Kernkompetenzzentrum
Finanz- & Informationsmanagement

Fraunhofer FIT
Projektgruppe
Wirtschaftsinformatik

Diskussionspapier

Business Continuity Management bei Finanzdienstleistungsunternehmen

von

Anna-Luisa Müller

Europäische Union
„Investition in Ihre Zukunft“
Europäischer Fonds für regionale Entwicklung

in: HMD - Praxis der Wirtschaftsinformatik 51 (2014) 3, S. 339-349

Universität Augsburg, D-86135 Augsburg
Besucher: Universitätsstr. 12, 86159 Augsburg
Telefon: +49 821 598-4801 (Fax: -4899)

Universität Bayreuth, D-95440 Bayreuth
Besucher: F.-v.-Schiller-Str. 2a, 95444 Bayreuth
Telefon: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-463

Business Continuity Management bei Finanzdienstleistungsunternehmen

Anna-Luisa Müller

HMD Praxis der Wirtschaftsinformatik

ISSN 1436-3011

HMD
DOI 10.1365/s40702-014-0045-9

Springer

HMD
DOI 10.1365/s40702-014-0045-9

Business Continuity Management bei Finanzdienstleistungsunternehmen

Anna-Luisa Müller

Eingegangen: 31. Januar 2014 / Angenommen: 15. April 2014

Zusammenfassung Die systematische Planung von Maßnahmen zur Fortführung der geschäftskritischen Prozesse gewinnt in jüngster Zeit zunehmend an Bedeutung, da statistisch ungefähr alle drei Jahre geschäftsgefährdende Ereignisse auftreten. Bei Finanzdienstleistungsunternehmen entsteht die erhöhte Angreifbarkeit von Geschäftsprozessen aufgrund der Konzentration wesentlicher Funktionen auf wenige Standorte, wenige Mitarbeiter und der steigenden Abhängigkeit von der Verfügbarkeit der IT-Systeme. Zudem werden die Gefährdungen der geschäftskritischen Prozesse nicht systematisch erfasst und die definierten Maßnahmen zur Geschäftsfortführung selten erprobt. Vor diesem Hintergrund werden im vorliegenden Beitrag unterschiedliche Rahmenwerke und die organisatorische Einordnung des Business Continuity Managements vorstellt, die Anwendung eines Vorgehensmodells zur praktischen Umsetzung in einer Bank aufgezeigt und Handlungsempfehlungen diskutiert.

Schlüsselwörter Business Continuity Management · Krisenmanagement · Notfallmanagement · Risikomanagement · Geschäftsprozesse · Bank · Finanzdienstleistungsunternehmen

1 Bedeutung des Business Continuity Managements

Wie schnell und effektiv Unternehmungen auf geschäftskritische Ereignisse wie bspw. Terrorismus, Umweltkatastrophen, Pandemien oder Computerviren reagieren

A.-L. Müller (✉)
Kernkompetenzzentrum Finanz- & Informationsmanagement,
Universitätsstr. 12, 86159 Augsburg, Deutschland
E-Mail: anna-luisa.mueller@fim-rc.de

Published online: 26 April 2014

können, hängt von der Funktionsfähigkeit ihres Geschäftsfortführungsmanagement (Business Continuity Management (BCM)) ab. Derartige Bedrohungen können die Geschäftstätigkeiten so weit beeinträchtigen, dass bis zu 90 % der Unternehmen, die durch eine Unterbrechung einen verheerenden Schaden an Daten, Systemen oder Betriebseinrichtung erlitten haben, innerhalb von 24 Monaten vom Markt verschwinden (Krell 2006). Volkswirtschaftlich bedeutende Branchen, wie bspw. Finanzdienstleister und Energieversorger, sind daher regulatorisch dazu verpflichtet, die Geschäftsfortführung sicherzustellen (Winkler et al. 2010). Dies bedeutet, dass sie Vorkehrungen dafür treffen müssen geschäftskritische Prozesse (d. h. diejenigen Prozesse, die im Ernstfall für den Fortbestand des Unternehmens von Bedeutung sind) weiterführen zu können. Es gilt hierbei die verschiedenen (inter-)nationalen Normen und Standards zum BCM zu beachten (vgl. Abb. 1). In der Bundesrepublik Deutschland bildet § 25a KWG „Besondere organisatorische Pflichten von Instituten“ die Basis des BCM von Finanzdienstleistern. Demnach muss eine ordnungsgemäße Geschäftsorganisation insbesondere ein angemessenes und wirksames Risikomanagement umfassen, auf dessen Basis ein Finanzdienstleister die Risikotragfähigkeit laufend sicherzustellen hat. Dieses Risikomanagement schließt die Festlegung eines angemessenen Konzepts zur Geschäftsfortführung ein. Die MaRisk-Anforderungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) konkretisieren diese Anforderungen und stellen daher den zentralen normativen Rahmen für das BCM dar. Zudem haben die vom British Standards Institute veröffentlichten Richtlinien (BS 25999-1:2006 und BS 25999-2:2007), ebenso wie die „Good Practice Guidelines” des Business Continuity Institute, der Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Standard 100-4), der Standard NIST SP 800-34 des National Institute of Standards and Technology und verschiedene ISO-Richtlinien (ISO 20000, 22399, 27001, 27002) das Ziel, den Steuerungsprozess für das BCM zu beschreiben und die wesentlichen Anforderungen an diesen Prozess zu definieren.

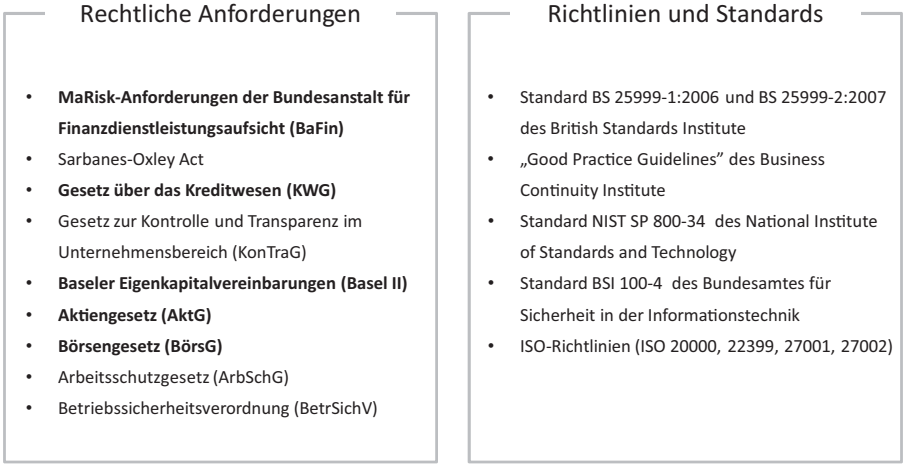

Abb. 1 Verschiedene rechtliche Anforderungen, Richtlinien und Standards des BCM

Ein Großteil der Finanzdienstleister realisierte erst durch die tragischen Ereignisse des 11. September 2001, dass die Sicherstellung der Geschäftsfortführung von großer Bedeutung ist (Smit 2005). Nur wenigen Banken und Versicherungen gelang es, nach dieser Unterbrechung ihre Geschäftstätigkeit direkt fortzuführen (Swartz 2003), da nur ungefähr die Hälfte der Unternehmen Geschäftsfortführungspläne implementiert hatte (Cerrulo und Cerrula 2004). Da die Implementierung eines BCM diverse Vorteile, wie bspw. kürzere Unterbrechungszeiten aufgrund der kontrollierten Wiederherstellung der geschäftskritischen Prozesse (Naujocks 2003), mit sich bringt, überrascht es, dass wenige Unternehmen ein durchgängiges BCM etabliert haben. Allerdings steht den genannten Vorteilen der Nachteil gegenüber, dass ein Großteil der Maßnahmen zur Geschäftsfortführung mit hohen Kosten verbunden ist und daher aufgrund von Budgetbeschränkungen entschieden werden muss, welche geschäftskritischen Prozesse als besonders schützenswert einzuschätzen sind.

Für Finanzdienstleister ist ein effektives und effizientes BCM von besonderer Bedeutung, da in dieser Branche in den aktuell volatilen und unvorhersehbaren Märkten geschäftskritische Ereignisse zwar nur selten eintreten, aber wenn dann nur kostenintensiv bekämpft werden können. Finanzdienstleister müssen daher die Geschäftsprozesse nach ihrem Gefährdungspotenzial priorisieren, BCM-Maßnahmen hinsichtlich der damit verbundenen Kosten und Nutzen bewerten und kostenintensive Maßnahmen nur für die hochkritischen Prozesse vornehmen. Vor diesem Hintergrund ist es Ziel des vorliegenden Beitrags, einen Überblick über das BCM von Finanzdienstleistern zu geben. Dabei werden Definitionen, Rahmenwerke und die organisatorische Einordnung des BCM vorstellt, die Anwendung eines Vorgehensmodells zur praktischen Umsetzung des BCM in einer Bank aufgezeigt und Handlungsempfehlungen diskutiert.

2 Begriffsdefinition und organisatorische Einordnung des Business Continuity Managements

In der Literatur existieren zahlreiche Definitionen für BCM (Gibb und Buchanan 2006). Im Allgemeinen wird unter Geschäftsfortführung ein Managementprozess verstanden, der das Gefahrenpotenzial einer Unternehmung in Bezug auf interne und externe Bedrohungen identifiziert und der effektive vorbeugende und reaktive Maßnahmen etabliert, mit dem übergeordneten Ziel der Sicherstellung der Weiterführung von geschäftskritischen Prozessen auf einem akzeptablen Niveau (Herbane et al. 1997, Naujocks 2003).

Die Vielzahl existierender Gefährdungen (wie bspw. unbefugtes Eindringen in IT-Systeme, Naturkatastrophen im Umfeld oder Störungen in der Stromversorgung) spiegeln sich in unterschiedlich ausgeprägten Unterbrechungen von Geschäftsprozessen (Störungen, Notfälle, Krisen und Katastrophen) wider (BSI 2008, Herbane et al. 1997, Naujocks 2003). Wie sich diese verschiedenen Unterbrechungen hinsichtlich ihrer Betroffenheit, Fristigkeit und Auswirkung charakterisieren lassen, ist detailliert in Tab. 1 dargestellt.

Tab. 1 Übersicht über die verschiedenen Ausprägungen von Unterbrechungen von Geschäftsprozessen

	Betroffenheit	Fristigkeit	Auswirkung
Störung	Ein Bereich/ggf. mehrere Bereiche	Kurzfristig	Klein bzw. lokal
Notfall	Mehrere Bereiche/ggf. gesamte Bank	Kurzfristig	Mittel
Krise	Gesamte Bank	Langfristig	Groß
Katastrophe	Gesamte Bank und Umfeld der Bank	Langfristig	Groß bzw. global

Auf strategischer Ebene können die Bestandteile

- Verständnis des Geschäftsmodells,
- Festlegung der Geschäftsfortführungsstrategien,
- Modellierung und Implementierung eines BCM
- Übungen,
- Überarbeitung der BCM-Tätigkeiten

unterschieden werden (Winkler et al. 2010). Das BCM umfasst damit im Zeitablauf sowohl die Vorsorge, die Bewältigung wie auch die Nachsorge der verschieden ausgeprägten Unterbrechungen (Smit 2005). Zur Vorsorge (Krisenplanung, recovery planning) zählen vorbeugende Maßnahmen, die den Schaden oder die Eintrittswahrscheinlichkeit von Risiken reduzieren und die Widerstandsfähigkeit des Unternehmens erhöhen (Krell 2006). Im Rahmen der Bewältigung ist dagegen dafür Sorge zu tragen, dass ein schnelles und sinnvolles Reagieren auf eine Unterbrechung möglich ist und dass die Anforderungen an die tägliche Arbeit trotz der Unterbrechung erfüllt werden. Um innerhalb eines angemessenen Zeitraums wieder vollständig in den Normalbetrieb zurückkehren zu können, ist eine adäquate Nachsorge von Bedeutung.

Da das BCM für die Wiederherstellung des ganzen Unternehmens verantwortlich ist, haben verschiedenste Unternehmensfunktionen organisatorische Schnittstellen zum BCM (BSI 2008). Das Spektrum der Tätigkeiten des BCM reicht von strategisch wichtigen steuernden (durch die Geschäftsführung) und prüfenden Tätigkeiten (z. B. durch Internal Audit) über die gestaltenden Aktivtäten im Qualitäts-und Risikomanagement bis hin zur operativen Bereitstellung der Infrastruktur durch IT und Gebäudemanagement. Abbildung 2 stellt die verschiedenen Tätigkeiten und zuständigen Funktionen entsprechend ihrer Einordnung in die operativen, prozessualen und strategischen Aktivitäten eines Unternehmens dar.

Im Hinblick auf die Rollen, Zuständigkeiten und Kompetenzen des BCM ist es in erster Linie von Bedeutung, eine unternehmensweite Koordination des BCM und damit die für die operativen Aufgaben zuständige Abteilung zu etablieren. Am häufigsten ist BCM in der Geschäftsleitung organisatorisch verankert (33 %), gefolgt von IT (28 %), Risikomanagement (13 %), Gebäudemanagement (8 %), Informationssicherheit (5 %), Betriebsschutz (3 %) und andere Abteilungen (10 %) (Krell 2006). Zudem sollte sich das Team der BCM-Verantwortlichen aus Vertretern verschiedener Funktionsbereiche zusammensetzen und die Verantwortlichen sollten anhand ihrer bisherigen Erfahrungen einen umfassenden Überblick über die relevanten Geschäftsprozesse des Unternehmens und der dafür benötigten Ressourcen haben (Herbane et al. 1997, Winkler et al. 2010). Es bedarf des Weiteren der Etablierung eines Krisenstabs/ Krisenmanagement-Teams, das sich aus leitenden Angestellten und erfahrenen Mitarbeitern zusammensetzt und die Verantwortung für die Bewertung von Unter-

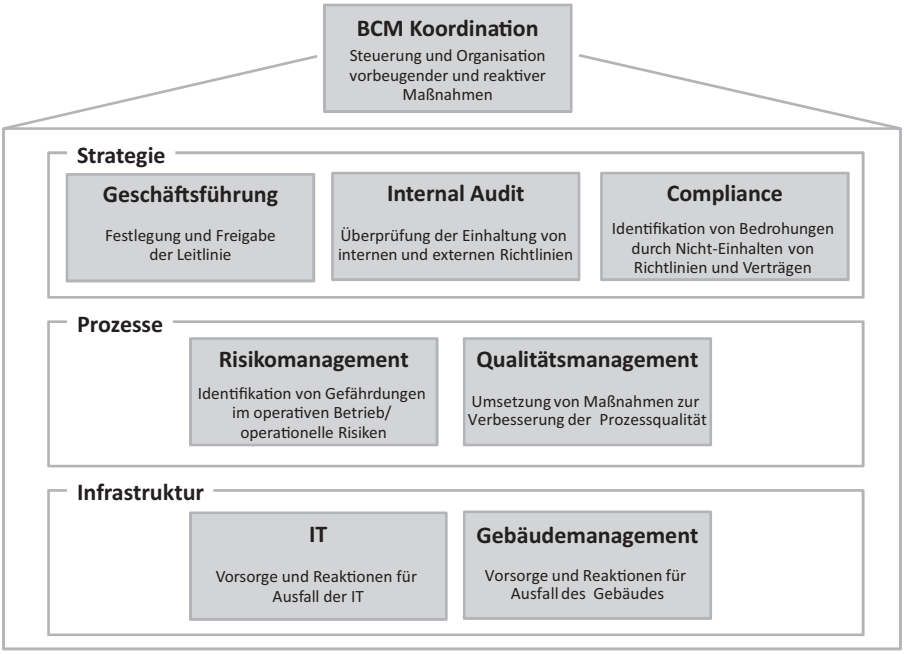

Abb. 2 Tätigkeiten des BCM und deren organisatorische Einordnung

brechungen und die Umsetzung der entsprechenden Vorgehensweisen zur Rückkehr zum Normalbetrieb trägt (Krell 2006). Zudem ist es von Bedeutung, bereichsspezifische Ansprechpartner für das BCM zu benennen, die die operative Verantwortung für die Umsetzung des BCM in einem dedizierten Geschäftsbereich haben, um die Anforderungen der jeweiligen spezialisierten Geschäftstätigkeiten entsprechend berücksichtigen zu können.

3 Praktische Umsetzung des Business Continuity Managements bei einem Finanzdienstleistungsunternehmen

Die jeweilige konkrete Ausgestaltung des BCM hängt von den Produkten, Dienstleistungen, Kunden sowie der strategischen Ausrichtung eines Unternehmens ab (Herbane et al. 1997). Ausgangspunkt und Basis des folgenden Erfahrungsberichts zur praktischen Umsetzung ist das BCM eines großen internationalen Finanzdienstleisters, der der Fortführung der kritischen Bankprozesse einen hohen Stellenwert beimisst und verschiedene Maßnahmen des BCM bereits umgesetzt hat. Die Erkenntnisse aus dem zugrundliegenden Projekt sind aufgrund der repräsentativen Größe (weltweite Standorte, Geschäfts- und Privatkundengeschäft, > 1.000 Mitarbeiter, Gewinn 150-200 Mio. €) auch auf andere Finanzdienstleister übertragbar. Die in Abschnitt 2 vorgestellten Phasen des BCM-Prozesses wurden auf den betrachteten Finanzdienstleister angepasst (vgl. das in Abb. 3 dargestellte Vorgehensmodell). Das Modell besteht aus fünf aufeinanderfolgenden Schritten, beginnend mit der Etablie-

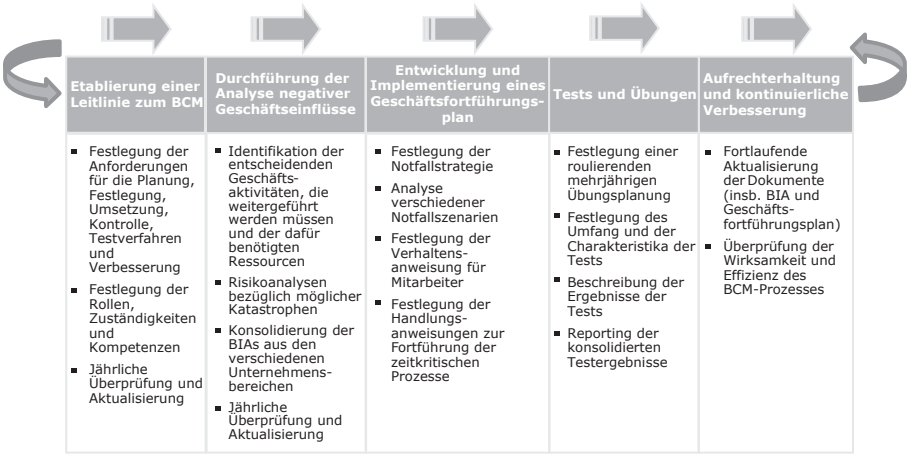

Abb. 3 Vorgehensmodell zur praktischen Umsetzung eines BCM beim betrachteten Finanzdienstleistungsunternehmen

rung einer Leitlinie zum BCM. Die allgemeinen Gestaltungshinweise zur Umsetzung werden jeweils ergänzt durch Erkenntnisse aus der Anwendung beim betrachteten Finanzdienstleister.

3.1 Etablierung einer Leitlinie zum BCM

Um BCM in einem Finanzdienstleister zu etablieren, sind anhand einer Leitlinie zum BCM, die von der Leitungsebene initiiert, mitentwickelt und freigegeben wird, die Rahmenbedingungen festzulegen (BSI 2008, Smit 2005). Die geltenden (inter-) nationalen Normen sind dabei zu beachten. Die Leitlinie stellt das übergeordnete Rahmenwerk des BCM dar und ist für alle rechtlichen Einheiten und alle Standorte eines Finanzdienstleisters verpflichtend. Sie definiert allgemein und standortübergreifend die Anforderungen für die Planung, Festlegung, Umsetzung, Kontrolle, Testverfahren und Verbesserung des BCM. Auch die Rollen, Zuständigkeiten und Kompetenzen (vgl. Abschnitt 2) im Hinblick auf die Planung des BCM werden hier festgelegt. Die Leitlinie ist jährlich zu überprüfen und bei Bedarf zu aktualisieren.

Im betrachteten Finanzdienstleister wurde u. a. festgelegt, dass IT für die unternehmensweite Koordination des BCM verantwortlich ist. Es wurde zudem definiert, dass sich das Krisenmanagement-Team neben der Geschäftsleitung aus den Leitern der Bereiche Personal, Gebäudemanagement, IT, Unternehmenskommunikation, Compliance und Operations zusammensetzt. Des Weiteren erfolgt die Planung von Arbeitsabläufen und Maßnahmen bei Unterbrechungen auf Basis der Annahme des Eintretens vier verschiedener Ausfallszenarien (Gebäudeausfall, Personalausfall, IT-Ausfall, Ausfall externer Dienstleister).

3.2 Durchführung der Analyse negativer Geschäftseinflüsse

Jährlich ist eine detaillierte Analyse negativer Geschäftseinflüsse (Business Impact Analysis (BIA)) durchzuführen. Ziel der BIA ist es, für jede relevante Abteilung an

jedem Standort die entscheidenden zeitkritischen Geschäftsprozesse zu identifizieren, die weitergeführt werden müssen, da sonst ein hoher Schaden (z. B. finanzieller Verlust, Verstoß gegen Gesetze oder Verträge, Imageschaden) für die Unternehmung zu erwarten ist (BSI 2008, Winkler et al. 2010). Zudem sollen die Wechselwirkungen dieser Prozesse mit anderen Funktionen (einschließlich externer Parteien) identifiziert und Minimalanforderungen an die benötigten Ressourcen (z. B. IT-Systeme, Kommunikationsdienste und Personalstärke) festgelegt werden (Naujocks 2003). Hierzu müssen die Bedrohungen für Prozesse und Ressourcen identifiziert und geschäftliche Schäden und sonstige Auswirkungen (wie bspw. auf die Reputation) bei einer Unterbrechung abgeschätzt und bewertet werden. Es sind also die Wiederanlaufparameter, wie bspw. der maximal zulässige Datenverlust (Recovery Point Objective, RPO), die Wiederanlaufzeit (Recovery Time Objective, RTO), die Notbetriebszeit (Work Recovery Time, WRT) und die maximal tolerierbare Ausfallzeit (Maximum Tolerable Period of Disruption, MTD) zu identifizieren (vgl. Abb. 4) und der Abhängigkeitsgrad des jeweiligen Geschäftsprozesses von den Ressourcen zu bestimmen. Es wird angestrebt, einen „Single Point of Failure“ (Ressourcen, deren Ausfall einen Komplettausfall von Geschäftsprozessen verursacht) zu vermeiden (BSI 2008).

Anhand der BIA wird bspw. für den geschäftskritischen Prozess des Wertpapierhandels des betrachteten Finanzdienstleisters identifiziert, dass er aufgrund der weltweiten Orderannahmeschlüsse an einem Handelstag innerhalb von maximal drei Stunden wieder funktionsfähig sein muss und kein Datenverlust betreffend der Markt- und Kundendaten tolerierbar ist. Dies gilt für jedes der betrachteten Ausfallszenarien. Bei der betrachteten Bank erfolgt die BIA zur Sicherstellung der Einheitlichkeit unter Verwendung einer Standardvorlage und wird mindestens jährlich überprüft und aktualisiert. Dabei wird die Aktualisierung durch die zentrale Koordination angestoßen und von den bereichsspezifischen Ansprechpartnern für die jeweiligen geschäftskritischen Prozesse durchgeführt. Die Überprüfung und Konsolidierung der Ergebnisse der BIA wird wiederrum durch die zentrale Koordination vorgenommen.

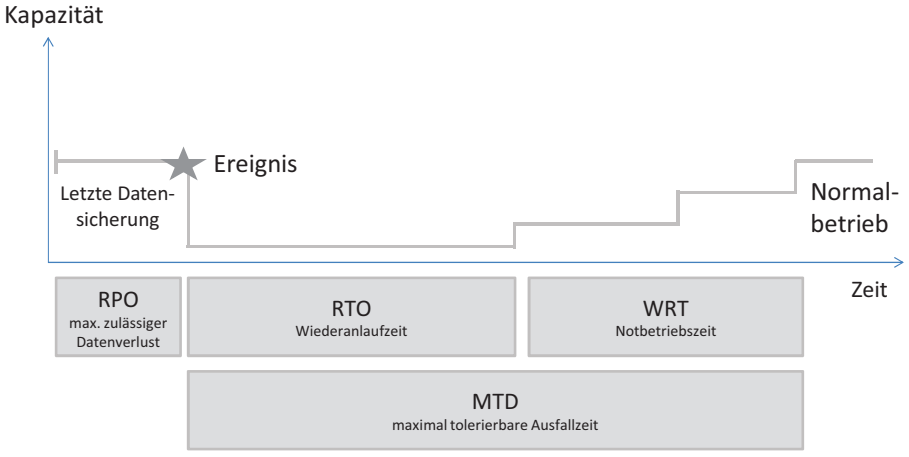

Abb. 4 Wiederanlaufparameter in Anlehnung an BSI (2008)

3.3 Entwicklung und Implementierung eines Geschäftsfortführungsplan

Die Entwicklung und Implementierung eines Geschäftsfortführungsplan erlaubt es Finanzdienstleistern, strukturiert auf Unterbrechungen des Geschäftsbetriebs zu reagieren (Winkler et al. 2010). Es wird definiert, wie in einen definierten Notbetrieb zu wechseln ist und wie aus diesem Notbetrieb über eine geplante Wiederherstellungsphase in den Normalbetrieb zurück zu kehren ist (Krell 2006). Der Geschäftsfortführungsplan stellt somit sicher, dass die relevanten Bereiche an jedem Standort eines Finanzdienstleisters über die dafür notwendigen Planungsprozesse verfügen. Nebst allgemeinen Informationen zur BCM-Organisation eines Finanzdienstleisters (u. a. Verhaltensanweisung für die Mitarbeiter, Kommunikationsregeln bei Geschäftsunterbrechungen oder Sammelpunkte beim Gebäudeausfall) beinhaltet der Geschäftsfortführungsplan die detaillierten Handlungsanweisungen zur Geschäftsfortführungs- und Wiederanlaufplanung der zeitkritischen Prozesse. Für alle kritischen Prozesse, die nach einer Unterbrechung des Geschäftsbetriebs zwingend zeitnah (bspw. innerhalb der ersten drei Tage) wieder benötigt werden und ohne die einem Finanzdienstleister der Entzug der Erlaubnis zum Betreiben von Bankgeschäfte durch die Bundesanstalt für Finanzdienstleistungsaufsicht droht, wird im Geschäftsfortführungsplan für jedes Ausfallszenario detailliert beschrieben, anhand welcher alternativen Bearbeitungsweisen das angestrebte Prozessergebnis erzielt werden kann. So hat man beim Personalausfall bspw. die Möglichkeit, auf Knowhow eines anderen Mitarbeiters zurückzugreifen.

Beim Eintreten des Ausfallszenarios „Ausfall des Gebäudes“ wird davon ausgegangen, dass ein für den Finanzdienstleister relevantes Gebäude aufgrund von bspw. Feuer, Sturm, Hochwasser, Erdbeben oder Explosion ausgefallen ist oder zumindest der Zutritt nicht mehr möglich ist. Je nach Art der Gebäudenutzung, z. B. Rechenzentren, Bürogebäude oder Filialen, sind die Auswirkungen auf den Geschäftsbetrieb unterschiedlich stark. Der betrachtete Finanzdienstleister hat daher die Möglichkeiten, wo und wie die Mitarbeiter beim Ausfall eines Standort arbeiten können, um die kritischen Prozesse fortzuführen, gegenüber gestellt und dies im Geschäftsfortführungsplan festgehalten. Diese Überlegungen sind insbesondere für den Hauptstandort des Finanzdienstleisters vorzunehmen da eine Vielzahl von Tätigkeiten dort ausgeführt wird, u. a auch der geschäftskritische Prozess des Wertpapierhandels dort angesiedelt ist und die Lage in Fluss- und Flughafennähe als per se gefährlich eingeschätzt wird. Die im Rahmen der Aktualisierung der BIA (Schritt 2) ermittelte Einschätzung betreffend der Kritikalität der Geschäftsprozesse bildet die Grundlage für diese Entscheidung. Darauf aufbauend sind die in der maximal tolerierbaren Ausfallzeit zu erwarteten Risiken (bzw. der zu erwartende Schaden aufgrund des längerfristigen Ausfalls der zeitkritische Geschäftsprozesse (z. B. Wertpapierhandel)) den möglichen Maßnahmen und den dafür zu erwartenden Kosten (z. B. für die Anmietung von alternativen Räumlichkeiten und die benötigte Infrastruktur) gegenüber zu stellen. Anhand dieser Evaluierung wurde im betrachteten Finanzdienstleister festgelegt, dass für den als relativ wahrscheinlich eingeschätzten Ausfalls des Hauptgebäudes ein alternativer Standort eingerichtet werden soll und eine Spontan-Reaktion nicht ausreichend ist um die Fortführung der geschäftskritischen Prozesse sicherzustellen. Betreffend der IT-Systemarchitektur am alternativen Standort kann auf verschiedene

Wiederherstellungsmodi zurückgegriffen werden (Sommer 2004): Bei einer Cold Standby-Lösung können Räumlichkeiten und Infrastruktur innerhalb eines definierten Zeitraums in Betrieb genommen werden. Die Einrichtung mit der benötigten Hardware und das Bespielen mit Software benötigen hierbei allerdings eine gewisse Zeit. Bei der zügigen Wiederherstellung (Warm Standby) ist die Infrastruktur bereits vorhanden, so dass die Wiederherstellung damit innerhalb 24–72 Stunden möglich ist. Wenn der Betrieb ohne größere Unterbrechungen sobald wie möglich wieder aufgenommen werden soll, kommt nur die sofortige Wiederherstellung (Hot Standby, d. h. eine gespiegelte Produktivumgebung mit den aktuellen Daten) in Frage. Für die essentiellen Bankprozesse wie bspw. Wertpapierhandel kommt aufgrund der hohen Bedeutung für den Fortbestand des betrachteten Finanzdienstleisters nur die letztgenannte Lösung in Frage.

3.4 Tests und Übungen

Die Funktionsfähigkeit des BCM wird über die laufende Durchführung von Tests und Übungen sichergestellt (Gibb und Buchanan 2006). Ziel der durchzuführenden Übungen ist es, zeitkritische Geschäftsprozesse in den Alternativverfahren (z. B. anderer Standort, andere IT-Services oder andere Mitarbeiter) durchzuführen und Schwachstellen und Verbesserungspotenziale zu identifizieren. Die Ergebnisse der Übungen werden von den Teilnehmern dokumentiert. Gewonnene Erkenntnisse und Nachweise der Funktionsfähigkeit des BCM sollen zudem den verantwortlichen internen und externen Anspruchsgruppen präsentiert werden (BSI 2008). Bei der Ausgestaltung der Übungsplanung gilt es verschiedene Aspekte zu berücksichtigen (Gibb und Buchanan 2006): Der Umfang der Übung kann von der einfachen Überprüfung von Einzelmaßnahmen bis hin zur komplexen Ernstfallübung des gesamten Unternehmens reichen. Des Weiteren können die Übungen real/physisch durchgeführt werden oder lediglich simuliert werden. Das definierte Übungsziel (bspw. schnellstmögliche Reaktion) bestimmt zudem die Ausgestaltung.

Die Planung der Übungen beim betrachteten Finanzdienstleister erfolgt auf Basis einer rollierenden mehrjährigen Übungsplanung. Es liegt die Prämisse zugrunde, dass die Übungen den normalen Geschäftsbetrieb nicht beeinträchtigen (erhaltendes Szenario). Im Rahmen eines dreijährigen Turnus werden rollierend jeweils entweder die Funktionsfähigkeit der BCM-Organisation (Kommunikation im Unterbrechungsfall, Entscheidungsfindungen im Krisenmanagement-Team) oder die Funktionsfähigkeit der kritischen Geschäftsprozesse in jedem der betrachteten Ausfallszenarien überprüft. Die rollierende mehrjährige Übungsplanung wird periodenorientiert von der BCM Koordination geplant und durch das Krisenmanagement freigegen. Besonderen Stellenwert nimmt dabei das Szenario „Ausfall der IT“ ein, das aufgrund der hohen Eintrittswahrscheinlichkeit jedes Jahr geprüft wird. Hierbei wird einerseits getestet, wie mit dem Ausfall eines Rechenzentrums und damit verbunden dem Ausfall einzelner Applikationen umgegangen wird. Andererseits wird geprüft, ob anhand der im Rahmen der Erstellung des Geschäftsfortführungsplans erarbeiteten alternativen Herangehensweisen das angestrebte Prozessergebnis erreicht werden kann. Die Übungen werden zudem an allen Standorten des Finanzdienstleisters durchgeführt.

3.5 Aufrechterhaltung und kontinuierliche Verbesserung

Um das BCM kontinuierlich verbessern zu können, müssen nicht nur angemessene Vorsorgemaßnahmen umgesetzt, reaktive Maßnahmen geplant und Dokumente fortlaufend aktualisiert werden, sondern auch der BCM-Prozess selbst muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden (BSI 2008). Änderungsbedarf ergibt sich auch bspw. bei Änderungen der Rahmenbedingungen wie gesetzlichen oder sonstigen Auflagen oder durch die strategische Neuausrichtung der Unternehmung. Zudem besteht die Notwendigkeit, die Fähigkeit von Finanzdienstleistern, Unterbrechungen bewältigen zu können, regelmäßig intern und extern beurteilen zu lassen (BSI 2008).

Beim betrachteten Finanzdienstleister wird intern anhand von Selbstbewertungen (Self-Assessments) kontrolliert, ob die Umsetzung von Maßnahmen korrekt nach den Vorgaben erfolgt, wie viele der Vorgaben umgesetzt sind und ob die vorgegebenen Prozesse gelebt werden. Im Rahmen der Durchführung von internen Revisionen wird zudem u. a. dokumentiert, ob die Leitungsebene ihre Überprüfungspflicht wahrnimmt. Es wird die Einhaltung von internen und externen Richtlinien überprüft sowie ein Vergleich zu Standards und Best Practices durchgeführt. Externe Revisionen werden durch die Aufsichtsorgane initiiert. Als Prüfungsmethoden werden sowohl intern als auch extern Dokumentenprüfungen, Interviews und Begehungen eingesetzt. Die Feststellungen der Überprüfungen werden mit dem sich ergebenden Handlungsbedarf in Revisionsberichten festgehalten.

4 Handlungsempfehlungen und Ausblick auf zukünftige Entwicklungen

Damit sichergestellt werden kann, dass die wesentlichen Prozesse nicht durch Unterbrechungen beeinflusst werden sollten neben den im Umsetzungsprozess genannten Aspekten die folgenden Faktoren beachtet werden. In erster Linie ist eine klare Kompetenzverteilung und die Etablierung einer entsprechenden Kultur des BCM von Bedeutung (Swartz et al. 2003). Zudem ist es notwendig, dass die Unternehmensleitung das Thema BCM unterstützt (Järveläinen 2013). Im betrachteten Unternehmen ist dies folgendermaßen geregelt: IT ist für BCM verantwortlich und der zuständige Vorstand nimmt die Leitung des Krisenmanagement-Teams wahr. Die Verantwortlichen für das BCM sollten darüber hinaus dazu beitragen, ein Bewusstsein für die möglichen Ausfälle im Unternehmen zu schaffen (Cerullo und Cerullo 2004), da die durchgängige Integration der Leitgedanken des BCM in die Unternehmenskultur ausschlaggebend für dessen Erfolg ist. Dazu finden im betrachteten Unternehmen regelmäßig Treffen des Krisenmanagement-Teams und der bereichsspezifische Ansprechpartner für das BCM statt. Zudem sind die Mitarbeiter aktiv in den BCM-Prozess (bspw. in die beschriebenen Risikoanalyen) mit einzubeziehen und durch Sensibilisierungs- und Schulungsmaßnahmen auf ihre Rollen und auf den Ernstfall vorzubereiten. Dies kann bspw. durch regelmäßige Evakuierungs- oder sonstige Notfallübungen geschehen. Dafür ist auch die entsprechende Kommunikation an alle relevanten Stakeholder von Bedeutung (Gibb und Buchanan 2006). BCM und die notwendigen proaktiven und reaktiven Maßnahmen sollten so Bestandteil der tägli-

chen operativen Arbeit werden (Järveläinen 2013). Je mehr Mitarbeiter sich proaktiv mit der Wiederherstellung der von ihnen verantworteten Tätigkeiten vertraut machen, desto mehr steigt die Fähigkeit einer Organisation auf Unterbrechungen reagieren zu können (Järveläinen 2013). Es gilt zudem zu beachten, dass Finanzdienstleister häufig auf verschiedenste Art und Weisen mit anderen Unternehmen vernetzt sind. Diese Abhängigkeiten sind vor allem in der BIA zu erfassen. So ist bspw. bei der Auslagerung (Outsourcing) von Dienstleistungen bzw. Geschäftsprozessen zu beachten, dass für die eigene Institution die Anzahl der Risiken steigt, die außerhalb des eigenen Einflussbereiches liegen. Damit verbunden ist ein Verlust an Kontrolle. Zusätzlich steigen die Risiken für die internen Geschäftsprozesse, die von diesen Dienstleistern abhängig sind (BSI 2008). In allen Phasen des Umsetzungsprozesses und insbesondere im Rahmen der regelmäßigen Aktualisierung der Analyse negativer Geschäftseinflüsse sowie bei den Übungen sollten derartige Abhängigkeiten berücksichtigt werden.

Literatur

Brandt C, Hermann F, Engel T (2009) Modeling and reconfiguration critical business processes for the purpose of a business continuity management respecting security, risk and compliance requirements at credit suisse using algebraic graph transformation. In: Enterprise distributed object computing conference workshops, 13th Proc. international workshop on dynamic and declarative business processes, IEEE Xplore Digital Library, S 64–71

Cerullo V, Cerullo MJ (2004) Business continuity planning: a comprehensive approach. Inform Syst Manage 21(3):70–78

Gibb F, Buchanan S (2006) A framework for business continuity management. Int J Inform Manage 26(2):128–141

Herbane B, Elliott D, Swartz E (1997) Contingency and continua: achieving excellence through business continuity planning. Business Horizons 40(6):19–25

Järveläinen J (2013) IT incidents and business impacts: validating a framework for continuity management in information systems. Int J Inform Manage 33(3):583–590

Krell E (2006) Business continuity. Management Society of Management Accountants of Canada, Mississauga

Naujoks U (2003) Notfallplanung in einer globalisierten Bank. In Wieczorek M, Naujoks U, Bartlett B (Hrsg) Business continuity. Springer, Heidelberg, S 109–127

Smit, N (2005) Business continuity management – a maturity model. Master's Thesis. Erasmus University Rotterdam

Sommer, J (2004) IT-Servicemanagement mit ITIL und MOF. mitp, Bonn

Swartz E, Herbane B, Elliott D (2003) Greater than the sum of its parts: business continuity management in the UK finance sector. Risk Management 5(1):65–80

Winkler U, Fritzsche M, Gilani W, Marshall M (2010) A model-driven framework for process-centric business continuity management. 7th International conference on the quality of information and communications technology, Porto, S 248–252