zertifizierungsprogramme anbieten. Allerdings ist nicht angegeben, ob

einige oder alle dieser Organisationen eine Zertifizierung nach dem NFPA 1600 anbieten. Die meisten dieser angegebenen Organisationen sind in den USA beheimatet, weiters sind auch internationale Organisationen wie das BSI in Großbritannien angegeben.

5.8.11 Rechtliche Begrenzungen

Rechtlichen Begrenzungen sind nicht gegeben.

5.8.12 Flexibilität

Der Standard ist nicht flexibel, offensichtlich da er nur die wichtigsten Punkte darlegt und diese verpflichtend sind. Daher muss der Standard, um ihn in jeder Hinsicht einzuhalten, Punkt für Punkt implementiert werden. Einzig in der Ausführung ist der Anwender flexibel, da keine Methoden oder Ratschläge zur Umsetzung gegeben werden. Die in Anhang A gegebenen zusätzlichen Informationen sind nicht verpflichtend, daher kann hier flexibel an den Guide herangegangen werden.

5.8.13 Organisatorisch/kulturell

In diesem Standard kann kein besonderer Eingriff in die organisatorische oder kulturelle Struktur eines Unternehmens festgestellt werden.

5.8.14 Welche Organisation steht dahinter?

Die National Fire Protection Association (NFPA) wurde im Jahr 1896 in den USA gegründet. Das Hauptquartier dieser Organisation ist in Qunicy, Massachusetts. Ihre Aufgabe ist es, die Auswirkungen von Feuer und anderen Risiken weltweit zu verringern. Dies erreicht sie durch das Erarbeiten von Standards, durch Forschung und Training sowie durch Bildungsarbeit (NFPA-About). Diese Organisation hat bereits über 300 Standards publiziert und ist selbst Mitglied in verschiedenen Gremien. Obwohl die NFPA eine vorwiegend US-Amerikanische Organisation ist, hat sie 75.000 Mitglieder aus der ganzen Welt. Über 80 verschiedene Unternehmen, primär aus den Vereinigten Staaten von Amerika, unterstützen sie. Das beste Beispiel für Bildungsarbeit der NFPA ist Sparky the Fire Dog, ein in den USA bekannter und beliebter Comic-Hund, der Kindern den Umgang mit verschiedenen Gefahrensituationen nahebringen soll.

5.8.15 Vorlage/Querverbindungen zwischen den Guides

Bei der Recherche konnte keine Querverbindung zu anderen Standards hergestellt werden. In dem Dokument selbst werden ausschließlich andere Standards der NFPA referenziert. Zusätzlich lediglich werden nur Kontaktdaten von verschiedenen Organisationen gegeben welche sich auch mit diesem Thema befassen, beziehungsweise im Notfall Ansprechpartner in der jeweiligen Region sind. Diese Kontaktdaten sind hauptsächlich auf die Vereinigten Staaten von Amerika beschränkt.

5.8.16 Zielgruppe

Die Zielgruppe des NFPA ist das Management. Hier sind sowohl das obere Management als auch der ausführende Teil der Manager angesprochen. Nicht geeignet ist der Standard als

Einführung in das Thema sowie für Mitarbeiter, die sich ausschließlich mit den Auswirkungen des BC-Prozesses beschäftigen müssen.

5.8.17 Gegebene Templates

Im NFPA 1600 sind keine Templates gegeben.

5.8.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.8.19 Integration von Organisationsprozessen

Derzeit konnte keine Integration von Organisationsprozessen festgestellt werden, die über Risikomanagement und Business Continuity hinausgehen.

5.8.20 Benötigte Vorkenntnisse

Sämtliche Anweisungen in diesem Dokument sind minimalistisch, somit bleibt die Arbeit der Erfahrung und dem Vorwissen des Anwenders überlassen. Vorwissen ist vor allem für die anfängliche Einführung in das Thema notwendig. Hierzu hat die NFPA auch einen eigenen Guide herausgegeben (NFPA-Guideline). Zur weiteren Anwendung sind vor allem Wissen im Bereich BC und Notfallmanagement notwendig, sowie Vorbildung im Bereich Projektmanagement.

5.8.21 Methoden

Die Beschreibung der Methoden im NFPA 1600 ist allgemein gehalten. Zu Vorgehen oder Ablauf werden keine Ratschläge gegeben. Ferner sind weder Rahmenbedingungen noch ergänzende Hinweise zu den Methoden gegeben.

5.8.22 Nur Einführung oder Überprüfung und Weiterführung

Es werden alle Phasen des BC-LifeCycle behandelt. Es werden zwar nicht alle Teile ausführlich ausgeführt, aber eine Grundinformation ist zu allen Teilen vorhanden. Vor allem die beide Phasen Testen und Erhaltung des BCM sind eher oberflächlich beschrieben.

5.8.23 Ergänzendes Material

In der digitalen Bibliothek der NFPA steht eine Einleitung zu dem Standard NFPA 1600 (NFPA - Guideline) zur Verfügung. Diese soll die Arbeit mit dem Standard erleichtern und bietet zahlreiche Formulare, Templates und Beispiele zu diesem Standard.

5.8.24 Phasen

Nach rechtlichen Abgrenzungen und einer Liste aller an der Erstellung beteiligter Personen, folgt der eigentliche Standard.

Dieser beginnt mit der üblichen allgemeinen Einleitung, in der Zielgruppe, Zweck und Anwendbarkeit beschrieben sind. Nach den referenzierten Publikationen folgt die

Begriffsdefinition, in der die wichtigsten Begriffe erklärt werden. Kapitel vier beschreibt das Management, welches das Programm ausführen soll. Auch die Evaluation des Programms fällt in diesen Bereich. Kapitel fünf beschreibt nun das Programm beziehungsweise dessen Elemente. Nach der allgemeinen Einleitung und den rechtlichen Rahmenbedingungen folgt als nächster Punkt das Risk Assessment. Darauf folgen die Prävention beziehungsweise Verringerung der Auswirkungen der Vorfälle. Der sechste Punkt befasst sich mit dem Management und der Logistik von allen Arten von Ressourcen. Danach folgt eine Erklärung zur gegenseitigen Hilfe zwischen Unternehmen. Anschließend wird das Planen besprochen. Hierbei werden in Unterpunkten sowohl der Prozess als auch die Art der zu erstellenden Pläne definiert. Der neunte Teil befasst sich mit dem Management von Zwischenfällen und der nächste Teil ist dem Thema Kommunikation gewidmet. Hier soll festgelegt werden, wer mit wem in welchen Fällen zu kommunizieren hat. Danach sollen aufbauend auf die Risikoanalyse Prozeduren erstellt werden, welche es ermöglichen, im Notfall richtig zu handeln. Der zwölfte Teil des BC-Programms befasst sich mit den örtlichen Anlagen beziehungsweise deren Lage im Notfall. Aufbauend auf den bisher genannten Maßnahmen und dem Training, das nun erklärt wird, werden im nächsten Punkt Bewertungen sowie korrigierende Maßnahmen erörtert. Bevor im letzten Punkt finanzielle und administrative Maßnahmen besprochen werden, wird noch auf die öffentliche Kommunikation, sowohl mit Medien als auch mit anderen öffentlichen Organen, eingegangen.

Der nun folgende Anhang A stellt zusätzliches erklärendes Material dar. Im Text des Standards wird mit Sternchen oftmals auf diesen verwiesen. Dieser Anhang ist ausschließlich erklärend, daher rechtlich nicht relevant, und übernimmt die Kapitelnummern des eigentlichen Standards. Dieser erklärt, wo notwendig, detaillierter den Vorgang. Da die Autoren den Standard selbst minimalistisch gestaltet haben, ist dies oft auch notwendig, um den Sinn hinter bestimmten Schritten zu erkennen.

Anhang B zählt diverse Organisationen auf, die im Feld der Business Continuity aktiv sind. Diese Organisationen sind zum Großteil nordamerikanische Behörden, wobei auch einige internationale Organisationen genannt werden.

Anhang C gibt zusätzliche Adressen an, welche indirekt mit BC zusammenhängen. Hier sind zum Beispiel Ärzte oder Chemiker genannt, die im Notfall kontaktiert werden können. In diesem Anhang sind die Adressen ausschließlich auf die Vereinigten Staaten von Amerika beschränkt.

Anhang D listet verschiedene Organisationen auf die Zertifizierungen und Akkreditierungen anbieten, welche in diesem Bereich erlangt werden können. Hier sind Organisationen aus aller Welt vertreten (beispielsweise das Business Continuity Institute (BCI) aus dem Vereinigten Königreich von Großbritannien).

In Anhang E wird ein Incident Management-System (IMS) beschrieben. Dieses System soll in einem Unternehmen verankert sein und enthält eine Mischung aus allen für das BCM relevanten Bereichen wie Ausrüstung, Personal, Kommunikation und vieles mehr. Dieser Anhang stellt eine noch genauere Beschreibung für den schon in Anhang A erklärten Punkt dar. Weiters sind auch diverse Publikationen gelistet, welche sich näher mit diesem Thema befassen.

Anhang F sind Referenzen auf Material, welches für den Anwender dieses Standards interessant sein kann. Hier wird vor allem auf die anderen Standards der NFPA verwiesen.

Da Werk schließt mit einem Index.

5.8.25 Beratung & Support

Die NFPA bietet keinen direkten Support an. Allerdings stehen externe Unternehmen zur Verfügung die sich auf Beratung zu diesem Standard spezialisiert haben.

5.8.26 Befolgung der Richtlinien der Aufsichtsbehörden

Die Richtlinien der Vereinigten Staaten von Amerika werden befolgt. So kann davon ausgegangen werden, dass bei Einhaltung dieses Standards mögliche Auswirkungen eines Rechtsprozesses als Folge eines Zwischenfalles geringer ausfallen können. Außerhalb der USA kann dies aber nicht garantiert werden.

5.8.27 Befolgung von internationalen IT-Standards

Der NFPA 1600 Standard befolgt keine internationalen IT-Standards. Dies liegt auch daran, dass er sich wenig mit dem Bereich IT und mehr mit Notfallmanagement im Allgemeinen beschäftigt.

5.9 Telecommunications Resilience

5.9.1 Sprache

Der Guide ist nur in englischer Sprache verfügbar.

5.9.2 Ort der Entstehung

Die Guideline ist in Großbritannien entstanden. Die Organisation, die sie erstellt hat, ist dort für die Sicherheit der Infrastruktur zuständig.

5.9.3 Zeit der Entstehung

Die erste Version dieses Standards ist im Mai 2004 entstanden. Eine überarbeitete Version wurde im März 2006 publiziert. (Telecommunications Resilience, 2006 S. 2)

5.9.4 Verfügbarkeit

Der Standard ist frei auf der Homepage des Centre for the Protection of National Infrastructure verfügbar.

5.9.5 Art

Der Aufbau des Telecom Resilience ist textuell. In einfacher Sprache werden die Punkte des Standards präsentiert. Als Hilfe werden zusätzlich immer wieder Empfehlungen gegeben, welche dann am Schluss auch gesammelt wiederholt werden.

5.9.6 Vorhandene Tools zur Unterstützung

Es sind keine Tools verfügbar, die speziell auf diesen Standard ausgerichtet sind. Es können allerdings kommerzielle Tools für bestimmte Schritte, beispielsweise für die Risikoanalyse, verwendet werden.

5.9.7 Allgemein/branchenspezifisch

Der Standard ist auf keine Branche beschränkt und ist für jedes Unternehmen sinnvoll. Dies ist dadurch gegeben, dass er themenspezifisch ist, sich daher auf das Thema Telekommunikation beschränkt. Da dieses Thema in der heutigen Zeit für fast ausnahmslos jedes Unternehmen relevant ist, kann auch keine Einschränkung in der Nutzung festgestellt werden (Telecommunications Resilience, 2006 S. 6-7).

5.9.8 Unternehmensgröße

Die Guideline ist für jedes Unternehmen nutzbar und sinnvoll, unabhängig von seiner Größe. Einzelne Ratschläge sind allerdings erst ab einer relativ großen Unternehmensgröße sinnvoll. Doch im Allgemeinen ist diese Guideline für alle Organisationen nutzbar (Telecommunications Resilience, 2006 S. 6-7).

5.9.9 Art der Verfügbarkeit

Der Guide kann ausnahmslos von der Homepage des CPNI im Format PDF heruntergeladen werden. Andere Vertriebsarten konnten nicht recherchiert werden.

5.9.10 Möglichkeiten zur Zertifizierung

Eine Möglichkeit zur Zertifizierung konnte nicht festgestellt werden.

5.9.11 Rechtliche Begrenzungen

Es gibt keine rechtlichen Begrenzungen.

5.9.12 Flexibilität

Die Guideline ist flexibel. Relevante Teile können je nach Bedarf verwendet und adaptiert werden..

5.9.13 Organisatorisch/kulturell

Da dieser Standard einen kleinen Teil der Unternehmensstruktur, nämlich die Telekommunikation, betrifft, entsteht kein grober Eingriff in das Unternehmen.

5.9.14 Welche Organisation steht dahinter?

Der Guide wurde ursprünglich vom National Infrastructure Security Co-Ordination Centre erstellt. Diese staatliche Organisation des United Kingdom war für Schutz und präventive Maßnahmen vor elektronischen Angriffen auf kritische Infrastruktur im Vereinigten Königreich verantwortlich. Im Februar 2007 wurde das NISCC mit anderen Organisationen

zum Centre for the Protection of National Infrastrcture (CPNI) zusammengelegt. Diese Organisation ist jetzt die publizierende Stelle für diesen Standard. Ob dieser allerdings in der neuen Organisation weiterentwickelt wird, ist unklar (Telecommunications Resilience, 2006 S. 1).

5.9.15 Vorlage/Querverbindungen zwischen den Guides

Eeine Querverbindung zu anderen Guides konnte nicht festgestellt werden. Dies kann vor allem darauf zurückgeführt werden, dass dieser Standard themenspezifisch ist.

5.9.16 Zielgruppe

Der Standard ist für alle die sich berufsmäßig mit der Kommunikation beschäftigen gedacht, wobei hauptsächlich das Management angesprochen ist.. Aber auch anderen Angestellten, die sich mit Planung und Implementierung von Kommunikationswegen beschäftigen, sollte dieser Standard bekannt sein. (Telecommunications Resilience, 2006 S. 6-7)

5.9.17 Gegebene Templates

In der Guideline sind keine Templates gegeben.

5.9.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.9.19 Integration von Organisationsprozessen

Es konnte keine besondere Integration von bestimmten Organisationsprozessen festgestellt werden. Dies lässt sich durch die Spezialisierung auf ein bestimmtes Thema, nämlich Telekommunikation, erklären.

5.9.20 Benötigte Vorkenntnisse

Es werden keine großen Anforderungen von diesem Standard gestellt. Allerdings ist Grundwissen im Bereich der Telekommunikation von Vorteil. Vor allem bei gewissen Hardwareproblemen ist es dadurch einfacher, die Lösungen zu begreifen.

5.9.21 Methoden

Die Methoden sind allgemein gehalten, es werden keine genauen Umsetzungsrichtlinien gegeben. Einzig die beiden im Anhang gegebenen Fragebögen (zur Selbstevaluation und zur Bewertung des Kommunikationsanbieters) sind eine detailliertere Hilfe.

5.9.22 Nur Einführung oder Überprüfung und Weiterführung

Der Guide ist in dieser Klassifikation schwer einzuordnen da er sich auf ein bestimmtes Thema fokussiert und sich nicht allgemein mit BC-Maßnahmen beschäftigt. Doch in diesem eingeschränkten Themenbereich ist eine Spezialisierung auf die Einführung der Maßnahmen gesetzt. Es werden vor allem die Risikoanalyse und die Bewertung der Infrastruktur behandelt. Selbst die Anweisungen zu den Maßnahmen die ergriffen werden sollen sind sehr

allgemein gehalten. Dies lässt sich vor allem dadurch erklären, dass die Telekommunikationsnetze überall so unterschiedlich sind, dass keine spezifischeren Ratschläge gegeben werden können.

5.9.23 Ergänzendes Material

Ergänzendes Material konnte im Zuge der Recherche nicht gefunden werden.

5.9.24 Phasen

Der Aufbau des Telecommunications Rezipienten Standards ist aufgrund seines spezifischen Themas schwer in den ursprünglichen Kategorien einzuordnen.

Er beginnt mit einer Einleitung und der Festlegung des Schwerpunktes. In diesem zweiten Kapitel werden unter anderem das Ziel und die Struktur der Guideline festgelegt. Im dritten Kapitel wird definiert, wofür BC nützlich ist. Hier wird anhand der Telekommunikation von England, welches die örtliche Zielgruppe ist, erklärt, warum BC notwendig ist. Des Weiteren wird mit der Kommunikation in New York am 11. September ein Beispiel für notwendige BC-Maßnahmen in diesem Bereich gebracht.

Im vierten Teil des Guides wird behandelt, welche Art von Maßnahmen für die Ausfallssicherheit getroffen wird. Hier wird als erstes ein Risk-Assessment durchgeführt. Anschließend wird besprochen, wie mit den verschiedenen Gefahrenkategorien umgegangen werden soll. Danach werden noch verschiedene spezifische Maßnahmen aus dem Bereich Telekommunikation besprochen, beispielsweise die Abhängigkeit von einem Provider, die Sorgfaltspflicht bei der Auswahl desselben oder die Transparenz der Dienste eines Anbieters.

Das fünfte Kapitel beschäftigt sich mit der Findung einer effektiven Lösung. Hier werden zuerst verschiedenen Hardware-Architekturen angesprochen, die verwendet werden können. Danach wird über das Thema der Wiederherstellung, zuerst von Diensten, danach von Hardware, gesprochen. Abschließend werden Ratschläge zur Wahl des Providers gegeben.

Im sechsten Kapitel werden die Empfehlungen, die im gesamten Dokument gegeben werden, zusammengefasst.

Anschließend folgen ein Glossar und die Danksagungen.

Im ersten Anhang wird ein Fragebogen angegeben, der dabei helfen soll, sich selbst in Hinsicht auf das Risikomanagement zu bewerten. Dazu wird in verschiedenen Gruppen (zum Beispiel Dienste, Hardware, Abhängigkeiten) unterteilt.

Der abschließende zweite Anhang ist ebenfalls ein Fragebogen, der dazu dienen soll, bei der Wahl des Providers für die Telekommunikation zu helfen. Diese Fragen sollten den verschiedenen Anbietern gestellt und die Ergebnisse dann miteinander verglichen werden, um einen optimalen Weg zu finden.

5.9.25 Beratung & Support

Von der Organisation die den Standard zurzeit vertreibt wird weder Beratung noch Support angeboten. Dies mag auch daran liegen, dass die Organisation, die den Standard ursprünglich erstellt hat, nicht mehr existiert. Allerdings konnte nicht festgestellt werden, ob es früher Beratung oder Support gibt.

5.9.26 Befolgung der Richtlinien der Aufsichtsbehörden

Der Standard befolgt keine Richtlinien von Aufsichtsbehörden. Er ist so allgemein gehalten, dass dies auch nicht möglich ist. Der Standard spiegelt Best Practices wieder und hält sich nicht an Gesetze. Allerdings kann davon ausgegangen werden, dass bei der Implementierung dieses Standards wenige Probleme mit Gesetzen auftreten werden (Telecommunications Resilience, 2006 S. 5-7).

5.9.27 Befolgung von internationalen IT-Standards

Es konnte keine Übereinstimmung mit internationalen IT-Standards festgestellt werden, was aber vor allem daher kommt, dass wenige Bereiche in der IT berührt werden. Daher kann auch keine Übereinstimmung mit solchen Standards festgestellt werden.

5.10 Australien BCM

5.10.1 Sprache

Der Guide ist ausschließlich in englischer Sprache erhältlich. Erklärt wird das durch sein Herkunftsland.

5.10.2 Ort der Entstehung

Die Guideline wurde in Australien erstellt. Der Sitz der ANAO befindet sich in Canberra, die meisten der Mitarbeiter, die an diesem Guide mitgearbeitet haben, kommen aus Australien.

5.10.3 Zeit der Entstehung

Im Jahr 2000 wurde der Standard „Business Continuity Management: Keeping the wheels in motion“ publiziert. Neun Jahre später, am 4. Juni 2009, wurde die aktuelle Version veröffentlicht. Es wurden die aktuellsten Forschungsergebnisse eingebaut. Ein besonderer Schwerpunkt wurde auf die Benutzerfreundlichkeit gelegt und praktische Beispiele sowie Case-Studies eingebaut (ANAO-Building resilience in public sector entities, 2009 S. III).

5.10.4 Verfügbarkeit

Der Standard ist auf der Homepage des ANAO frei zum Download verfügbar (ANAO-Building resilience in public sector entities, 2009).

5.10.5 Art

Der Aufbau des Standards ist textuell, auf 174 Seiten folgen exakte Erklärungen. Fakten die im eigentlichen Standard nicht genau erklärt werden, werden im anschließenden Workbook genau und mit Beispielen erläutert.

5.10.6 Vorhandene Tools zur Unterstützung

Speziell für diesen Standard sind keine Tools verfügbar, allerdings kann auf die üblichen kommerziellen Tools zurückgegriffen werden.

5.10.7 Allgemein/branchenspezifisch

Der Guide ist branchenspezifisch zu sehen. Allerdings ist hier nicht eine Branche im herkömmlichen Sinn gemeint, sondern alle Arten von Regierungsorganisationen. Wie der Name der Guideline schon sagt, bezieht er sich vor allem auf Bereiche im öffentlichen Sektor. Ein Großteil der Ratschläge ist auch auf Unternehmen im privaten Sektor anwendbar, allerdings wurde auf dies keine besondere Rücksicht genommen (ANAO-Building resilience in public sector entities, 2009 S. 1-2, 8).

5.10.8 Unternehmensgröße

Da der Standard für Regierungsorganisationen geschrieben wurde und diese im Normalfall groß sind, ist der Guide insgesamt auf große Unternehmen angelegt (ANAO-Building resilience in public sector entities, 2009 S. 1-2).

5.10.9 Art der Verfügbarkeit

Der Standard ist ausschließlich digital zu erwerben, und auf der Homepage des ANAO entweder als PDF zum Downloaden oder als HTML (ANAO - HTML-Version) zur direkten Ansicht in einem Webbrowser verfügbar.

5.10.10 Möglichkeiten zur Zertifizierung

Es besteht keine Möglichkeit zur Zertifizierung.

5.10.11 Rechtliche Begrenzungen

Besondere rechtliche Begrenzungen konnten nicht festgestellt werden.

5.10.12 Flexibilität

Der Standard ist als flexibel zu betrachten. Durch den großen Umfang der Guideline können die Teile herausgesucht werden, die relevant sind. Dies wird auch durch die ausführlichen Erklärungen vereinfacht. Der Standard enthält Teile, die immer befolgt werden sollten, jedoch ist der Standard flexibel genug um auch nur einzelne Schritte ausführen zu können.

5.10.13 Organisatorisch/kulturell

Besondere Eingriffe in die Unternehmenskultur sind nicht notwendig.

5.10.14 Welche Organisation steht dahinter?

Das Australian National Audit Office (ANAO) (ANAO-About) ist eine staatliche australische Organisation, die sich primär mit der Bewertung und Überprüfung von staatlichen Organisationen im Auftrag des Parlaments beschäftigt. Dabei geht es in erster Linie um finanzielle Aspekte und Leistungsbewertungen. Diese Organisation gibt es bereits seit der ersten parlamentarischen Sitzung in Australien im Jahr 1901. Seit 1997 hat die Organisation erweiterte Rechte.

Um es den überprüften Organisationen zu vereinfachen, die geforderten Normen zu erfüllen, erstellt das ANAO zusätzlich Better Practice-Guides. Auch andere Publikationen und Seminare sollen dabei helfen, die Normen bestmöglich zu erfüllen (ANAO - Publications).

5.10.15 Vorlage/Querverbindungen zwischen den Guides

Der australische BC-Standard hat primär Verbindungen zu anderen Guides aus diesem Kontinent. Hier sind einerseits die beiden australischen Standards HB 221:2004 und HB 292:2006 zu nennen. Andererseits sind auch von derselben Organisation verfasste Werke maßgeblich in diesen Standard hineingeflossen. Hier sind diverse Berichte der ANAO über finanzielle Aspekte zu nennen (ANAO audits of the Financial Statements of General Government Sector Agencies), andererseits der Vorgänger dieses Standards, der „ANAO Business Continuity Management: Keeping the wheels in motion 2000“ (siehe →5.10.3). Auch andere australische Werke werden als Referenzen angeführt (ANAO-Building resilience in public sector entities, 2009 S. 6-7).

5.10.16 Zielgruppe

Das Dokument richtet sich besonders an das obere Management und die für BCM zuständigen Manager. Aber auch für alle anderen Mitarbeiter die sich mit diesem Thema beschäftigen ist der Guide interessant. Für den einfachen Mitarbeiter welcher nur die Auswirkungen des neuen Managements trägt, ist der Standard nicht notwendig.

5.10.17 Gegebene Templates

Im dem, diesem Standard beigefügten Workbook finden sich eine Vielzahl von verschiedenen Templates, die den gesamten Business Continuity-Prozess, wie er im Guide beschrieben ist, von der Planung über die Einführung bis hin zum Testen und Aktualisieren der Pläne, abdecken.

5.10.18 Benötigte Ressourcen

Nicht berücksichtigt.

5.10.19 Integration von Organisationsprozessen

In dem Standard werden mehrere Prozesse aufgeführt die integriert werden sollen. Dazu zählen Change Management (ANAO-Building resilience in public sector entities, 2009 S. 18-19), Records Management (ANAO-Building resilience in public sector entities, 2009 S. 40) und Corporate Governance (ANAO-Building resilience in public sector entities, 2009 S. 93).

5.10.20 Benötigte Vorkenntnisse

Zum grundlegenden Verständnis dieses Standards sind wenige Vorkenntnisse notwendig. Die meisten Vorgänge sind detailliert beschrieben und sind oft auch mit einem Beispiel genauer erklärt. Allerdings kann Vorwissen in den Bereichen BC und Risikomanagement sowie im Bereich der allgemeinen Betriebswirtschaftslehre hilfreich sein und erleichtert den Umgang mit den angeführten Prozessen.

5.10.21 Methoden

Die Methoden sind in dieser Guideline detailliert beschrieben. Vor allem in Kombination mit dem ebenfalls im gleichen Dokument vorhandenen Workbook ist eine genaue Beschreibung aller Vorgänge vorhanden. Gemeinsam mit zahlreichen Beispielen, Templates und Checklisten ist so eine umfangreiche Hilfe in den meisten Bereichen gegeben.

5.10.22 Nur Einführung oder Überprüfung und Weiterführung

Sämtliche üblichen Schritte eines Business Continuity Frameworks sind gegeben. Von der Analyse und Design, über die Einführung bis hin zu Training und permanenter Weiterentwicklung sind alle Bereiche vorhanden (ANAO-Building resilience in public sector entities, 2009 S. 9-12).

5.10.23 Ergänzendes Material

Ergänzendes Material ist nicht vorhanden. Lediglich im Anschluss an den eigentlichen Standard findet sich ein Workbook, in welchem genau an den Standard angepasst verschiedene Templates, Checklisten und weitere Beispiele vorhanden sind. Dieses weitere erklärende Material soll vor allem dabei helfen, den Standard auf seine eigenen Bedürfnisse anzupassen.

5.10.24 Phasen

Prinzipiell gliedert sich der Standard in zwei große Teile, und zwar einerseits die Guideline selbst, andererseits das daran angehängte Workbook.

Der Standard beginnt mit einer Einleitung, in der die Grundkonzepte vorgestellt und BCM definiert wird. Ferner werden auch Schlüsselbegriffe wie Risk Management und Inicdent Management definiert. Abschließend werden in der Einleitung Kriterien für Business Continuity Frameworks erarbeitet. Daher werden generische Charakteristika erarbeitet, und zwar jeweils für kleinere und größere Entitäten. Dazu wird noch die Stelle in diesem Guide genannt, an der diese Kriterien behandelt werden.

Das erste Kapitel trägt den Titel “Managing business continuity as an integrated program of work” und beschäftigt sich mit der Erstellung eines BC-Planes und der Integration desselben im Unternehmen. Daher werden auch die wichtigsten Begriffe definiert.

Das zweite Kapitel befasst sich mit der Einbettung des BCM in ein Unternehmen beziehungsweise in die Unternehmenskultur. Auch hier wird der Einfluss des BCM auf verschiedene Unterbereiche des Managements wie Change Managements besprochen.

Kapitel drei beschäftigt sich mit der Analyse des Unternehmens. Daher wird geklärt, wie ein Unternehmen seine Operationen und Umgebung analysieren kann. Es werden sowohl die Vorbedingungen als auch die Ausführung dieser Business Impact-Analyse besprochen. Diesem Teil wird in dem Dokument offensichtlich eine große Wichtigkeit zugesprochen da dieser Teile im Vergleich zu den anderen ausführlich beschrieben ist.

Im nächsten Teil werden auf Basis dieser Analyse die verschiedenen Schritte besprochen, die notwendig sind, um einen geeigneten BC-Ansatz zu erstellen. Hierzu werden die einzelnen Einflussfaktoren wie Personen, Technologien oder Kommunikationswege besprochen. Es wird auch von der Chance gesprochen, aus der Krise einen Vorteil zu schlagen.

Das fünfte Kapitel hat das Aufbauen von vorbereitenden Maßnahmen und Reaktionen im Notfall zum Thema. Es wird besprochen, welche Handlungen im Vorhinein gesetzt werden können um im Notfall die Auswirkungen einer Geschäftsunterbrechung zu minimieren. Andererseits wird aber auch geklärt, wie der Business Continuity Plan auszusehen hat um in solch einem Fall entsprechend reagieren zu können.

Das darauf folgende Kapitel widmet sich dem Eintritt eines Notfalles. Wie soll reagiert werden wenn ein solcher auftritt. In diesem Zusammenhang wird vor allem besprochen wie der Notfallplan aktiviert und angewendet werden muss. Ebenso wird auf die Zuständigkeiten eingegangen welche in den einzelnen Situationen notwendig sind. Am Ende des Kapitels wird auch auf die Rückkehr zum Normalbetrieb eingegangen.

Im letzten Kapitel des Standards wird das Üben und Aktualisieren des Standards besprochen. Es werden verschiedene Schritte besprochen, welche dazu dienen sollen, den Plan zu testen, zu aktualisieren und bestmöglich im Unternehmen zu integrieren.

Im folgenden Anhang sind zu jedem der genannten Kapitel noch weitere Informationen sowie Referenzen auf andere Standards zu finden.

Abschließend findet sich im selben Dokument neben dem Standard noch das Workbook. Dieses folgt im Aufbau den oben genannten Kapiteln und bietet zusätzliche Beispiele sowie Templates und Checklisten. Dieses Workbook soll das Verständnis erleichtern und den Standard für verschiedene Situationen etwas flexibler machen. Abbildung 5 zeigt den genauen Aufbau des Workbooks.

5.10.25 Beratung & Support

Das ANAO bietet für staatliche Organisationen Beratung an. Da sie die kontrollierende Gesellschaft für diese Betriebe ist, ist sie verpflichtet, auch Verbesserungsmöglichkeiten anzubieten. Für private Gesellschaften konnte kein Support festgestellt werden.

5.10.26 Befolgung der Richtlinien der Aufsichtsbehörden

Da das ANAO in Australien eine Aufsichtsbehörde ist, welche andere staatliche Betriebe überprüft (siehe 5.10.14), ist dieser Standard mit den derzeit geltenden Richtlinien

kompatibel. Der Guide soll es diesen Betrieben erleichtern, die geltenden Regeln bestmöglich umzusetzen.

5.10.27 Befolgung von internationalen IT-Standards

Internationale IT-Standards werden nicht unterstützt. Dies liegt daran, dass IT-Standards in dieser Guideline nicht vorkommen.

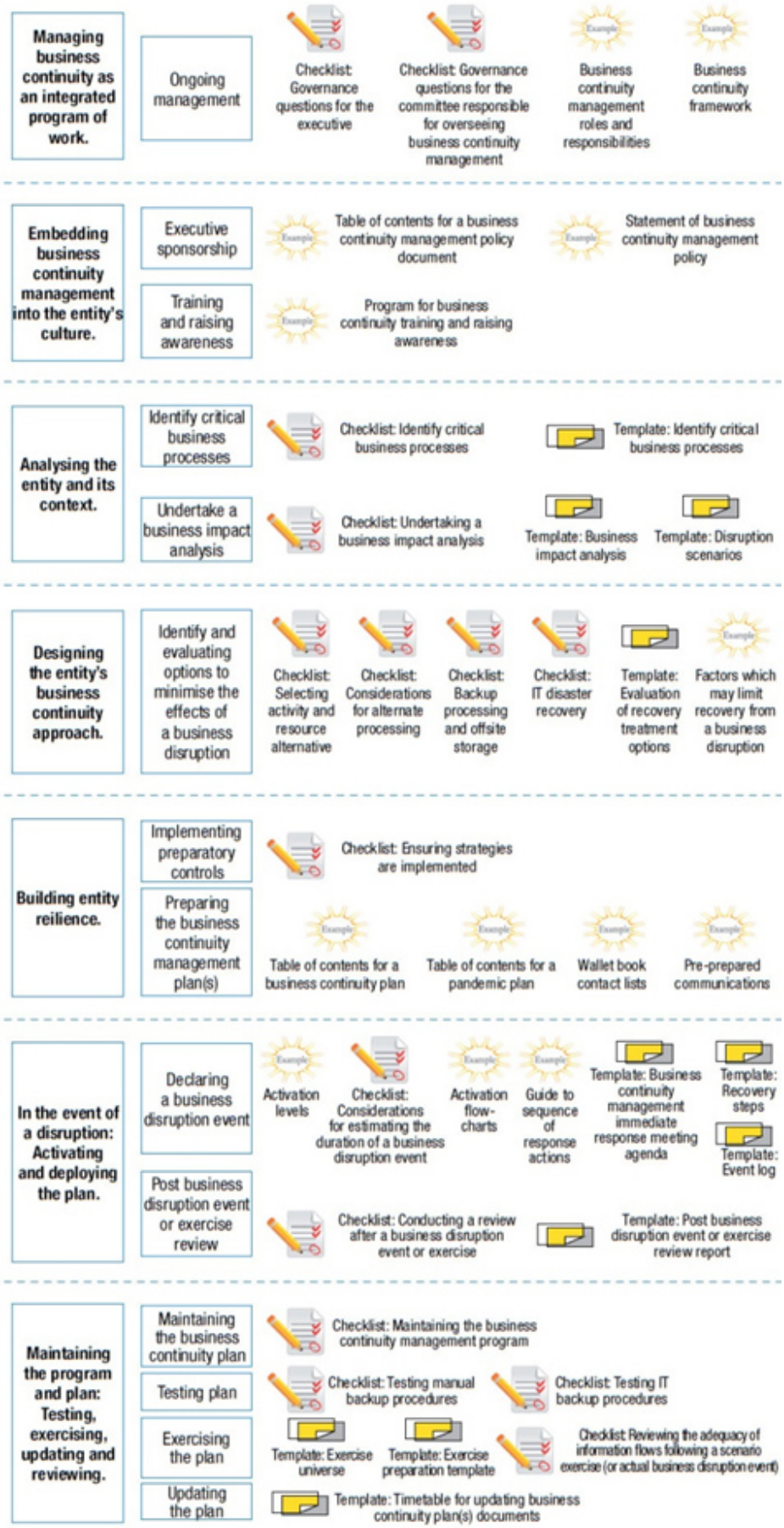

Abbildung 5 - (ANAO-Building resilience in public sector entities, 2009)

6 State-of-the-Art

Business Continuity Management ist ein Themenbereich, welcher von praktischen Ansätzen geprägt ist. Viele der Inputs und Weiterentwicklungen entstehen aus praktischen Erfahrungen. Hingegen ist die Menge der akademischen Forschung zu dem breit gefassten Thema BCM eher gering. Theoretische Untersuchungen zu allgemeinen Fragen, wie der Wirksamkeit oder der Effizienz der unterschiedlichen Ansätze, sind kaum zu finden. Auch ein Vergleich, wie er in der vorliegenden Arbeit vorgenommen wurde, kann nicht gefunden werden.

Bei genauer Prüfung des ganzheitlichen Business Continuity Managements in seine einzelnen Bestandteile, sind einige wissenschaftliche Ansätze ersichtlich.

Als Anhaltspunkte sollen die Grundphasen des BS 25999 genommen werden. Die erste Phase der Gliederung nach BS 25999 umfasst das Verstehen und Bewerten des eigenen Unternehmens. In diesen Bereich fallen Risikomanagement und Business Impact-Analyse. Werden diese beiden Themenbereiche unabhängig von BCM gesehen, liegt umfangreiche Literatur vor. Aber auch im Kontext des hier behandelten BCM liegen mehrere Arbeiten vor. Zum Beispiel beschreibt Cha in seiner Arbeit die unterschiedlichen Bedürfnisse hinsichtlich des Risikomanagements für reines Risikomanagements und Business Continuity (Cha, et al., 2008). In ihrer Arbeit findet sich auch einen Ansatz, diese beiden Prozesse möglichst zu vereinen und Redundanzen zu vermeiden. Tjoa verwenden Risk-Oriented Process Evaluation, um bei Management und Simulation von Geschäftsprozessen ausdrücklich auf den Faktor Risiko Rücksicht nehmen zu können (Tjoa, et al., 2007). Im Bereich RA und BIA lassen sich noch eine Vielzahl weiterer Ansätze finden, und zwar sowohl im Zusammenhang mit BC als auch unabhängig davon.

Der zweite Teil befasst sich mit der Entwicklung einer Strategie, welche auf den Ergebnissen der zweiten Phase aufbaut. Hier sind einige branchenspezifische Ansätze erkennbar. Anders gesagt wird beschrieben, welche Ansätze einzelne Unternehmen wählen um ein effizientes BCM zu implementieren. Arduini und seine Forschungskollegen bewerten die Wichtigkeit eines BC-Systems in der Finanzindustrie. Ferner wird begründet, weshalb gerade diese Branche besonders auf BCM bauen soll (Arduini, et al., 2010). Der Japaner Satoshi beschreibt den Einsatz eines BCM Systems im Bereich der Stromversorgung eines der größten Telekommunikationssysteme der Welt (der japanischen Nippon Telegraph and Telephone Corporation). Sie beschreiben einige Katastrophen aus der Sicht des Business Continuity Managements, besonders des Business Continuity-Plans (Satoshi, et al., 2008). Ein chinesisches Forscherteam um Wenxin fasst in seinem Paper die Probleme bezüglich der BC bei der Erstellung eines E-Government-Systemes in China zusammen (Wenxin, et al., 2008).

Als dritter Teil im Business Continuity Management kommt die Planungsphase. Die dazu vorgefundene Literatur beschäftigt sich primär mit verschiedenen Methoden, um gute Pläne zu erstellen. Neue Ansätze und Methoden werden entworfen, um die Planung zu verbessern. Die Art Verbesserungen divergieren hier stark. Die Ansätze reichen von allgemeingültigen Ratschlägen über mathematische Modelle bis hin zu alternativen Modelliersprachen. Kepenach gibt grundlegende Ratschläge, um den geeigneten BC-Plan zu entwerfen (Kepenach, 2007). Böhmer sucht einen formal-mathematischen Ansatz und verwenden Prozessalgebra und Modallogik um die BC-Pläne zu verifizieren (Boehmer, et al., 2009).

Zalewski versucht die Business Continuity-Pläne mit Hilfe der ARIS-Technologie zu implementieren und dadurch Simulationen der Pläne zu ermöglichen (Zalewski, et al., 2008).

In der letzten Phase des BS 2599 Lebenszyklus werden zuerst die Maßnahmen bewertet. Böhmer geht hier einen anderen Weg und versucht die Maßnahmen nicht nach der Durchführung zu bewerten, sondern diese anhand des Business Continuity Planes beziehungsweise des Disaster Recovery Planes ex-ante zu messen (Boehmer, 2009). Dies soll bei einer möglichst effizienten und frühen Leistungsmessung helfen. Zur Festigung des BCM in der Unternehmenskultur gehören Maßnahmen gesetzt. Trim beschreiben, wie mit Hilfe von Verhandlungssimulationen BC in einem Unternehmen gestärkt werden kann (Trim, et al., 2009). Abschließend folgen im BS25999 das Training und die Verbesserung der BC-Maßnahmen. Hier konnten im Zuge dieser Arbeit keine aktuellen Forschungsergebnisse gefunden werden.

Zusammenfassend muss gesagt werden, dass in gewissen Bereichen noch deutlich zu wenig geforscht wird, wohingegen in anderen Disziplinen eine ausgiebige und vielfältige Forschung vorhanden ist. In den Bereichen Risikoanalyse und Business Impact-Analyse ist umfangreiche Forschung vorhanden. Hier ist es aus Sicht des Autors nicht mehr notwendig, einen weiteren Forschungsschwerpunkt zu setzen. Auch die Planungsphase wird immer wieder aus verschiedenen Sichten untersucht. Hier werden sowohl neue Methoden entwickelt als auch alte verbessert. Hier ist ebenfalls kein Forschungsmanko festzustellen. Etwas anders sieht dies allerdings in einigen anderen Bereichen aus. Vor allem im Bereich der Übung und Verbesserung der implementierten Maßnahmen gibt es aktuell wenig Forschung. Die Gründe hierfür sind nicht offensichtlich. Möglicherweise ist dieses Gebiet entweder nicht wichtig genug oder zu viel von praktischen Gesichtspunkten geprägt. Arbeiten aus den Jahren 1998 und 1999 (Morwood, 1998) (Paton, 1999) belegen, dass es in diese Richtung durchaus auch Forschungsmöglichkeiten gibt. Auch im Bereich der strategischen Planung ist ein deutliches Manko festzustellen. Hier sind außer wenigen Fallbeispielen keine Forschungen zu finden.

Wünschenswert ist daher ein Forschungsschwerpunkt in dem ansonsten rein praktisch dominierten Gebiet des BCM. Studien zur Bewertung der unterschiedlichen Möglichkeiten bei Training und Umsetzung des BCM sind sicher für viele von Interesse. Ferner sind die Auswirkungen von unterschiedlichen BC-Strategien auf verschiedene Unternehmen interessant. In diesen beiden Bereichen sollten eindeutig intensivere Forschung betrieben werden.

Abschließend werden noch einige wissenschaftliche Arbeiten gezeigt, welche sich mit bestimmten Technologien beschäftigen. Hier finden sich bevorzugt Materialien zu Themengebieten in denen BCM bereits eine wichtige Rolle spielt, wie zum Beispiel der Finanzindustrie oder der staatlichen Unternehmen. Was umgekehrt nicht im internationalen Forschungsbereichen zu finden ist, sind Vergleiche der einzelnen BCM-Ansätze. Hier werden weder bestimmte Aspekte verglichen, noch wird ein genereller Vergleich gemacht, wie er in dieser Arbeit zu finden ist.

Bajgoric beleuchtet zum Beispiel die Auswirkungen der IT auf das Business Continuity Management (Bajgoric, 2006). Quirchmayr untersucht etwas spezifischer die sicherheitsrelevanten Aspekte der IT im BCM. Er beschreibt den Zusammenhang von früher oder später anzunehmenden Sicherheitslücken im Zusammenhang mit den Anforderungen des

BCM (Quirchmayr, 2004). Auf einen noch kleineren Bereich spezialisieren sich Singhal und sein Team (Singhal, et al., 2010). Sie untersuchen ausschließlich den Aspekt der Datensicherung unter Berücksichtigung von Business Continuity. Brandt verwendet algebraische Graphentransformation als Methode, um BC-Prozesse in Übereinstimmung mit Anforderungen hinsichtlich der Sicherheit und Gesetzmäßigkeit zu bringen (Brandt, et al., 2009). In einem ganz anderen Fachbereich bewegt sich Davison (Davison, 2007). Dieser diskutiert die ethischen Probleme, die bei BCM auftreten können. Hier werden beispielsweise Probleme beim Datenschutz bei der Sicherung von Daten erwogen.

7 Wissenschaftliche Methode

Diese Arbeit ist eine Literaturdiplomarbeit zu einem Thema, welches bis jetzt in der Form noch nicht existiert. Ein derartiger Vergleich, welcher mehrere Aspekte der unterschiedlichen Standards vergleicht, konnte nicht gefunden werden.

Diese Diplomarbeit ist als reine Literaturdiplomarbeit zu verstehen. Durch Literaturrecherche werden geeignete Werke gesucht. Die verwendete Literatur wird allgemein in zwei Bereiche unterteilt: Einerseits in praxisorientierte Schriften, beispielsweise Best Practices oder Erfahrungsberichte von Experten. Aus diesem Bereich werden die verglichenen Standards ausgewählt.

Anderseits wird auch akademische Literatur als Quelle herangezogen. Hier sollen vor allem die Grundlagentheorien des Business Continuity Management, die im akademischen Umfeld erarbeitet werden, betrachtet werden. Dabei soll herausgefunden werden, in welchen Bereichen sich die Schwerpunktforschung im akademischen Bereich dieses Themas bewegt und welche Bereiche noch nicht ausreichend erforscht wurden (siehe auch Kapitel 6, State-of-the-art).

In einer Vorstufe zu dieser Diplomarbeit wurden verschiedene Kriterien erarbeitet, welche zum Vergleich der einzelnen Ansätze verwendet werden sollen. Hierbei wird ein besonderer Schwerpunkt auf Kriterien gelegt, welche eine möglichst objektive Bewertung ermöglichen. Ferner sollte ein möglichst breites Spektrum an unterschiedlichen Bewertungspunkten geschaffen werden, sodass für möglichst viele Anwendungsbereiche aussagekräftige Kriterien vorhanden sind. Schlussendlich wurden 27 verschiedene Kriterien ausgewählt.

Diese Kriterien lassen sich in mehrere Gruppen einteilen. Es gibt solche Kriterien die den äußeren Zustand des Standards beschreiben, ohne dabei auf den Inhalt des Standards einzugehen. Diese sind eindeutig identifizierbar und für jede Organisation gleich. Dazu sind zu zählen: Sprache (4.1), Ort der Entstehung (4.2), Zeit der Entstehung (4.3), Verfügbarkeit (4.4), Art der Verfügbarkeit (4.9), Welche Organisation steht dahinter (4.14), Vorlage/Querverbindungen zwischen den Guides (4.15) sowie Beratung & Support (4.25).

Eine weitere Gruppe an Kriterien beschreibt solche die bei der Auswahl der Standards eine eher untergeordnete Rolle spielen sollten. Diese Merkmale beschreiben daher „weiche“ Kriterien, welche zumeist als nice-to-have zu bezeichnen sind. Dazu sind zu zählen: Art (4.5), Vorhandene Tools zur Unterstützung (4.6), Flexibilität (4.12), Organisatorisch/kulturell (4.13), Gegebene Templates (4.17), Benötigte Vorkenntnisse (4.20), Methoden (4.21) sowie Ergänzendes Material (4.23).

Die dritte Gruppe befasst sich mit den kritischen Aspekten des BCM. Diese Aspekte können einen Standard für ein Unternehmen nicht anwendbar machen. Zu diesen Kriterien sind zu zählen: Allgemein/branchenspezifisch (4.7), Unternehmensgröße (4.8), Möglichkeiten zur Zertifizierung (4.10), Rechtliche Begrenzungen (4.11), Zielgruppe (4.16), Benötigte Ressourcen (4.18), Integration von Organisationsprozessen (4.19), Ausschließlich Maßnahmen zur Einführung von BCM oder auch Überprüfung und Weiterführung (4.22), Befolgung der Richtlinien der Aufsichtsbehörden (4.26) sowie Befolgung von internationalen IT-Standards (4.27). Eine Sonderstellung nimmt hier das Kriterium 284.24 ein, welches eine

Art Kurzbeschreibung des Standards ist. Dieses soll einen Überblick über die einzelnen Phasen vermitteln. Auch dieses Merkmal kann bei der Entscheidung für oder gegen einen Standard von Relevanz sein.

Eine Beschreibung der einzelnen Kriterien ist in Kapitel 4 zu finden. Von allen ausgewählten Kriterien hat sich eines als nicht anwendbar herausgestellt, und zwar Benötigte Ressourcen (4.18). Einige weitere Kriterien haben bei der praktischen Anwendung nicht die erhofften Differenzen ergeben. Vor allem die Toolunterstützung, die Flexibilität sowie Beratung & Support haben geringe Unterschiede zwischen den einzelnen Standards hervorgebracht.

Als nächster Schritt folgt die Auswahl der Guidelines. Hier ist die Schwierigkeit, aus der Vielzahl der unterschiedlichen Guides eine sinnvolle und wissenschaftlich vertretbare Auswahl zu treffen (siehe 3.1). Es wurden schlussendlich 10 unterschiedliche Standards ausgewählt.

Der Hauptteil der Diplomarbeit bewertet anfänglich jeden einzelnen Standard nach den erarbeiteten Kriterien (Kapitel 5). Anschließend wird anhand der einzelnen Vergleiche herausgearbeitet, welche Guidelines sich für welches Anwendungsgebiet am besten eignen (Kapitel 8). Gleichzeitig sollen damit auch die Stärken und Schwächen der einzelnen Werke bewertet werden. Anhand dieser Gegenüberstellung und der zuerst durchgeführten Einzelbewertungen soll der an Business Continuity Interessierte schnell und einfach den am besten geeigneten Standard identifizieren können.

8 Conclusio

Übersichtstabelle

	GPG (BCI)	BSI 100-4	BS 25999	FSA	ISO 22399	ASIS SPC.1	SP 800-34	NFPA 1600	GPG Telekom	Australien Draft
Sprache	En	De, En	En, De, Esp	En	En	En	En	En, Esp	En	En
Aktuellste Version	2008	2008	2006/2007	2006	2007	2009	2002/ 2010	2007/2010	2006	2009
Freie Verfügbarkeit	☑	☑	☒	☑	☒	☑	☑	☑	☑	☑
Art	Ausführlich	Ausführlich	Liste	Liste	Ausführlich	Ausführlich	Ausführlich	Liste	Ausführlich	Ausführlich
Branchen-bindung	☒	☒	☒	☑	☒	☒	☐	☒	☐	☒
Zertifizierung	☑	☐	☑	☒	☒	☑	☒	☒	☒	☒
Zielgruppe	Jeder	(BCM-) Manager	(BCM-) Manager	(BCM-) Manager	(BCM-) Manager	(BCM-) Manager	Jeder	(BCM-) Manager	(BCM-) Manager	(BCM-) Manager
Templates	☐	☑	☒	☒	☒	☒	☑	☒	☒	☑
Vorkenntnisse	☑	☐	☐	☒	☐	☐	☑	☒	☐	☐
Methoden	☑	☑	☐	☒	☒	☒	☑	☒	☒	☑
Ergänzendes Material	☑	☐	☐	☒	☒	☑	☒	☒	☒	☑

☑ wird erfüllt ☐ teilweise erfüllt ☒ nicht erfüllt

8.10.1 Sprache

Die allgemein übliche Sprache im BCM ist zumeist Englisch. Daher sind die meisten Standards auch in dieser Sprache verfügbar. Zusätzlich kommen auch fast alle getesteten Guidelines aus dem englischen Sprachraum. Einzig der BSI 100-4 kommt aus Deutschland und ist somit ursprünglich nicht in Englisch geschrieben. Inzwischen gibt es jedoch auch für dieses Werk eine Übersetzung. Hervorzuheben ist weiters der BS 25999 Standard, der neben der englischen Originalversion auch noch in deutscher und spanischer Sprache verfügbar ist. Auch der NFPA 1600 ist in Spanisch erhältlich.

Aus deutschsprachiger Sicht ist also für den Fall einer zwingenden Verfügbarkeit in der Muttersprache neben dem deutschen BSI 100-4 auch noch der BS 25999 interessant.

8.10.2 Aktuellste Version

Die meisten Standards sind in einer aktuellen Version verfügbar. Durch die große Nachfrage an Business Continuity ist es für die Verfasser der Guides leicht möglich, immer wieder neue Versionen herauszugeben.

Der SP 800-34 wurde in dieser Arbeit noch in seiner Version aus dem Jahr 2002 getestet, ebenso wurde NFPA 1600 in der Revision aus dem Jahr 2007 verwendet. Bei beiden Standards ist inzwischen eine neuere Version (2010) verfügbar. Alle Standards sind in den Jahren 2006 bis 2010 entstanden und entsprechen damit weitgehend dem aktuellen wissenschaftlichen Standard.

8.10.3 Freie Verfügbarkeit

Von den verwendeten Standards sind die meisten frei verfügbar. Alle Standards, die frei verfügbar sind, sind auf der Homepage des jeweiligen Verfassers zu finden. Manche Anbieter (das deutsche BSI und das amerikanische ASIS) bieten ihren Standard in einer gedruckten Version kostenpflichtig an (EUR 40,- das BSI und USD 107,- das ASIS). Dies wurde jedoch nicht berücksichtigt, da der Standard dann trotzdem frei verfügbar ist.

Zwei Standards sind allerdings kostenpflichtig. Einerseits der BS 25999, andererseits der ISO 22399. Beim zweiteiligen BS 25999 wird pro Teil 100 Britische Pfund verrechnet. Der ISO-Standard schlägt sich mit CHF 124 zu Buche.

Daher kann gesagt werden, dass alle getesteten Standards mit vernünftigem finanziellem Aufwand erstanden werden können. Auch die kostenpflichtigen Guides sind nicht teuer.

8.10.4 Art

Grundsätzlich sagt die Art der Beschreibung nichts über die Qualität des Standards aus. Die textuell ausführlichen Standards ermöglichen es auch dem nicht so geübten Anwender sich leichter einzulesen. Die drei in einer Liste verfassten Guides sind kurz und prägnant geschrieben und eignen sich nicht dazu, Erklärungen zu liefern. Diese Standards eignen sich eher dazu, die Ideen der Reihe nach abzuarbeiten.

Eine eindeutige Unterscheidung zwischen den einzelnen Standards ist in diesem Kriterium schwierig, da eine Bewertung von den individuellen Vorlieben des Lesers abhängt. Einzig ein Neuling in diesem Themenbereich sollte sich mit einen der textuell beschriebenen Standards in das Thema einlesen. Zu einer praktischen Umsetzung eignen sich beide Formen gleichwertig.

8.10.5 Branchenbindung

Die meisten Guidelines werden unabhängig von einer Branche geschrieben. Dies kann einfach damit erklärt werden, dass es sich in wenigen Branchen rentiert, einen spezifischen Guide ausschließlich für ein bestimmtes Arbeitsgebiet zu erstellen. Zumeist reicht es, die vorhandenen Standards anzupassen. Daher sind auch die meisten in diesem Vergleich angeführten Standards branchenunabhängig.

Der einzige Standard, welcher tatsächlich an eine Branche gebunden ist, ist der Business Continuity Management Practice Guide der Financial Services Authority. Dieser Guide ist speziell auf das Bankwesen bezogen, eine Branche, für die spezielle BCM-Guides vorhanden sind.

Speziell zu erwähnen sind der SP 800-34 sowie der Good Practice Guide für Telecommunications Resilience. Der SP 800-34 ist zwar allgemein anwendbar, ist aber speziell für öffentliche Institutionen der Vereinigten Staaten von Amerika geschrieben. Der GPG für Telecommunications Resilience ist zwar nicht im eigentlichen Sinne branchengebunden, aber von der Thematik auf ein Fachgebiet, nämlich die Telekommunikation, beschränkt. Somit ist dieser Standard nur für Unternehmen interessant, welche eine starke Abhängigkeit von Telekommunikationsmittel haben.

8.10.6 Zertifizierung

Große Organisationen bieten manchmal Zertifizierungen zu den von ihnen publizierten Standards an. So auch vier der hier verglichenen Standards.

Das Business Continuity Institute bietet als eine der größten Plattformen eine Zertifizierung von einzelnen Personen an. Ebenso bietet die American Society for Industrial Security (ASIS) Zertifizierungen für Einzelpersonen an. Diese Organisation offeriert verschiedene Stufen an Zertifikaten, die aufeinander aufbauend sind und mit erweiterter Erfahrung und verbessertem Wissen erlangt werden können.

Das British Standards Institute bietet zu dem zweiten Teil seines BS 25999 eine Zertifizierung für Organisationen an, wofür wird ein Unternehmen nach dieser Guideline geprüft wird. Wenn die Organisation die gegebenen Standards erfüllt, wird sie zertifiziert.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik bietet ebenfalls eine Zertifizierung an. Allerdings ist diese nicht auf den BSI 100-4 beschränkt und auch keine eigentliche Zertifizierung gegen diesen Standard. Die Zertifizierung beim BSI findet mit dem ISO 27001 Standard statt. Werden sämtliche BSI 100 Standards (BSI 100-1 bis BSI 100-4) ist das Unternehmen kompatibel zu ISO 27001. Allerdings sind alle vier Standards zu erfüllen, nicht nur der in der Arbeit verglichene BS 100-4. Das BSI bietet auch eine Zertifizierung für Personen an. Diese sind dann berechtigt, Organisationen zu bewerten und zertifizieren.

8.10.7 Zielgruppe

Generell sind die verwendeten Guidelines primär an Manager gerichtet, welche sich näher mit dem Thema BCM beschäftigen. Diese benötigen die meisten Informationen aus diesen Werken. Doch auch Personen, welche sich nicht aktiv an der Implementierung eines BC-Systems beteiligen, dieses jedoch auf die eine oder andere Art unterstützen, benötigen bestimmte Informationen.

Dafür eignen sich vor allem der GPG des BCI und der SP 800-34 des NIST. Diese sind entsprechend einfach geschrieben, fordern wenige Vorkenntnisse und erklären auch einfache Vorgänge. Daher sind diese beiden Guides vor allem für Anfänger im Bereich Business Continuity geeignet.

Die anderen Werke eignen sich nicht unbedingt als Einstiegsliteratur für diesen Themenkomplex. Allerdings können einzelne Passagen durchaus empfehlenswert sein, um gewisse Probleme lösen zu können. Die drei Guides welche listenartig geschrieben sind (siehe 8.10.4), sind noch am wenigsten dazu geeignet, sich zu einem Thema zu informieren. Sollte einer dieser Standards in einem Unternehmen umgesetzt werden, empfiehlt es sich, zur Erstinformation ergänzende Literatur heranzuziehen.

8.10.8 Templates

Benötigt man Templates, gibt es drei Standards, die solche bieten. Der BSI 100-4 bietet die Struktur eines Notfallhandbuches und eines Geschäftsfortführungsplanes. Diese beiden Templates sind im Anhang des Standards zu finden.

Der SP 800-34 hat verschiedene Templates integriert. So sind im Anhang ein Template für einen Notfallplan sowie für eine Business Impact Analysis gegeben. Aber auch im Standard selbst sind immer wieder Templates, oft in einfacher Form, gegeben. Beispielsweise ist ein Recovery Strategy Budget Planning Template (Seite 27) zu finden.

Noch umfangreicher ist in diesem Bereich der Guide des Australian National Audit Office. Dieser bietet in seinem Workbook, welches anschließend an die eigentliche Guideline steht, eine Vielzahl an unterschiedlichen Templates an. So sind vor allem zu der Analysephase (zum Beispiel BIA) sowie zu der Phase des Testens und Übens (zum Beispiel Übungsprogramme), aber auch für die Phase der Betriebsstörung (beispielsweise ein Eventlog) verschiedene Templates gegeben.

Zu erwähnen ist weiters auch der GPG des BCI. Dieser hat zwar keine Templates im Werk integriert, für Mitglieder des BCI gibt es jedoch eine Vielzahl an Templates auf der Homepage des BCI zu finden.

8.10.9 Vorkenntnisse

Hier heben sich zwei Standards positiv heraus. Sowohl der GPG als auch der SP 800-34 eignen sich dazu, sich ohne Vorkenntnisse in das Thema einzulesen und grundlegende Informationen zu sammeln.

Umfangreiche Vorkenntnisse verlangen der FSA-Guideline sowie auch der NFPA 1600. Diese beiden Werke erfordern, sich zuvor bereits in die Materie einzuarbeiten.

Die restlichen Werke sind zwar nicht als Ganzes anfängerfreundlich, jedoch können Teile daraus entnommen und zur Erklärung einzelnen Probleme oder Phasen verwendet werden. Auch das Einarbeiten in diese Standards ist nicht schwierig, erfordert allerdings zumeist das Hinzuziehen von komplementären Quellen.

8.10.10 Methoden

Genau beschriebene Methoden erleichtern oft die Umsetzung eines BC-Programmes. Eine solche bieten einige Guidelines:

Allen voran sind hier der GPG und der SP 800-34 zu nennen. Beide beschreiben ausführlich die durchgeführten Methoden. Auch der BSI 100-4 Standard und der australische BCM-Guide beschreiben die Methoden ausführlich. Der BS 25999 beschreibt im ersten Teil die Methoden genau. Im zweiten Teil (der auch für die Zertifizierung wichtig ist) wird allerdings auf genaue Methodenbeschreibungen nicht eingegangen.

Die anderen Standards beschreiben die angewendeten Methoden nicht ausführlich.

8.10.11 Ergänzendes Material

Als ergänzendes Material wurden ausschließlich Unterlagen der Organisation gewertet, welche den Standard verfasst hat. Material von externen Stellen wurde nicht eingerechnet.

Die größte Anzahl an zusätzlichen Unterlagen bietet das BCI für seinen GPG an. Diverse Whitepapers und Schulungen sind auf der Homepage zu finden. Das ASIS bietet für den SPC.1-2009 ebenfalls diverse Unterlagen und Schulungen an. Der Australische BCM Guide bietet zwar wenig zusätzliche Unterlagen an, jedoch ist das angefügte Workbook so umfangreich und informativ, dass dies auch als ergänzendes Material gewertet wurde.

Das Bundesamt für Sicherheit und Informationstechnik bietet zu dem Standard zwar keine zusätzlichen Materialien an, jedoch gibt es die Standards BS 100-1, BS 100-2 und BS 100-3, welche den hier verglichenen Standard ergänzen. Die BSI Group bietet zu ihrem Standard BS 25999 nur wenige sinnvolle Unterlagen an. Einige wenige Whitepapers sind zu finden.

Zu den weiteren Standards sind keine ergänzenden Unterlagen aufzufinden.

9 Fazit

Abschließend kann in dieser Arbeit festgestellt werden, dass es komplex ist, unterschiedliche Standards miteinander zu vergleichen. Selbst mit einer genauen Vorbereitung durch eine detaillierte Erstellung von Kriterien die für den Vergleich herangezogen werden, ist es nicht immer möglich, alle Standards in sämtlichen Bereich miteinander zu vergleichen. Auch hat sich ein Kriterium als gänzlich unanwendbar herausgestellt. Dennoch hat sich gezeigt, dass die meisten Kriterien anwendbar und aussagekräftig sind.

Die Kernaussage dieser Arbeit ist, dass es keinen „ultimativen" Standard gibt, sondern dass sich jeder einzelne Standard für bestimmte Situationen eignet. Jeder Standard hat individuelle Vor- und Nachteile. Während sich die einen durch geringe Einarbeitungszeit und leichte Sprache auszeichnen, sind andere für konkrete Situationen oder bestimmte Branchen geeignet. In dieser Arbeit wurden für alle Standards die wesentlichen Charakteristika herausgearbeitet. Dadurch kann der interessierte Leser relativ einfach alle in dieser Arbeit beschriebenen Standards kennenlernen.

In der Conclusio wurde das Problem von der anderen Seite betrachtet. Es wurden für die wichtigsten Kriterien jeweils die besten, weil geeignetsten, Werke beschrieben. Das Ziel dahinter ist, das Thema auch für Personen, welche wenige Vorkenntnisse im Bereich BCM haben, zu vereinfachen einen geeigneten Standard zu finden. Der Anwedner sucht sich die für sein Unternehmen wichtigen Kriterien heraus und kann rasch potentielle Standards für seinen Verwendungszweck finden.

In der vorliegenden Arbeit wurde ferner eine fundierte Grundlage für den Vergleich von unterschiedlichen Standards geschaffen. Dies ist quasi als Nebenprodukt der eigentlichen Arbeit entstanden, kann sich aber ebenso als wertvoll herausstellen wie der in der Arbeit durchgeführte Vergleich. Mit dem erarbeiteten Set an Kriterien sowie den bereits verglichenen Referenzwerken sollte es ohne größeren Aufwand auch in Zukunft möglich sein, weitere BCM-Werke mit den in dieser Arbeit erarbeiteten Kriterien zu vergleichen. Da im Bereich BCM ständig Weiterentwicklungen vor sich gehen und auch regelmäßig neue Standards publiziert werden, ist dieser Teil der Arbeit vermutlich jener, welche eine längere Aktualität hat.

10 Literaturverzeichnis

ANAO - HTML-Version. [Online] [Zitat vom: 24. 09 2010.] http://www.anao.gov.au/BetterPracticeGuides/toc.html.

ANAO - Publications. [Online] [Zitat vom: 24. 09 2010.] http://www.anao.gov.au/director/publications.cfm.

ANAO-About. [Online] [Zitat vom: 24. 09 2010.] http://www.anao.gov.au/director/aboutus.cfm.

ANAO-Building resilience in public sector entities. 2009. Business Continuity Management: Building resilience in public sector entities. *Australien National Audit Office.* [Online] 2009. [Zitat vom: 29. 04 2010.] http://www.anao.gov.au/uploads/documents/Business_Continuity_Management_.pdf.

Arduini, Fabio und Morabito, Vincenzo. 2010. Business continuity and the banking industry. *Commun. ACM.* 2010, Bd. 53, 3, S. 121-125.

ASIS - Certification. [Online] [Zitat vom: 24. 09 2010.] http://www.asisonline.org/certification/handbook.pdf.

ASIS - Download. [Online] [Zitat vom: 24. 09 2010.] http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf.

ASIS - Toolkit. [Online] [Zitat vom: 24. 09 2010.] http://www.asisonline.org/toolkit/toolkit.xml.

ASIS International. 2004. *ASIS Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery.* s.l. : ASIS International, 2004. 1-887056-56-4.

ASIS SPC.1-2009. 2009. Organization Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use. *American National Standard.* [Online] 2009. [Zitat vom: 29. 04 2010.] http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf.

ASIS-About. [Online] [Zitat vom: 24. 09 2010.] http://www.asisonline.org/about/history/index.xml.

ASIS-Education. [Online] [Zitat vom: 24. 09 2010.] https://www.asisonline.org/education/index.xml.

ASIS-Shop. [Online] [Zitat vom: 24. 09 2010.] http://www.abdi-secure-ecommerce.com/asis/ps-907-37-1842.aspx.

Bajgoric, Nijaz. 2006. Information technologies for business continuity: an implementation framework. *Information Management & Computer Security.* 2006, Bd. 14, 5, S. 450-466.

BCI - Code of Ethics. Code of ethics. [Online] [Zitat vom: 24. 09 2010.] http://www.thebci.org/codeofethics.htm.

BCI - E-Learning. [Online] [Zitat vom: 24. 09 2010.] http://www.thebcicertificate.org/pdf/elearning_overview.pdf.

BCI - Glossary. [Online] [Zitat vom: 24. 09 2010.] http://www.thebci.org/glossary.pdf.

BCI GPG. 2010. A Management Guide to Implementing Global Good Practice in Business Continuity Management. *The Business Continuity Institute.* [Online] 29. 04 2010. [Zitat vom: 29. 04 2010.] http://www.thebci.org/gpgdownloadpage.htm.

BCI-About. About the BCI. [Online] [Zitat vom: 24. 09 2010.] http://www.thebci.org/about.htm.

BCI-Bookstore. [Online] [Zitat vom: 24. 09 2010.] http://www.thebci.org/bookstore.htm.

—. [Online] [Zitat vom: 24. 09 2010.] http://www.rothstein.com/bcibooks/.

BCI-Certificate. Certificate Information. [Online] [Zitat vom: 24. 09 2010.] http://www.thebcicertificate.org/pdf/BCI_Certificate_Candidate_Info_Pack2008.pdf.

BCI-E-Learning. [Online] [Zitat vom: 24. 09 2010.] http://www.thebcicertificate.org/pdf/elearning_overview.pdf.

BCI-Membership Criteria. Membership Criteria. [Online] [Zitat vom: 24. 09 2010.] http://www.thebci.org/BCIProfessionalCompetencies%20_2_.pdf.

Boehmer, W., Brandt, C. und Groote, J.F. 2009. Evaluation of a Business Continuity Plan using Process Algebra and Modal Logic. Toronto : IEEE, 2009, S. 147-152.

Boehmer, Wolfgang. 2009. Survivability and Business Continuity Management System According to BS 25999. *Survivability and Business Continuity Management System According to BS 25999.* s.l. : IEEE, 2009.

Brandt, C., Hermann, F. und Engel, T. 2009. Modeling and reconfiguration of critical business processes for the purpose of a Business Continuity Management respecting security, risk and compliance requirements at Credit Suisse using algebraic graph transformation. 2009.

BS25999-1 Code of Practice. 2006. *Business continuity management. Code of Practice.* s.l. : British Standard, 2006. 0 580 49601 5.

BS25999-2 Specification. 2007. *Business continuity management. Specification.* s.l. : British Standard, 2007. 978 0 580 59913 2.

BS25999-Zertifizierung. [Online] [Zitat vom: 24. 09 2010.] http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/.

BSI 100-4 english. [Online] [Zitat vom: 24. 09 2010.] https://www.bsi.bund.de/cae/servlet/contentblob/748954/publicationFile/41759/standard_100-4_e_pdf.pdf.

BSI Self-assessment Online. [Online] [Zitat vom: 24. 09 2010.] http://shop.bsigroup.com/en/Navigate-by/Assessment-Tools/Assessment-Tools/Self-assessment-tools/BCM2/BS25999-2-/.

BSI-IT-Grundschutz-Standards. [Online] [Zitat vom: 24. 09 2010.] https://www.bsi.bund.de/cln_174/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html.

BSI-Leitbild. [Online] [Zitat vom: 24. 09 2010.] https://www.bsi.bund.de/cln_174/DE/DasBSI/Leitbild/leitbild_node.html.

BSI-Shop. [Online] [Zitat vom: 24. 09 2010.] http://shop.bsigroup.com/.

BSI-Standard 100-1. 2008. BSI-Standard 100-2 IT-Grundschutz Vorgehensweise. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] 2008. [Zitat vom: 29. 04 2010.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001.pdf?__blob=publicationFile.

BSI-Standard 100-2. 2008. BSI-Standard 100-2 IT-Grundschutz Vorgehensweise. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] 2008. [Zitat vom: 29. 04 2010.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002.pdf?__blob=publicationFile.

BSI-Standard 100-3. 2008. BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] 2008. [Zitat vom: 29. 04 2010.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003.pdf?__blob=publicationFile.

BSI-Standard 100-4. 2008. BSI-Standard 100-4 Notfallmanagement. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] 2008. [Zitat vom: 29. 04 2010.] https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/31045/standard_1004.pdf.

BSI-Zertifizierungsstandard. [Online] [Zitat vom: 24. 09 2010.] https://www.bsi.bund.de/cae/servlet/contentblob/476492/publicationFile/30756/zertifizierte-IT_pdf.pdf.

Cha, Shi-Cho, et al. 2008. RiskPatrol: A risk management system considering the integration risk management with business continuity processes. Taipei : IEEE, 2008, S. 110-115.

Comission on Terrorist Attacks. Comission on Terrorist Attacks upon the United States. [Online] [Zitat vom: 24. 09 2010.] http://govinfo.library.unt.edu/911/report/911Report_Ch12.htm.

Crisis Commander. [Online] [Zitat vom: 24. 09 2010.] http://www.crisiscommander.com/.

Davison, Christopher B. 2007. Ethics of business continuity and disaster recovery technologies: A conceptual orientation. *International Journal of Computers.* 2007, Bd. 9, 1, S. 54-63.

Financial Services Authority. 2008. [Online] 2008. [Zitat vom: 24. 09 2010.] http://www.fsc.gov.uk/section_file.asp?objectid=0&object=linkfile&docid=2188.

—. 2005. UK Financial Sector Continuity. [Online] 2005. [Zitat vom: 29. 04 2010.] http://www.fsc.gov.uk/upload/public/Files/9/Web%20-%20Res%20Bench%20Report%2020051214.pdf.

FSA - About. [Online] [Zitat vom: 24. 09 2010.] http://www.fsa.gov.uk/Pages/About/Who/index.shtml.

FSA BCM. 2006. Business Continuity Management Practice Guide. *Financial Services Authority.* [Online] 2006. [Zitat vom: 29. 04 2010.] http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf.

FSA-Tool. [Online] [Zitat vom: 24. 09 2010.] http://www.fsa.gov.uk/Pages/About/Teams/Stability/Current/guide/index.shtml.

How to Deploy BS 25999. 2008. How to Deploy BS 25999 second edition. *BSI Management Systems America.* [Online] 2008. [Zitat vom: 29. 04 2010.] http://www.avalution.com/PDF/How_to_Deploy_BS_25999_second_edition.pdf.

Impact Ware. [Online] [Zitat vom: 24. 09 2010.] http://www.impactaware.com/.

International Organization for Standardization. 2009. ISO/PAS Publicly available specification. [Online] 04. 10 2009. http://www.iso.org/iso/standards_development/processes_and_procedures/deliverables/iso_pas_deliverable.htm.

ISO 22399. 2007. Societal security - Guideline for incident preparedness and operational continuity management. *International Organization for Standardization.* 2007.

Kepenach, Richard J. 2007. Business Continuity Plan Design: 8 Steps for Getting Started Designing a Plan. s.l. : IEEE, 2007.

Morwood, Gregory. 1998. Business continuity: awareness and training programmes. *Information Management & Computer Security.* 1998, Bd. 6, 1, S. 28-32.

NFPA - Guideline. [Online] [Zitat vom: 24. 09 2010.] http://www.nfpa.org/catalog/product.asp?catalog_name=NFPA+Catalog&pid=IM160007&link_type=search&order_src=A647&src=nfpa.

NFPA 1600. 2007. Standard on Disaster/Emergency Management and Business Continuity Programs. *National Fire Protection Association.* [Online] 2007. http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf.

NFPA-About. [Online] [Zitat vom: 24. 09 2010.] http://www.nfpa.org/categoryList.asp?categoryID=143&URL=About%20NFPA.

NFPA-Guideline. [Online] [Zitat vom: 24. 09 2010.] http://www.nfpa.org/catalog/product.asp?catalog_name=NFPA+Catalog&pid=IM160007&link_type=search&order_src=A647&src=nfpa.

NFPA-Shop. [Online] [Zitat vom: 24. 09 2010.] http://www.nfpa.org/catalog/.

NIST - About. [Online] [Zitat vom: 24. 09 2010.] http://csrc.nist.gov/groups/index.html.

NIST 800-34 - Download. [Online] [Zitat vom: 24. 09 2010.] http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

NIST 800-34. 2002. NIST Special Publication 800-34: Contingency Planning Guide for Information Technology Systems. *National Institute of Standards and Technology.* [Online] 2002. [Zitat vom: 29. 04 2010.] http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

Paton, Douglas. 1999. Disaster business continuity: promoting staff capability. *Disaster Prevention and Management.* 1999, Bd. 8, 2, S. 127-133.

Quirchmayr, Gerald. 2004. Survivability and business continuity management. *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - Volume 32.* Dunedin, New Zealand : s.n., 2004, S. 3-6.

Resilience Benchmarking Project. 2005. Resilience Benchmarking Project Discussion Paper. *UK Financial Sector Continuity.* [Online] 2005. [Zitat vom: 29. 04 2010.] http://www.fsc.gov.uk/upload/public/Files/9/Web%20-%20Res%20Bench%20Report%2020051214.pdf.

Satoshi, Iwai, et al. 2008. Business Continuity Management of NTT FACILITIES, INC. s.l. : IEEE, 2008.

Security Management. [Online] [Zitat vom: 24. 09 2010.] http://www.securitymanagement.com/.

Singhal, R., Bokare, S. und Pawar, P. 2010. Enterprise Storage Architecture for Optimal Business Continuity. 2010.

Telecommunications Resilience. 2006. Telecommunications Resilience. *National Infrastructure Security Co-Ordination Centre.* [Online] 2006. [Zitat vom: 29. 04 2010.] http://www.cpni.gov.uk/docs/re-20040501-00393.pdf.

Tjoa, Simon, Jakoubi, Stefan und Quirchmayr, Gerald. 2007. Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology. 2007, S. 179-186.

Trim, Peter und Lee, Yang-Im. 2009. Negotiation oriented simulation exercises that incorporate business continuity and international security. *On the Horizon.* 2009, Bd. 17, 4, S. 378-387.

Wenxin, Xiang, Yinghai, Wang und Zhaoyu, Zhang. 2008. The Research on Business Continuity Planning of E-government Based on Information Security Risk Management. s.l. : IEEE, 2008, S. 446-450.

Zalewski, Andrzej, et al. 2008. Modeling and Analyzing Disaster Recovery Plans as Business Processes. *Proceedings of the 27th international conference on Computer Safety, Reliability, and Security.* Newcastle upon Tyne, UK : s.n., 2008, S. 113-125.