Grete/Naujoks (Hrsg.)

Arbeitsbuch Business Continuity und Notfallmanagement in Banken

Notfall-Resilienz für Banken, Sparkassen und deren Dienstleister nachhaltig und wirksam erhöhen

FCH AG, 2023

Zitiervorschlag:

Autor in: Grete/Naujoks (Hrsg.), Arbeitsbuch Business Continuity und Notfallmanagement in Banken, 2023, Rn. XX.

Hinweis: Zur besseren Lesbarkeit und Unterstützung des Leseflusses wurde im nachfolgenden Buch auf die Verwendung des generischen Maskulinums zurückgegriffen. Selbstverständlich schließen jedoch alle Formulierungen und Personenbezeichnungen alle Geschlechter gleichermaßen ein.

ISBN: 978-3-95725-126-8

FCH AG
Im Bosseldorn 30, 69126 Heidelberg
www.FCH-Gruppe.de
info@FCH-Gruppe.de
Satz: FCH AG
Druck: VERLAGSDRUCKEREI SCHMIDT,
Neustadt an der Aisch

Grete/Naujoks (Hrsg.)

Arbeitsbuch Business Continuity und Notfallmanagement in Banken

Notfall-Resilienz für Banken, Sparkassen und deren Dienstleister nachhaltig und wirksam erhöhen

Bärbel Adamek
BA Coachings und Trainings

Holger Berens
Vorstandsvorsitzender
Bundesverband für den Schutz Kritischer Infrastrukturen e.V.

Dr. Jens Gampe
Gruppe IT-Aufsicht, Referat GIT 3 –
Grundsatz IT-Aufsicht und Prüfungswesen
Bundesanstalt für Finanzdienstleistungsaufsicht

Dr. Patrick Grete (Hrsg.)
Referat TK 22
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Markus Held
Referatsleiter Informationssicherheit in der IT-Konsolidierung
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Susanne Kufeld
CSO, Head of Corporate Security OCS Corporate Security – COO
UniCredit Bank AG

Uwe Naujoks (Hrsg.)
Partner, Geschäftsbereichsleiter Risikomanagement
WG-DATA GmbH

Thomas Otto
Partner | Lead CIO Advisory Banking
Sopra Steria SE

Frank Romeike
Geschäftsführender Gesellschafter
RiskNET GmbH

FCH AG, 2023

Inhaltsübersicht

Inhaltsverzeichnis

Vorwort der Herausgeber

Es scheint aktuell eine gute Zeit für das Thema Kontinuitätsmanagement zu sein. Die Krisen stapeln sich. Lässt man mal die größeren Krisen wie Finanz- und Schuldenkrise sowie die Flüchtlingskrise des letzten Jahrzehnts außen vor und schaut nur auf dieses Jahrzehnt, dann hat es mit einer Pandemie begonnen, der mit Maßnahmen begegnet wurde, die weltweite Lieferketten und die Art des Arbeitens insgesamt stark verändert hat. Seit über einem Jahr zeigt auch der Ukraine-Krieg große Auswirkungen auf die Energie- und Treibstoffpreise. Aber nicht nur die Preise sind relevant, denn einige Rechenzentren kühlen mit Gas. Aber auch schleichende Krisen zeigen sich: Die Klimakatastrophe führt zunehmend dazu, dass Flüsse im Sommer zu wenig Wasser führen und dann auch nicht so viel Kühlwasser für Kraftwerke und Rechenzentren zur Verfügung stehen.

Als Leserin oder Leser dieses Buches aus der Bankenwelt werden Sie aber vielleicht abwinken; brauchen Sie doch schnellen Input, um der Aufsicht gute Dokumente eines Kontinuitätsmanagements nach den aktuellen Standards vorzulegen. Dieses Buch wird Ihnen dabei nach unserer Auffassung eine große Hilfe sein, aber der richtige Rahmen für dieses Anliegen ist wichtig. Ein rein extrinsisch getriebenes BCM ist wenig nachhaltig und wird keinen Mehrwert generieren. Daher gestatten Sie uns kurz, einen Blickwinkel zu präsentieren, der Ihnen intrinsische Motivationen für ein BCM verdeutlicht.

Die im ersten Absatz begonnene Aufzählung der verschiedenen Ursachen für potenzielle Ausfälle könnte man sehr lange fortführen, aber ein mehr an Informationen führt nicht unbedingt zu besseren Entscheidungen, sondern eher zu Abstumpfung und Fatalismus oder zu wenig zielführendem Aktionismus. Aus der Brille des Kontinuitätsmanagers läuft es auf einen Mangel an Resilienz hinaus und deutet darauf, dass sowohl bei den vorgenannten Krisen als auch im Kontinuitätsmanagement allgemein der Mensch mehr in den Fokus rücken sollte und basierend auf den Ursachen die prozessualen Auswirkungen entsprechend bewertet werden müssen.

In dieser Gemengelage wurden wir vom FCH angefragt, ein neues Buch zum Kontinuitätsmanagement herauszugeben. Äußerer Anlass ist die Veröffentlichung des neuen BSI-Standards 200-4, in den die vielfältigsten Erfahrungen mit dem über einem Jahrzehnt alten BSI-Standard 100-4 – dem ersten deutschen Standard zum Kontinuitätsmanagement – eingeflossen sind. Als Ausbilder und Berater mit langjähriger Erfahrung ist es vielleicht Ihre Erwartung als Leserin

und Leser, dass wir die »Gunst der Stunde« nutzen, um den o. g. blinden Aktionismus in geeignete Bahnen zu lenken und die nun aktuell zur Verfügung stehenden Budgets in lukrative Aufträge (nicht nur) für die Autorinnen und Autoren zu verwandeln. Eine klassische Win-Win-Situation, an dessen Ende dem Top-Management und den Regulatoren grün eingefärbte Excel-Listen vorgelegt werden können.

Wir haben uns bewusst gegen eine solche »krisengewinnlerische« Ausrichtung dieses Buches entschieden und sind dem Verlag dankbar, dass wir damit offene Türen eingerannt haben. Kontinuitätsmanagement als ein Verkaufsprodukt zu begreifen, um Top-Management zu beruhigen, heißt – zugespitzt – deren mentale Zustände auszunutzen und wenn man dies aus vornehmlich pekuniären Interessen mit dem BCM macht, zeigt man, dass man wenig von der Wichtigkeit eines Kontinuitätsmanagements verstanden hat. Alle Krisen kennen Krisengewinnler, aber der Erfolg der meisten von ihnen ist von kurzer Dauer und man erkennt die ruchlosen unter ihnen daran, dass sie erst seit kurzem im Geschäft sind (und schnell wieder verschwinden) – man denke bspw. an die »Maskendeals«. Sich von Personen mit diesem Mind-Set Kontinuitätsmanagement verkaufen zu lassen, wird nicht zur nachhaltigen Etablierung einer BCM-Kultur in Ihrem Unternehmen führen.

Beim Kontinuitätsmanagement geht es darum, dass die zeitkritischen Geschäftsprozesse, auch bei plötzlich eintretenden, widrigen Umständen, weiterlaufen und damit der Fortbestand gesichert bleibt. Es geht nicht darum, Papier zu schwärzen oder Excel-Tapeten zu erstellen, um etwas in der Schublade zu haben, was zwar schön aussieht (und ggf. einen Regulator erfreut), aber in der Praxis nur aufgrund einer äußeren Krise eingekauft wurde und wenig gelebt wird. Gelebt werden kann nur etwas von Menschen, die – bezogen auf die Arbeitswelt – bewusst entschieden haben, einen Teil ihrer Lebenszeit mit der Arbeit in einer Institution zu verbringen und die – fokussiert auf Kontinuitätsmanagement – bemerken, dass die Kontinuität explizit gesteuert werden muss und es dafür Werkzeuge und einer gelebten BCM-Kultur bedarf.

Die Intention dieses Buches ist es, das komplexe Thema des BCM aus den unterschiedlichen Blickwinkeln zu betrachten, und zwar mit dem Fokus »aus der Praxis für die Praxis«. Lassen Sie sich inspirieren von den Ansichten und langjährigen Erfahrungen der nachfolgend kurz vorgestellten Autoren.

Der erste Teil des Buches adressiert vor allem die strategische Ebene. Die mit Erfahrung in der Bankenaufsicht ausgestatteten Autoren Dr. Held und Dr. Gampe erläutern hier den aktuellen Sachstand zu Normen und Standards

des BCM für den Bankensektor. Die Herausgeber sensibilisieren in ihrem Beitrag für die Notwendigkeit eines planvollen Vorgehens – insbesondere, wenn es schnell gehen muss. Herr Romeike zeigt in seinem Beitrag, wie sinnvoll gelebtes BCM zu institutioneller Resilienz beiträgt. Herr Dr. Grete weist in seinem Beitrag auf die wichtige Schnittstelle zur IT hin und wie diese sinnvoll gestaltet werden kann. Herr Berens schließt diesen Teil mit seinem Blickwinkel auf das Bankenumfeld in den nächsten Jahren ab und wie BCM dazu beiträgt, sich dort weiter zu behaupten.

Der zweite Teil adressiert vor allem die operative Ebene. Herr Naujoks gibt einen Überblick über den Lebenszyklus des BCM im Wandel der Zeit und auf die praktische Umsetzung fokussiert. Dr. Grete zeigt in seinem zweiten Beitrag die Wichtigkeit von Softskills für das Gelingen einer BIA. Dr. Held erläutert in seinem Beitrag, wie aktuell die Leistungsfähigkeit von IT-Dienstleistern hinsichtlich der Ziele des BCM bewertet werden kann. Herr Otto geht in seinem Beitrag auf die Rolle des gesamten Auslagerungsmanagements für das BCM ein. Frau Kufeld teilt in ihrem Beitrag einen Teil ihrer Erfahrung zur Organisation und Arbeit eines Krisenstabs im BCM. Frau Adamek geht in ihrem Beitrag auf die Softskills der Menschen mit bestimmten Rollen im BCM ein, die neben den Hardskills entscheidend für ein funktionierendes BCM sind. Ein weiterer Beitrag von ihr mit wahren Geschichten, in denen aufgrund menschlicher Faktoren aus Übungen Notfälle wurden, runden dieses Buch ab.

Die in diesem Buch durch die Autorinnen und Autoren selbst gewählte zumeist männliche Form bezieht sich immer zugleich auf die weibliche, männliche und diverse Person. Die Autorinnen und Autoren verzichteten in der Regel auf Mehrfachbezeichnungen zugunsten der besseren Lesbarkeit. Entsprechende Begriffe und Rollenbezeichnungen gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter und Geschlechtsidentitäten. Es ist die Überzeugung des Verlags, der Herausgeber und der Autorinnen und Autoren, dass Kontinuitätsmanagement durch Menschen aller Geschlechter oder Geschlechtsidentitäten getragen wird – die BCM-Kultur hängt nicht von diesen beiden Eigenschaften ab. Die verkürzte Sprachform hat lediglich redaktionelle Gründe, der Verzicht auf Binnen-I o. ä. geht auf die Entscheidung zurück, Nicht-Muttersprachler und Menschen, die auf Screen-Reader angewiesen sind zu inkludieren und beides beinhaltet keinerlei Wertung.

Uwe Naujoks & Dr. Patrick Grete

A.

Aufsichtliche Anforderungen an das (IT-)Notfallmanagement – Eine Einführung

A. Aufsichtliche Anforderungen an das (IT-)Notfallmanagement – Eine Einführung[1]

I. Einleitung

»Mögest Du in interessanten Zeiten leben!« lautet den Aufzeichnungen eines britischen Kolonialbeamten zufolge ein alter chinesischer Fluch. Leider leben wir im 21. Jahrhundert in überaus interessanten Zeiten. Der 11. September 2001 und der daraus resultierende, mehr als zehn Jahre dauernde »War on Terror« sowie die auf die Insolvenz von Lehman Brothers 2007 folgende Weltfinanzkrise erscheinen aus heutiger Sicht nur als Präludium für die Schrecken unserer Zeit: 1

- Die Corona-Pandemie lässt seit 2020 die Verwundbarkeit der westlichen Gesellschaften offenkundig werden, indem sie Gesundheitssysteme, politische Gewissheiten und sozialen Konsens angreift.
- Die russische Invasion der Ukraine 2022 zielt auf die Zerstörung der in der Schlussakte von Helsinki kodifizierten europäischen Friedensordnung und führt in einen neuen Kalten Krieg.
- Beide Großereignisse belasten internationale Lieferketten teils bis zum Zerreißen und wirken als Treiber für eine mögliche neue Finanzkrise.
- Die Volksrepublik China, die vor kurzem noch als zuverlässiger Handelspartner erschien, wirkt zunehmend als kaum berechenbarer Antagonist des Westens im Ringen um eine regelbasierte Weltordnung.
- Physische Angriffe auf Unterseepipelines und -kabel und auf Kommunikationsknotenpunkte zeigen die intrinsische Verwundbarkeit von Infrastrukturen.
- Gleichzeitig steigt die Cyber-Bedrohungslage erstmalig auf ein Niveau, welches katastrophale Auswirkungen von Cyber-Angriffen greifbar macht (z. B. durch den Ausfall von Krankenhäusern, Universitäten, Kommunalverwaltungen und insbesondere Wirtschaftsunternehmen – auch im Finanzsektor).
- Als »Grundrauschen« könnten »normale« Naturkatastrophen gezählt werden, deren nicht immer gut funktionierende Bewältigung allerdings die Handlungsfähigkeit von Staaten infrage stellt (z. B. die Flutkatastrophe im Ahrtal).

1 Hinweis: Dieses Kapitel ist keine Publikation der Bundesanstalt für Finanzdienstleistungsaufsicht bzw. des Bundesamts für Sicherheit in der Informationstechnik, sondern ausschließlich eine private fachliche Meinungsäußerung der Autoren.

- Der Sturm des amerikanischen Kapitols durch Verschwörungsgläubige Anfang 2021 ist nur ein besonders herausragendes Beispiel für die drastische Radikalisierung von Gruppierungen aus verschiedenen Teilen des politischen und weltanschaulichen Spektrums und ihre steigende Bereitschaft, Gewalt und Sabotage anzuwenden.

2 Die Geschäftsleitung eines Instituts steht auch und gerade in schwierigsten Zeiten in der Verantwortung, sicherzustellen, dass die IT-Anwendungen und die IT-Systeme des Instituts sicher betrieben und weiterentwickelt werden und zugleich jederzeit die sich verändernden geschäftlichen und regulatorischen Anforderungen erfüllen. Dies ist schon unter alltäglichen Umständen ein hehres Ziel, welches erhebliche Kosten und Mühen verursacht. Jedoch müssen zusätzlich zum Alltag auch solche Situationen sicher bewältigt werden, in denen der Zufall mit voller Wucht zuschlägt, in denen alles schiefgeht, was schiefgehen kann – sei es beispielsweise ein Gebäudeausfall, ein großflächiger Ausfall von Personal oder auch der berüchtigte »Bagger um die Ecke«, der das für den Geschäftsbetrieb zwingend notwendige Datenkabel zerlegt.

3 Dies zu ermöglichen ist das Ziel des Notfallmanagements. Sein praktischer Kern besteht in der Bestimmung zeitkritischer Geschäftsaktivitäten und der Ableitung von Geschäftsfortführungsplänen für die betroffenen Geschäftsprozesse sowie Plänen für die Wiederherstellung des Normalbetriebs (insb. Wiederanlaufpläne für die IT-Systeme).

Beispiel: Der hungrige Marder

4 Im Herbst 2008 kam es in der Region Hannover nachts zu einem Stromausfall, der laut Medienberichten von einem Marder verursacht worden war, der in einem Umspannwerk der Stadtwerke Hannover ein Kabel durchgenagt hatte. Der Stromausfall betraf ein Rechenzentrum der S-Finanzgruppe, so dass bei 150 Sparkassen in Nord- und Ostdeutschland Geldausgabeautomaten, Kontoauszugsdrucker und Online-Banking bis 11:30 morgens ausfielen. Das Notfallmanagement eines Rechenzentrums hat in einer solchen Situation insbesondere auf die Klärung des Vorfalls, die Wiederherstellung der Stromversorgung und den Wiederanlauf der betroffenen IT-Systeme hinzuwirken. Das Notfallmanagement der betroffenen Institute muss dann beispielsweise klären, ob ein Notbetrieb in den Filialen möglich und sinnvoll ist.

Beispiel: Corona-Pandemie

5 Pandemieplanung ist ein klassisches Element des Notfallmanagements. Dementsprechend wurde bei Feststellung der Corona-Pandemie durch die WHO

und der Verfügung von Maßnahmen durch die Bundes- und Landesregierungen in Häusern mit existierendem Notfallmanagement die Notfallorganisation aktiviert und mit der Initiierung und Überwachung der betrieblichen Corona-Maßnahmen betraut.

II. Grundsätzliche Aufgaben und Prämissen des (IT-)Notfallmanagements

Geschäftsaktivitäten/-prozesse werden im Regelbetrieb durch verschiedene Ressourcen unterstützt, zum Beispiel Menschen, Räumlichkeiten, IT-Systeme. Diese Ressourcen können durch interne oder externe Ereignisse unverfügbar werden, womit der Regelbetrieb undurchführbar wird. 6

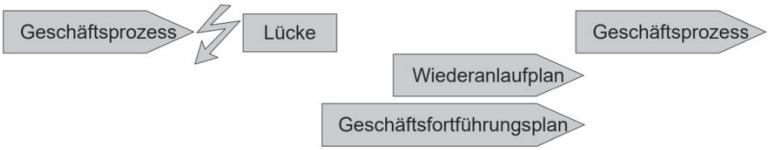
Ziel des Business Continuity Management (BCM) oder auch Betriebliches Kontinuitätsmanagement (nachfolgend auch als Notfallmanagement bezeichnet) ist es, sicherzustellen, dass bei einem Ausfall von Ressourcen, die normalerweise den Ausfall der Geschäftsaktivitäten bedingen würde, eine behelfsmäßige und geplante Durchführung wesentlicher Geschäftsaktivitäten initiiert und zugleich die Wiederherstellung der Ressourcen und ein geregelter Übergang zum Regelbetrieb betrieben wird. 7

Das Notfallmanagement ist ein ganzheitlicher Managementprozess in einem mindestens jährlich zu durchlaufenden Regelkreis, der potenzielle Bedrohungen erfassen, die Auswirkungen dieser Bedrohungen ermitteln und potentielle Maßnahmen zur Schadensvermeidung/-minimierung vorab definieren soll. Das Notfallmanagement soll insoweit mit Strategien, Plänen und Handlungen auf negative Ereignisse im Unternehmen reagieren, um insbesondere geschäfts- und zeitkritische Tätigkeiten und Prozesse zu schützen bzw. möglichst umgehend mit vorab festgelegten Alternativen auf das schlagend gewordenen Risiko zu minimieren. 8

Um dieses Ziel zu erreichen werden in einer *Risikoanalyse* (Rest-)risiken identifiziert, die zu einem Ausfall von Ressourcen führen können und in einer *Business Impact Analyse* zeitkritische Geschäftsprozesse und die für sie geltendenen zeitlichen Parameter bezüglich maximal tolerierbarer Ausfallzeit des Geschäftsprozesses, eine maximal tolerierbare Zeit des Datenverlusts (Recovery Time Objective) sowie eine Wiederanlaufzeit für die den Geschäftsprozess stützenden Ressourcen (Recovery Point Objective). 9

10 Auf dieser Basis werden für die zeitkritischen Geschäftsprozesse Geschäftsfortführungspläne und für die sie stützenden Ressourcen Wiederanlaufpläne definiert. Tritt ein Notfall ein, so muss die zeitliche Lücke zwischen Ausfall des Geschäftsprozesses und Wirkung des Geschäftsfortführungsplans unterhalb der Recovery Time Objective liegen.

11 Die folgende Grafik illustriert diese Grundprinzipien.



12 Zur Notfallvorsorge gehört weiterhin die Definition von Kommunikationswegen und einer besonderen Aufbauforganisation zur Bewältigung von Notfällen und Krisen. Dementsprechend folgen der Aufbau und die kontinuierliche Weiterentwicklung eines Notfallmanagementsystems strategischen Entscheidungen der Geschäftsleitung, die sich grundsätzlich in der Geschäftsstrategie des Instituts, bezogen auf das IT-Notfallmanagement sich explizit in der IT-Strategie wiederfinden müssen.

III. Aktuelle Aufsichtsrechtliche Anforderungen

1. Europäische Anforderungen seitens der EBA

a) Leitlinien für das Management von IKT- und Sicherheitsrisiken (EBA/GL/2019/04)

13 Die Leitlinien legen für die in Tz. 6 benannten Unternehmen Anforderungen an die Informationssicherheit, soweit die Informationen auf IKT-Systemen gehalten werden und Maßnahmen für das Management von Risiken fest, insbesondere betreffend die operationellen und sicherheitsrelevanten Risiken (IKT- und Sicherheitsrisiken).

14 Ab Tz. 77 werden die aufsichtlichen Anforderungen beschrieben, die für ein solides BCM notwendig sind, um die Fähigkeit zur kontinuierlichen Erbringung