Business Continuity Management – praxisnahe Lösungen

Notfallmanagement macht Sinn. Auf den Punkt gebracht, sichert es im Krisenfall die Aufrechterhaltung des Geschäftsbetriebs. Mit der „Bankenaufsichtliche Anforderungen an die IT (BAIT)“ - Novelle wurden die Anforderungen an das Notfallmanagement konkretisiert. Doch – wie sollte es aufgebaut sein und worauf ist zu achten?

Das Notfallmanagement oder auch Business Continuity Management (BCM) folgt vor allem dem Zweck, den Geschäftsbetrieb im Krisenfall fortführen zu können. Es soll gewährleisten, dass auch unter erschwerten Voraussetzungen, trotz eines kritischen Vorfalls, der Geschäftsbetrieb auf einem akzeptablen, vordefinierten Level fortgeführt werden kann. Dazu werden im BCM geeignete Strategien und Maßnahmen definiert, um – beispielsweise bei technischen Störungen, den Geschäftsbetrieb „lähmenden“ Personalausfällen oder auch bei Hackerangriffen – handlungsfähig zu bleiben.

Als Teil des Wirtschafts- und Finanzsystems hat das BCM für Banken darüber hinaus eine formale Bedeutung. Mit dem Notfallmanagement sind bestimmte aufsichtsrechtliche Pflichten und gesetzliche Bestimmungen verbunden, die die Bank erfüllen muss.

Notfallmanagement nun auch für IT-Systeme

Die gesetzliche Grundlage zur Festlegung eines angemessenen BCM, insbesondere der Einbindung von IT-Systemen, ist in § 25a Abs. 1 Nr. 5 KWG geregelt. Daran anknüpfend greifen die Mindestanforderungen an das Risikomanagement (MaRisk) das Notfallmanagement (MaRisk AT 7.3) auf.

Gemäß MaRisk AT 7.3 sind im Notfallmanagement

- zeitkritische Aktivitäten und Prozesse,
- Auswirkungsanalysen,
- Risikoanalysen (MaRisk AT 7.3 Tz. 1) sowie
- das Notfallkonzept und Notfallszenarien (MaRisk AT 7.3 Tz. 2) und
- die Überprüfung des Notfallkonzepts (MaRisk AT 7.3 Tz. 3) zu berücksichtigen.

Ein wesentlicher Bestandteil und Basis eines BCM ist die Business-Impact-Analyse (BIA). In ihr werden zunächst Prozesse und Funktionen in der Organisation identifiziert, um dann die Auswirkungen möglicher Störungen oder Ausfälle zu beschreiben. In der sogenannten Auswirkungsanalyse wird die Zeitkritikalität der jeweiligen Geschäftsprozesse ermittelt und werden geeignete Vorsorgemaßnahmen ausgearbeitet.

Ergänzend sind nun in den BAIT die Anforderungen an das IT-Notfallmanagement konkretisiert worden (Kapitel 10 „IT-Notfallmanagement“). Insbesondere die Differenzierung der Verfügbarkeitsanalyse (Business Impact)

- in der Wiederanlaufzeit (Recovery Time Objective – RTO) und
- in dem maximal tolerierbaren Zeitraum eines Datenverlustes (Recovery Point Objective – RPO)

ist dabei zu beachten.

Es reicht nicht mehr aus, nur die zeitkritischen Prozesse im Notfallkonzept zu berücksichtigen. Vielmehr müssen auch „IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen“ sowie die „Abhängigkeiten zwischen den IT-Systemen“ (BAIT Tz. 10.4) eingebunden werden.

Schlankes BCM?

Fakt ist, dass sowohl die technischen als auch die organisatorischen Konstellationen – samt den personellen Zuständigkeiten – einem steten Wandel unterworfen sind. Um dem Rechnung zu tragen und die Handlungsfähigkeit auch dann in einem Notfall zu gewährleisten, sind die aufsichtsrechtlichen Anforderungen an die Aktualität gestiegen.

Die Business-Impact-Analyse (BIA) ist mindestens einmal jährlich durchzuführen. Wenn vorab ein anlassbezogener Grund vorliegt, wird zudem eine unterjährige Analyse erforderlich. Dies gilt übrigens auch für Objekte aus dem Informationsverbund, die zeitkritische Auswirkung bei einem Ausfall haben können. Darüber hinaus sind für „alle speziell relevanten Szenarien zu den zeitkritischen Aktivitäten und Prozessen“ jährlich Notfalltests und Übungen durchzuführen.

Die aufgeführten Konkretisierungen können bei bestehenden Lösungen zu einer – signifikanten – Ausweitung des BCM und damit des Gesamtaufwands führen. Zu fragen ist, wie angesichts dessen noch ein praxisnahes und effizientes Notfallmanagement aufgestellt werden kann.

Umsetzung

In der Praxis sind längst noch nicht alle Umsetzungsfragen abschließend beantwortet. Es erscheint deshalb zweckmäßig, sich bis auf Weiteres an dem bewährten Umsetzungsrahmen – dem Standard 200-4 des Bundesamts für Sicherheit in der Informationstechnik (BSI) – zu orientieren. Für die Bank selbst ist es zunächst wichtig, einen internen Mitarbeiter als Notfallbeauftragten zu benennen und zu qualifizieren.

Folgende weitere Schritte sind zu empfehlen und zu beachten:

1

Business-Impact-Analyse (BIA) durchführen

Mit Hilfe der Business-Impact-Analyse wird in Zusammenarbeit mit den Informationseigentümern (i.d.R. der jeweilige Fachbereich) die Zeitkritikalität der Prozesse ermittelt.

Bezeichnung	Besondere Zeit	MaRisk	MTA
Interne Prozesse			
Betriebliche Grundfunktionen			
Bereitstellung Informations- und Kommunikationstechnologie		Nein	
Entsorgung von Datenträgern/Belege		Nein	
Meldewesen		Nein	< 7 Tage
Rechnungswesen		Nein	
Ver-/Entsorgung, Überwachung, Störungsmanagement		Nein	< 7 Tage
Kunde			
Kontokorrent / Kontoführung		Nein	< 7 Tage
Managementprozesse			

Beispielhafte Darstellung der Geschäftsprozess-Übersicht der BIA

2

Szenarien festlegen

Des Weiteren sind Szenarien nach Relevanz festzulegen, die einen Notfall auslösen können. An dieser Stelle wird mit Pflicht-Szenarien und Kann-Szenarien gearbeitet. Die sogenannten Pflicht-Szenarien sind grundsätzlich durch die Bank zu berücksichtigen.

Bezeichnung	Gefährdungen	Direkt relevant
Gebäudeausfall	G 0.001 Feuer,G 0.002 Ungünstige klimatische Bedingungen,G 0.003 Wasser,G 0.004 Verschmutzung, Staub, Korrosion	IT-Systeme,Netze/Kommunikationsverbindungen,Räume und Lokationen
Infrastrukturkomponentenausfall	G 0.008 Ausfall oder Störung der Stromversorgung,G 0.009 Ausfall oder Störung von Kommunikationsnetzen,G 0.010 Ausfall oder Störung von Versorgungsnetzen	IT-Systeme,Netze/Kommunikationsverbindungen,Räume und Lokationen

Beispielhafte Darstellung der Übersicht der Szenarien der BIA

WAZ	RPO	Status
	tägliche Sicherung	Aktiv
	tägliche Sicherung	Aktiv
160	tägliche Sicherung	Aktiv
	tägliche Sicherung	Aktiv
160	tägliche Sicherung	Aktiv
160	tägliche Sicherung	Aktiv

3

Festlegung organisatorischer Rahmenbedingungen/Einheiten

Im Folgenden sollte überprüft werden, ob im bisherigen Notfallkonzept die Angaben zu den

- Filialen/Geschäftsstellen,
- Abteilungen,
- Räumungsbereichen,
- BCM-Rollen der Mitarbeiter (z. B. Brandschutzhelfer, Ersthelfer, Krisenmanagement-Leitung, Krisenmanagement-Team etc.) und
- externen Stellen (z. B. Kontaktdaten Dienstleister, Versorgungsunternehmen, Hilfsdienste wie Polizeidienststellen, Krankenhaus, Ärzte etc.) aktuell sind.

Ressource	Szenario	Maßnahmenart
agree21AZV		
Cyber-Angriff		
agree21AZV	Cyber-Angriff	Korrektive Maßnahme
agree21AZV	Cyber-Angriff	Präventive Maßnahme
Dienstleisterausfall		
agree21AZV	Dienstleisterausfall	Korrektive Maßnahme
agree21AZV	Dienstleisterausfall	Präventive Maßnahme
agree21Banking (CBS)		
Cyber-Angriff		
agree21Banking (CBS)	Cyber-Angriff	Korrektive Maßnahme

Beispielhafte Darstellung der Übersicht der Soll-Übungen

4

Überprüfung der Anweisungen zu den Objekten und den zeitkritischen Geschäftsprozessen

Ferner sind die Objekte (IT-Systeme, IT-Anwendungen etc.), die zeitkritische Auswirkungen auf den Geschäftsbetrieb haben, hinsichtlich der Wiederanlauf-, Notbetriebs- und Wiederherstellungsplanung sowie auf Geschäftsprozessebene die Geschäftsfortführungs- und Wiederherstellungsplanung zu prüfen und zu aktualisieren.

Objekt	Wa	N/G	Wh	A	Status
Objekt					
agree21AZV	✔	✔	✔		abgeschlossen
agree21Banking (CBS)	✔	✔	✔		abgeschlossen
agree21Client	✔	✔	✔		abgeschlossen
agree21Client 'Mobil'	✔	✔	✔		abgeschlossen
agree21Debitkarten	✔	✔	✔		abgeschlossen
agree21eBanking-ZV	✔	✔	✔		abgeschlossen
Prozess					
Basis-Zahlungsverkehr					
agree21AZV	✔	✔			abgeschlossen
agree21ZV	✔	✔			abgeschlossen
agree21ZV-unbar	✔	✔			abgeschlossen
ipsYdion ZV	✔	✔			abgeschlossen

Beispielhafte Darstellung der Übersicht der Anweisungen

5

Aktualisierung der Notfalldokumente

Die Aktualität der neben den o.g. Notfallanweisungen auch benötigten Dokumente ist ebenfalls regelmäßig zu überprüfen

Die Verfügbarkeit der vollständigen Notfalldokumente muss jederzeit gewährleistet sein. Dies kann in ausgedruckter Form, als PDF auf einem gesonderten Laptop oder in einem sicheren Cloud-basierten Datenraum erfolgen.

Titel	Bearb.datum
Handbuch Krisenstab	30.10.2023 14:06:17
Leitlinie Business Continuity Management	17.10.2023 16:37:29
Notfallhandbuch Krisenstab	30.10.2023 14:08:07
Notfallplan Sofortmaßnahmen	30.10.2023 14:09:19

Beispielhafte Darstellung der Übersicht der Notfallhandbücher und Notfall-Rahmendokumente

6

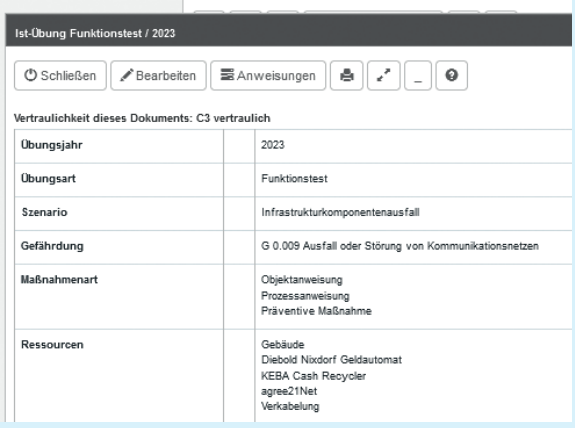
Festlegung der Soll-Übungen

Die Soll-Übungen, die unterschiedliche Szenarien und Maßnahmenarten berücksichtigen, werden durch das System generiert/festgelegt.

8

Durchführung und Dokumentation der Ist-Übungen

Nach Festlegung der Übungsplanung sind die Ist-Übungen durchzuführen. Ein Abgleich zwischen Soll- und Ist-Übungen kann vorgenommen werden.



Beispielhafte Darstellung der Dokumentation zu den Ist-Übungen (Alle Screenshots stammen aus dem Tool BCM kompakt der DZ CompliancePartner.)

7

Festlegung der Übungsplanung

Anschließend ist die jährliche Übungsplanung aufzustellen.

Beispielhafte Darstellung der Übersicht Übungsplanung

Fazit

Um im Krisenfall handlungsfähig zu sein, sind die kritischen Geschäftsprozesse und -ressourcen in einem zentralen Notfallmanagement zu identifizieren und mit entsprechenden Gegenmaßnahmen zu hinterlegen. Dabei sind insbesondere die Auswirkungen von Störungen und Ausfällen zu analysieren. Mit der Business-Impact-Analyse steht und fällt das Notfallmanagement.

Abschließend ist festzuhalten, dass die Anforderungen insgesamt gestiegen sind. Um den Aufwand einzugrenzen, sollte eine intelligente Softwarelösung in Betracht gezogen werden. Sie sorgt für die erforderliche Transparenz und Nachvollziehbarkeit bei der Dokumentation – und stellt vor allem im Notfall sicher, dass wichtige Informationen griffbereit sind. ▬

Weiterführende Infos zu den BAIT:
https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/bait/bankaufsichtliche-anforderungen-an-die-it-598580, abgerufen am 31.10.2023

Notfallmanagement der DZ CompliancePartner

Ein Finanzinstitut muss seine Kernprozesse und die Auswirkungen von Ausfällen genau kennen, um angemessen auf kritische Situationen reagieren zu können: Mit dem Beratungskonzept der DZ CompliancePartner in Verbindung mit der digitalen Lösung „BCM kompakt“ haben Sie Ihre – bankindividuellen – zeitkritischen Geschäftsprozesse und Ressourcen im Blick und können im Ernstfall die erforderlichen Maßnahmen ergreifen.

Michaela Eckmann
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: michaela.eckmann@dz-cp.de

Benjamin Wellnitz
Bereichsleiter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de