

## Business Continuity Management

# Überleben in der Krise

Was, wenn der Worst Case im Unternehmen eintritt? Feuer, Überschwemmung und andere Schadenereignisse mehr. Was im Ernstfall zu tun ist, muss im betrieblichen Kontinuitätsmanagement geregelt sein. Das Business Continuity Management besteht aus fünf zentralen Punkten.

### Uwe Müller-Gauss

Der Eintritt eines Schadens stellt für jede Unternehmung eine Belastung dar. Je nach Höhe des Ausmasses kann dieser Schaden den laufenden Betrieb kaum oder gar fatal beeinflussen. Das betriebliche Kontinuitätsmanagement (Business Continuity Management, BCM) beschäftigt sich vor allem mit dem sogenannten Worst Case – also dem, was im schlimmsten Fall passieren kann. Das Kontinuitätsmanagement befasst sich daher mit den folgenden Fragestellungen:

- Welche der identifizierten Risiken können im schlimmsten Fall die Unternehmung so stark beeinflussen, dass ein Fortführen der Geschäftstätigkeit nicht mehr möglich ist?
- Wenn ein solch fataler Schaden tatsächlich eingetreten ist, was braucht es, um zu einer normalen Geschäftstätigkeit zurückkehren zu können?

Eine typische Schadenssituation im BCM tritt überraschend ein und hat sehr schnell fatale Konsequenzen auf den Geschäftsbetrieb. Die vorausschauende Planung fokussiert auf eine rasche Wiederherstellung der Handlungsfähigkeit.

In der Medizin würde man das BCM im ersten Fall mit einem Defibrillator an der Wand vergleichen. Der Worst Case des Herzstillstandes ist eingetreten. Der Defibrillator kann helfen, den Patienten ins Leben zurückzuholen. Eine darauf folgende Rehabilitation hilft danach, zu einem möglichst normalen Leben zurückzukehren. Die Tatsache, dass der Herzstillstand zum Beispiel aufgrund

eines Infarktes allenfalls durch gesündere Ernährung, weniger Rauchen und mehr Sport hätte vermieden werden können, wäre Teil des vorangegangenen Risikomanagements des Patienten gewesen.

Es wird empfohlen, sich bei der Ausgestaltung des BCM vor allem auf die Konsequenzen und nicht auf die Ursachen der Schäden vorzubereiten.

### Integraler Bestandteil der Unternehmensstrategie

Die oberste Leitung sollte nach Einführung des Risikomanagementsystems eine Strategie entwickeln, wie sie grundsätzlich mit dem Thema BCM umgehen möchte. Die BCM-Strategie sollte im Idealfall ein integraler Bestandteil der Unternehmensstrategie sein. Sind einzelne Restrisiken im Verlauf des Risikomanagements bewusst in Kauf genommen worden, so muss die BCM-Strategie explizit über diese Risiken und ihr schlimmstes Ausmass Auskunft geben.

Ein modernes Risikomanagementsystem besteht aus einem präventiven Teil (Plan A), in dem die Risiken ermittelt, bewertet und gemäss der Unternehmensstrategie vermieden, vermindert, übertragen und selber getragen und dann gemanagt werden. Zum Risikomanagementsystem gehört auch ein reaktiver Teil: Er hat zum Ziel, Ereignisse, welche trotz sorgfältigem Risikomanagement eintreten, bewältigen zu können.

### BCM besteht aus fünf Modulen

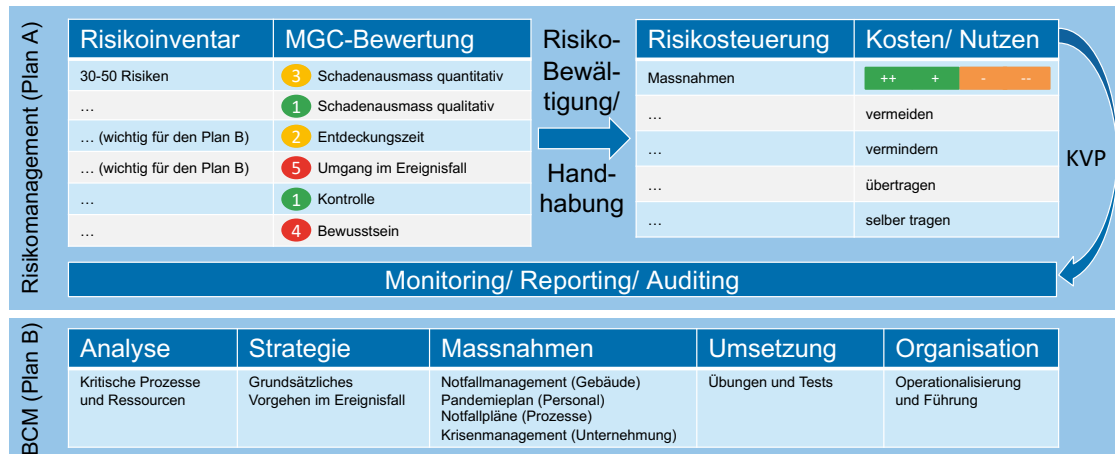
Ein BCM-System besteht aus den folgenden fünf Modulen (in Anlehnung an ISO 22301, SwissBanking «Empfehlungen für



### Autor

Uwe Müller-Gauss ist Gründer und Inhaber der auf Sicherheit, Risiko-, Krisen- und Kontinuitätsmanagement spezialisierten Müller-Gauss Consulting Pfäffikon ZH. Er ist Dipl. Tech. Kaufmann eidg. FA et dipl. Entrepreneur NDS FH et Executive Master of Business Administration. Als Dozent unterrichtet er im Bereich Management & Law an der Hochschule Luzern zu den Themen Compliance, Risiko-/Krisenmanagement und BCM.

Das Risikomanagement-System.



Quelle: Müller-Gauss Consulting / HSLU Hochschule Luzern / Institut für Finanzdienstleistungen Zug

das Business Continuity Management», 2013, und den Schweizerischen Versicherungsverband «Business Continuity Management [BCM] für Versicherungsunternehmen in der Schweiz – Mindeststandards und Empfehlungen», 2015:

1. *Business Impact Analyse*: Sind die Risiken der Unternehmung im Laufe der Einführung eines Risikomanagements identifiziert worden, ist im BCM festzustellen, auf welche Weise die identifizierten Risiken spezifische Geschäftsabläufe beeinflussen. Für diese kritischen Geschäftsprozesse werden die jeweiligen Auswirkungen eines kompletten oder teilweisen Ausfalls der entsprechenden Ressourcen beurteilt. Diese Beurteilung schliesst auch gegenseitige Abhängigkeiten zwischen den Geschäftsbereichen (sogenannte Prozessabhängigkeiten und Vererbungen) und Abhängigkeiten von externen Dienstleistern und Lieferanten (Outsourcing) mit ein. Die Business Impact Analyse ist bei Banken mindestens jährlich und bei Versicherungen alle drei Jahre durchzuführen und bei Bedarf ad hoc zu überprüfen (z.B. neue Geschäftsfelder oder Einsatz neuer Technologien).
2. *Business-Continuity-Strategie*: Sie definiert die maximal tolerierbaren Ausfallzeiten; bezeichnet aufgrund der Business-Impact-Analyse diejenigen Geschäftsbereiche, die dem BCM zugewiesen sind; legt die grundsätzlichen Lösungsansätze (Handlungsoptionen)

im Ereignisfall fest und legt den Umfang der Business-Continuity-Massnahmen für die Bereiche Personal, Facilities, Technik/Telekommunikation/Informatik und externe Dienstleister fest. Die Akzeptanz von Auswirkungen ohne vorbereitete Überbrückungs- und Wiederherstellungsmassnahmen kann ebenfalls eine Option darstellen.

3. *Business-Continuity-Massnahmen*: Basierend auf der Business-Impact-Analyse und im Rahmen der Vorgaben aus der Business-Continuity-Strategie wird mit den Business-Continuity-Massnahmen beschrieben, wie das Unternehmen Business Continuity wahrnimmt. Die Massnahmen definieren das Vorgehen und die Mittel zur Überbrückung und Wiederherstellung der zeitkritischen oder wichtigen Geschäftsprozesse und die dazu notwendigen Ressourcen (Personal, Facilities, Technik/Telekommunikation/Informatik, externe Dienstleister) und sollte mindestens einmal pro Jahr auf ihre Aktualität überprüft und im Bedarfsfall angepasst werden. Wesentliche Änderungen im Geschäftsbetrieb (Reorganisationen, Aufbau eines neuen Geschäftsfelds usw.) können ebenfalls eine Überarbeitung der Planung erforderlich machen. Business-Continuity-Massnahmen bestehen im Wesentlichen aus den folgenden vier Massnahmenpaketen:
  - a) Unternehmensweites Krisenmanagement, damit die Unternehmung dank eines eingeübten Krisenstabs

auch in der Krise jederzeit handlungs- und entscheidungsfähig bleibt.

- b) Standort- und gebäudespezifische Notfall- und Evakuierungsorganisation, welche die rasche Evakuierung resp. Ereignisbewältigung auf dem Schadenplatz sicherstellt.
  - c) Pandemieplan, damit sich weniger Mitarbeitende an einer neuen, leicht übertragbaren Krankheit (es wird ein Grippevirus sein) anstecken und somit die essenziellen Geschäftsprozesse aufrechterhalten werden können.
  - d) Mehrere Notfallpläne, welche die zeitgerechte Wiederaufnahme resp. den Betrieb eines vordefinierten Notbetriebs für geschäftskritische Prozesse und Ressourcen ermöglichen/ sicherstellen.
4. *Übungen und Tests*: Mit Übungen und Tests werden die Umsetzbarkeit und die Fähigkeit zur Ereignisbewältigung trainiert und überprüft. Die Periodizität für die Durchführung der Übungen und Tests der definierten Massnahmen (z.B. Wiederanlauf kritischer IT-Systeme) ist vorzugeben. Testergebnisse sind zu protokollieren und entsprechende Erkenntnisse in den Business-Continuity-Massnahmen zu berücksichtigen.
  5. *Operationalisierung und Führung*: Das BCM muss im Unternehmen verankert (z.B. in der Unternehmensstrategie oder in der Geschäftspolitik) und in der

Governance-Struktur des Unternehmens berücksichtigt sein. Es muss eine geeignete Organisation für Business-Continuity-Funktionen und Gremien zur Ereignisbewältigung (z.B. Krisen- oder Notfallmanagement) definiert sein. Die Rollen, Verantwortlichkeiten und Kompetenzen dieser Funktionen und Gremien müssen ebenfalls bestimmt sein. Gleichzeitig sind die Ressourcen zu planen und die notwendige Ausbildung für diese Funktionen sicherzustellen. Die Periodizität und der Umfang der internen Berichterstattung (z.B. Reporting an die Geschäftsleitung) müssen geregelt sein.

Am einfachsten ist ein BCM am Beispiel eines Totalausfalls der IT zu beschreiben: Angenommen, ein Wasserschaden im Keller hat den Serverraum überflutet. Die Server sind nicht mehr zu retten. Selbst wenn regelmässig Rücksicherungen der Daten auch an einem externen Standort durchgeführt werden, so wäre die Unternehmung allenfalls für eine längere Zeit nicht handlungsfähig; es sei denn, es existiert ein Konzept, wie der Zugriff auf diese extern gelagerten Daten durch die Mitarbeitenden der Unternehmung erfolgen soll. Kann das ganze Gebäude nicht

mehr benutzt werden, kämen Fragen zu Ausweicharbeitsplätzen hinzu. Zumindest ein Notbetrieb muss gewährleistet sein, damit die wichtigsten Anfragen beantwortet werden können. Eine Fortführung des Geschäftsbetriebes sollte durch die Massnahmen des BCM-Systems selbst beim Eintritt fataler Risiken gewährleistet werden können.

**BCM nützt nicht immer vor Schäden**

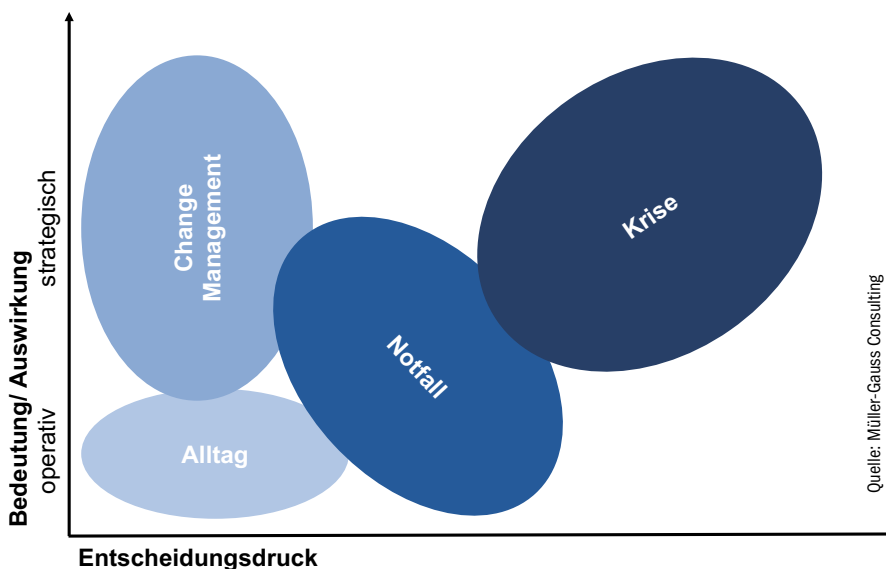
Die Luftfahrtindustrie weist vermutlich einen der höchsten Maturitätsgrade im Sicherheitsbereich auf. Von Anfang an hat man sich mit ausgeklügelten Systemen und Checklisten auf Zwischenfälle vorbereitet. So hat auch der Kapitän des US-Airways-Flugs 1549 am 15. Januar 2009 den Airbus A320-214, nachdem beide Triebwerke nach Vogelschlag ausgefallen sind, sicher auf dem Hudson River notgewässert und alle 155 Personen konnten unverletzt aussteigen und warteten auf den Flugzeugtragflächen (das Bild ging um die Welt) auf die Rettungsboote, die sie an Land brachten. Der Kapitän wurde weit über die Landesgrenzen hinaus als Held gefeiert. Schliesslich hat er doch den Worst Case abgewendet. Die Versicherung allerdings war weniger be-

geistert vom Totalschaden und liess den Flug in mehreren Simulatoren nachfliegen. Aufgrund der Simulationen war für sie klar, dass der Kapitän auch zurück zum Flughafen fliegen und den A320 ohne Totalschaden hätte landen können. Das aus dem Fluss geborgene und grösstenteils intakt gebliebene Flugzeug wurde als Totalschaden abgeschrieben. Wie sehr sich die Versicherung am Totalschaden schlussendlich beteiligt hat, darüber schweigen sich die Parteien aus.

**Kosten, Nutzen und Mehrwert**

Der Aufbau eines BCM-Systems ist mit zeitlichem Aufwand und auch mit Kosten verbunden. In der Regel werden die Investitionen aber überschätzt. Viele Unternehmen haben sich bereits im Rahmen ihres Risikomanagements mit Schadensereignissen und gefährdeten Geschäftsaktivitäten auseinandergesetzt. Es kann ausreichen, zuerst Schwächen und Verbesserungsmöglichkeiten von bestehenden Strukturen zu evaluieren und dann um organisatorische und technische Elemente zu ergänzen, die das Unternehmen notfall- und krisentauglich gestalten. Der Nutzen für Unternehmen, sich mit einem BCM-System sorgfältig auf den möglichen Eintritt von Schäden vorzubereiten, zahlt sich aus. Tritt ein Schaden ein, werden seine Auswirkungen minimiert und die Einsparungen des Unternehmens zur Bewältigung entsprechend maximiert. Aber auch wenn keine Schäden eintreten; Kunden, Analysten, Rating-Agenturen und Investoren haben längst Checklisten entwickelt, mit denen ein Unternehmen im Bereich BCM bewertet wird. Zudem lassen sich Versicherungsprämien für Betriebsunterbrüche im Sinne der Schadensprävention optimieren. Der grösste Mehrwert wird aber durch die Steigerung stabiler Strukturen (Resilienz) erwirkt. Die Sensibilisierung der Stakeholder für eine verantwortungsvolle Unternehmensführung wächst. Mit einem BCM-System wird das Vertrauen von Kunden, Partnern und Mitarbeitenden in das Unternehmen gestärkt. Denn Kontinuität der Geschäftstätigkeit bedeutet nachhaltige Erfolgssicherung für alle.

Spannungsfeld eines BCM-Systems.



Quelle: Müller-Gauss Consulting



**MÜLLER-GAUSS CONSULTING**

Security | Risk | Crisis | Continuity Management

Hörnlistrasse 75b • 8330 Pfäffikon • [uwe.mueller@gauss-consulting.ch](mailto:uwe.mueller@gauss-consulting.ch)