Udo Milkau

Operational Resilience in Finanzinstituten

Grundlagen, Beispiele und Anwendungen

Springer Gabler

Operational Resilience in Finanzinstituten

Udo Milkau

Operational Resilience in Finanzinstituten

Grundlagen, Beispiele und Anwendungen

Springer Gabler

Udo Milkau
Frankfurt am Main, Deutschland

ISBN 978-3-658-36896-8 ISBN 978-3-658-36897-5 (eBook)
https://doi.org/10.1007/978-3-658-36897-5

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Lektorat/Planung: Guido Notthoff
Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Ein im Jahr 2021 geschriebenes Buch über Operational Resilience ist zwangsläufig von den großen „Disruptionen“ von 2020/2021 geprägt: von der Covid-19-Pandemie mit der Entwicklung der mRNA-Impfstoffe in Rekordzeit bis zu den weltweiten Extremwetterereignissen und der Flutkatastrophe vom Juli 2021 im Ahrtal. Dies wird man beim Lesen des Buches immer wieder feststellen. Diese Ereignisse relativieren eine Scheuklappensicht auf Banken und Finanzinstitute.

Dennoch möchte ich mit einem engeren Fokus beginnen. Als im Mai 2021 ein guter Freund mit mir über dieses Buchprojekt sprach, machte er eine bemerkenswerte Feststellung: „Banken erstellen mit hohem Aufwand Risikokalkulationen aus der etablierten Perspektive von Value-at-Risk (für die Schätzung von kurzfristigen Risiken innerhalb eines Konfidenzintervalls) – und dann passiert trotzdem alle zwei bis drei Jahre ein ‚Jahrhundertevent‘: von Lehman Brothers, Wirecard oder Greensill, Covid-19 oder ein Cybervirus, eine erwartbar ‚unerwartete‘ Entscheidung der ECB, der nächste Geldwäscheskandal, eine ‚überraschende‘ Formulierung in einer Regulierung der European Commission wie kürzlich zur Artificial Intelligence, eine weitere Twitternachricht von Elon Musk, bis zu einem in Suezkanal quer stehenden Containerschiff mit den Auswirkungen auf den Welthandel und dessen Finanzierung.“

Höchstwahrscheinlich waren all die oben genannten Beispiele schon vorab „irgendwie“ plausibel, und jedes Ereignis hat den Blick auf große, seltene und meist vernetzte Risiken gelenkt. Dann treten diese „disruptiven“ Probleme meist wieder in den Hintergrund, und man geht zum „kalkulierbaren“ Tagesgeschäft über. Scheinbar sind solche seltenen Ereignisse zumindest in der Gesamtsicht gar nicht so selten. Und oft sind sie mit zunehmenden Abhängigkeiten infolge der Digitalisierung oder der Globalisierung verbunden.

Dieses Zusammentreffen von neuen Abhängigkeiten, der zumindest gefühlten Häufung von Jahrhundertevents in den vergangenen zwei Dekaden und einem Wunsch nach mehr „Resilience“ in den heute unruhigen Zeiten bildet den Kern dieses Buchs. Dabei soll es den theoretischen Hintergrund für eine „Operational Resilience“ mit einer pragmatischen Perspektive auf mögliche Umsetzungen verbinden. Ein spezieller Schwerpunkt liegt dabei auf der Weiterentwicklung der Wahrscheinlichkeitsrechnung für „wiederholte Spiele“ –

die Standardbeispiele der Statistik wie Würfeln oder Lotto – in den Bereich des Unvorhersehbaren und einem Aufbau von Grundlagen für eine Wiederherstellung der Betriebsfähigkeit, nachdem eine unvorhergesehene Disruption dann doch eingetreten sein wird.

Hinzu kommt noch ein oft vergessener Punkt. Ein „Risiko" setzt – im Gegensatz zu einer statistischen Schätzung von Eintrittswahrscheinlichkeiten – immer die Perspektive von uns Menschen als Entscheider und unsere Wahl voraus, was wir in einem bestimmten Kontext als „Risiko" oder als Normalität sehen wollen. Dies gilt für jeden Einzelnen, für die Gesellschaft als Ganzes, aber auch für ein Unternehmen wie eine Bank, was wir als künftiges Risiko sehen wollen und wie dies unsere heutigen Entscheidungen bestimmt.

Dabei sind zwei Sichtweisen – beide menschlich – weit verbreitet: Entweder man setzt auf die Fortschreibung des Bekannten und damit auf die Statistik von „wiederholten Spielen", was uns eine Kontrollillusion erlaubt. Die Zukunft hält sich zwar nie an unsere Spielregeln, aber wenn wir dies gerne glauben wollen, dann können wir Risiken gut „managen" – und dies im ursprünglichen Wortsinn: „ein Pferd in der Manege handhaben" (von italienisch „maneggiare"). Natürlich funktioniert dies auch zumindest so lange, wie wiederkehrende Schäden aus Konsumentenkrediten oder Zahlungsverzögerungen durch Prozessunterbrechungen betroffen sind und diese iterativ immer besser gehandhabt werden können.

Oder man konstruiert als fatalistischer Pessimist kategorisch solche Szenarien, dass immer das Schlimmste passieren wird, dass wir in einer exponentiellen Entwicklung auf eine finale Katastrophe zusteuern und dass sofort „alles" dagegen getan werden muss.

Weder Kontrollillusion noch Panik sind geeignete Mittel, um mit seltenen, aber schwerwiegenden Disruptionen und potenziellen Großschäden innerhalb langer Zeiträume umzugehen. Hier ist die Industrie teilweise weiter als Banken. Sowohl vor dem Hintergrund der Covid-19-Pandemie mit Ausfällen von Personal, staatlichen Quarantänemaßnahmen bzw. Einschränkungen, Umstellung auf Work-at-Home usw. als auch aufgrund von Unterbrechungen von globalen Lieferketten verändert sich das Paradigma des Just-in-Time (mit Minimalisierung der Lagerhaltung) bzw. Just-in-Sequence (mit Synchronisierung von Produktionsabläufen ohne Puffer) hin zu der Frage, wie eine Produktion just in case (mit einer Ausrichtung auf den „Case" der Kunden) und mit bewusst vorgesehenen Puffern gestaltet werden kann.

Mittlerweile hat auch die Bankenaufsicht dieses Problem in den Blick genommen. So haben Anfang 2021 sowohl das Basel Committee on Banking Supervision (BCBS) als auch die Bank of England ihre Prinzipien für „Operational Resilience" in Finanzinstituten veröffentlicht. Da im Deutschen der Begriff „Resilienz" primär in der Psychologie angesiedelt – und durch diese Konnotation daher für die hier betrachteten Fragen nicht passend – ist, soll im Folgenden die englische Form Operational Resilience als Terminus technicus verwendet werden.

Dabei werden insbesondere aktuelle Arbeiten von Terje Aven und dessen Arbeitsgruppe an der University of Stavanger im Bereich des industriellen Risikomanagements (u. a. für Offshore-Plattformen oder Flüssiggasanlagen) einbezogen werden, aber auch ältere Arbeiten wie die des deutschen Soziologen Niklas Luhmann von 1991 zur „Soziologie des Ri-

sikos“. Und auch die ganz aktuelle Debatte über die Rolle von Banken bezüglich der Risiken des Klimawandels spielt natürlich eine Rolle.

Letztlich wird es darum gehen, wie große Risikoereignisse in Finanzinstituten, welche vielleicht einmal in zehn oder hundert Jahren eintreten könnten – dann aber mit massiven bis zu katastrophalen Auswirkungen –, im Eintrittsfall gehandhabt und nachfolgend als Lerneffekt einbezogen werden können. Da heute das Bankgeschäft faktisch ein technisches „digitales“ Geschäft mit vielfältigen Verbindungen zwischen den vielen Beteiligten geworden ist, wird die Frage der Abhängigkeiten im digitalen Zeitalter einen wichtigen Teil darstellen.

Dennoch soll die technologische Betrachtung nicht den Blick dafür verstellen, dass jedes Risiko eine Frage der Beurteilung durch uns Menschen ist. Gerade bei „High-severity/low-frequency“-Ereignissen, welche schwere Folgen bzw. hohe Schäden nach sich ziehen, aber außerhalb von banktypischen Planungszeiträumen liegen – Jahresplanung, Mittelfristplanung, Laufzeit von Vorstandsmandaten oder Bereichsleiterverträgen, Möglichkeiten der Vorstellung der Mitarbeiterinnen und Mitarbeiter oder Zeithorizont der Kapitalgeber etc. – stellt sich die fundamentale Frage, wie viel Kosten eine Vorsorge gegen solche Risiken ein Entscheider befürworten soll, wenn doch erst ein Nachfolger oder eine Nachnachfolgerin mit einem möglichen Eintritt konfrontiert werden wird.

Wenn Entscheidung bzw. Vorbeugung und Konsequenz bzw. (vermiedener) Schaden weit auseinanderfallen, dann sind neue Konzepte der Risikobetrachtung und Verantwortung notwendig. Und noch fokussierter hat dies – wenn auch in einem ganz anderen Kontext – Christian Drosten mit seinem Zitat aus dem März 2020 ausgedrückt: „*There is no glory in prevention!*“ Wer will schon heute hohe Kosten beantragen und verantworten, wenn diese sich erst irgendwann und irgendwo gegen eine Schadensvermeidung aufrechnen lassen könnten? Alle später noch zu diskutierenden Maßnahmen wie Redundanz, Flexibilität, Adaption oder Transformation kosten im Hier und Jetzt viel Geld.

Insgesamt steht die Idee einer Operational Resilience zur Wiederherstellung der Betriebsfähigkeit auch bei (sehr) seltenen disruptiven Störungen zwei Problemen von Menschen gegenüber: Zum einen ist unsere Strength of Knowledge limitiert, sodass wir jenseits der bequemen Annahme von wiederholten Spielen künftige Risiken nur schwer formalisiert greifen können. Und Friedrich von Hayek hat zu Recht – insbesondere in seiner Rede zur Verleihung des Preises in Erinnerung an Alfred Nobel am 11.12.1974 – vor der Gefahr einer „Pretence of Knowledge“ gewarnt, wo unsere menschliche Erkenntnis grundsätzlich limitiert ist. Zum anderen sind heute in der Wirtschaft die Incentivestrukturen in der Regel nicht darauf ausgelegt, dass Ausgaben „auf Verdacht“, aber ohne kurzfristigen Business Case innerhalb von Reportingperioden dem Verantwortlichen einen persönlichen Nutzen einbrächten, wenn sie auch dem Unternehmen als solchen (sehr) langfristig eine Stabilität gegen die Unbestimmbarkeit der Zukunft verschaffen könnten.

Dieses Buchs soll die verschiedenen Perspektiven zusammenbringen: von der (mehr industriell orientierten) Risk Science über die aktuelle (und sich entwickelnde) Regulatorik zur Operational Resilience in Banken bis zu bekannten (aber vielleicht vergessenen) soziologischen und spieltheoretischen Einsichten über das menschliche Verhalten im

Angesicht von Risiken. Nicht zuletzt sollen praktische Erfahrungen im aktiven Umgang mit „Disruptionen“ aus anderen Industrien hier einfließen. Und schließlich hilft auch ein weiter Blick zurück, wie Kaufleute in den letzten zweitausend Jahren mit dem Unvorhersehbaren umgegangen sind: Sie zeigten Mut zur Zukunft, ohne diese „kalkulieren“ zu können.

Dabei ist mir bewusst, dass dies nicht ohne gewisse Stoßstellen möglich ist und auch einige Fragen offen bleiben müssen. Doch ist nicht nur allgemein die Strength of Knowledge begrenzt, sondern insbesondere die von mir, und daher bitte ich bei allen vorhandenen Missverständnissen um Nachsicht. Ebenso um Nachsicht bitte ich dafür, dass mir zu einigen englischsprachigen Fachbegriffen (wie eben Strength of Knowledge) keine guten Übersetzungen eingefallen sind. Ebenso werden viele Zitate im originalsprachlichen Original wiedergegeben werden, ohne dass nach einer Übersetzungsmöglichkeit gesucht wurde. Außerdem wird bei Begriffen wie Kunde, Experte, Mitarbeiter usw. im Plural das generische Maskulinum der deutschen Sprache verwendet, wobei generisch weibliche und anderweitige Geschlechteridentitäten ausdrücklich eingeschlossen sind.

Letztlich ergeht mein Dank schon vorab an die Leser, welche mir dies vergeben müssen. Und noch mehr Dank sagen möchte ich meiner Gattin Ritva Tikkanen für ihre Geduld mit mir sowie vielen Freunden, welche mich bei diesem Buch unterstützt haben – davon seien nur Hans-Christian Boos, Andreas Gamer und Wolfgang König ausdrücklich genannt.

Frankfurt Udo Milkau
November 2021

Inhaltsverzeichnis

Teil I

Grundlagen

Risiko und Resilience im digitalen Zeitalter

1

Zusammenfassung

Operational Resilience ist ein neues Konzept gegenüber Operational Risk Management, welches von der Widerstandsfähigkeit von ökologischen Systemen gegenüber Schocks übernommen wurde und eine Wiederherstellung der ökonomischen Betriebsfähigkeit unter der Annahme beschreibt, dass gemäß eines seltenen, aber plausiblen Szenarios einmal in der Zukunft eine Disruption eingetreten sein wird. Im Kern ist Operational Resilience damit der Antagonist zu einer Kontrollillusion, alles ex ante absehen, kalkulieren und schützen zu können. Während das traditionelle Operational Risk Management von einer Ex-ante-Definition einer „Risk Policy" und dem nachgelagerten Reporting von eingetretenen Ereignissen ausgeht, beginnt Operational Resilience bei der Annahme, dass „irgendwann" einmal eine Disruption der Betriebsfähigkeit eingetreten sein wird. Dies spiegelt sich in neuen aufsichtsrechtlichen Ansätzen wider, wobei die Frage nach den heutigen Kosten für Maßnahmen gegen „irgendwann" zu erwartende Vorkommnisse unbeantwortet bleibt.

Die aktuellen Veröffentlichungen des Basel Committee on Banking Supervision (BCBS 2021) und der Prudential Regulation Authority der Bank of England (PRA 2021a, b) und das U.S. Interagency Paper (Fed 2020) zur „Operational Resilience" in Finanzinstituten reihen sich in eine Entwicklung seit wenigen Jahren ein. Dabei zeigen die grundlegenden Definitionen des BCBS von 2001 und 2021 die Weiterentwicklung innerhalb von zwanzig Jahren (Zitate):

U. Milkau, *Operational Resilience in Finanzinstituten*,
https://doi.org/10.1007/978-3-658-36897-5_1

> Operational Risk: „loss resulting from inadequate or failed internal processes, people and systems or from external events“ (BCBS 2001)

> Operational Resilience: „ability of a bank to deliver critical operations through disruption“ (BCBS 2021)

Die unterschiedliche Ausrichtung, welche sich aus diesem Paradigmenwechsel vom Management von Verlusten (aus operationellen Risikoereignissen) hin zur Aufrechterhaltung des Betriebs (im Falle einer Disruption) ergibt, ist in Tab. 1.1 zusammengefasst. Dabei muss man „Aufrechterhaltung des Betriebs“ etwas umfassender als wortwörtlich verstehen. Wenn eine abrupte Disruption – also ein plötzliches „Zerreißen“ oder ein Ausfall eines gesamten Systems – auftritt, dann wird es in diesem Moment auch keinen Service mehr geben können. Während es bei kleineren Ausfällen zum Beispiel von einzelnen Verbindungen in einem Netzwerk noch möglich sein kann, redundante Verbindungen zu nutzen, wird ein solches Netzwerk bei einer massiven „Ruption“ wortwörtlich zerreißen. Und gerade „digitale“ Systeme verhalten sich bezüglich Störungen in der Regel sehr digital: Sie laufen („eins“) oder sie sind ausgefallen („null“). Wenn diese Disruption – der Systemausfall – eingetreten sein wird, dann geht es um die Wiederherstellung der Betriebsfähigkeit. Dies hat u. a. die NATO (2021) in eine entsprechende Definition einbezogen (Zitat):

> … resilient to resist and recover from a major shock such as a natural disaster, failure of critical infrastructure, or a hybrid or armed attack.

Ebenso hat die deutsche Bankenaufsicht BaFin (2021) am 15.11.2021 zehn gleichrangige mittelfristige Ziele veröffentlicht, worunter als zweiter Punkt „Operative Resilienz“ genannt ist (Zitat):

> Mit Blick auf die operative Stabilität und Sicherheit der von ihr beaufsichtigten Unternehmen und insbesondere deren Technologieplattformen achtet die BaFin auf die Resilienz dieser Unternehmen. Im Fokus stehen die Bekämpfung der stark zunehmenden Cyberrisiken und die Änderungen im Risikoprofil der Unternehmen durch die Fragmentierung der Wertschöpfungsketten, vor allem durch wesentliche Auslagerungen.

Dabei definiert die BaFin „Operative Resilienz“ – abweichend von den obigen Definitionen – im Zusammenhang mit „Cyberrisiken“ und „Änderungen im Risikoprofil“, sodass diese „Operative Resilienz“ weniger als Operational Resilience, sondern im Sinne einer erweiterten Definition einer Cyber Security (vgl. Tab. 1.1) zu sehen ist, wie dies auch in der europäischen Gesetzesvorlage DORA zugrunde gelegt wird (siehe weiter unten im Text und Tab. 1.2). Daher wird auf diese spezifische Definition der BaFin nicht weiter eingegangen, sondern die Aspekte im Zusammenhang mit DORA diskutiert werden.

Anzumerken ist, dass u. a. die Bank of International Settlement den Begriff „Resilience“ auch in einem anderen Kontext, nämlich der finanziellen Tragfähigkeit bei marktgetriebenen Schocks, verwendet. Dabei können die identischen Auslöser wie u. a. die

Tab. 1.1 Gegenüberstellung von Operational Risk Management und Operational Resilience

	Operational Risk	*Operational Resilience*
Definitionen	Management von Verlusten aus Risikoereignissen durch Regelwerk, Governance, Analyse, Reporting	Wiederherstellung des Betriebs im Falle einer eingetretenen (!) Disruption in der Zukunft
Probleme	Ökonomische Definition, was ein „Verlust" sei: eine aktuell offene Position, ein temporärer Verlust in einer Berichtsperiode (aber mit späterer Kompensation) oder ein realisierter Schaden?	Menschengemachte Selektion, was eine Disruption sei – oder in anderen Worten die Unterscheidung, was als ein „normales" versus ein „disruptives" Ereignis festgelegt sein soll
Grundansatz	Ex-ante-Festlegung für den Umgang mit Risiken: - Vermeidung - Reduktion - Minderung - Akzeptanz	Vorsorge für den Fall einer eingetretenen Disruption mittels: - Redundanz - Flexibilität - Adaption - Transformation
Fokus	Modellierung von Verlustereignissen im Bankbetrieb in jeweils verschiedenen Geschäftsfeldern[a]	Verständnis der Abhängigkeiten und entsprechenden abgeleiteten Maßnahmen[a]
Ziele	Kalkulation von Risikozuschlägen zum regulatorischen Kapital	Maßnahmen für die aktive Wiederherstellung der Betriebsfähigkeit im Notfall, d. h. nach einem „disruptiven" Ereignis
Annahmen	Wiederholte (zwar unregelmäßig, aber kontinuierlich) Ereignisse mit Potenzial für finanzielle Schäden	Seltene (zwar plausible, aber ggf. erstmalige) Disruptionen mit Gefahr der Betriebsunterbrechung
Häufigkeit bzw. Zeitskala	Häufig mit kurz- bis mittelfristig wiederholten Ereignissen (vgl. Kap. 3)	Selten bis sehr selten und nur auf langen Zeitskalen (im Sinne von sogenannten Tail Risks; vgl. Kap. 4)
„Strength of Knowledge"	Datenbasierte Erfahrung mit regelmäßigen Mustern bzw. der Annahme solcher Regelmäßigkeiten	Hypothesenbasierte plausible Szenarien über seltene Ereignisse, welche bisher nicht „erfahren" wurde
Statistik	Wahrscheinlichkeitsverteilung	Insbesondere sogenannte Heavy Tails, d. h. seltene, aber schwerwiegende Ereignisse

Vergleich von Kernaspekten eines Operational Risk Management mit dem Konzept der Operational Resilience

[a]Anmerkung: Selbst im Rahmen von „Business Continuity Planing" (BCP) wird meist ein Siloansatz verfolgt und zum Beispiel der Ausfall eines Rechenzentrums durch einen entsprechenden Back-up berücksichtigt, wohingegen der Ausfall der Verbindung für Großbetragszahlungen hin zur Zentralbank durch eine Nachrichtenübermittelung per Fax ersetzt würde.

Covid-19-Pandemie diskutiert werden: zum einen aus der Sicht des Eigenkapitals von Banken (siehe das BIS Bulletin von Ikeda et al. 2021) und zum anderen bezüglich der operativen Betriebsfähigkeit. Für die Betrachtung in diesem Buch soll der rein finanzielle

Tab. 1.2 Vergleich der aktuellen Veröffentlichungen zu Operational Resilience

	BCBS	PRA	Fed	DORA	Bemerkungen
Governance	x	x	x	(x)	Institute sollen auf der bestehenden Governance für Operational Risk Management aufbauen, um eine Operational Resilience zu entwickeln. Dies berücksichtigt aber nicht die unterschiedlichen Schwerpunkte von Ex-ante-Festlegung zum Umgang mit Operational Risk vs. konkreten Maßnahmen, wenn eine Disruption eingetreten sein wird.
Operational Risk Management	x	x	x	(x)	Institute sollen auf entsprechende Funktionen des Operational Risk Management aufbauen. Dies berücksichtigt nicht die notwendigen Erweiterungen für aktive Handlungen im Falle eins disruptiven Ereignisses.
BCP[a] und Test	x	x	x	(x)	Da BCP schon seit Langem ein etablierter Ansatz für IT-Systeme (und speziell IT-Betrieb in Rechenzentren) ist, überdeckt dies die neue und weit umfassendere Perspektive von BCBS bzgl. „*critical operations and their interconnections and interdependencies, including those through relationships with, but not limited to, third parties and intragroup entities*“.
Interconnections & Interdependencies	x		x		Dieser Punkt wird nur in BCBS (2021) adressiert, stellt aber einen grundsätzlichen Aspekt von Operational Resilience dar (d. h. Abhängigkeiten). Dabei beschreibt BCBS nur ein „Mapping“ der kritischen Verbindungen, ohne auf konkrete Maßnahmen im Falle einer Disruption und auf Verbindungen zwischen „Silos“ einzugehen.
(Out-)Sourcing	x	x	x	(x)	Die Frage, ob und wie (Out-)Sourcing zu Risiken beiträgt, wird später diskutiert. Nur BCBS hat dem zumindest soweit Rechnung getragen, als dass alle Beziehungen einbezogen werden sollen.
Incident Management und Reporting	x		x	(x)	Der Umgang mit Vorfällen ist vom Schwerpunkt des Reportings geprägt, und enthält keine Ansätze für aktive Maßnahmen.
Cyber Security	x		x	x (!)	Dies ist der Schwerpunkt von DORA, aber nur ein (wichtiger) Teilaspekt von Operational Resilience.

Vergleich der verschiedenen Ansätze des Basel Committee on Banking Supervision (BCBS 2021), der Prudential Regulation Authority der Bank of England (PRA 2021a) und der Aufsichtsbehörden in den USA (Fed 2020) zur „Operational Resilience“ sowie der European Commission (2020) zum „Digital Operational Resilience Act“ (DORA).

(Fortsetzung)

Tab. 1.2 (Fortsetzung)

DORA bezieht sich dabei ausschließlich auf IT-Risiken und definiert (Zitat): „*‚digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective*". Damit greift DORA kürzer als BCBS und PRA, da DORA nur altbekannte Konzepte des Operational Risk Management zusammenfasst, aber das Konzept einer Wiederherstellung der Betriebsfähigkeit nach einer eingetretenen Disruption nicht einbezieht.
[a] BCP steht für Business Continuity Planning bzw. für den im Deutschen eher selten übersetzten Begriff des betrieblichen Kontinuitätsmanagements (BKM).

Aspekt nicht weiter betrachtet werden, da er ein Teil der allgemeinen Kapitalanforderungen ist.

Da viele der methodischen Ansätze von 2001 mittlerweile überarbeitet wurden und seit 2017 ein neuer „Standardised Approach" für die Berechnung der Kapitalzuschläge für Operational Risk existiert (BCBS 2017), wäre es bestenfalls von historischem Interesse, die gesamte Entwicklung im Operational Risk Management nachzuzeichnen. Dennoch stellt der ursprüngliche Ansatz für ein Operational Risk Management (Zitat aus BCBS 2001), „*A key issue in the area of operational risk management – as well as in the development of regulatory capital requirements – is the collection and analysis of loss data*", auch heute immer noch das Grundgerüst für den Umgang mit Operational Risk in Finanzinstituten dar, welches mit einer Sammlung von Daten aus der Vergangenheit beginnt.

Dagegen ist die Blickrichtung einer Operational Resilience in die Zukunft gerichtet und setzt sogar als Ausgangspunkt voraus, dass eine Disruption schon eingetreten sein wird – trotz aller Bemühungen des Operational Risk Management. Dabei stimmt die oben genannte Definition (BCBS 2021) auch mit der modernen Sicht in anderen Disziplinen wie der Ökologie überein, wo beispielsweise Brian Walker und David Salt (2012) folgende einfache Beschreibung nutzen (Zitat): „*resilience is the ability to cope with shocks and keep functioning in much the same kind of way.*" Eine Übersicht über die verschiedenen Definitionen von „Operational Resilience" in der Literatur ist bei Kijan Vakilzadeh und Alexander Haase (2021) zu finden.

Bemerkenswerterweise hat sich auch in der Ökologie der Begriff der „Resilience" über die Jahre fortentwickelt, da noch Holling (1996) einen Unterschied zwischen einer einfachen „engineering resilience" und einer integrierten „ecological resilience" machen wollte. In der aktuellen Definition sind die Begriffe „operations" oder „functioning" die Schlüssel, da sie triviale Konstrukte (wie das mechanische Bild einer Kugel im Potenzialtrog mit einer kontinuierlichen „analogen" Systemeigenschaft) verwerfen und eindeutig auf Systeme mit einer Funktion für deren Umwelt verweisen – egal ob dies nun Banken oder Bewässerungssysteme mit deren jeweiliger Funktion für die Gesellschaft und die Wirtschaft sind. Das Wiederherstellen der Betriebsfähigkeit („operations") ist damit auch kein Selbstzweck, sondern immer im sozialen Kontext mit Kunden oder Nutzern eingebettet. Dies schlägt den Bogen zu einem in diesem Buch wichtigen Punkt, dass nämlich die Menschen – bei allem Reden von „Systemen" – am Ende immer die maßgeblichen Beteiligten sind: ob als Betroffene oder als Problemlöser.

Abgrenzung der Definition von „Operational Risk" zu anderen Risikobegriffen
Die verwendete Definition von „Operational Risk" schließt Risiken aus Rechtsverstößen und entsprechendem Fehlverhalten (Conduct Risk) ein, aber nicht das sogenannte Reputational Risk btr. öffentlicher Wahrnehmung (und ggf. Auswirkungen auf die Unternehmensbewertung) und das Strategic Risk bzgl. der Ausrichtung der Geschäftstätigkeit. In den letzten Jahren ist zudem der Begriff „Non-financial Risk" aufgekommen, welcher unterschiedlich in der Abgrenzung zu bzw. Überlappung mit Operational Risk verwendet wird und auf eine Unterscheidung zum traditionellen „Financial Risk" mit Markt-, Kredit- und Liquiditätsrisiken zielt, auch wenn alle Risiken in Finanzinstituten letztlich einen finanziellen Schaden darstellen. In diesem Buch wird der Begriff „Operational Risk" im Sinne der BCBS-Definition verwendet

1.1 Operational Risk und Operational Resilience aus aufsichtsrechtlicher Sicht

Im Ansatz des BCBS von 2001 wurden u. a. verschiedene Punkte als Treiber von operationellen Risiken beschrieben: „… *highly automated technology, the growth of e-commerce, large-scale mergers and acquisitions that test the viability of newly integrated systems, the emergence of banks as very large-volume service providers, the increased prevalence of outsourcing*". Diese primär technologische Sicht ist kritisch zu hinterfragen, da in den letzten zwanzig Jahren – auch neben dem Sonderfall der Finanzmarktkrise mit einem systemischen Versagen vieler Institutionen – insbesondere kriminelle Handlungen sogenannter Rogue Trader, Manipulationen wie beim LIBOR, ein Bankenkartell im Markt für Staatsanleihen, illegale Cum-ex-Geschäfte, Verkauf von „unangemessenen" Produkten an Privatkunden oder immer wieder massive Einzelengagements (Stichwort: Greensill Capital) sowie die resultierenden Strafzahlungen nach Gerichtsurteilen die größten Operational-Risk-Verlustfälle waren. Zum Problem der menschlichen Gier und falschen Incentivestrukturen soll später noch kurz zurückgekommen werden.

Zum anderen ist auch heute die Diskussion um Operational Resilience noch immer von der Sichtweise eines „risikovermeidenden" Operational Risk Management geprägt, wie als anekdotisches Beispiel in einer aktuellen Zusammenstellung des Beratungshauses McKinsey & Company (Barriball et al. 2021) aufgeführt wird (Zitat): „*Building operations resilience – Successful companies will redesign their operations and their supply chains to protect their business against a wider and more acute range of potential shocks and disruptive events*."

Dies geht am Kern einer Operational Resilience vorbei, da es ein Widerspruch ist, trotz des Eintritts eines „disruptiven" Events die Betriebsfähigkeit und die Leistungserbringung für die Kunden aufrechterhalten zu können. Eine Operational Resilience ist gerade der Antagonist zu einer Kontrollillusion, alles ex ante absehen, kalkulieren und schützen zu können.

Dem haben auch die neuen Prinzipien des BCBS (2021) Rechnung getragen, wenn von einem (Zitat): „*evolving operational risk landscape*" gesprochen wird. Auch wenn Banken in der Covid-19-Pandemie – zumindest bisher – ohne merkliche Beeinträchtigungen der

operativen Betriebsfähigkeit geblieben sind, hat – leider – die Covid-19-Pandemie grundsätzlich einen notwendigen Paradigmenwechsel unterstrichen:

1. Bei Operational Resilience geht es um die unkalkulierbaren „seltenen, aber plausiblen" Disruptionen, welche man nicht ex ante vermeiden kann, sondern welche unvermeidbar auftreten werden.
2. Es betrifft insbesondere die Abhängigkeiten der heutigen „digitalen" Systeme, welche hochgradig vernetzt, aber auch so optimiert sind, dass sie faktisch keine Puffer mehr vorhalten (Zeit-, Kapazitäts-, Lagerpuffer).
3. Solche Disruptionen besitzen keine monokausalen Ursachen und resultieren in der Regel aus einer Kombination von menschlichen Fehlern (von der Gier bis zur Kontrollillusion) zusammen mit „digitalen" Abhängigkeiten zwischen verschiedenen Systemen als Kristallisationspunkt für nachfolgende Betriebsunterbrechungen.
4. Und der damit verbundene Blick richtet sich auf seltene Ereignisse, welche nur auf langen Zeitskalen (im Sinne von sogenannten Tail Risks, siehe weiter unten) beobachtbar sind. Dabei bedeutet „selten" aber keineswegs, dass man diese Möglichkeiten heute vernachlässigen könnte, sondern dass diese Ereignisse im Mittel eben „selten" auftreten. Aber auch wenn ein Ereignis durchschnittlich nur einmal im Jahrhundert (kurz: Jahrhundertereignis) auftritt, so kann dies morgen geschehen oder in zweihundert Jahren. Und selbst wenn es morgen eingetreten sein wird, dann ändert dies nichts an der Wahrscheinlichkeit für übermorgen – genauso wenig, wie zehnmal „schwarz" beim Roulette irgendetwas daran ändert, dass die Wahrscheinlichkeit beim nächsten (elften) Spiel wieder 50:50 ist.

Leider ist der Begriff der „Disruption" in BCBS (2021) nicht definiert. Darüber hinaus wird „Disruption" auch gerne in der Managementliteratur im Sinne der Aufmerksamkeitsökonomie verwendet, wobei dort auch noch meist von der engen Definition von „Disruptive Technologies" von Joseph L. Bower und Clayton M. Christensen (1995) abgewichen wird. Man kann aber als Definition in dem hier relevanten Kontext davon ausgehen, dass Unterbrechungen von kritischen Betriebsfunktionen (mit Auswirkungen auf eine Bank oder das Finanzsystem als solches) und der Ausfall von vernetzten Infrastrukturen in dem Sinne zu verstehen sind.

In der Formulierung der vorliegenden Ansätze sind die Aufsichtsbehörden (BCBS 2021; PRA 2021a; Fed 2020) sowie die European Commission (2020) mit deren Vorschlag zu einem „Digital Operational Resilience Act" (DORA) nur wenig über das traditionelle Konzept des Operational Risk Management hinausgegangen, wie dies in Tab. 1.2 zusammengefasst ist. Dabei ist es unbestritten, dass die traditionellen Funktionen – von der Verantwortung und Definition eines Risikoappetits bis zum Business Continuity Planning und Reporting von Incidents (Vorfällen) – das Fundament jedes Operational Risk Management bilden.

Die oben genannte Evolution zu einer Operational Resilience unter der Prämisse „wenn eine Disruption eingetreten sein wird" (also einer Perspektive des „Futur II") mit dem

aktiven Wiederherstellen der Betriebsfähigkeit verschiebt den Fokus von der Ex-ante-Kalkulation von Risikokapital mit etablierten statistischen Methoden zu einem Neuland, wo Disruptionen gerade nicht mehr kalkulierbar, sondern nur noch plausibel sind. Die Aufsichtsbehörden in den USA (Fed 2020) haben dies gemeinsam folgendermaßen formuliert (Zitat):

> While potential hazards may not be prevented, the agencies consider that a flexible operational resilience approach can enhance the ability of firms to prepare, adapt, withstand, and recover from disruptions and to continue operations.

Im Gegensatz zu dieser Formulierung einer „flexiblen" Operational Resilience hat die PRA (2021b) in UK einen anderen Ansatz gewählt, wenn von den Instituten die Festlegung einer Schwelle einer „Impact Tolerance" verlangt wird (Zitat):

> … require firms to ensure they are able to deliver their important business services within impact tolerances in severe but plausible scenarios. … firms to use a time-based metric for all impact tolerances, but, where appropriate, firms should use a time-based metric in conjunction with other metrics. For example, a firm could set its impact tolerance at a certain volume of interrupted transactions due to the disruption of the firm's important business service, in conjunction with the disruption continuing after a certain number of hours.

Grundsätzlich ist die selbstverantwortliche Festlegung einer solchen „Katstrophenschwelle" eine neue Idee, da die Blickrichtung von (traditionellen) Schadenhöhen auf operative Auswirkungen auf den Betrieb bzw. Betriebsstillstand geändert wird.

In der Umsetzung eines solchen im Operational Risk Management bisher nicht verwendeten Ansatzes stellen sich aber eine Reihe von Fragen: Wie verhalten sich (konzeptionell an BCP mit vertraglichen Wiederanfahrzeiten für kritische Systeme angelehnte) Ausfallzeiten zu kritischen Zeitpunkten wie zum Beispiel Cut-off-Zeiten im Großbetragszahlungsverkehr und ein Ausfall eines Wertpapierordersystems kurz vor Börsenbeginn an der Wall Street? Was bedeutet der Ansatz, selbstverantwortlich die Szenarien als Grundlage für die Schwelle festzulegen? Und schließlich scheint selbst die Darstellung in Figure 2 in PRA (2021a) nicht schlüssig zu sein, wenn dort in einer statistischen Schadenhöhe-Schadenhäufigkeit-Verteilung (s. u. für Details zu dieser Darstellungsform) eine ausfallzeitbezogene Impact-Tolerance-Schwelle eingezeichnet ist? Eigentlich besagt eine solche *„Impact Tolerance"* als (Zitat) „*the maximum tolerable level of disruption … measured by a length of time*" nur eine Abschätzung, wann große Schadensereignisse zu längerfristigen Betriebsstörungen führen. Aber wir wissen ja gerade nicht wann und wie und was einmal eingetreten sein wird. Hier zeigt sich das Eingeständnis der Fed (2020) „*hazards may not be prevented*" als ein weiterentwickelter Ansatz.

Letztlich ist es dieses „Futur II", welches den Unterschied ausmacht: Während man im Operational Risk Management heute mögliche Risiken „in den Griff bekommen" möchte, geht eine Operational Resilience davon aus, dass – trotz allem heutigen Management – seltene, aber plausible Disruptionen einmal in Zukunft eingetreten sein werden.

Dieser Paradigmenwandel hin zu „unvermeidbaren“ Disruptionen aufgrund von Vernetzung und Abhängigkeiten findet sich als Grundmuster in diesem Buch wieder. Auf der einen Seite spiegelt sich der Übergang vom „Operational Risk“ zur „Operation Resilience“ in der Weiterentwicklung der methodischen Grundlagen von einer Berechnung von Wahrscheinlichkeiten sich wiederholender Ereignisse zur Betrachtung von seltenen, aber „disruptiven“ Ereignissen, zu welchen nur begrenzt Informationen verfügbar sind. Auf der anderen Seite eröffnet die Sicht auf solche Disruptionen die Möglichkeit zur Übernahme von Erfahrungen und Konzepten aus anderen Industrien, welche schon immer eine „High-risk Industry“ waren (wie u. a. Offshore-Ölbohrung, Kernkraft oder Flugverkehr) oder zumindest risikosensitive Unternehmungen darstellen (wie u. a. Elektrizitätsnetzwerke mit der Anforderung der Betriebsweiterführung auch im Falle des Ausfalls von einzelnen Komponenten). Schließlich führt das Konzept der „vorsorgenden“ Operational Resilience zur Frage der Intertemporalität, wenn die Verantwortlichen heute eine Investitionsentscheidung für die vorsorgenden Maßnahmen zu treffen haben, welche sich erst in Zukunft auszahlen mag – und dies immer als Entscheidung unter Unsicherheit.

1.2 Intertemporale Entscheidungen und die Kosten

Mit dem letzten Punkt spannt sich der Bogen der Operational Resilience von Unternehmen bis zu Entscheidungen in der Gesellschaft über die Einführung bzw. Nutzung von „risikoreichen“ Technologien mit zeitlich, strukturell oder sozial übergreifenden Auswirkungen (vgl. Linnenluecke 2017). Zum einen adressiert dies die *„willingness to accept costs to avert uncertain dangers“*, wie dies Charles Weiss (2006) zutreffend beschrieben hat. Zum anderen führt dies zum „Vorsorgeprinzip“, welches Anfang der 1970er-Jahre in Deutschland als umweltpolitisches Handlungsprinzip entwickelt wurde. Auch wenn dieses „Precautionary Principle“ in der Regel nur auf möglichen Risiken für Umwelt, Menschen oder Gesundheit bezogen wird, so ist sein Kern die Frage, wie „vorhersagbar“ künftige Risiken sein müssen, um Entscheidungen treffen zu können – oder um die dahinterliegenden Technologien kategorisch abzulehnen.

Die European Commission (2000) hat dazu in einer Verlautbarung vor über zwanzig Jahren folgendes Dilemma herausgestellt (Zitat):

> Decision-makers faced with an unacceptable risk, scientific uncertainty and public concerns have a duty to find answers.

Dies umschreibt das Spannungsfeld zwischen einer bewusst zu treffenden Selektion, was als ein unakzeptables bzw. umgekehrt als ein akzeptables „Risiko“ zu gelten habe, der Frage der wissenschaftlichen Unsicherheit, welche bis auf den Sonderfall von „wiederholten Spielen“ immer besteht, und einem öffentlichen Bedenken, welches auch ein schwankender Zeitgeist vor dem Hintergrund von anstehenden politischen Wahlen sein mag.

Da es nicht Gegenstand dieses Buches sein kann, näher auf das „Precautionary Principle“ einzugehen, muss auf die vielfältige Literatur dazu und zum Beispiel auf eine kritische Analyse von Sunstein (2002) verwiesen werden. Das „Precautionary Principle“ und „Operational Resilience“ stellen aber verbundene Sichtweisen dar: Wie soll unter Unsicherheit aufgrund einer begrenzten „Strength of Knowledge“ (siehe Abschn. 3.1) entschieden werden, wenn die Konsequenzen intertemporal sind. Entweder ist heute eine Innovation als unakzeptable abzulehnen und in der Abwägung ein entgehender ökonomischer Vorteil in der Zukunft zu verantworten. Oder es ist eine Investition als Vorkehrung gegen eine künftige, aber seltene Betriebsunterbrechung durchzuführen und entsprechend heute als zusätzliche Kosten darzustellen. Schon vor über fünfzig Jahren stellte Chauncey Starr (1969) die Frage (Zitat): *„What is our society willing to pay for safety?“*

Auch wenn die damit verbundene Diskussion sich auf die generelle Nutzung von Technologien (von der Kernenergie über genetisch verändertes Saatgut bis zur Rolle von Ölunternehmen vor dem Hintergrund der globalen Erwärmung) und deren mögliche Umweltschäden bezogen hat, so kann man dies durchaus auf den Fall von „eigenen“ Risiken von Unternehmen beziehen, wenn man statt öffentlicher Entscheidungen über Technologien in einer Gesellschaft dann individuelle Entscheidungen über Geschäftstätigkeiten in einem Unternehmen (oder eben nicht) betrachtet.

Dabei kann man drei Abstufungen unterscheiden, was die Klassifikation von möglichen Risiken der Geschäftsaktivitäten anbelangt:

1. Will man „kategorische Risiken“ unabhängig von jeder Bewertung bzw. Bewertbarkeit einer Wahrscheinlichkeit des Eintritts – also grundsätzlich und unabhängig vom Wissensstand um mögliche Schaden-Nutzen-Potenziale – ausschließen?
2. Will man „katastrophale Risiken“ nur nach dem höchstmöglichen Schaden beurteilen, ohne aber die Wahrscheinlichkeit des Eintritts, konkrete Folgen oder den möglichen Nutzen der betrachteten Technologie einzubeziehen – bzw. will man dafür eine maximale Vorsorge unabhängig von den Kosten oder anderen Nebenwirkungen treffen? Und will man dies mit oder ohne Vergleiche zu bestehenden Substitutionsmöglichkeiten einschließlich der ihnen wiederum innewohnenden Schaden-Nutzen-Potenziale tun?
3. Will man Risiken – unter Bewertung der limitierten „Strength of Knowledge“ – sowohl symmetrisch in einer Kosten-Nutzen-Rechnung betrachten als auch notwendige Vorsorgemaßnahmen und Alternativen in eine solche Bewertung einbeziehen?

Im Gegensatz zur Industrie stellen sich diese Fragen für Banken bezüglich ihrer kritischen Prozesse kaum, da die operativen Prozesse wie beispielsweise der Zahlungsverkehr keine Risiken für Menschen oder Umwelt bedingen (wenn man Geldwäsche etc. einmal als Sonderfall unberücksichtigt lässt).

Diese Fragen lassen sich aber umgekehrt interpretieren, zu wie viel Investitionen man in einer Bank heute bereit ist, um nach unvorhersehbaren Disruptionen dann „irgendwann“ die Betriebsfähigkeit wiederherstellen zu können. Auch hier ist ein „kategorischer Ansatz“, das heißt ein unbegrenzt großes Investment zur „absoluten“ Vorsorge, sowohl

wirtschaftlich unsinnig als auch konzeptionell fehlgeleitet, da gerade das begrenzte Wissen um die Zukunft keine „absolute Vorsorge“ zulässt. Es sind also Entscheidungen unter Unsicherheit zu treffen (vgl. Kap. 12).

Letztlich zeigt sich, dass bei disruptiven Ereignissen ein „Risiko“ nur unzureichend durch das in der Vergangenheit genutzte Konzept von statistischen Verteilungen im Sinne von „Risiko = Eintrittswahrscheinlichkeit * Schadenhöhe“ beschrieben werden kann. Schon McNeil, Frey und Embrechts (2005) haben die Vielfältigkeit der Definitionen angesprochen und *„any event or action that may adversely affect an organization's ability to achieve its objectives and execute its strategies*“ als Variante formuliert. Seit 2009 hat die International Standard Organisation (ISO) daher eine neue Definition ISO31000 von Risiko als (Zitat): „*effect of uncertainty on objectives*“ (Purdy 2010) eingeführt. Auch diese Definition ist nicht ohne Kritik geblieben (siehe u. a. Aven 2017), da sie versucht, einen vielschichtigen Begriff in wenigen Worten zu formulieren. Eine umfangreichere Beschreibung ist daher das Glossary der Society for Risk Analysis (2018), welches einen guten Einstieg in die Problematik einer Definition von „Risiko“ bietet.

1.3 „Vergessene“ Kunden

Da sowohl „Risiko“ als auch Operational Resilience nicht unabhängig vom Kontext betrachtet werden können, ist in Abb. 1.1 schematisch der soziotechnische Kontext dargestellt. Sowohl Risiko als auch Resilience können nicht als isolierte Wahrscheinlichkeits-

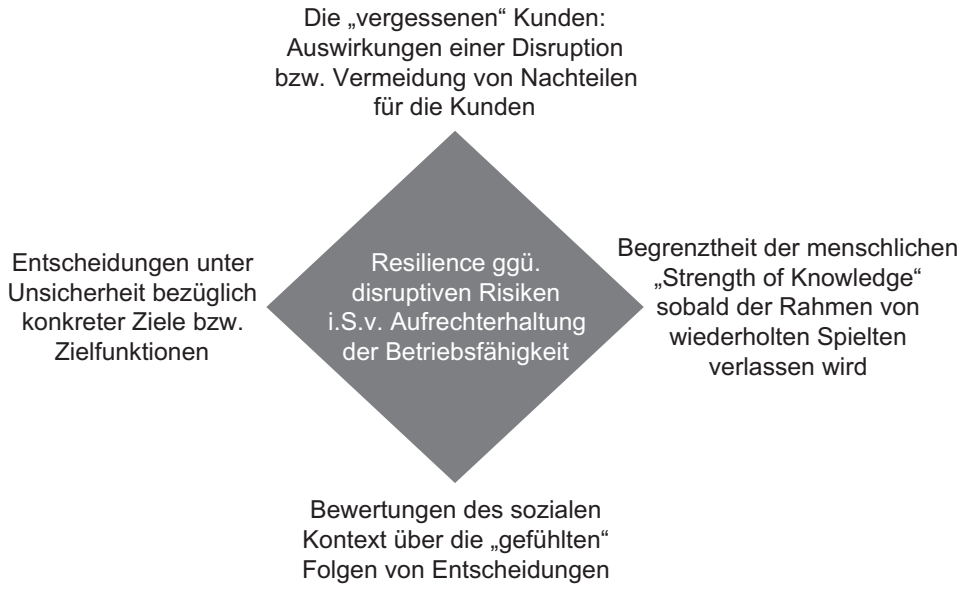

Abb. 1.1 Operational Resilience im Spannungsfeld von Entscheidung, Unsicherheit und sozialem Kontext sowie den dabei meist „vergessenen“ Kunden. (Quelle: eigene Darstellung)

rechnung formuliert werden, da immer der Kontext der (menschlichen) Entscheidung unter Unsicherheit, die Begrenztheit des (menschlichen) Wissens und die soziale Einbettung in die (menschliche) Gesellschaft den Rahmen bildet.

Leider wird in der Debatte um Operational Resilience meist ein entscheidender Punkt scheinbar vergessen: die Kunden bzw. das konsequent zu Ende gedachte Ziel, negative Folgen einer disruptiven Betriebsstörung für die Kunden soweit wie möglich zu vermeiden. In einem gemeinsamen Diskussionspapier der Bank of England (2018), der Prudential Regulation Authority (PRA) und der Financial Conduct Authority (FCA) vom Juli 2018 wird die Wirkung auf Kunden bzw. das Ziel, diese zu minimieren, noch ausdrücklich angesprochen (Zitat):

> Impact on consumers and market participants (4.14) The supervisory authorities are also concerned by the potential harm that operational disruptions could cause to users of a firm's or FMI's business service, including both consumers and market participants. (4.15) … seek to minimise the amount of harm caused by operational disruption.

Diese Perspektive ist in den Prinzipienpapieren des BCBS (2021) und der PRA (2021a) dann aber nicht mehr vorhanden. Bestenfalls sind die Kunden noch adäquat darüber zu informieren, was passiert ist. Ein Denken „vom Kunden her" ist aber verloren gegangen.

Daher bin ich meinem langjährigen Kollegen Leigh Meyer, Managing Director bei der Citi und Leiter der Operation in Belfast, zu Dank verpflichtet, dass er in einer Präsentation bei der Operation Managers Group der ECB (Meyer 2020) den Zusammenhang prägnant herausstellte (Zitat, Hervorhebungen im Original):

> Operational Resilience is all about the client, and local market stability and integrity … Operational resilience brings a paradigm shift in banking's focus on risk, culture and conduct – the risk is no longer *‚how much money will I lose'*, but *‚how much money may my client lose'*

Dabei ist zu unterscheiden, was übliche Operational-Risk-Ereignisse sind, welche auch finanzielle Schäden für Kunden wie zum Beispiel bei verspäteten Kapitalmaßnahmen bedeuten können, und was eben Betriebsunterbrechungen durch Disruptionen sind, welche dann in der Regel breit gestreute Wirkungen auf Kunden haben. Hierbei war das Diskussionspapier der Bank of England (2018) nicht trennscharf genug zwischen „normalen" Operational-Risk-Fällen und „disruptiven" Ausfällen. Dennoch ist es wichtig, die Wirkungen auf die Kunden keineswegs „zu vergessen", sondern diese letztlich immer als Prämisse allen weiteren Betrachtungen zur Operational Resilience voranzustellen – auch wenn dies im Folgenden nicht immer wiederholt werden soll.

Bevor im dritten Kapitel ein modernes Konzept von „Risiko" und „Resilience" dargestellt wird, soll im folgenden Kapitel eine Bewertung vorgenommen werden, wie relevant der Fall von solch seltenen, aber schwerwiegenden Disruptionen wirklich ist. Wie schon in Tab. 1.1 ausgeführt, können solche Fälle als ein „Tail Risk" beschrieben werden, das

heißt als Events in den Ausläufern von statistischen Verteilungsfunktionen. Und entsprechend finden sich „Heavy Tails“ dann in den Konstellationen, in welchen die „seltenen“ Fälle gar nicht so selten sind – zumindest nicht so selten, wie diese nach oft genutzten statistischen Verteilungsfunktionen auftreten sollten.

Unterscheidung zwischen Operational Resilience und „Antifragilität“

Der Bestsellerautor Nassim Nicholas Taleb führte die Begriffe einer „Fragilität“ und einer „Antifragilität“ ein (siehe speziell: Taleb und Douady 2013), wobei die Herleitung sehr langatmig und wenig zielgerichtet ist.

Die Grundidee ist aus der Finanzmathematik von Derivaten entnommen und entspricht dem Vega-Faktor, welcher die Kursveränderung eines Optionsscheins in Abhängigkeit von der Volatilität des Basiswerts beschreibt: Ein hohes Vega bedeutet eine starke Sensitivität des Optionswerts gegen Volatilitätsänderungen des Basiswerts, und entsprechend steigt bei einer Volatilitätszunahme der Optionswert. Diese Idee der „Wertzunahme bei steigender Volatilität“ einer externen Basisgröße wird dann zu „*Antifragile: Things that gain from disorder*“ (Taleb 2012) verallgemeinert. Im Gegensatz dazu aber verwenden selbst Taleb und Douady (2013) wieder das Beispiel einer Kaffeetasse auf dem Tisch für eine „Fragilität“, welche nicht von kleinen Rüttlern ge-/zerstört wird, aber von einem starken (Erd-)Beben – was zur Frage der Reaktion auf extreme äußere Ereignisse (sogenannte Tail Events) führt, aber nicht auf Volatilitäten.

Außerhalb des Bereichs der Finanzmathematik gibt es keine (natürlichen) Systeme, welche eine Abhängigkeit von der Volatilität eines externen Einfluss zeigen. Natürlich bestimmen externe Parameter immer das Systemverhalten: ob bei der globalen Erwärmung (Temperatur), dem Knochenwachstum (mechanische Stimulation), der Lebensdauer von Bauteilen (Zahl und Stärke der Schwingungsbelastungen) bzw. Stärke von Stahl (durch Schmieden erzeugte Störungen im Material zur Stabilisierung) oder ganz allgemein der Evolution (bis hin zu Einschlägen von Meteoriten).

Es gibt aber weder eine „Antifragilität“ im genannten Sinne von *„Things that gain from disorder*“ noch in dem Sinne, dass Systeme auf extreme äußere Ereignisse irgendwie „mit Gewinn“ reagieren würden.

Literatur

Basel Committee on Banking Supervision (BCBS, 2021) “Principles for Operational Resilience”, Bank of International Settlement, 31.3.2021 (verfügbar unter: https://www.bis.org/bcbs/publ/d516.htm, abgerufen am 6.4.2021).

Bank of England – Prudential Regulation Authority (PRA, 2021a) “Statement of Policy – Operational resilience”, Supervisory Statement 1/21, 29.3.2021 (verfügbar unter: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-21.pdf, abgerufen am 6.3.2021).

Bank of England – Prudential Regulation Authority (PRA, 2021b) “Operational resilience: Impact tolerances for important business services”, 29.3.2021 (verfügbar unter: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/statement-of-policy/2021/operational-resilience-march-2021.pdf, abgerufen am 6.3.2021).

Fed (2020) “Sound Practices to Strengthen Operational Resilience”, Interagency Paper of Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, 30.10.2020 (verfügbar unter: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf, abgerufen am 12.7.2021).

Basel Committee on Banking Supervision (BCBS, 2001) "Sound Practices for the Management and Supervision of Operational Risk", 20.12.2021 (verfügbar unter: https://www.bis.org/publ/bcbs86.pdf, abgerufen am 5.6.2021).

NATO (2021) "Resilience and Article 3", NATO Topics, Resilience and Article 3, 11.6.2021 (verfügbar unter https://www.nato.int/cps/en/natohq/topics_132722.htm, abgerufen am 20.9.2021).

BaFin (2021) „Mittelfristziele der BaFin", Die BaFin, 15.11.2021 (verfügbar unter https://www.bafin.de/DE/DieBaFin/ZieleStrategie/Ziele/ziele_node.html und https://www.bafin.de/SharedDocs/Downloads/DE/Aufsichtsrecht/dl_Mittefristziele_2021.pdf, abgerufen am 16.11.2021).

Ikeda, Yuuki, Will Kerry, Ulf Lewrick und Christian Schmieder (2021) "Covid-19 and bank resilience: where do we stand?", BIS Bulletin, No 44 , 22.7.2021 (verfügbar unter: https://www.bis.org/publ/bisbull44.pdf, abgerufen am 26.7.2021).

Barriball, Edward, Katy George, Ignacio Marcos, und Philipp Radtke (2021) "Jump-starting resilient and reimagined operations", in: McKinsey & Company "The Next Normal – Reimagining operational resilience", Feb. 2021 (verfügbar unter: https://www.mckinsey.com/business-functions/operations/our-insights/the-need-for-resiliency, abgerufen am 6.6.2021).

Bower, Joseph L. und Clayton M. Christensen (1995) "Disruptive Technologies: Catching the Wave", Harvard Business Review, Vol. 73/1, January–February 1995, pp. 43–53.

European Commission (2020) 'Digital Operational Resilience Act (DORA)' (verfügbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN, abgerufen 24.9.2020).

Basel Committee on Banking Supervision (BCBS, 2017) "Basel III: Finalising post-crisis reforms", Bank of International Settlement, 7.12.2017 (verfügbar unter: https://www.bis.org/bcbs/publ/d424.pdf, abgerufen am 18.4.2021).

Walker, Brian und David Salt (2012) "Resilience Practice", Island Press, Washington, USA.

Vakilzadeh, Kijan und Alexander Haase (2021) "The building blocks of organizational resilience: a review of the empirical literature", 20.4.2021, Continuity & Resilience Review, Vol. 3/1, pp. 1–21.

Holling, Crawford Stanley (1996) "Engineering resilience versus ecological resilience", in: National Academy of Engineering "Engineering within ecological constraints", edited by Peter C. Schulze, pp. 31–44, National Academy Press, Washington D.C., USA.

Linnenluecke, Martina K. (2017) "Resilience in Business and Management Research: A Review of Influential Publications and a Research Agenda", International Journal of Management Reviews, Vol. 19/4, pp. 4–30.

Weiss, Charles (2006) "Precaution: the willingness to accept costs to avert uncertain dangers" in: Marti, Kurt, Yuri Ermoliev Marek Makowski und Georg Pflug (Hrsg.) "Coping with uncertainty: modelling and policy issues", Lecture Notes in Economics and Mathematical Systems book series, Vol. 581, pp. 315–330, Springer Nature Switzerland.

European Commission (2000) "Communication on Precautionary Principle", 2.2.2000 (verfügbar unter: https://ec.europa.eu/commission/presscorner/detail/en/IP_00_96, abgerufen am 21.5.2021).

Sunstein, Cass R. (2002) "Beyond the Precautionary Principle", University of Chicago Law School, John M. Olin Program in Law and Economics, Working Paper No. 149, 2002 (verfügbar unter: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1086&context=law_and_economics, abgerufen am 27.5.2021).

Starr, Chauncey (1969) "Social Benefit versus Technological Risk", Science, Vol. 165, 19.9.1969, pp. 1232–1238.

McNeil, Alexander John, Rüdiger Frey und Paul Embrechts (2005) "Quantitative Risk Management: Concepts, Techniques, and Tools", Princeton University Press, Princeton, New Jersey, USA (Revised Edition, 2015).

Purdy, Grant (2010) “ISO 31000:2009 – Setting a New Standard for Risk Management”, Risk Analysis, Vol. 30, pp. 881–886.

Aven, Terje (2017) “The flaws of the ISO 31000 conceptualisation of risk”, Journal Risk and Reliability, Vol. 231/5, pp. 467–468.

Society for Risk Analysis (2018) “Risk Analysis Glossary”, Aug. 2018 (verfügbar unter: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf, abgerufen am 8.6.2021).

Bank of England (2018) “Building the UK financial sector’s operational resilience”, Discussion Paper, Bank of England, Prudential Regulation Authority (PRA) und Financial Conduct Authority (FCA), Juli 2018 (verfügbar unter: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf, abgerufen am 20.8.2021).

Meyer, Leigh (2020) “Business Unusual – Driving the Conversation on Operational Resilience”, Folienpräsentation, ECB OMG Meeting, 10.6.2020 (verfügbar unter: https://www.ecb.europa.eu/paym/groups/pdf/omg/2020/202006/2020-06-10_item_2_Operations_resilience-Citi.pdf, abgerufen am 20.8.2021).

PRA (2021a) „Operational resilience“, Prudential Regulation Authority, Bank of England, Statement of Policy, March 2021, available at: https://www.bankofengland.co.uk/-/media/boe/files/prudentialregulation/statement-of-policy/2021/operational-resilience-march-2021.pdf, accessed 8.7.2022.

PRA (2021b) „PS6/21 | CP29/19 | DP1/18 Operational Resilience: Impact tolerances for important business services“, Policy Statement 6/21, Update 3.6.2021, available at: https://www.bankofengland.co.uk/prudentialregulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper, assessed 8.7.2022.

Taleb, Nassim Nicholas und Raphael Douady (2013) „Mathematical Definition, Mapping, and Detection of (Anti)Fragility“, Quantitative Finance, Vol. 13/11, 4.12.2013, pp. 1677–1689 (verfügbar unter: https://hal.archives-ouvertes.fr/hal-01151340/document, abgerufen am 7.6.2021).

Taleb, Nassim Nicholas (2012) “Antifragile: Things that Gain from Disorder”, Random House, New York, USA.

Perspektiven von Resilience – drei Beispiele

2

Zusammenfassung

Da es die Beschreibung von Operational Resilience als Wiederherstellung der Betriebsfähigkeit im Falle einer Disruption offen lässt, was eine Disruption sein soll, bietet sich erster Zugang durch drei Beispiele an, welche verschiedene Perspektiven abdecken. Zum einen kann aus Statistiken der finanziellen Verluste von Operational-Risk-Events geschlossen werden, dass auch bei „seltenen" Ereignissen mit großen Schäden die aggregierten Schäden pro Magnitude keinesfalls abnehmen. Zum anderen bedingen konkrete Betriebsunterbrechungen nicht immer finanzielle Schäden, können aber gerade auch nach langjährigem „erfolgreichem" Betrieb eintreten. Und schließlich führt die Digitalisierung zu neuen Rahmenbedingungen, welche in Zukunft zu Disruptionen führen können, da auch diese „digital" sind: Systeme laufen so lange, bis einmal eine Unterbrechung eintritt.

Die Vorstellung von einer Disruption als seltenes, aber plausibles Ereignis mit dem Potenzial einer Betriebsunterbrechung für ein Finanzinstitut ist keine sattelfeste Definition ohne jeden Diskussionsbedarf. So mag der Einschlag eines Meteoriten – zumindest als Hypothese – das „Ende" der großen Dinosaurier gewesen sein, aber Krokodile haben überlebt – und Vögel und Säugetiere verdanken dieser Disruption sogar ihre Erfolgsgeschichte.

Es wurde schon im letzten Kapital angesprochen, dass eine „Disruption" ähnlich wie auch ein „Risiko" in ein Spannungsfeld von Entscheidungshandeln, Unsicherheit über die Erreichung von Zielen und einem äußeren, gesellschaftlichen Rahmen eingebettet ist. Was für ein Institut eine existenzielle Betriebsunterbrechung sein mag (so zum Beispiel ein längerfristiger Ausfall der Orderverarbeitung in einer spezialisierten Wertpapierhandels-

U. Milkau, *Operational Resilience in Finanzinstituten*,
https://doi.org/10.1007/978-3-658-36897-5_2

bank), kann in einem anderen Institut nur einen untergeordneten Prozess betreffen (also ein identischer Ausfall, aber beispielsweise in einer Hypothekenbank). Und heute kann eine Unterbrechung der Erreichbarkeit einer Bank über deren Social-Media-Kanäle aus Sicht der Kunden mehr disruptiven Charakter haben als ein Ausfall der Bargeldversorgung an den Geldausgabeautomaten dieser Bank.

Die Frage der „Betriebsunterbrechung" ist gerade im digitalen Zeitalter kontextabhängig, soll aber bis auf Weiteres so verstanden werden, dass es sich um ein Ereignis mit großer Wirkung und großen Folgen für ein Finanzinstitut handelt, wobei dies faktisch auch immer einen großen finanziellen Verlust nach sich zieht – selbst wenn „nur" viele Kunden massiv verärgert sind und damit die Wechselbereitschaft signifikant ansteigt. Damit bleibt der Bereich von systemischen Risiken im Finanzsystem unberücksichtigt, wobei aber die Auswirkungen eines systemischen Risikovorkommnisses durchaus eine auslösende Disruption für ein Institut sein kann. Auch wenn dies eine axiomatische Festlegung darstellt, so soll im Folgenden immer ein individuelles Unternehmen oder individueller Konzern betrachtet werden.

2.1 Abgrenzungsprobleme zwischen Risiko und Disruption

Wie selten sind „seltene, aber plausible" Szenarien überhaupt? Dabei kann man getrost das Dinosauriersterben außen vor lassen, aber auf die Kernfrage von Entscheidungen zur Vorsorge gegen Betriebsunterbrechungen zurückkommen und diese als Maßstab nehmen. Schwierigkeiten in der Analyse bestehen darin, dass zwischen Betriebsstörungen und Betriebsunterbrechungen kaum unterschieden wird und beide wiederum ungekennzeichnet in die allgemeinen Operational-Risk-Statistiken wie „Gesamtverluste je Business-Line und Event-Typ" eingehen. Grundsätzlich verschiedene Kategorien von Ereignissen mit unterschiedlichem Potenzial für Disruptionen werden normalerweise nicht getrennt und nur bezüglich der Höhe eines eingetretenen Schadens registriert.

Beispiele für die verschiedenen Kategorien sind in der nachfolgenden Liste einmal zusammengestellt, wobei auch auf den Aspekt von regulierten Instituten (mit Statistik) versus nichtregulierten Unternehmungen (ohne Statistik) eingegangen wird. Dies erscheint gerade vor dem Hintergrund der Digitalisierung angebracht, da die unregulierten Aktivitäten durchaus stellvertretend für ähnliche Betriebsprozesse in regulierten Instituten stehen können:

- Betriebsstörungen, zum Beispiel von einzelnen technischen Systemen und entsprechenden bankfachlichen Prozessen wie zum Beispiel Verfügbarkeit des Onlinebanking oder Abwicklung von SEPA-Zahlungen, welche nach Behebung der technischen Störung aber in der Regel nachträglich abgearbeitet werden können und „nur" zu Verzögerungen und ggf. Kundenbeschwerden führen.
- Betriebsunterbrechungen, zum Beispiel in Folge eines erpresserischen Hackerangriffs mit Verschlüsselung der Daten (Ransomware-Attacke) wie im Mai 2021 bei der US-