

## **Business Continuity Management (BCM)**

Theorie und Praxis am Beispiel einer Schweizer Privatbank

*Bruno Gantenbein und Peter Morf*

**Die Tatsache, dass Unternehmen heutzutage in zunehmendem Masse auf ihre IT-Systeme angewiesen sind, hat dazu geführt, dass die IT-Abteilungen in den vergangenen zwanzig Jahren bei der Katastrophenvorsorge federführend waren. Jedoch ist die blossе Sicherung und Wiederherstellung von Daten und Systemzugängen nicht ausreichend, solange die Angestellten keine Telefone abnehmen und die Lieferanten dringend benötigte Komponenten nicht anliefern können. Simple Vorkommnisse wie ein länger andauernder Stromunterbruch oder das Versagen der Telekommunikationsinfrastruktur können bereits den Zusammenbruch von kritischen Geschäftsfunktionen verursachen.**

### Einführung

Der Begriff Business Continuity kann definiert werden als „die Gesamtheit der Prozesse, Verfahrensweisen, Entscheidungen und Aktivitäten“, welche sicherstellen, dass eine Unternehmung während eines längeren betrieblichen Unterbruchs trotzdem weiter funktionieren kann.

Anders ausgedrückt: es müssen proaktive und reaktive Vorkehrungen getroffen werden, um zum einen Krisen oder Katastrophen möglichst zu vermeiden, und zum anderen, sollten diese dennoch auftreten, die schnellst mögliche *Rückkehr* zu „business as usual“ zu gewährleisten.

Business Continuity umfasst zwei unterschiedliche Bereiche:

BCP - Business Continuity Planning:

- Es werden Business Continuity Pläne entwickelt, deren Umsetzung betriebliche Unterbrüche, Krisen und Katastrophen vermeiden und nach einem solchen Betriebsunterbruch die möglichst rasche Wiederaufnahme der Geschäftstätigkeit ermöglichen sollen.
- Entsprechende Schulungen und Tests stellen die Tauglichkeit dieser Business Continuity Pläne sicher.

BCM - Business Continuity Management:

- Das fortlaufende Management der Business Continuity Pläne in Bezug auf Aktualität und Verfügbarkeit ist jederzeit gewährleistet.
- Die betriebliche Stabilität und die Verfügbarkeit der kritischen Geschäftsprozessen unterstehen einer stetigen Kontrolle, mit dem Ziel, Unterbrüche der Geschäftstätigkeit möglichst gering zu halten.

Traditionellerweise stellte die Behebung von Störungen (IT Disaster Recovery) den Ausgangs- und Endpunkt der Unternehmensstrategie in Bezug auf unvorhergesehene Ereignisse dar. Bis anhin konnten so IT-Systeme und Daten nach einem Ausfall wieder in Betrieb genommen werden. Bedingt durch das Aufkommen von Business Continuity Management jedoch wurde der Fokus vermehrt auch auf die Prävention als ausschliesslich auf die Behebung von Störfällen (DR) gerichtet. Disaster Recovery ist nun als Teil des Gesamtprozesses BCM zu betrachten.

BCM deckt den gesamten Lebenszyklus von der Prävention bis zur Behebung von kritischen Störfällen ab. Obwohl die Initiative ursprünglich von der IT ausging, umfasst BCM die gesamte Organisation eines Unternehmens. Es ist eine geplante und kontrollierte Vorgehensweise zur Vorwegnahme und/oder Reaktionen auf Ereignisse, die wichtige geschäftliche Geschäftsprozesse unterbrechen könnten. Proaktive Massnahmen dienen der Prävention von Unterbrüchen organisatorischer Abläufe und reaktive Massnahmen dienen der Behebung von kritischen Unterbrüchen in der Abwicklung von Geschäftsfällen.



## Business Continuity Management (BCM)

Theorie und Praxis am Beispiel einer Schweizer Privatbank

Das Business Continuity Institute<sup>1</sup> empfiehlt bei der Erarbeitung und Umsetzung einer BCM Planung die Anwendung folgender Grundsätze:

- BCM soll integrierter Bestandteil der Corporate Governance sein.
- BCM Aktivitäten müssen mit der Geschäftsstrategie und deren Zielen abgestimmt werden und diese direkt unterstützen.
- BCM muss die organisatorische Stabilität unterstützen und die Verfügbarkeit von Produkten und Dienstleistungen optimieren.
- BCM ist ein Führungsprozess, der vor allem etabliert werden soll, um dem Unternehmen einen Mehrwert zu liefern und nicht nur aus regulatorischen oder anderen unternehmenspolitischen Erwägungen.
- Alle BCM Strategien, Pläne und Lösungen müssen auf höchster Führungsebene angesiedelt und überwacht werden.

Die Einhaltung dieser Grundsätze erleichtert die Entwicklung einer effektiven BCM Planung und soll dem Unternehmen folgende Mehrwerte schaffen:

<b>IT Perspektive</b>	<b>Business Perspektive</b>
<ul style="list-style-type: none"><li>• Rasche System- und Daten-Wiederherstellung</li></ul>	<ul style="list-style-type: none"><li>• Kundenzufriedenheit</li></ul>
<ul style="list-style-type: none"><li>• Katastrophenvorsorge</li></ul>	<ul style="list-style-type: none"><li>• Erfüllung gesetzlicher Vorschriften</li></ul>
<ul style="list-style-type: none"><li>• IT Fokus auf Geschäftsprozesse</li></ul>	<ul style="list-style-type: none"><li>• Verbesserung der Geschäftsprozess Qualität</li></ul>
<ul style="list-style-type: none"><li>• Definierte und getestete Krisenorganisation</li></ul>	<ul style="list-style-type: none"><li>• Sicherstellung der Kontinuität der Geschäftsprozesse</li></ul>
	<ul style="list-style-type: none"><li>• Eignerzufriedenheit</li></ul>

Es gilt zu bedenken, dass nicht nur Störungen katastrophalen Ausmasses eine Unternehmung beeinträchtigen können; auch ein vergleichsweise geringfügiger Vorfall kann kostspielige Auswirkungen nach sich ziehen. Dies umfasst folgende mögliche Störungsarten, wie Gefährdungen der Informationssicherheit, Störungen technischer Einrichtungen und Systeme, Zusammenbruch der öffentlichen Grundversorgung, Organisierte und/oder vorsätzliche Störungen und Umweltkatastrophen .

Obwohl sich unvorhergesehene Ereignisse unmittelbar auf die Einsatzfähigkeit einer Unternehmung und dadurch auf den Umsatz auswirken, sind dies nicht die Gründe, die letztendlich zum Scheitern vieler Unternehmen führen. Es sind vor allem die nachhaltigen Folgen, welche manchen Unternehmen den ultimativen „K.O.-Schlag“ versetzen, die sich u.a. wie folgt auswirken können: Schädigung von Reputation und Markenloyalität, Abwanderung von Kunden zur Konkurrenz, Geschäftspartner sehen sich nach Alternativen um, oder Gefährdung der Finanzierung.

Ein Unternehmen, das im Falle eines unvorhergesehenen Ereignisses nicht in der Lage ist, ihren Kunden das notwendige Minimum an Service bieten zu können, beraubt sich selbst vielleicht schon bald ihrer eigentlichen Existenzgrundlage.

<sup>1</sup> siehe [www.thebci.org](http://www.thebci.org)



## Business Continuity Management (BCM)

Theorie und Praxis am Beispiel einer Schweizer Privatbank

BCM wird heute viel breiter ausgelegt als früher und umfasst Krisen- und Katastrophenmanagement in Verbindung mit der Prävention und der Wiederaufnahme der IT- und der Geschäftstätigkeiten. Ausgehend von einem Top-Level schliesst dies die Identifizierung von kritischen Geschäftsprozessen und deren Umsatzquellen wie auch die Erhaltung der Reputation der Unternehmung als Ganzes mit ein.

Zusammengenommen lassen diese Faktoren BCM zur geteilten Verantwortung des gesamten Top-Managements werden, vom CEO über den COO bis hin zu den Linienfunktionen, welche für die kritischen Geschäftsprozesse verantwortlich sind. Obwohl die Einbindung der IT für den Business Continuity Prozess zentral bleibt, kann das IT-Management alleine nicht festlegen, welche Prozesse geschäftskritisch sind und welche finanziellen Mittel zum Schutz dieser Ressourcen eingesetzt werden sollen. Es ist wichtig, dass BCM die volle Unterstützung des Top-Managements erhält, um sicherzustellen, dass die Initiative in ihrer Umsetzung nicht blockiert wird. Ein Mitglied des Managements sollte als Sponsor fungieren mit der Verantwortung, BCM unternehmensweit ins Leben zu rufen. Mit dieser Unterstützung auf höchster Ebene sollte es möglich sein, auftretende Schwierigkeiten bei der Entwicklung, Implementierung und Etablierung von BCM zu meistern.

Zudem sollte ein BCM-Koordinator ernannt werden, der direkt an den verantwortlichen BCM-Sponsor aus dem Top-Management rapportiert. Idealerweise ist dies jemand, der sich mit Geschäftsstrukturen, Geschäftsprozessen, der IT und Mitarbeitern auskennt. Diese Person sollte ein guter Teamleader sein, der im Wesentlichen auch über Fähigkeiten im Programm-Management, in der Kommunikation und im zwischenmenschlichen Bereich verfügt.

### BCM Lösungsansatz

Bei der Entwicklung und Etablierung von Business Continuity Management wurde auf dem Prozess basiert, wie er in der Abbildung dargestellt ist.

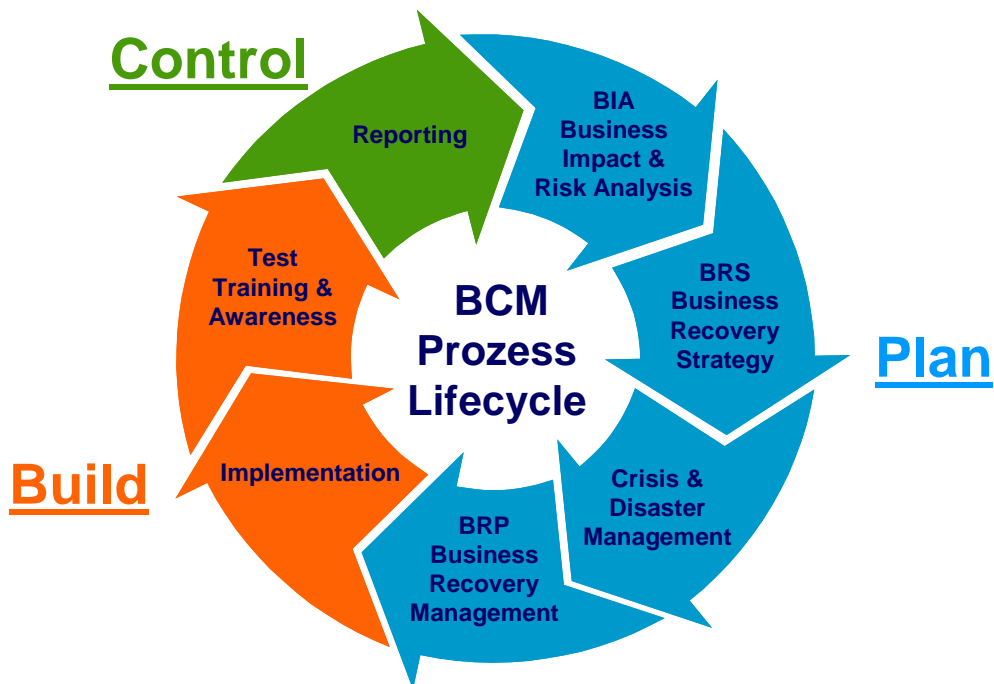


Abbildung 1: BCM Prozess Lifecycle



## Business Continuity Management (BCM)

Theorie und Praxis am Beispiel einer Schweizer Privatbank

Wir unterscheiden dabei die drei Kernprozesse Plan – Build – Control mit insgesamt sieben Phasen.

Diese **erste Phase** des BCM Prozess Lifecycles, die **Business Impact- und Risiko-Analyse**, ist notwendig, um von Beginn weg feststellen zu können, in welchen Bereichen das Unternehmen anfällig für Störungen ist. Es bedarf bestmöglicher Kenntnisse der wichtigen Geschäftsprozesse sowohl intern wie auch der ganzen Wertschöpfungskette zwischen Unternehmen, Kunden und Lieferanten.

Ebenfalls in dieser Phase werden die Beteiligung und das Verständnis von Mitarbeitern und anderen Abteilungen eingeholt, und es wird abgeklärt, ob innerhalb des Unternehmens bereits Pläne und Vorgehensweisen für den Umgang mit unvorhergesehenen Ereignissen bestehen.

Es gibt zwei Aspekte, die bei der Risikobewertung jeweils zu beachten sind:

- Eintretenswahrscheinlichkeit eines Risikos
- Auswirkungen bei Eintreten eines Risiko

Viele Unternehmen definieren die Risikoeinschätzung hinsichtlich der Kosten:

- Wie hoch dürfen die finanziellen Einbussen maximal sein?
- Wie würden Zulieferer, Kunden und potentielle Kunden reagieren, wenn das Unternehmen in die Schlagzeilen geriete, weil es nicht auf den Störfall vorbereitet war?

Bei der Analyse haben wir mit einem Klassifikationsraster gearbeitet, welches die verschiedenen Plattformen des Unternehmens (Gebäude, IT, Geschäftsprozesse, Lieferanten, Mitarbeiter) gleichzeitig bewertet und klassifiziert. Die Schadensklassifikation haben wir unterteilt in, schwerwiegend, beträchtlich, mässig, gering, sehr gering.

In der **zweiten Phase**, der **Entwicklung der Business Recovery Strategie**, wird die ermittelte Risikoklassifikation pro Plattform-Element den ermittelten Katastrophen-Szenarien gegenübergestellt. Unabhängig von der Art des Unternehmens, kommt wahrscheinlich eine der folgenden Strategien zum Einsatz:

- Risiken akzeptieren – keine Veränderungen vornehmen
- Risiken akzeptieren, jedoch mit einer anderen Firma oder einem Business Continuity Partner eine gegenseitige Vereinbarung treffen, um die Hilfeleistung nach einem Vorfall sicherzustellen
- Risiken möglichst reduzieren und Vorkehrungen zur Hilfeleistung nach einem Vorfall treffen
- Risiken soweit reduzieren, bis keine externe Hilfestellung mehr erforderlich ist

Die Einstellung gegenüber Risiken beruht teilweise auf den Kosten, die bei der Gewährleistung einer nachhaltigen Notfallplanung anfallen. Bei der Berechnung dieser Kosten müssen sowohl finanzielle als auch zeitliche Aufwendungen berücksichtigt werden.

In der **dritten Phase** wurde für die Clariden Bank die **Krisen- und Katastrophen-Organisation** eingerichtet, indem die Organisation auf 3 Levels etabliert wurde. Ausgehend vom zentralen Krisenmanagement (CCM) müssen auch die lokalen Krisenmanagement-Teams (LCM) organisiert werden. Es werden überall dort lokale Krisenmanagement-Teams installiert, wo bei einem schwerwiegenden Störfall essentielle Wiederherstellungsaktivitäten (BRM) notwendig sind. Für deren Organisation müssen sowohl geografische als auch funktionale Überlegungen einfließen.

Einer der Schlüsselprozesse in der Krisen- und Katastrophen-Organisation ist die Krisenkommunikation des Unternehmens (intern und extern).



## Business Continuity Management (BCM)

Theorie und Praxis am Beispiel einer Schweizer Privatbank

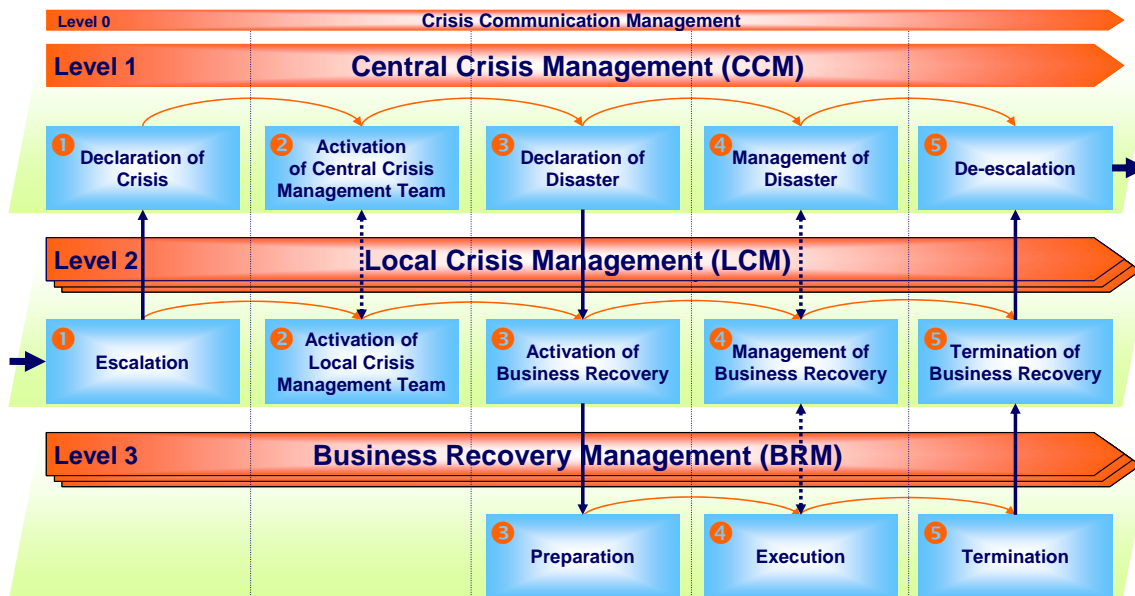


Abbildung 2: Drei Levels und fünf Phasen der Krisen- und Katastrophen-Organisation

Nachdem die Strategie festgelegt ist, kann in der **vierten Phase** die **Business Recovery Planung entwickelt** werden. BCM Pläne können je nach Unternehmen unterschiedlich aussehen. Die guten Business Continuity Pläne jedoch weisen einige Gemeinsamkeiten auf:

- Konzentration auf das Wesentliche
- Klarheit über das spezifische Aufgabengebiet, die Zuständigkeiten, Verantwortlichkeiten und Stellvertretungen
- Verwendung von leicht verständlichen und anwendbaren Checklisten
- Klare, direkte Instruktionen für die entscheidende erste Stunde nach einem Zwischenfall
- Auflistung der Punkte, die erst nach der ersten Stunde berücksichtigt werden müssen

Ein guter Plan ist einfach, ohne allzu vereinfachend zu sein. Es können niemals alle erdenklichen Ereignisse detailliert geplant werden, und es gilt zu bedenken, dass die Betroffenen in einem Notfall schnell reagieren müssen. Dies wird durch unnötige Detailbeschreibungen nur erschwert. Die Clari-den Bank hat mit der Vorgabe von geeigneten Dokumentationsvorlagen die Entwicklung der BCM Pläne erleichtert, sodass solche Pläne an verschiedensten Orten entwickelt werden konnten.

In der **fünftten Phase** müssen die beschriebenen **Business Recovery Planungen** auch **umgesetzt** werden. Dabei sind schon in der Entwicklungsphase eine Anzahl Präventionsmassnahmen zu ergreifen :

- Umsetzung von BCM-unterstützenden Grundsätzen und Richtlinien der IT-Architektur, wie z.B. redundante Netzwerk-Leitungen, gespiegeltes Rechenzentrum, gespiegelter Backup, usw.)
- Organisation von alternativen Räumlichkeiten bei Ausfall eines Gebäudes, inkl. der notwendigen IT-Komponenten
- Umsetzung von alternativen Geschäftsprozessen für die Überbrückungszeit bis die defekte Plattform wieder verfügbar ist
- Umsetzung eines Kommunikationskonzeptes für die adäquate interne und externe Kommunikation während einer Krise oder einer Katastrophe



## Business Continuity Management (BCM)

Theorie und Praxis am Beispiel einer Schweizer Privatbank

Der BCM Plan ist ein aktives Arbeitsdokument, und es kann vorkommen, dass Schwachstellen erst nach der Aktivierung entdeckt werden, weshalb in der **sechsten Phase** die **BCM Pläne geschult** und **getestet** werden. Tests und Probeläufe stellen sicher, dass die Pläne zusammenhängend und stabil sind, sollten sie je zum Einsatz kommen.

Probeläufe stellen auch ein gutes Training für Mitarbeiter dar, die Verantwortung für Business Continuity tragen. Mögliche Arten des Trainings umfassen schriftliche Übungen, Kommunikations- und Entscheidungsübungen, wie z.B. Mobilisierung des Krisenmanagement-Teams oder vollständige Katastrophenübungen

Und zu guter Letzt wird in der **siebten Phase** dem Top-Management **Rechenschaft über BCM Aktivitäten** und den aktuellen Zustand der Vorbereitungen abgeliefert. Die oberste Unternehmensführung muss die Berichterstattung über den gesamten BCM Prozess mindestens einmal jährlich zur Kenntnis nehmen und unterzeichnen.

### Schlussfolgerung

**BCM ist ein von der obersten Unternehmensführung gesteuerter und geschäftsorientierter Vorgang**, der die strategischen und operationellen Rahmenbedingungen unterstützt. BCM reflektiert und überprüft die Art und Weise, wie ein Unternehmen seine Produkte und Dienstleistungen erbringt. BCM erhöht die Widerstandsfähigkeit gegenüber Störungen, Unterbrechungen und Ausfällen.

Grössere Unternehmen haben im Allgemeinen mehr zu verlieren - und sehen sich auch mehr Verlustrisiken gegenüber - als kleinere Unternehmen. Dem gegenüber zwingt eine kleinere Grösse einem Unternehmen engere Grenzen auf, was die Fähigkeit anbelangt, kritische Störungen zu absorbieren und auf Unterbrechungen zu reagieren. Aus diesen Gründen ist BCM von hohem Stellenwert für Unternehmen aller Grössenordnungen.

---

*Zu den Autoren:*

*Bruno Gantenbein ist als Senior Consultant bei der Unternehmensberatung Intercaï (Schweiz) AG tätig. Er ist spezialisiert auf ganzheitliche IT Governance Beratung, insb. IT Strategie Entwicklung und Reorganisation von IT-Organisationen.*

*Peter Morf ist als Head Information Security bei der Clariden Bank tätig. Als BCM Coordinator und BCM Projektleiter ist er verantwortlich für den Aufbau und die Etablierung von BCM für die Gesamtbank.*