SwissBanking

August 2013

Empfehlungen für das Business Continuity Management (BCM)

Inhaltsverzeichnis

1 Ausgangslage und Zielsetzung

Verschiedene Entwicklungen der letzten Jahre, insbesondere im Bereich Terrorismus, Pandemie und Naturkatastrophen, haben auf die Verletzlichkeit von Finanzmarktteilnehmern und -systemen hingewiesen. Die Sensibilisierung für derartige Ereignisse und ihre möglichen Auswirkungen hat stark zugenommen.

Dementsprechend bestehen auf der Ebene internationaler Organisationen sowie in verschiedenen Ländern Vorgaben und Empfehlungen im Bereich des Business Continuity Management (BCM) mit Anforderungen an die Finanzmarktteilnehmer wie auch an die Aufsichtsbehörden.

Die Eidgenössische Finanzmarktaufsicht (FINMA) erachtet ein adäquates Business Continuity Management als Bewilligungsvoraussetzung zum Geschäftsbetrieb gemäss Art. 3 Bankengesetz und unterstützt die Selbstregulierung der Schweizerischen Bankiervereinigung (SBVg).

Die vorliegende Selbstregulierung der Schweizerischen Bankiervereinigung richtet sich an deren Mitglieder und enthält Empfehlungen („best practice") zur Ausgestaltung eines institutsspezifischen BCM. Dabei ist den Besonderheiten der jeweiligen Ausgangslage, insbesondere der Risikosituation und systemischen Relevanz der einzelnen Institute, Rechnung zu tragen.

Drei Kapitel der vorliegenden Empfehlungen sind von der FINMA gemäss Rundschreiben 2008/10 „Selbstregulierung als Mindeststandard" anerkannt und gelten als aufsichtsrechtlicher Mindeststandard, dessen Einhaltung von den Prüfgesellschaften geprüft wird. Verbindlich sind die Definition einer Business Continuity Management Strategie (Kapitel 4.4), die Durchführung einer Business Impact Analyse (Kapitel 4.5.1) sowie die Festlegung von Business Recovery Optionen (Kapitel 4.5.2).

In den Geltungsbereich der vorliegenden Empfehlungen fallen Banken und Effektenhändler (im Folgenden: Institute). Eine Auswirkung der Empfehlungen auf das zivilrechtliche Verhältnis zwischen dem Institut und seinen Kunden ist nicht beabsichtigt.

2 Grundlagen

Die vorliegenden Empfehlungen lehnen sich an verschiedene vergleichbare Standards an (vgl. auch die weiterführenden Quellen in Anhang D). Insbesondere orientieren sie sich

- an den „High-Level Principles for Business Continuity“ des Joint Forum bzw. des Basler Ausschusses für Bankenaufsicht[1]
- am „British Standard for Business Continuity Management BS 25999“[2] resp. am ISO 22301[3].

Die erwähnten „High-Level Principles“ beinhalten folgende Empfehlungen:

1. Finanzmarktteilnehmer und Aufsichtsbehörden sollten über ein effektives und umfassendes Business Continuity Management verfügen. Die Verantwortung für die Sicherstellung der Business Continuity Fähigkeit liegt bei Verwaltungsrat (Board of Directors) und Geschäftsleitung (Senior Management).
2. Finanzmarktteilnehmer und Aufsichtsbehörden sollten in ihrem Business Continuity Management das Risiko bedeutender operationeller Störungen berücksichtigen.
3. Finanzmarktteilnehmer sollten Recovery-Ziele (Recovery Time Objectives, RTO) entwickeln, welche ihre Systemrelevanz bzw. das von ihnen ausgehende Risiko für das Finanzsystem berücksichtigen.
4. Die Business Continuity Pläne sowohl der Teilnehmer des Finanzmarkts als auch der Aufsichtsbehörden sollten Massnahmen der internen und externen Kommunikation für den Fall grösserer Betriebsunterbrüche definieren.
5. Für den Fall internationaler Implikationen von Betriebsunterbrüchen sollten die entsprechenden Kommunikationskonzepte insbe-

[1] Basel Committee on Banking Supervision, Bank for International Settlements, August 2006, www.bis.org.
[2] British Standards Institution, September 2008, www.bsigroup.com.
[3] International Organization for Standardization (ISO), Mai 2012, www.iso.org.

sondere auch die Kommunikation mit ausländischen Aufsichtsbehörden umfassen.

6. Finanzmarktteilnehmer und Aufsichtsbehörden sollten ihre Business Continuity Pläne austesten, deren Wirksamkeit evaluieren und ihr Business Continuity Management gegebenenfalls anpassen.

7. Den Aufsichtsbehörden wird empfohlen, das Business Continuity Management der beaufsichtigten Institute im Rahmen der laufenden Überwachung zu beurteilen.

Des Weiteren soll den Ergebnissen der Arbeitsgruppe „BCP Finanzplatz Schweiz", welche unter dem Vorsitz der Schweizerischen Nationalbank (SNB) die beiden Prozesse „Grossbetragszahlungen SIC" und „Liquiditätsversorgung via Repos" als kritisch identifiziert hat, Rechnung getragen werden.[4]

3 Anwendungsbereich bzw. Bedrohungen

Die Institute haben alle potentiell relevanten Bedrohungen zu berücksichtigen, welche für das Unternehmen zu einer Krise führen können. Dabei wird unter einer „Krise" eine Bedrohungssituation verstanden, welche kritische Entscheidungen erfordert und mit den ordentlichen Führungsmitteln und Entscheidungskompetenzen nicht bewältigt werden kann. Insofern ist die Bewältigung von „Störungen" ausdrücklich nicht Gegenstand dieser Empfehlungen („Availability Management", vgl. Begriffsdefinitionen in Anhang A und Anhang B). Beispiele für Krisensituationen sind:

- „unfallartige" Ereignisse wie z.B. Brand oder Explosion
- Terrorangriffe, Sabotage
- Naturkatastrophen wie z.B. Flut oder Erdbeben.

Im Sinne von „best practice" wird jedoch empfohlen, sich bei der Ausgestaltung des Business Continuity Managements vor allem auf die

[4] Schweizerische Nationalbank (SNB), Business Continuity im schweizerischen Finanzsektor, 2006 und 2009, www.snb.ch.

Konsequenzen und nicht auf die Ursachen von Krisen vorzubereiten. Für die Wiederherstellung kritischer Geschäftsprozesse bzw. Geschäftstätigkeiten sollten nach einem Unterbruch gemäss den definierten Recovery Zielen die Business Recovery Optionen verschiedene Auswirkungen berücksichtigen (vgl. Kapitel 4.5.2).

Im Rahmen des BCM sind die relevanten Bedrohungen durch die Institute jeweils gemäss Impact (Schweregrad) zu identifizieren bzw. definieren und zu beurteilen.

Konsequenz solcher Ereignisse kann insbesondere sein, dass Mitarbeitende und/oder Infrastrukturen (v.a. Gebäude bzw. Arbeitsplätze, Führungsinfrastruktur, Telekommunikation) für kritische Geschäftsprozesse nicht mehr oder nur noch teilweise einsatzfähig sind. Ebenso können Probleme bei den IT-Dienstleistungen oder Infrastruktur-Anbietern dazu führen, dass kritische Geschäftsprozesse nicht mehr durchgeführt werden können.

Im Bereich von Pandemien sind Schadenszenarien und Empfehlungen des Bundesamts für Gesundheit (BAG) zu berücksichtigen. Bei der Pandemieplanung soll dem Umstand Rechnung getragen werden, dass sich die Auswirkungen einer grossflächigen Infektionskrankheit hinsichtlich Dauer und Vorhersehbarkeit des Eintretenszeitpunkts massgeblich von klassischen BCM Krisensituationen unterscheiden.

Die BCM Krisensituation

- tritt überraschend ein und hat rasch massive Konsequenzen auf den Geschäftsbetrieb und
- die Planung fokussiert auf die rasche Wiederherstellung der Handlungsfähigkeit.

Indessen weist eine Pandemie

- eine längere Vorlaufzeit bis zur Kulmination der Erkrankungen auf und
- erfordert die Planung der Aufrechterhaltung kritischer und die Sistierung weniger kritischer Geschäftsprozesse.

Es wird empfohlen zumindest auf Institutsebene einen Pandemieplan zu erstellen. Aktuelle Informationen hierzu sind auf der entsprechenden Homepage des BAG[5] abrufbar.

In vielen Geschäftsprozessen werden Leistungen durch externe Dienstleister und Lieferanten erbracht, die ebenfalls kurzfristig ausfallen können. Wird bei kritischen Geschäftsprozessen die Unterstützung externer Dienstleister und Lieferanten beigezogen, soll deren BCM Maturität in geeignetem Rahmen beurteilt werden.

Im Rahmen der Business Recovery Optionen (Kapitel 4.5.2) kann unter anderem der Transfer von externen zu internen Dienstleistern geprüft werden. Ebenfalls können vorsorglich redundante oder alternative Anbieter verpflichtet werden.

In Ergänzung zum FINMA-Rundschreiben 2008/7 „Outsourcing Banken – Auslagerung von Geschäftsbereichen bei Banken" wird im Sinne einer „best practice" empfohlen, grundsätzlich immer Umgehungslösungen für den Ausfall kritischer externer Dienstleister und Lieferanten zu planen.

Das BCM muss die Einhaltung gesetzlicher, regulatorischer, vertraglicher und interner Vorschriften auch im Krisenfall bestmöglich sicherstellen.

4 Empfehlungen

4.1 Definition und Umfang

Unter Business Continuity Management (BCM) ist ein unternehmensweiter Ansatz zu verstehen, mit dem sichergestellt werden soll, dass kritische Geschäftsprozesse im Falle von massiven, einschneidenden internen oder externen Ereignissen aufrechterhalten werden können. BCM zielt damit u.a. auf eine Minimierung der finanziellen, rechtlichen und reputationsbezogenen Auswirkungen solcher Ereignisse.

[5] Bundesamt für Gesundheit (BAG), Influenza-Pandemieplan Schweiz, Januar 2009, www.bag.admin.ch.

Insgesamt soll BCM die – zu einem im Vorfeld definierten Grad – Fortführung bzw. zeitgerechte Wiederaufnahme der Geschäftstätigkeit in Krisensituationen sicherstellen. BCM bezieht sich deshalb grundsätzlich auf alle Geschäfts- und Organisationsbereiche eines Unternehmens. Zu unterscheiden sind planerische Massnahmen des BCM im Vorfeld und das Krisenmanagement (Führung in der Krise) im Anwendungsfall.

4.2 Verantwortlichkeiten

Die Verantwortung für das Business Continuity Management liegt beim Verwaltungsrat und bei der Geschäftsleitung jedes einzelnen Instituts (vgl. dazu auch das FINMA-Rundschreiben 2008/24 „Überwachung und interne Kontrolle bei Banken").

Der Verwaltungsrat ist verantwortlich für die Überwachung der Einhaltung der schriftlich dokumentierten BCM Strategie. Die Geschäftsleitung konkretisiert diese und regelt weitere Zuständigkeiten, Kompetenzen und Informationsflüsse in internen Reglementen und Weisungen. Insbesondere regelt die Geschäftsleitung (mit Genehmigung durch den Verwaltungsrat) das Verhältnis zwischen Geschäftsleitung und der Krisenorganisation (Krisenstab).

4.3 Risikoanalyse

Im Rahmen des Business Continuity Management kann für kritische Ressourcen eine Risikoanalyse durchgeführt werden oder auf bestehende Risikoanalysen aus anderen Bereichen (z.B. Riskmanagement) verwiesen werden. Die Risikoanalyse dient im Kontext des BCM dazu die Gefährdungen zu identifizieren, die eine Unterbrechung von Geschäftsprozessen verursachen können. Dabei wird im Rahmen des BCM grundsätzlich davon ausgegangen, dass solche Gefährdungen eintreten können. Auch wenn nicht immer eine vollständige Identifizierung aller Risiken möglich ist, werden so doch potenzielle Gefährdungen erhoben und bewertet. Allenfalls lässt sich durch gezielte Massnahmen die Eintrittswahrscheinlichkeit eines Krisenszenarios auf ein akzeptables Niveau senken.

4.4 Business Continuity Management Strategie (verbindlicher Mindeststandard)

In der Business Continuity Management Strategie definiert das Institut seine grundsätzliche Herangehensweise an das Thema Business Continuity Management.

Die Business Continuity Management Strategie kann integraler Bestandteil der Unternehmensstrategie des Instituts sein oder aber separat bestehen. Falls einzelne Restrisiken bewusst in Kauf genommen werden, so muss die Strategie explizit darüber Auskunft geben. Diesbezügliche Entscheide sind schriftlich festzuhalten.

In der BCM Strategie sind folgende Aspekte zu regeln:

- Definition und Festlegung des Umfangs des BCM (Scope)
- Verankerung des BCM in der Unternehmensorganisation
- Schaffung einer der Unternehmensorganisation angepassten Governance-Struktur
- Definition der Rollen und Verantwortlichkeiten im Zusammenhang mit BCM
- Festlegung von Bedrohungen resp. deren Auswirkungen auf die Ressourcen des Unternehmens (Planungsgrundlage)
- Definition der Periodizität der Durchführung von Reviews und Tests der Pläne und Massnahmen
- Definition der Berichterstattung, Kommunikation und Schulung.

4.5 Elemente des Business Continuity Management

4.5.1 Business Impact Analyse (verbindlicher Mindeststandard)

Die Business Impact Analyse (BIA) liefert die notwendigen Informationen über die kritischen Geschäftsprozesse und Ressourcen. Für diese kritischen Geschäftsprozesse werden im Rahmen des BCM die jeweiligen Auswirkungen eines kompletten oder teilweisen Ausfalls der entsprechenden Ressourcen beurteilt. Jeder Geschäftsbereich bestimmt seine kritischen Prozesse und Ressourcen.

Diese Beurteilung schliesst auch gegenseitige Abhängigkeiten zwischen den Geschäftsbereichen (sogenannte Prozess-Abhängigkeiten) und Abhängigkeiten von externen Dienstleistern und Lieferanten (Outsourcing) mit ein.

Diese Analyse, aus welcher die Recovery-Ziele abgeleitet werden, soll mindestens zum Ergebnis haben:

- die definierte Zeitspanne bis zur Wiederherstellung der kritischen Geschäftsprozesse (Recovery Time Objective, RTO)
- den gewünschten Wiederherstellungsgrad der kritischen Geschäftsprozesse bezüglich des definierten RTO
- den Mindestumfang der (Ersatz-)Ressourcen (Gebäude, Mitarbeitende, IT/Daten, externe Dienstleister und Lieferanten), die im Krisenfall verfügbar sein müssen, um den gewünschten Wiederherstellungsgrad zu erreichen.

Die BIA ist jährlich zu überprüfen, wobei sich Art und Umfang einer solchen Überprüfung insbesondere nach der spezifischen Risikosituation des jeweiligen Instituts richten.

4.5.2 Business Recovery Optionen (verbindlicher Mindeststandard)

Die Business Recovery Optionen legen auf operationeller Ebene das grundlegende Vorgehen dar, mit dem das Unternehmen – für die gemäss Kapitel 4.5.1 ausgewählten Geschäftsbereiche – seine in der Business Impact Analyse festgelegten Recovery Ziele für die zugrunde gelegten Bedrohungen und deren Auswirkungen auf die Ressourcen erreichen will. Die Recovery Ziele sollen in schriftlicher Form festgehalten werden und die festgelegten Recovery Optionen für die kritischen Ressourcen beinhalten. So soll im Minimum dargelegt werden, welche Business Recovery Optionen für Ausfälle von

- Personal
- Gebäuden
- IT-Systemen oder IT-Infrastruktur (inkl. Kommunikationssystemen)

- externen Dienstleistern und Lieferanten (Outsourcing) wie z.B. Informationsprovider

grundsätzlich zur Verfügung stehen. Diese Business Recovery Optionen sollen dann in den jeweiligen Business Recovery Plänen konkret ausformuliert werden. Die Akzeptanz eines Restrisikos kann eine Business Recovery Option darstellen. Diese ist analog herzuleiten und schriftlich festzuhalten.

4.5.3 Business Recovery Pläne

Business Recovery Pläne beschreiben die für die Fortsetzung (Continuity) bzw. die Wiederherstellung (Recovery) der kritischen Geschäftsprozesse (inkl. Einhaltung gesetzlicher, regulatorischer, vertraglicher und interner Vorschriften) notwendigen Vorgehensweisen, Ersatzlösungen und die dafür mindestens benötigten Ersatzressourcen. Entsprechende Pläne sollten mindestens enthalten: Beschreibung des Anwendungsfalls (auslösende Bedrohung), Vorgehensweise bzw. Massnahmenkatalog mit Prioritäten sowie notwendige Ersatzressourcen.

Business Recovery Pläne sollten mindestens einmal pro Jahr auf deren Aktualität überprüft und im Bedarfsfall angepasst werden. Wesentliche Änderungen im Geschäftsbetrieb (Reorganisationen, Aufbau eines neuen Geschäftsfelds usw.) können ebenfalls eine Überarbeitung der Pläne erforderlich machen.

4.5.4 Business Continuity Reviews

Business Continuity Reviews beinhalten eine Bestandsaufnahme der von den einzelnen Geschäftsbereichen erstellten BCM Dokumentation und eine Bewertung, ob die Dokumente den definierten Prüfkriterien entsprechen. Es wird empfohlen, konsistente Prüfkriterien sowie einen klaren Prozess zur Überwachung und Behebung offener Punkte zu definieren.

4.5.5 Business Continuity Tests

Mit Business Continuity Tests wird die Umsetzung von Business- und IT Disaster Recovery Plänen und die Fähigkeit der Krisenmanagement-Organisation ausgetestet bzw. überprüft. Schwerpunkte sowie Kadenz der einzelnen Tests sind in Abhängigkeit der Kritikalitätsbeurteilung (vgl. Business Impact Analyse) vorzunehmen. Durch das gleichzeitige Testen einzelner Organisationseinheiten kann die Fähigkeit des Gesamtinstituts zur Bewältigung von Krisensituationen beurteilt werden.

Es wird empfohlen, die einzelnen Testaktivitäten in Form einer systematischen Testplanung zu koordinieren, die Berichterstattung einheitlich zu regeln sowie einen Prozess für die Überwachung und Behebung von Schwachstellen festzulegen.

Die Planung soll so ausgelegt werden, dass die wichtigsten Massnahmen (inkl. der Krisenorganisation) mindestens einmal jährlich überprüft resp. getestet werden.

4.6 Krisenmanagement

Ziel ist es, ein Krisenmanagement zu definieren, mit dem das Unternehmen Krisensituationen wirksam und zeitgerecht bewältigen kann. In Situationen, welche kritische Entscheidungen verlangen und mit ordentlichen Massnahmen und Entscheidungskompetenzen nicht bewältigt werden können, wird der Krisenstab einberufen. Dieser übernimmt die Aufgabe der Krisenbewältigung bis zur Wiederherstellung eines ordnungsgemässen Zustands.

Es wird empfohlen, Auslösung, Zuständigkeiten und Kompetenzen des Krisenstabs vorgängig klar zu regeln und die Krisenorganisation auf Geschäftstätigkeit und geographische Struktur des Instituts auszurichten. Besonderer Wert ist auf die bestmögliche Sicherstellung der Erreichbarkeit der Verantwortungsträger auch in Krisensituationen zu legen.

4.7 Berichterstattung, Kommunikation und Schulung

4.7.1 Berichterstattung

Über die BCM Aktivitäten sowie den Stand der Vorbereitung der Krisenbewältigung sollen in einem definierten Rhythmus stufengerechte Berichte zuhanden von Verwaltungsrat und Geschäftsleitung erstellt werden. Darin sind insbesondere die Ergebnisse von Business Continuity Reviews und Business Continuity Tests darzustellen.

4.7.2 Kommunikation

Kommunikation spielt in der Krisenbewältigung eine entscheidende Rolle. Der systematischen und sorgfältigen Vorbereitung von Kommunikationskonzepten und -plänen (interne als auch externe Kommunikation) im Krisenfall ist deshalb besondere Beachtung zu schenken. Dabei geht es im Speziellen um die Wahrung eines hohen Grades an Professionalität und um die Aufrechterhaltung von Glaubwürdigkeit und Vertrauen gegenüber den verschiedenen Stakeholder eines Unternehmens.

Kommunikationspläne sollen insbesondere die Erreichbarkeit im Krisenfall sicherstellen (Namenslisten und Telefonnummern von Aufsichtsbehörden, Mitarbeitenden, Medien, Kunden, Gegenparteien, Dienstleistern etc.). Einer allfälligen internationalen Dimension ist mit speziellen Kommunikationsmassnahmen Rechnung zu tragen.

Im Falle einer Krise bzw. einer Auslösung der Krisenorganisation soll der Aufsichtsbehörde eine entsprechende Meldung erstattet werden.

4.7.3 Schulung und Sensibilisierung

Es muss sichergestellt werden, dass die Mitarbeitenden hinsichtlich ihrer Aufgaben, Verantwortlichkeiten und Kompetenzen, die sich aus den jeweiligen BCM Aktivitäten ergeben, ausreichend geschult werden. Dabei ist sowohl der Ausbildung von neuen Mitarbeitenden als auch einer regelmässigen Auffrischung des Ausbildungsstands beste-

hender Mitarbeitender Rechnung zu tragen. Besondere Beachtung ist der Ausbildung der Mitglieder der Krisenorganisation zu schenken.

Zusätzlich soll mit Hilfe eines laufenden Informationsprogramms sichergestellt werden, dass bei neuen und bestehenden Mitarbeitenden eine Sensibilisierung für die Bedeutung des BCM geschaffen und aufrechterhalten wird.

5 Inkrafttreten

Die vorliegenden Empfehlungen sind vom Verwaltungsrat der SBVg mit Beschluss vom 24. Juni 2013 verabschiedet und von der FINMA am 12. Juli 2013 genehmigt worden. Sie treten per 1. Oktober 2013 in Kraft und sind bis am 30. September 2014 umzusetzen. Sie ersetzen die Richtlinien mit demselben Titel, welche am 1. Januar 2008 in Kraft getreten waren.

Basel, den 29. August 2013

Anhang A – Glossar

Availability Management

Verfahren, das die Definition, Analyse, Planung, Messung und Optimierung aller Aspekte, welche die Verfügbarkeit der IT-Services beeinflussen, umfasst. Das Availability Management stellt sicher, dass die gesamte IT-Infrastruktur, alle IT-Prozesse, -Tools, -Aufgaben etc. den in den Service-Level-Agreements definierten Vorgaben für die Verfügbarkeit entsprechen. Ereignisse, welche die Verfügbarkeit beeinträchtigen, können mit den üblichen Managementverfahren und Entscheidungskompetenzen kontrolliert werden.

Business Continuity Management (BCM)

Unternehmensweiter Management-Ansatz (Policies und Standards), mit dem sichergestellt werden soll, dass die kritischen Geschäftsprozesse im Fall (interner oder externer) Ereignisse aufrechterhalten oder zeitgerecht wiederhergestellt werden können. BCM umfasst damit die Phasen der Planung und Umsetzung sowie des Controllings und deckt das gesamte entsprechende Umfeld (Bereiche, Prozesse, Techniken) ab, welches erforderlich ist, um die Verfügbarkeit kritischer Geschäftsprozesse nach einem Ereignis unterbruchsfrei betreiben oder innerhalb definierter Zeitspannen wiederaufnehmen zu können.

Business Continuity Management Strategie

In der BCM Strategie definiert das Institut seine grundsätzliche Herangehensweise an das Thema Business Continuity Management. Zu diesem Schritt gehört unter anderem auch die Festlegung einer verantwortlichen Stelle für BCM, die Definition von Rollen und Verantwortlichkeiten und das Definieren des Scopes der BCM Aktivitäten.

Diesbezügliche Entscheide sind schriftlich festzuhalten.

Business Continuity Reporting

Berichterstattung (inkl. an Verwaltungsrat und Geschäftsleitung) über Aktivitäten im Bereich des Business Continuity Management, insbesondere über den Stand der Vorbereitungen zur Krisenbewältigung. Das Business Continuity Reporting hat im Speziellen die Ergebnisse von Business Continuity Reviews und Business Continuity Tests darzustellen.

Business Continuity Tests

Systematische Überprüfung in regelmässigen Intervallen der Business Continuity Pläne, insbesondere hinsichtlich Umsetzung, Wirksamkeit und Aktualität.

Verfügt das Unternehmen über eine betriebsinterne IT Organisation, sind selbstverständlich auch die IT Disaster Recovery Pläne regelmässig zu testen.

Business Impact Analyse (BIA)

Prozess der Identifikation und (quantitativen und qualitativen) Messung der Auswirkungen von Unterbrüchen der Geschäftstätigkeit oder einzelner Ressourcen und Prozesse. Die BIA umfasst insbesondere die Identifikation kritischer Geschäftsprozesse und der für das Business Recovery benötigten Ressourcen, basierend auf einer Analyse von Abhängigkeiten und Auswirkungen sowie einer Bewertung und Klassifikation potentieller Schäden.

Business Recovery

Wiederherstellung spezifischer Prozesse bzw. Geschäftstätigkeiten nach einem Unterbruch zu einem vordefinierten Wiederherstellungsgrad bzw. nach einem Schadenereignis zu treffende Massnahmen (vgl. Business Recovery Pläne). Dies kann in verschiedenen Schritten erfolgen bis die ordentliche Geschäftstätigkeit bzw. die volle Kapazität wiederhergestellt ist.

Business Recovery Optionen

Definition der grundsätzlichen Vorgehensweise zur Aufrechterhaltung einer kontinuierlichen Geschäftstätigkeit bzw. im Falle eines Ausfalls kritischer Ressourcen (inkl. Festlegung der Risiko-Akzeptanz, Analyse von Handlungsoptionen und Grundsatzentscheiden über die Bereitstellung von Ersatzressourcen). Die Business Recovery Optionen basieren auf der Business Impact Analyse und bilden die Basis für die Business Recovery Pläne.

Business Recovery Plan

Umfassend vorbereiteter Massnahmenplan (inkl. Checklisten und Arbeitshilfen), um eine kontinuierliche Geschäftstätigkeit bzw. eine geordnete und zeitgerechte Wiederaufnahme der kritischen Geschäftsprozesse im Krisenfall zu ermöglichen.

Krise

Bedrohungssituation, welche kritische Entscheidungen erfordert und im Rahmen der ordentlichen Führungsstruktur (Führungsmittel, Entscheidungskompetenzen) nicht bewältigt werden kann.

Krisenstab (auch: Crisis Management Team (CMT) oder Notfallorganisation)

Team, welches im Krisenfall für die Krisenbewältigung bis zur Wiederaufnahme eines ordnungsgemässen Zustands verantwortlich ist (Minimierung des wirtschaftlichen Schadens sowie von Reputationsrisiken).

Kritische Geschäftsprozesse

Geschäftsprozesse eines Unternehmens, deren Ausfall die Aufrechterhaltung der Kundendienstleistungen, die Einhaltung der regulatorischen Verpflichtungen des Unternehmens und/oder die Bewirtschaftung von Risikopositionen verunmöglichen oder erheblich erschweren und dadurch zu einem kritischen (direkten oder indirekten) Schaden führen kann.

Kritische Ressourcen

Ressourcen einer Unternehmung (Personal, Gebäude, IT/Daten, externe Dienstleister und Lieferanten etc.), welche bei Ausfall zum Unterbruch oder Ausfall von (kritischen) Geschäftsprozessen führen. Kritische Ressourcen werden im Rahmen der Business Impact Analyse identifiziert.

Recovery Point Objective (RPO)

Definierter, maximal akzeptabler Datenverlust im Falle einer Krise.

Recovery Time Objective (RTO)

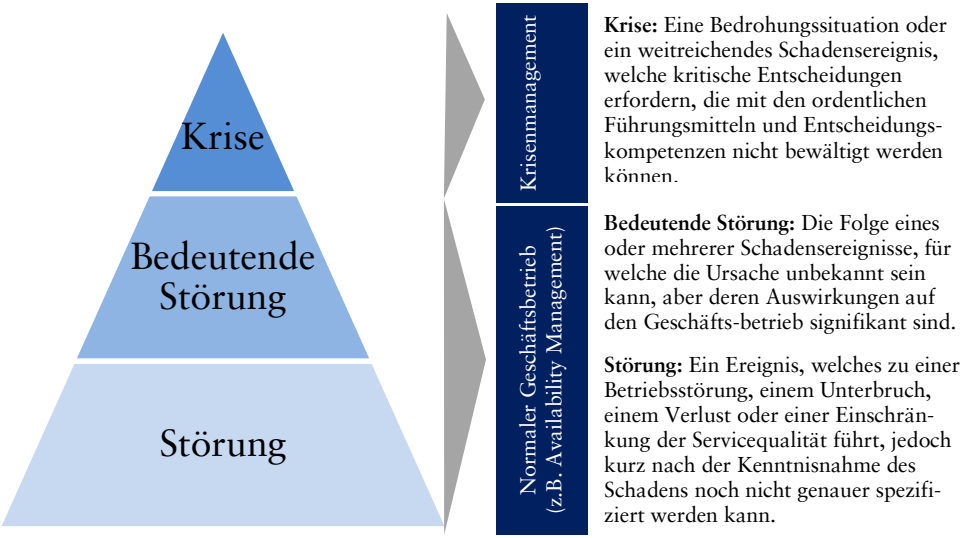
Definierter Zeitraum, innerhalb welchem kritische Geschäftsprozesse und/oder IT-Services wiederhergestellt werden müssen.

Störung

Ereignis, das zu einem Unterbruch von Geschäftstätigkeiten, einem Verlust und/oder einer Einschränkung der Servicequalität führt, jedoch (im Unterschied zu einer Krise) im Rahmen des Availability Management Prozesses bewältigt werden kann.

Anhang B – Schweregrade von Ereignissen

Je nach Schweregrad der Folgen, die aus einem oder mehrerer Ereignisse entstehen, handelt es sich um eine Störung, eine bedeutende Störung oder eine Krise. Business Continuity Management bezieht sich nur auf die Krisenvorsorge und das Krisenmanagement.



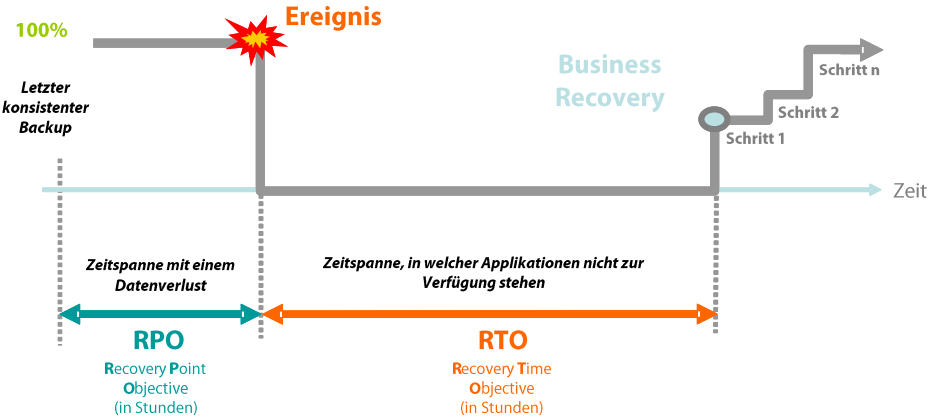
Krise: Eine Bedrohungssituation oder ein weitreichendes Schadensereignis, welche kritische Entscheidungen erfordern, die mit den ordentlichen Führungsmitteln und Entscheidungskompetenzen nicht bewältigt werden können.

Bedeutende Störung: Die Folge eines oder mehrerer Schadensereignisse, für welche die Ursache unbekannt sein kann, aber deren Auswirkungen auf den Geschäfts-betrieb signifikant sind.

Störung: Ein Ereignis, welches zu einer Betriebsstörung, einem Unterbruch, einem Verlust oder einer Einschränkung der Servicequalität führt, jedoch kurz nach der Kenntnisnahme des Schadens noch nicht genauer spezifiziert werden kann.

Anhang C – Verlauf einer Krise

Verlauf einer Krise am Beispiel des Impact Types "Verlust von IT/Daten"



Anhang D – Weiterführende Quellen

Bei der Implementierung eines betrieblichen Business Continuity Managements können u.a. die folgenden Standards herangezogen werden. Die Auswahl ist nicht abschliessend.

Australian Prudential Regulatory Authority (APRA), Prudential Standard APS 232 „Business Continuity Management" und Guidance Note 232,
www.apra.gov.au

Basel Committee on Banking Supervision (BCBS), High-Level Principles for Business Continuity, Bank for International Settlements, August 2006,
www.bis.org/publ/joint17.htm

British Standards Organisation, Business Continuity Management Standard, BS 25999-2:2007,
www.bsigroup.com/en/Standards-and-Publications/

Bundesamt für Bevölkerungsschutz (BABS), Risiko- und Gefährdungsanalyse im Bevölkerungsschutz – Eine Umfragestudie über laufende Arbeiten in den Kantonen, März 2011,
www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/dokumente/Unterlagen_Risiken.html

Bundesamt für Gesundheit (BAG), Pandemieplan – Handbuch für die betriebliche Vorbereitung, November 2007,
www.bag.admin.ch/influenza/01120/01134/03058/04319/index.html?lang=de

Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-4 – Notfallmanagement, 2008,
www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

Business Continuity Institute, The BCI Good Practice Guidelines 2008 bzw. 2010,
www.thebci.org/

Federal Reserve System (Fed), Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 2003, www.federalreserve.gov

Financial Services Authority (FSA), Business Continuity Management Practice Guide, November 2006, www.fsa.gov.uk/pubs/other/bcm_guide.pdf

Information Security Forum, Aligning Business Continuity and Information Security, März 2006, www.securityforum.org

International Organization for Standardization (ISO), ISO/IEC 27031:2011: Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44374

International Organization for Standardization (ISO), ISO 22301:2012: Societal security – Business continuity management systems – Requirements, www.iso.org/iso/catalogue_detail?csnumber=50038

Schweizerische Nationalbank (SNB), Business Continuity im Schweizerischen Finanzsektor, Januar 2006 und September 2009, www.snb.ch/de/iabout/finstab/id/finstab_bcp

Schweizerische Bankiervereinigung
Aeschenplatz 7
Postfach 4182
CH-4002 Basel
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org