Business Continuity Management (BCM) für Versicherungsunternehmen in der Schweiz – Mindeststandards und Empfehlungen

Juni 2015

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Empfänger:
Alle von der Finma beaufsichtigten Versicherungsunternehmen

Herausgeber:
Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14
Postfach
CH-8022 Zürich

Tel. +41 44 208 28 28
Fax +41 44 208 28 00
info@svv.ch
www.svv.ch

Zuständiges Gremium:
Ausschuss Finanz & Regulierung

Kontaktperson:
Alex Schönenberger
Ressort Finanz & Regulierung
Schweizerischer Versicherungsverband SVV
Postfach, CH-8022 Zürich

Bestelladresse:
alex.schoenenberger@svv.ch

Stand: Juni 2015

Ausgangslage

Ausserordentliche Ereignisse und Situationen können die Geschäftstätigkeit eines Versicherungsunternehmens wesentlich beeinträchtigen. Damit die Überlebensfähigkeit und die Geschäftstätigkeit aufrechterhalten und weitergeführt werden kann, sind geeignete Massnahmen zur Ereignisbewältigung und Sicherstellung der Geschäftsfortführung kritischer Prozesse zu treffen (Business Continuity Management).

Das vorliegende Dokument richtet sich an alle von der Eidgenössischen Finanzmarktaufsicht (Finma) beaufsichtigten Versicherungsunternehmen und enthält Mindeststandards und Empfehlungen zur Ausgestaltung eines unternehmensspezifischen Business Continuity Managements.

Dabei ist den Besonderheiten des jeweiligen Unternehmens – insbesondere der Grösse, der Komplexität und des Risikoprofils – Rechnung zu tragen.

In den Geltungsbereich fallen Versicherungsunternehmen in der Schweiz. Eine Auswirkung der Mindeststandards und Empfehlungen auf das zivilrechtliche Verhältnis zwischen dem Unternehmen und seinen Kunden ist nicht beabsichtigt.

Zielsetzungen und Verantwortung

Das Business Continuity Management soll die Überlebensfähigkeit und die Aufrechterhaltung sowie Weiterführung der Geschäftstätigkeit bei ausserordentlichen Ereignissen und Situationen sichern. Dabei sind alle Ereignisse gemeint, die zur Gefährdung der Geschäftstätigkeit des Unternehmens führen können, wie zum Beispiel:

– technisches oder menschliches Versagen;
– Cyber-Angriffe;
– Pandemie;
– Naturkatastrophen;
– Terrorismus.

Das Business Continuity Management zielt auf eine Minimierung der finanziellen, rechtlichen und reputationsbezogenen Auswirkungen bei solchen Ereignissen und Situationen ab.

Der Verwaltungsrat ist verantwortlich für die Sicherstellung der Business Continuity. Er kann seine Kompetenzen an die Geschäftsleitung oder an andere Funktionen delegieren.

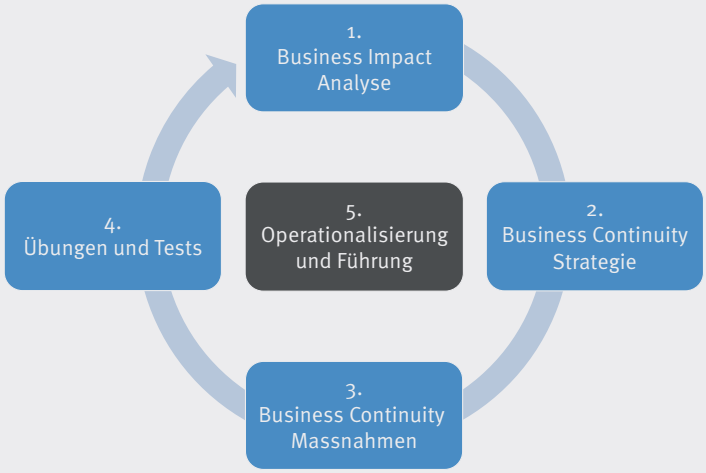
Die Mindeststandards definieren die Mindestanforderungen für die Versicherungsunternehmen in der Schweiz.

Die Empfehlungen dienen zur möglichen weitergehenden Ausgestaltung des Business Continuity Managements eines Unternehmens.

Grundlagen

Die vorliegenden Mindeststandards und Empfehlungen lehnen sich an verschiedene anerkannte Standards an (vgl. Quellenverzeichnis im Anhang). Insbesondere orientieren sie sich am International Standard ISO 22313: «Societal Security – Business Continuity Management Systems – Guidance». In Anlehnung an den ISO-Standard gehören zu einem ganzheitlichen Business Continuity Management folgende Elemente gemäss Abbildung.

Die Elemente des Business Continuity Managements



Anwendungsbereich

Unter Business Continuity Management ist ein unternehmensweiter Ansatz zu verstehen. Mit diesem soll sichergestellt werden, dass kritische Geschäftsprozesse während und nach massiven, einschneidenden internen oder externen, ausserordentlichen Ereignissen aufrechterhalten, zeitgerecht fortgeführt oder fristgerecht wieder hergestellt werden können.

Die Unternehmen haben alle potentiell relevanten Risiken und Bedrohungen zu berücksichtigen, welche für sie zu ausserordentlichen Situationen führen können. Darunter werden Situationen verstanden, welche mit den ordentlichen Führungsmitteln und Entscheidungskompetenzen nicht bewältigt werden können und welche die Geschäftsfortführung des Unternehmens gefährden können. Insofern ist die Bewältigung von «Störungen», die keine wesentliche und nachhaltige Beeinträchtigung der Geschäftstätigkeit bewirken können, ausdrücklich nicht Gegenstand des Business Continuity Managements.

Bei der Ausgestaltung des Business Continuity Managements wird vor allem auf die Konsequenzen (Auswirkungen der Restrisiken auf der Zeitachse) und nicht auf die Ursachen von ausserordentlichen Situationen abgestützt. Für die Wiederherstellung kritischer Geschäftsprozesse bzw. Geschäftstätigkeiten sollten nach einem Unterbruch verschiedene Business Continuity Optionen für die betriebsnotwendigen Ressourcen

- Personal,
- Facilities (zum Beispiel Gebäude / Arbeitsplatzinfrastruktur / Energieversorgung),
- Technik / Telekommunikation / Informatik (Daten / Systeme) und
- externe Dienstleister

berücksichtigt werden.

Das Business Continuity Management muss insbesondere die Einhaltung gesetzlicher, regulatorischer, vertraglicher und interner Vorschriften auch bei ausserordentlichen Situationen bestmöglich gewährleisten.

Mindeststandards

Das Business Continuity Management eines Versicherungsunternehmens muss folgende Inhalte als aufsichtsrechtliche Mindeststandards umfassen, deren Einhaltung periodisch durch die interne Revision oder eine entsprechende unabhängige Stelle geprüft wird. Der Umfang und der Detaillierungsgrad dieser Inhalte muss den Anforderungen des jeweiligen Unternehmens Rechnung tragen.

1. Business Impact Analyse

Im Rahmen der Business Impact Analyse müssen zeitkritische und wichtige Geschäftsprozesse und deren Ressourcen identifiziert und ausgewiesen werden.

Für diese zeitkritischen Geschäftsprozesse müssen die Auswirkungen eines kompletten oder teilweisen Ausfalls der benötigten Ressourcen beurteilt werden, als Grundlage für notwendige Überbrückungs- und Wiederherstellungsmassnahmen. Die Analyse berücksichtigt insbesondere die Konsequenzen auf
- den Betrieb (Operationen),
- die Finanzen,
- die Reputation und
- die Compliance.

Die Beurteilung muss auch die relevanten Abhängigkeiten zwischen den Geschäftsprozessen berücksichtigen (Prozessabhängigkeiten).

Die Business Impact Analyse ist mindestens alle drei Jahre durchzuführen und bei Bedarf zu überprüfen (zum Beispiel neue Geschäftsfelder oder Einsatz neuer Technologien).

2. Business Continuity Strategie

Die Business Continuity Strategie
- definiert die maximal tolerierbaren Ausfallzeiten;
- bezeichnet aufgrund der Business Impact Analyse diejenigen Geschäftsbereiche, die dem Business Continuity Management zugewiesen sind;
- legt die grundsätzlichen Lösungsansätze (Handlungsoptionen) im Ereignisfall fest;
- 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. Dies ist in der Business Continuity Strategie entsprechend zu dokumentieren.

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 Business Continuity 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).

Die betroffenen Geschäftsbereiche und ihre Mitarbeitenden sind über die Business Continuity Massnahmen zu informieren (zum Beispiel kritische Geschäftsprozesse über notwendige Ausweicharbeitsplätze) und, wo notwendig, auszubilden (zum Beispiel beim Einsatz von technischen Ausweichsystemen).

4. Übungen und Tests

Mit Übungen und Tests werden die Umsetzbarkeit und die Fähigkeit zur Ereignisbewältigung trainiert und überprüft.

Die Periodizität für die Durchführung von Übungen und Tests der definierten Massnahmen (zum Beispiel 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 Business Continuity Management muss im Unternehmen verankert (zum Beispiel in der Unternehmensstrategie oder in der Geschäftspolitik) und in der Governance-Struktur des Unternehmens entsprechend berücksichtigt sein.

Es muss eine geeignete Organisation für Business Continuity Funktionen und Gremien zur Ereignisbewältigung (zum Beispiel Krisen- oder Notfall-Management) 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 (zum Beispiel Reporting an die Geschäftsleitung) müssen geregelt sein.

Empfehlungen

Die nachfolgenden Empfehlungen sollen als Hinweise und Hilfe bei der weiteren Ausgestaltung des Business Continuity Managements dienen. Deren Anwendung und Umsetzung ist insbesondere abhängig von der Struktur und der Massgabe der Risikosituation des Unternehmens. Sie folgen den Vorgaben in der Business Continuity Strategie.

Vorgaben an das Business Continuity Management

Die Vorgaben an das Business Continuity Management im Bereich Technik / Telekommunikation / Informatik können über folgende zeitliche und inhaltliche Erwartungen bezüglich der Wiederherstellung von Geschäftsprozessen definiert werden:

- erforderliche Zeitspanne bis zur Wiederherstellung der kritischen Geschäftsprozesse (Recovery Time Objective RTO);
- gewünschter Wiederherstellungsgrad der kritischen Geschäftsprozesse bezüglich des definierten RTO;
- maximal akzeptierter Datenverlust im Falle eines Ereignisses (Recovery Point Objective RPO).

Externe Dienstleistungen

In vielen Geschäftsprozessen werden Leistungen durch externe Dienstleister und Lieferanten erbracht (Outsourcing), die ebenfalls ausfallen können. Wird bei kritischen Geschäftsprozessen die Unterstützung externer Dienstleister und Lieferanten beigezogen, empfiehlt sich, deren Maturität in Bezug auf das Business Continuity Management in geeignetem Rahmen zu beurteilen.

Es wird empfohlen, für den Ausfall kritischer externer Dienstleister und Lieferanten, wo möglich und sinnvoll, Umgehungslösungen zu planen. Im Rahmen der Business Continuity Planung kann unter anderem der Transfer von externen zu internen Dienstleistern oder umgekehrt geprüft werden.

Krisenmanagement

Es wird empfohlen, ein geeignetes Krisenmanagement und eine entsprechende Krisenkommunikation zu definieren, mit denen das Unternehmen ausserordentliche Ereignisse wirksam und zeitgerecht bewältigen kann. In Situationen, welche kritische Entscheidungen verlangen und die mit ordentlichen Massnahmen und Entscheidungskompetenzen nicht bewältigt werden können, wird ein geeignetes Gremium (zum Beispiel Krisenstab oder Notfallorganisation) einberufen. Dieses übernimmt die Aufgabe der Krisenbewältigung bis zur Wiederherstellung eines ordnungsgemässen Zustands.

In diesem Fall sollte die Alarmierung der Krisen- oder Notfallorganisation klar geregelt sein, ebenso wie die Zuständigkeiten, Kompetenzen und Eskalationskriterien. Die Organisation sollte die Geschäftstätigkeit und die geographische Struktur des Unternehmens berücksichtigen.

Krisenkommunikation

Kommunikation nach innen und aussen ist ein entscheidender Faktor in der Ereignisbewältigung. Der Vorbereitung von Kommunikationskonzepten und -plänen sollte deshalb besondere Beachtung geschenkt werden. Dabei geht es insbesondere um die Aufrechterhaltung von Glaubwürdigkeit und Vertrauen gegenüber den verschiedenen Stakeholdern des Unternehmens.

Kommunikationspläne können vor allem die Erreichbarkeit im Krisenfall sicherstellen (Namenslisten und Kontaktdaten von Kunden, Medien, Mitarbeitenden, Aufsichtsbehörden, Gegenparteien, Dienstleistern usw.). Sie erleichtern eine regelmässige und präventive Kommunikation mit den verschiedenen Interessengruppen (Kunden, Mitarbeitende, Aktionäre, Investoren usw.). Einer allfälligen internationalen Dimension ist mit speziellen Kommunikationsmassnahmen Rechnung zu tragen.

Review des Business Continuity Managements

Business Continuity Reviews beinhalten eine Bestandesaufnahme der erstellten Business Continuity Management Dokumentation und eine Beurteilung, ob diese den eigenen Business Continuity Vorgaben entsprechen. Es wird empfohlen, konsistente Prüfkriterien sowie einen klaren Prozess zur Überwachung und Behebung offener Punkte zu definieren.

Übungen und Tests

Schwerpunkte sowie Kadenz der einzelnen Übungen und Tests sollten in Abhängigkeit der Kritikalitätsbeurteilung gemäss Business Impact Analyse oder gemäss interner Richtlinien festgelegt werden.

Es kann wertvoll sein, dass ein Prozess für die Überwachung und Behebung von Schwachstellen festgelegt ist.

Berichterstattung

Über die Business Continuity Management Aktivitäten und den Stand der Vorbereitung der Ereignisbewältigung sollten in einem definierten Rhythmus stufengerechte Berichte zuhanden der verantwortlichen Funktionen erstellt werden. Darin sollten insbesondere die Ergebnisse von Business Continuity Reviews und Business Continuity Übungen und Tests dargestellt werden.

Wesentliche Erkenntnisse aus der Berichterstattung können intern und extern (Outsourcing) kommuniziert werden.

Inkrafttreten

Die vorliegenden Mindeststandards und Empfehlungen sind vom Ausschuss Finanz & Regulierung des Schweizerischen Versicherungsverbandes SVV mit Beschluss vom 9. Juni 2015 verabschiedet worden. Sie treten per 1. Oktober 2015 in Kraft und sind bis zum 31. Juli 2017 umzusetzen.

Die Finma anerkennt die Mindeststandards im Sinne von Art. 7 Abs. 3 FINMAG per 23. September 2015.

Quellenverzeichnis

International Organization for Standardization (ISO), ISO 22313:2012: Societal security – Business Continuity Management Systems – Guidance
www.iso.org/iso/catalogue_detail?csnumber=50038

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/catalogue_detail?csnumber=44374

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

Glossar

Als Nachschlagewerk für Begriffsdefinitionen empfiehlt der SVV den Standard ISO 22301:2012 Societal security – Business Continuity Management Systems – Requirements, Kapitel 3 «Terms and definitions».

ASA | SVV

Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14
Postfach
CH-8022 Zürich

Tel. +41 44 208 28 28
Fax +41 44 208 28 00
info@svv.ch
www.svv.ch