TRENDS UND ENTWICKLUNGEN

Operationelle Risiken in Zeiten von Corona-Maßnahmen

Bis vor kurzem waren operationelle Risiken vor allem auf Schwachstellen zurückzuführen, die aus der raschen Entwicklung und der zunehmenden Abhängigkeit von technologischer Infrastruktur zur Bereitstellung der Bankdienstleistungen resultieren. Infolge der Corona-Pandemie hat sich das typische operationelle Risikoprofil einer Bank verschoben und verschärft. Gleichzeitig sind die wirtschaftlichen und geschäftlichen Unsicherheiten gewachsen. Welche Trends sind erkennbar, und wie können Banken darauf reagieren?

Die Corona-Maßnahmen der Regierungen wirken sich belastend auf Mitarbeiter, Informationssysteme, betriebliche Einrichtungen sowie die Beziehungen zu Drittanbietern und Kunden aus. Aus interner Sicht haben operationelle Risiken durch ausgefallene Prozesse und Systeme aufgrund der stärkeren Abhängigkeit von virtuellen Medien und Fernarbeit zugenommen. Hinzu kommen erhöhte externe Bedrohungen wie Cyber-Risiken.

Eine effektive Reaktion auf diese Risiken hat in der Wahrnehmung vieler Bankmanager zwar eine hohe Priorität. Die Konzeption und Umsetzung von konkreten und wirksamen Maßnahmen stehen den meisten Instituten jedoch noch bevor.

Das Baseler Komitee hat auf diese Entwicklungen bereits im August mit einer Aktualisierung seiner Leitlinien für das Management operationeller Risiken reagiert. Zusätzlich wurden Prinzipien für die Operational Resilience als zusätzlicher separater Standard formuliert, womit die regulatorischen Rahmenbedingungen eine wesentliche zusätzliche Dimension erhalten. Beide Dokumente standen bis zum 6. November zur Konsultation.

Während die IT- und Cyber-Risiken bereits im Jahr 2020 Aufsichtsprioritäten der EZB darstellen – in Deutschland gerade auch vor dem Hintergrund der bankaufsichtlichen Anforderungen an die IT (BAIT) – ist ein verstärkter Fokus auf die Operational Resilience im Jahr 2021 absehbar.

Im Zuge der Novellierung der Kapitaladäquanzverordnung (CRR) ist voraussichtlich ab Anfang des Jahres 2023 ein neuer Standardansatz zur Bestimmung der aufsichtsrechtlichen Eigenmittelanforderungen für operationelle Risiken anzuwenden. Im Folgenden betrachten wir die Situation mit Fokus auf die Regionalbanken.

Ausgangssituation bei deutschen Regionalbanken

Innerhalb der operationellen Risiken haben Rechtsrisiken als übergreifende Querschnittsrisiken für Regionalbanken erfahrungsgemäß die höchste Relevanz, gefolgt von Systemrisiken (mangelhafte oder fehlende Infrastruktur, inkl. IT und Cyber), Prozess- und Verfahrensrisiken (mangelhafte Ablauforganisation) und externen Risiken (Naturgewalt, Krieg, Politik). Die niedrigste Relevanz haben Personenrisiken (menschliches Fehlverhalten, sei es fahrlässig oder kriminell). Die Corona-Krise hat besonders System-, Prozess- und Verfahrensrisiken sowie externe Risiken verschärft.

Die realisierten operationellen Schadensfälle bei deutschen Regionalbanken belaufen sich auf schätzungsweise 450 Mio. € pro Jahr (basierend auf einer empirischen Analyse von Prof. Andreas Höfer, Hochschule der Deutschen Bundesbank), also etwa zwei Basispunkte der kumulierten Bilanzsummen. Angesichts eines durchschnittlichen Betriebsergebnisses vor Bewertung von rund 75 Basispunkten im Jahr 2019 haben operationelle Schäden somit nur eine geringe Auswirkung auf die Ertragssituation (laut den Bilanzzahlen der Sparkassen-Finanzgruppe bzw. der Ertragsentwicklung der Genossenschaften).

Die relative Bedeutung solcher Risiken nimmt allerdings tendenziell deutlich zu, und zwar sowohl durch externe Entwicklungen wie Corona als auch durch die anhaltende Ertragserosion im Nullzinsumfeld.

Regulatorische Eigenmittelanforderungen werden von Sparkassen und Genossenschaftsbanken bislang mit dem Basisindikatoransatz (in seltenen Fällen mit dem derzeitigen Standardansatz) bestimmt. Diese Anforderungen betragen im Durchschnitt etwa 30 Basispunkte der Bilanzsumme, also ein Vielfaches der realisierten Schäden. Mit dieser sehr konservativen Kalibrierung ihrer Ansätze trägt die Aufsicht der Tatsache Rechnung, dass operationelle Schäden sich empirisch sehr ungleich auf die Institute verteilen; es handelt sich um ausgesprochene Tail-Risiken.

Diese Ungleichverteilung und die wachsende relative Relevanz machen es für Regionalbanken zunehmend interessant, zumindest

punktuell auf Versicherungslösungen zurückzugreifen, um Planungssicherheit und Stabilität im Krisenfall zu verbessern. Bei einzelnen Risiken sind Versicherungen bereits als weitgehend branchenüblich anzusehen – etwa bei Sprengungen von Geldautomaten. Für operationelle Risiken im Allgemeinen gilt dies allerdings noch lange nicht.

Aktualisierung der Prinzipien für das Management operationeller Risiken

Der regulatorische Rahmen für operationelle Risiken wurde vom Baseler Komitee ursprünglich im Jahr 2003 formuliert. 2011 erfolgte eine Aktualisierung, um Entwicklungen und Erkenntnisse aus der Finanzmarktkrise zu berücksichtigen, und 2014 folgte eine großflächige Untersuchung zum Umsetzungsstand der Anforderungen in den Banken und zur Vollständigkeit und Angemessenheit der Prinzipien.

Die Untersuchung zeigte nach Einschätzung des Komitees teilweise erhebliche Schwächen bei der Umsetzung seitens der Banken, insbesondere bei der Einrichtung von drei Verteidigungslinien, den Mechanismen zur Risikoerkennung und -bewertung und der Management-Verantwortung für das Risikomanagement. Zudem zeigte die Untersuchung punktuelle Lücken in den Anforderungen selbst auf, besonders hinsichtlich IT- und Cyber-Risiken.

Mit der aktuellen neuerlichen Überarbeitung und Ergänzung der Vorgaben reagiert das Baseler Komitee nun auf die Auswirkungen der Corona-Krise. Die Überarbeitung schärft einzelne Vorgaben und betont zusätzlich den übergreifenden Kontext der Stabilität des Finanzsystems. Abgesehen von redaktionellen Schärfungen und zusätzlichen Erläuterungen sind folgende Änderungen wesentlich:

- Das erste Prinzip für das operationelle Risikomanagement (Operational Risk Cul-

ture) in der Version aus dem Jahr 2014 verpflichtete die Unternehmensführung, eine starke Risikomanagement-Kultur zu etablieren und Anreize für professionelles und verantwortungsbewusstes Verhalten zu setzen. In der neuen Version von August 2020 wird es dahingehend geschärft, dass Mitarbeiter angemessene Schulungen hinsichtlich Risikomanagement und Ethik erhalten müssen.

- Das zweite Prinzip sieht nun vor, dass das Operational Risk Management Framework (ORMF) vollständig in den übergreifenden Risikomanagementprozess der Bank zu integrieren ist.
- Das siebte Prinzip schreibt zusätzlich vor, dass das Change Management einer Bank inhaltlich umfassend aufgestellt, angemessen ausgestattet und zwischen den relevanten Verteidigungslinien abgestimmt sein muss.
- Das achte Prinzip stellt in der neuen Version klar, dass „Monitoring und Reporting" das proaktive Management operationeller Risiken unterstützen sollen.
- Ein neues und zusätzliches zehntes Prinzip betrifft spezifisch ICT (Information and Communication Technology)-Risiken. Demnach ist eine ICT-Governance zu implementieren, die die Geschäftstätigkeit der Bank im Einklang mit ihrer Risikostrategie vollständig unterstützt. Es sind Maßnahmen zur Risikoidentifizierung, zum Schutz, zur Reaktionsfähigkeit und zur Wiederherstellung vorgeschrieben, die regelmäßig getestet werden sollen.
- Das elfte (vormals zehnte) Prinzip betrifft den Bereich Business Continuity Planning. In der ursprünglichen Version wurde hierunter auch die Operational Resilience subsummiert, die nun in einem eigenen Standard detailliert wird (siehe unten).
- Das zwölfte (vormals elfte) Prinzip „Role of Disclosure" sieht vor, dass die Offenlegung der Bank Investoren nicht nur einen Einblick in den Ansatz für das Management operationeller Risiken geben soll, sondern zusätzlich auch in das tatsächlich bestehende Risiko.

Insgesamt handelt es sich um inkrementelle und situative Schärfungen und Konkretisierungen bestehender Anforderungen. Das ICT-Prinzip ist gänzlich neu. Ebenso verhält es sich mit den Anforderungen an Operational Resilience, die bei den Banken absehbar konkreten Handlungsdruck verursachen werden.

Bedeutung und Neuigkeit der Operational Resilience

Unter Operational Resilience ist die Fähigkeit zu verstehen, entscheidende unternehmensbezogene Dienstleistungen und Geschäftstätigkeiten auch unter widrigen Umständen ohne Unterbrechung aufrechterhalten zu können. Ein Institut soll sich selbst vor Bedrohungen und potenziellen Ausfällen schützen, auf Störungen und Ereignisse proaktiv reagieren und im Notfall eine schnelle Wiederherstellung seiner operativen Handlungsfähigkeit gewährleisten können.

Operational Resilience ist somit vor allem ein Ergebnis des effektiven Managements von operationellen Risiken und setzt voraus, dass Verantwortlichkeiten auf Führungsebene verbindlich geregelt sind und eine klare End-to-End-Sicht auf priorisierte unternehmensbezogene Dienstleistungen das Handeln leitet.

Eine solche ganzheitliche Sicht zu etablieren ist herausfordernd, weil die Geschäftstätigkeit im Rahmen granularer, arbeitsteiliger Geschäftsprozesse organisiert ist. Es besteht ein komplexer und vielschichtiger Zusammenhang zwischen Dienstleistungen und Geschäftstätigkeiten einerseits und Geschäftsprozessen, Systemen, Medien und Auslagerungen zu ihrer Erbringung andererseits. Inhaltlich besteht die Herausforderung deshalb darin, Zusammenhänge, Abhängigkeiten und Wechselwirkungen der relevanten Geschäftsprozesse, Systeme und Tätigkeiten systematisch zu erkennen und hinreichend zu entflechten.

Operationalisierung der Operational-Resilience-Anforderungen

Um ein effektives Business Continuity Management (BCM) zu operationalisieren, sollen messbare Kenngrößen (KPI) und Schwellen-

werte festgelegt werden, deren Überschreitung vorbestimmte Maßnahmen auslöst. Die Abhängigkeit von externen oder gruppeninternen Dienstleistern für wesentliche Auslagerungen ist dabei gleichfalls zu berücksichtigen.

Dienstleister müssen ihrerseits die Erwartungen ihres Auftraggebers an die Operational Resilience erfüllen. Ein Institut muss sich hiervon überzeugen und Pläne haben, wie es nahtlos auf alternative Dienstleister ausweichen oder entsprechende Leistungen notfalls selbst erbringen kann. Diese Anforderung verschiebt die Kosten-Nutzen-Abwägung deutlich zulasten der Auslagerungsoption und verschärft den Konsolidierungsdruck auf Regionalbanken.

Im Hinblick auf die Stabilität des Finanzsystems bedeutet Operational Resilience, dass ein einzelnes Institut Schocks absorbieren kann und sich an sie anzupassen vermag, anstatt dazu beizutragen. Die Top-Down-Sichten sowohl der Aufsicht als Hüter der Systemstabilität als auch des Bankmanagements rücken somit noch stärker in den Fokus als bei den bisherigen Anforderungen.

Aufbauend auf den etablierten Funktionen für das Management von operationellen Risiken ist der Vorstand der Bank dafür verantwortlich, die Anforderungen an die Operational Resilience zu überprüfen und unter Berücksichtigung von allgemeinem Risikoappetit und individuellem Risikoprofil des Instituts festzulegen. Der zweiten Führungsebene obliegt die Umsetzungsverantwortung, und sie muss dem Vorstand hierzu besonders im Krisenfall berichten.

Während die meisten Anforderungen allgemein formuliert sind, geht das Baseler Komitee in diesem Kontext spezifisch auf IT- und Cyber-Risiken ein. Diesbezügliche Notfallpläne müssen Schutz, Erkennung, Reaktion und Wiederherstellung abdecken, also alle Aspekte des Störungsmanagements. Beim Zugriff auf IT-Ressourcen entsteht ein Zielkonflikt zwischen weitgehenden Zugriffsmöglichkeiten von außerhalb der Betriebsgebäude, um Arbeitsfähigkeit beispielsweise während des Corona-Lockdowns zu gewährleisten, und den daraus resultierenden Angriffsmöglichkeiten für Cyber-Kriminelle. War die Möglichkeit zur Fernarbeit früher eher ein Zugeständnis an Mitarbeiter, spielt sie nun zunehmend eine wichtige Rolle im Business Continuity Management.

Eigenmittelanforderungen für operationelle Risiken

Die Berechnungsgrundlage für die derzeit noch aktuellen Basisindikator- und Standardansätze ist der Dreijahresdurchschnitt des sogenannten maßgeblichen Indikators. Dieser bestimmt sich aus Posten der Gewinn- und Verlustrechnung und kann inhaltlich als Maß für den Rohertrag im Kerngeschäft aufgefasst werden. Die Eigenmittelanforderung ergibt sich durch die pauschale Gewichtung des maßgeblichen Indikators mit 15 Prozent.

Ein solcher Ansatz ist erkennbar nicht risikosensitiv. Realisierte Schäden, die den Rohertrag schmälern, führen paradoxerweise zu nominell niedrigeren Eigenmittelanforderungen in den Folgejahren, wenngleich die Aufsicht in solchen Fällen typischerweise im Rahmen des SREP manuell gegensteuert.

Vom BCBS ist ein neuer Standardansatz (Calculation of RWA for Operational Risk – Standardised approach) geplant, der sowohl den Basisindikatoransatz als auch den bisherigen Standardansatz ablösen soll. Dessen Einführung wurde aufgrund der Corona-Krise um ein Jahr auf Anfang 2023 verschoben.

Der neue Ansatz basiert auf einem neuen Geschäftsindikator (Business Indicator, BI), der aus Finanz-, Service- und Zins-Komponenten besteht. Anhand der Höhe des BI werden Banken in Kategorien eingeordnet, deren BI multipliziert mit gestaffelten Prozentsätzen die Geschäftsindikator-Komponente (Business Indicator Component, BIC) ergibt.

Diese BIC ist als Bemessungsgrundlage für das Eigenmittelerfordernis zunächst ebenso starr wie der maßgebliche Indikator im derzeitigen Basisindikatoransatz. In einem nächsten Schritt kann die BIC allerdings mit einem Verlust-Skalierungsfaktor (Internal Loss Multiplier, ILM) multipliziert werden, der sich aus dem Verhältnis der tatsächlichen historischen Verluste eines Instituts zu seiner BIC bestimmt. Dieses Vorgehen soll eine systematische Risikosensitivität ermöglichen. Die Berechnung des ILM erfordert eine mindestens zehnjährige Schadenfallhistorie, an deren Datenqualität hohe Anforderungen gestellt werden.

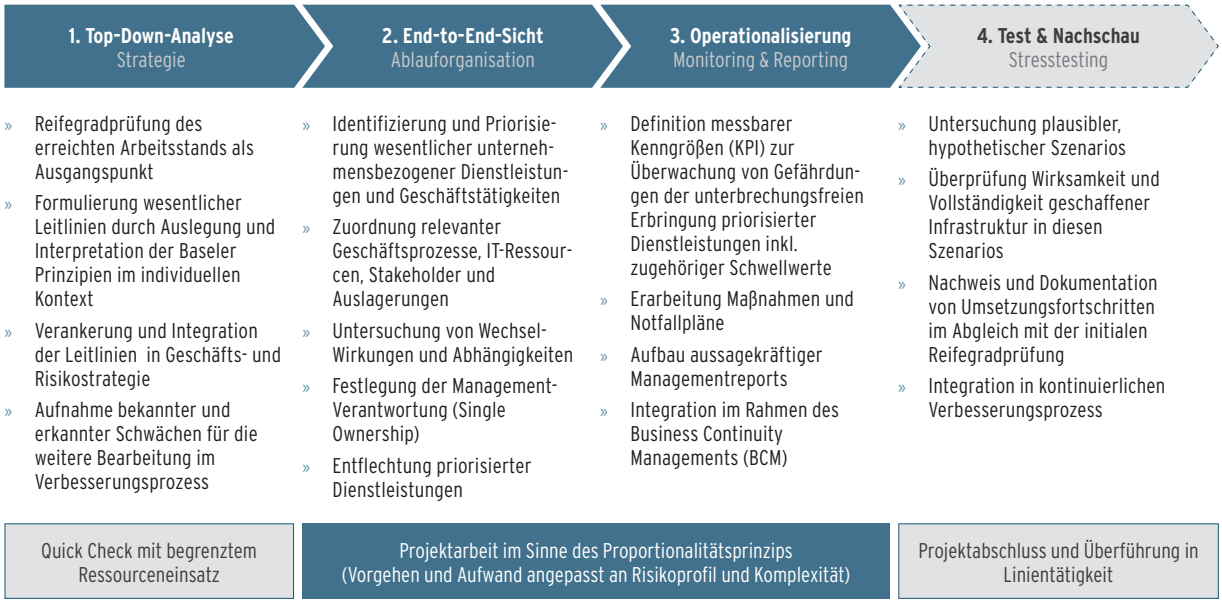
Für alle Banken, die einen BI von weniger als 1 Mrd. € haben, ist die Berechnung eines ILM optional. Dies trifft auf so gut wie alle deutschen Regionalbanken zu. Regionalbanken dürfen den ILM zwar freiwillig berechnen, doch voraussichtlich werden die Institute von dieser Möglichkeit kaum Gebrauch machen. Grund ist, dass der operative Aufwand hierfür deutlich schwerer wiegt als die möglicherweise erzielbaren Vorteile hinsichtlich Eigenmittelentlastung und Risikosensitivität.

Handlungsdruck und Vorgehensmodell

Der Trend zu immer engerer und anspruchsvollerer Regulierung setzt sich auch in den beschriebenen Standards zum operationellen Risiko und zur Operational Resilience fort. Das Management von operationellen Risiken ist gerade bei Regionalbanken vielfach noch eher rudimentär ausgeprägt und erfolgt reaktiv unterhalb der ersten Führungsebene; Ausnahmen hiervon gibt es vor allem bei Instituten, die bereits wesentliche Schadensereignisse aufarbeiten mussten.

Ob zusätzlicher Regulierungsdruck tatsächlich nennenswerte Verbesserungen in der Breite erbringen kann, bleibt abzuwarten. Eine Überforderung der Banken mit unwirtschaftlichen und teils unpraktikablen Anforderungen ist längst erkennbar. Dieser Aspekt spielt in den Überlegungen des Komitees nach wie vor keine erkennbare Rolle.

1 | Vorgehensmodell zur Umsetzung der neuen Baseler Standards



Quelle: BLC.

Ein konstruktiver Ansatz zum Umgang mit den neuen Standards fokussiert auf die Schnittmenge zwischen sinnvollen Maßnahmen aus eigenen Erwägungen und den neuen Anforderungen. Ein solches Vorgehen kann wie in der Abbildung ▸ **1** ersichtlich gegliedert werden:

- Top-Down-Analyse des erreichten Reifegrads: Ausgehend von einer Analyse des Status quo soll das Zielbild zur Operational Resilience und zum Management operationeller Risiken in der Geschäfts- und Risikostrategie verankert und integriert werden. Hierzu sind wesentliche Leitlinien zu formulieren, die die Prinzipien der Baseler Standards interpretieren und in den individuellen Kontext übersetzen. Gleichzeitig sollen bekannte und erkannte Schwächen sowie mögliche Quick Wins für die weitere Bearbeitung priorisiert werden.
- Schaffung einer ganzheitlichen Sicht: Unternehmensbezogene Dienstleistungen und Geschäftstätigkeiten, die im Rahmen einer End-to-End-Sicht hinsichtlich ihrer Operational Resilience zu betrachten sind, sollen identifiziert und priorisiert werden. Die Priorisierung soll mit Leitlinien aus der Top-Down-Analyse begründet und unterlegt werden. Relevante Geschäftsprozesse, IT-Ressourcen, Stakeholder und Auslagerungen sollen den priorisierten Dienstleistungen zugeordnet werden. Es ist eine eindeutige Managementverantwortung (Single Ownership) vorzusehen. Mögliche Wechselwirkungen und Abhängigkeiten mit anderen Geschäftstätigkeiten sind zu berücksichtigen und möglichst zu verringern.
- Operationalisierung: Es sollen messbare Kenngrößen (KPI) für die priorisierten Dienstleistungen erarbeitet werden, die Gefahren für die zuverlässige Erbringung priorisierter Dienstleistungen anzeigen können. Zu den KPI gehören Schwellenwerte, deren Überschreitung zugehörige Maßnahmen im Rahmen des Business Continuity Managements auslöst. Auf Grundlage dieser Definitionen sollen regelmäßige aussagekräftige Managementreports erfolgen.

Die beschriebene Operationalisierung eignet sich auch dazu, Verbesserungen gegenüber der im Rahmen der Top-Down-Analyse erhobenen Reifegradprüfung festzustellen und somit Umsetzungserfolge zu dokumentieren. In plausiblen hypothetischen Szenarios kann die Aussagekraft der Managementreports überprüft und die Eignung der Maßnahmen und Notfallpläne untersucht werden.

FAZIT

Der regulatorische Rahmen für operationelle Risiken wurde aktualisiert und erhält im Hinblick auf Operational Resilience und ICT-Risiken wesentliche zusätzliche Inhalte. Im Abgleich der neuen Anforderungen mit den Reaktionsmöglichkeiten, die Regionalbanken infolge der Corona-Krise aus eigenem Interesse verfolgen, ergeben sich Impulse für ein verbessertes Risikomanagement. Dessen Verfolgung wird die Aufsicht absehbar ohnehin einfordern. Parallel hierzu müssen Institute die Anwendung des neuen Standardansatzes für operationelle Risiken ab dem Jahr 2023 vorbereiten.

Autor

Dr. Tobias Sander ist als Senior Manager bei Berg Lund & Company tätig und darüber hinaus als Gastautor zu regulatorischen Themen aktiv.