D 7465

Zeitschrift für das gesamte
KREDITWESEN

74. Jahrgang · 1. September 2021
17-2021

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019

Digitaler Sonderdruck

BANKEN AUFSICHT

Die Dekade operationeller Widerstandsfähigkeit hat begonnen

Frank Mehlhorn / Sami Khiari

Foto: Adobe Stock / Alex

Frank Mehlhorn / Sami Khiari

Die Dekade **operationeller Widerstandsfähigkeit** hat begonnen

2021 war bislang ein spannendes Jahr für die Entwicklung einer Regulierung zur operationellen Widerstandsfähigkeit (Operational Resilience) von Finanzdienstleistungsunternehmen. Ende März dieses Jahres haben die britischen Aufsichtsbehörden ihren erstmals im Jahr 2018 vorgeschlagenen Ansatz[1] für operationelle Widerstandsfähigkeit finalisiert, einige Tage später veröffentlichte der Basler Ausschuss für Bankenaufsicht (BCBS) seine endgültigen „Principles for Operational Resilience“[2] für Banken. In der EU werden die politischen Verhandlungen über den Digital Operational Resilience Act (DORA)[3] sowohl im Europäischen Parlament als auch im Europäischen Rat fortgesetzt und die entsprechende Council Working Group hat Anfang Januar die Arbeit aufgenommen.

Die Ansätze von Regulatoren und Standardsetzern zur Steigerung der operationellen Resilienz in Finanzdienstleistungsunternehmen stimmen in ihren Zielen und in ihrer Ausrichtung mehr und mehr überein. Diese Angleichung stellt eine gute Gelegenheit für grenzüberschreitende Finanzdienstleistungsunternehmen dar, ihre Arbeit auf Gruppenebene stärker zusammenzuführen, um ihre operationelle Widerstandsfähigkeit in den kommenden Jahren weiter voranzubringen.

Nicht nur, aber gerade Covid-19 hat jüngst aufgezeigt, dass die Bedrohungsherde zunehmen und vielschichtig sind (zum Beispiel Cyberattacken[4]). Es ist im Sinne eines jeden Finanzinstituts, diese Gefahren früh zu erkennen und sich entsprechend aufzustellen. Die Aufseher greifen nunmehr weltweit diese Entwicklungen auf, nachdem insbesondere in den vergangenen Jahren die finanzielle Resilienz im Fokus stand.

Grundsätze des Basler Ausschusses führen zu höherer Konvergenz

Die finalen Grundsätze des Baseler Ausschusses (BCBS) für Operational Resilience legen Prinzipien fest, die Bankenaufsichtsbehörden (mittelfristig) in ihren Vorschriften berücksichtigen werden. Zahlreiche Aufseher und Regelsetzer wollen die BCBS-Prinzipien analysieren und einen kritischen Abgleich mit bestehenden Regelungen vornehmen.

Im Hinblick auf die Ziele stimmen die BCBS-Prinzipien jedenfalls grundsätzlich mit dem Rahmen überein, der erstmals 2018 von den britischen Regulierungsbehörden entwickelt wurde. Zudem lässt sich eine Verbindung zu dem CERT® Resilience Management Model (CERT®-RMM) erkennen, welches durch das Software Engineering Institute (SEI) der Carnegie Mellon University entwickelt wurde. Der Ansatz nimmt für sich in Anspruch, über ISO27000 Series, NIST Special Publications, ITIL, BS25999 oder COBIT hinauszugehen.[5]

„Die Bedrohungsherde nehmen zu und sind vielschichtig.“

Welche Position nimmt nun die europäische Bankenaufsicht ein? Die European Banking Authority (EBA) ist der Ansicht, dass das Thema Operational Resilience derzeit ausreichend im existierenden regulatorischen Rahmenwerk beispielsweise durch die „EBA Guidelines on Outsourcing Arrangements“[6], die „EBA Guidelines on Internal Governance“[7] und die „EBA Guidelines on ICT and Security Risk Management“[8] abgedeckt ist. Aus direkten Gesprächen mit der EZB lässt sich jedoch auch ableiten, dass die Aufsicht trotzdem die Notwendigkeit der Weiterentwicklung und Adressierung spezieller Aspekte sieht, obwohl viele Themen der operationellen Resilienz bereits grundsätzlich geregelt sind und von den Banken abgedeckt werden.

Zum Beispiel erfolgt sehr selten die erforderliche Einbindung des höchsten Management Levels, das heißt Vorstand, Geschäftsführung, Board of Directors oder Ähnliches. Aus Sicht der EZB braucht es eine dedizierte Governance für Budget, Ressourcen und Verantwortlichkeit. Die Zentralbank will sehen, dass das Management sich ausreichend Zeit nimmt, um dieses Querschnittsthema gesamthaft über die Ressorts hinweg zu besprechen. Banken sollten daher damit rechnen, dass im Rahmen von On-site-Inspektionen nach den Inhalten gefragt wird – nichts zu tun und auf eine erste Frage der EZB zu warten, wird definitiv nicht ausreichen. Zudem soll in der nächsten Zeit ein Abschnitt zu Operational Resilience in das „Supervisory Review Process (SREP) Manual“ aufgenommen werden. Hierbei ist

allerdings noch nicht ganz klar, inwieweit bei weniger gut aufgestellten Banken gegebenenfalls Kapitalaufschläge verordnet oder andere aufsichtliche Maßnahmen eingeleitet werden.

Auch Regulierungsbehörden in anderen europäischen Ländern haben Konsultationen zu Standards begonnen oder Leitlinien veröffentlicht, die weitgehend auf dem nun finalisierten BCBS-Ansatz basieren. Dies schließt die von der US-Notenbank und anderen Bundesbehörden im Oktober 2020 herausgegebenen „Interagency Paper on Sound Practices to Strengthen Operational Resilience“[9] sowie die von der irischen Zentralbank im April 2021 veröffentlichte Konsultation[10] zu branchenübergreifenden Leitlinien der operationellen Widerstandsfähigkeit ein. Die schweizerische Financial Market Supervisory Authority (FINMA) konzentriert sich beispielsweise insbesondere auf technologiegetriebene Risiken und auf Risiken im Zusammenhang mit Auslagerungen. Die Implementierung der BCBS-Prinzipien ist in Planung, aber noch am Anfang.

Ein Blick nach Asien zeigt, dass die japanische Financial Services Agency (JFSA) sich positiv über die BCBS-Prinzipien äußert. Offiziell ist noch nichts entschieden, aber man geht davon aus, dass Schritte eingeleitet werden, um in einen Dialog mit den lokalen Banken einzutreten. Am wahrscheinlichsten ist derzeit die Einführung eines neuen Kapitels in den Richtlinien für die Aufsicht. Die JFSA vertritt die Ansicht, dass Operational Resilience eine neue Art des Denkens beim Management operationeller Risiken begründen sollte. In einem stufenweisen Ansatz sollen zunächst die großen Finanzinstitute abgedeckt werden.

Die Hong Kong Monetary Authority (HKMA) hat im April 2021 die von ihr beaufsichtigten Banken angeschrieben und auf die Veröffentlichung der BCBS „Principles for Operational Resilience“ und die „Revisions to the Principles for the Sound Management of Operational Risk“[11] verwiesen. Die HKMA nimmt zur Kenntnis, dass viele Konzepte und Anforderungen in den „Principles for Operational Resilience“ bereits in existierenden Richtlinien abgedeckt sind, prüft aber, inwiefern weitere Orientierungshilfen für Banken notwendig sind, um die neuen Prinzipien in Hongkong zu implementieren. Die HKMA sieht dabei die Notwendigkeit, die operationelle Resilienz durch die Anwendung eines flexiblen und ganzheitlichen Rahmenwerkes zu steigern.

Notwendige Standortbestimmung für Banken

Aufgrund des prinzipienbasierten Charakters der Basler „Principles for Operational Resilience“ ist derzeit noch nicht final absehbar, welche Anforderungen die EZB und BaFin im Rahmen des aufsichtlichen Überprüfungsprozesses (SREP) an Banken stellen werden. Möglicherweise kommt es letztendlich doch zu konkreten Änderungen im Regelwerk für Banken, zum Beispiel in den Mindestanforderungen für das Risikomanagement (MaRisk) oder den Bankaufsichtlichen Anforderungen an die IT (BAIT). Die EBA wird parallel prüfen, inwiefern Änderungen notwendig werden, wenn der Digital Operational Resilience Act (DORA, Details hierzu weiter unten) in Kraft tritt.

Die Unsicherheit im Hinblick auf die weitere regulatorische Entwicklung sollte Banken vor dem Hintergrund der zuvor beschriebenen Konvergenz und Stoßrichtung der weltweiten Aufsichtsbestrebungen nicht davon abhalten, eine Standortbestimmung auf Basis des Basler Papieres vorzunehmen. In einem sich dynamisch verändernden Umfeld bietet die Beschäftigung mit operationeller Resilienz zudem die Möglichkeit, eine Reihe von strategischen Vorteilen zu erzielen. Hier können exemplarisch die Steigerung der Prozesseffizienz und Robustheit der Leistungserbringung, besserer Kundenservice, die Generierung von sicherem Wachstum auf Basis eines besseren Verständnisses von Risiken sowie die zielgerichtete Lenkung von Investitionen genannt werden.

Der endgültige BCBS-Standard fordert zunächst einmal von Banken, einen Ansatz zur Steuerung der operationellen Widerstandsfähigkeit zu definieren und angemessene finanzielle, technische und weitere Ressourcen zu allokieren. Hierzu ist unter anderem die Definition eines Risikoappetits und einer sogenannten Toleranz für Unterbrechungen erforderlich. Der Ansatz ist von der Geschäftsleitung zu verabschieden und geeignet an alle relevanten Stakeholder zu kommunizieren. Die Erreichung der festgelegten Ziele ist durch die Geschäftsführung regelmäßig zu überwachen.

Im Hinblick auf die Einführung des zuvor beschriebenen Überbaus und der Definition einer angemessenen Governance be-

Frank Mehlhorn

Director Bankenaufsicht, Bundesverband deutscher Banken e. V., Berlin

Dr. Sami Khiari

Partner, PwC Deutschland, Frankfurt am Main

„Operationale Resilience ist die Fähigkeit der Unternehmen und des Finanzsystems als Ganzes, Schocks zu absorbieren und sich an sie anzupassen, anstatt zu ihnen beizutragen.“ So definiert die Bank of England die operationelle Widerstandsfähigkeit in ihrem Papier aus dem Jahre 2018. Gerade in den vergangenen Monaten hat sich gezeigt, dass die Bedrohungsherde für Finanzdienstleistungsunternehmen zunehmen. So können unvorhersehbare Ereignisse wie Hackerangriffe, Naturkatastrophen, Pandemien, menschliche Fehler oder eine Verkettung von unglücklichen Zufällen zu ernst zu nehmenden Problemen führen. Aufsichtsbehörden in den meisten europäischen Ländern haben jüngst Konsultationen oder Leitlinien veröffentlicht, die sich intensiv dem Thema der operationellen Widerstandsfähigkeit widmen. Die beiden Autoren werfen einen Blick auf die unterschiedlichen Ansätze und raten Instituten in Deutschland, sich möglichst schnell mit diesem Thema zu beschäftigen. (Red.)

steht derzeit der größte Handlungsbedarf bei Finanzinstituten. Insofern noch nicht geschehen, sollten Banken ihr Portfolio der Geschäftsaktivitäten daraufhin untersuchen, welche Prozesse bei Unterbrechungen besondere Bedeutung für die Sicherheit und Solidität der Bank haben, materiell aus der Perspektive der Aufsicht oder relevant für das Funktionieren des Finanzsystems sind. Für jeden der als kritisch identifizierten Prozesse sind dann Toleranzen (beispielsweise Zeitmetriken) für Unterbrechungen festzulegen, die auch bei Eintritt von schweren, aber plausiblen Szenarien nicht überschritten werden sollten.

Eines wird sofort klar: Banken, bei denen die Notfallplanung noch abteilungsbezogen beziehungsweise in funktionalen Silos erfolgt oder sich auf die technologische Resilienz konzentriert, werden sich auf eine längere Reise begeben müssen als Banken, die bereits eine End-to-End-Perspektive auf Prozesse und Dienstleistungen etabliert haben. Denn nur letztgenannte Perspektive erlaubt die vollständige Identifikation von Abhängigkeiten und Interdependenzen sowie die Berücksichtigung aller notwendigen Ressourcen (Personen, Technologie, Prozesse, Daten, Drittparteien, Gebäude und Infrastruktur), die für die Erbringung der wichtigen Geschäftsprozesse notwendig sind. Das Basler Papier spricht in diesem Zusammenhang von sogenannten Mappings.

Mappings müssen in einer Detailtiefe ermittelt und dokumentiert werden, sodass Verwundbarkeiten identifiziert werden können. Das Mapping stellt zudem die Basis für Tests dar, inwiefern der kritische Bankbetrieb nach Unterbrechungen innerhalb der Toleranzen wieder aufgenommen werden kann. Wenn eine Bank im Rahmen dieser Tests feststellt, dass die Toleranzen bei Eintritt von schweren, aber plausiblen Szenarien nicht eingehalten werden können, müssen die Prozesse verbessert und entsprechend robuster ausgestaltet werden.

Ein wichtiger Aspekt bei der Beschäftigung mit der operationellen Resilienz ist die Betrachtung, inwieweit man die diversen Risikomanagement-Rahmenwerke in Banken harmonisieren und integrieren kann oder auch muss (Operational Risk, Business Continuity Risk, Third Party Risk, Information & Communication Technology Risk und Recovery & Resolution Planning). Bei geeigneter Integration können Banken Potenziale zur Kostenreduktion realisieren.

Großbritannien geht einen Schritt weiter

Während deutsche Banken sich zunächst dafür entscheiden könnten, die weitere Entwicklung noch etwas abzuwarten (auch wenn dies nicht zu empfehlen ist), gilt dies für britische Banken und damit auch für die Tochtergesellschaften internationaler Banken im Vereinigten Königreich nicht. Die britischen Aufsichtsbehörden Prudential Regulation Authority (PRA) und Financial Conduct Authority (FCA) haben im März 2021 ihre finalen Vorgaben[12),13),14)] veröffentlicht. Im Gegensatz zum Basler Dokument, das zunächst einmal einen Standard für Banken setzt, ist die Umsetzung der Vorgaben der PRA und FCA für im Vereinigten Königreich regulierte Firmen verbindlich. Die britische Regulierung betrifft dabei nicht nur Banken, sondern auch Versicherungsunternehmen.

> „Banken sollten prüfen, welche Prozesse besondere Bedeutung für die Sicherheit und Solidität haben."

Bis zum 31. März 2022 müssen diese Firmen daher ihre wichtigen Dienstleistungen („important business services") identifizieren sowie entsprechende Toleranzen für maximal tolerierbare Unterbrechungen („impact tolerances") festlegen. Hierzu sind in Analogie zu den BCBS-Prinzipien die notwendigen Ressourcen für die Erbringung der Dienstleistungen (Mapping) zu dokumentieren und entsprechende Tests durchzuführen. Verwundbarkeiten, durchgeführte Szenario-Tests, Lessons Learned, geplante Maßnahmen zur Verbesserung der operationellen Widerstandsfähigkeit und angewandte Methoden sind in Form eines sogenannten Self-Assessments schriftlich festzuhalten.

Bis spätestens zum 31. März 2025 – aber in Abstimmung mit der Aufsicht so schnell wie möglich – sollen die Firmen darauf aufbauend sicherstellen, dass sie die gesetzten Toleranzen für Unterbrechungen bei schweren, aber plausiblen Szenarien einhalten können. In diesem Zusammenhang wird deutlich, dass die britischen Aufsichtsbehörden nicht nur erwarten, dass das Risikomanagement verbessert wird, sondern dass die operationelle Resilienz nachweislich erhöht wird.

Für dual regulierte Firmen, die neben der Regulierung durch die PRA ebenso unter die Regulierung der FCA fallen, gibt es eine weitere Besonderheit: Unter den Begriff der „important business services" fallen in diesem Fall auch Dienstleistungen, deren Ausfall gegebenenfalls nicht akzeptable Schäden für einen oder mehrere Kunden bedeuten würden. Dieser Ansatz geht in der Folge weit über die Beurteilung der Bedeutung einer Dienstleistung für Marktintegrität und Stabilität hinaus, die in der Regel eng mit der Größe und dem Marktanteil eines Unternehmens korreliert. FCA-beaufsichtigte Firmen müssen daher explizit überprüfen, welche Dienstleistungen für bestimmte Kunden oder Kundengruppen so wichtig sind, dass ihnen bei einer Unterbrechung ein nicht tolerierbarer Schaden entstehen könnte. Dies erfordert in der Regel auch einen Dialog mit einer repräsentativen Auswahl von Kunden.

Es ist zu erwarten, dass die britische Regulierung eine sehr große Außenwirkung über die Grenzen des Vereinigten Königreichs hinaus entfalten wird. Das liegt darin begründet, dass die Prudential Regulation Authority im Rahmen eines Konsultationspapieres im Januar 2021 einen Entwurf für ein Supervisory State-

ment veröffentlicht hat, das den Ansatz zur Beaufsichtigung von Niederlassungen und Tochtergesellschaften internationaler Banken im Vereinigten Königreich beschreibt[15]. Dort wird explizit ausgeführt, dass die PRA auch die Robustheit des Operational Resilience Regimes in den Heimatstaaten der Banken berücksichtigen wird, um sicherzustellen, dass eine operationelle Unterbrechung auf Konzernebene kein unverhältnismäßiges Risiko für den Konzern insgesamt und damit auch für die Erbringung der Dienstleistungen im Vereinigten Königreich darstellt. Auch die FCA hat sich auf die Fahne geschrieben, die britischen Verbraucher und das britische Finanzsystem zu schützen und entsprechende Anforderungen in einem im Februar 2021 veröffentlichten Dokument festgehalten.[16]

Die in den Veröffentlichungen niedergelegte Erwartungshaltung der britischen Aufseher wird dazu führen, dass viele internationale Banken, die derzeit unter den Bedingungen des Temporary Permission Regimes[17] im Vereinigten Königreich ihre Dienstleistungen anbieten, ihre UK-Niederlassungen in Töchter umwandeln werden, die als britische Banken auch den oben beschriebenen Regeln und Fristen unterliegen. Aber auch für den Fall, dass internationale Banken weiterhin Niederlassungen im United Kingdom betreiben und damit nicht unmittelbar der für britische Banken geltenden Regulierung unterliegen, hat die Aufsicht umfangreiche Anforderungen im Zusammenhang mit Operational Resilience formuliert.

Die europäischen Anforderungen

Der Digital Operational Resilience Act (DORA) der EU kann als Übersetzung der Prinzipien des Basler Bankenausschusses in konkrete Regelungen für das Risikomanagement im Bereich der Informations- und Kommunikationstechnologien (IKT) angesehen werden. Das Besondere ist, dass die DORA-Regelungen erheblich umfangreicher und konkreter sind als die Basler Prinzipien und für eine viel größere Anzahl von Unternehmen gelten. Der Anwendungsbereich umfasst über 20 000 Finanzunternehmen in der EU, darunter unter anderem Kreditinstitute, Versicherungsunternehmen, Einrichtungen der betrieblichen Altersvorsorge, Anlageverwaltungsgesellschaften sowie Marktinfrastrukturen und sogar IKT-Drittanbieter.

DORA fokussiert noch stärker auf Prozesse, Kontrollen und Verfahren, die Unternehmen benötigen, um Störungen zu verhindern und den Betrieb aufrechtzuerhalten, wenn dennoch eine Störung auftritt. DORA wird wahrscheinlich bislang nicht dagewesene regulatorische Anforderungen für Finanzunternehmen einführen. Zudem werden als kritisch designierte IKT-Drittanbieter erstmals einem Aufsichtsrahmen unterworfen.

Wenn DORA auf politischer Ebene finalisiert ist, müssen die drei europäischen Aufsichtsbehörden ESA, nämlich die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA), in Abstimmung mit der Europäischen Zentralbank und der Agentur der Europäischen Union für Cybersicherheit (ENISA) gemeinsame Entwürfe technischer Regulierungsstandards erarbeiten.

Diese und vergleichbare weltweite Aufsichtsentscheidungen werden in hohem Maße bestimmen, wie kompatibel die verschiedenen Regelungen für ein grenzüberschreitendes Institut sind und welche Auswirkungen sich ergeben.

Internationale Zusammenarbeit von großer Bedeutung

In diesem Zusammenhang macht jedoch Hoffnung, dass im Dezember 2020 die Europäische Zentralbank gemeinsam mit der US-Notenbank und der PRA im UK eine koordinierte Erklärung zur aufsichtlichen Zusammenarbeit im Bereich der operationellen Widerstandsfähigkeit herausgegeben hat. Alle drei Behörden erkannten das gemeinsame Interesse in diesem Bereich an und verpflichteten sich, ihre Arbeit eng aufeinander abzustimmen.

Neu ist, dass dieses Interesse über bisher existierende Abstimmungen bei der Aufsicht grenzüberschreitender Institute hinausgeht. Die Aufseher meinen es ernst und zielen darauf ab, gemeinsam einen globalen Ansatz zu nutzen. So soll ein widerstandsfähigerer Finanzsektor insgesamt geschaffen werden, in dem Betriebsstörungen weniger wahrscheinlich sind und die Anfälligkeit für systemische Risiken weitgehend reduziert wird.

> „Alle drei Behörden verpflichten sich, ihre Arbeit eng aufeinander abzustimmen."

In der Erklärung werden konkret Bereiche genannt, in denen systemrelevante Banken weiteren Fortschritt erreichen sollen. Dazu zählen unter anderem:[18]

– Erzielung kontinuierlicher Verbesserungen bei der ganzheitlichen Betrachtung von Resilienz einschließlich der Berücksichtigung der möglichen Auswirkungen von Unterbrechungen auf das Finanzsystem,

– Ausbau des Verständnisses, dass operationelle Resilienz das Ergebnis eines klugen Risikomanagements ist und weiterer Praktiken einschließlich effektiver Reaktions- und Wiederherstellungspläne zum Management von Ereignissen beinhaltet. Es geht nicht nur um die Unterlegung von operationellen Risiken mit Risikokapital,

– Anerkenntnis, dass operationelle Widerstandsfähigkeit nicht nur eine Frage von resilienter Technologie ist,

– Anerkenntnis der Wichtigkeit von operationeller Resilienz einschließlich der Im-

plementierung effektiver Standards für die Überwachung und das Risikomanagement von Drittparteien, die kritische Dienstleistungen erbringen,

– Schaffung eines umfassenden Verständnisses für die Bandbreite und Typen von potenziellen Disruptionen, die eine Bank oder einen Dienstleister treffen können.

Aktive Rolle der Banken

Dabei muss man aber festhalten, dass kein Ausmaß an regulatorischer Konvergenz wirklich alle Unterschiede zwischen den Regeln und Leitlinien beseitigen wird, die zu Operational Resilience existieren. Beispielsweise bestehen bereits zwischen den übergeordneten BCBS-Grundsätzen und den endgültigen Vorgaben der Aufsichtsbehörden des Vereinigten Königreichs Unterschiede, die das Potenzial haben, mehr als nur kosmetisch zu sein.

Ein solcher Bereich ist beispielsweise die Identifizierung dessen, was in einem Unternehmen die relevanten Geschäftsaktivitäten sind. Das britische Rahmenwerk legt insbesondere großen Wert auf die Fokussierung auf Dienstleistungen (sogenannte „important business services"), die ein Unternehmen für externe Endnutzer erbringt (insbesondere Kunden), während das BCBS den Begriff „critical operations" verwendet, der eher der in den USA und in der EU innerhalb von DORA verwendeten Terminologie entspricht. Inwiefern diese Unterschiede in der Terminologie tatsächlich Auswirkungen in der Praxis haben werden, bleibt abzuwarten.

Sicher ist jedoch, dass britische Banken durch die zusätzliche FCA-Regulierung insbesondere auch die Auswirkungen beziehungsweise den Schaden für einzelne Gruppen respektive Kundengruppen analysieren müssen, während Banken in der EU sich möglicherweise darauf konzentrieren können, wie eine Störung die Finanz- und Marktstabilität per se gefährden könnte. Das könnte dazu führen, dass Institute in England eine längere Liste ihrer wichtigen Geschäftsprozesse haben werden als in anderen Ländern. Dies erhöht dann konsequenterweise die Komplexität und den Aufwand für die Umsetzungsaktivitäten.

Interessant ist zudem, dass die Prinzipien des Basler Ausschusses beispielsweise explizite Standards zum Abhängigkeitsrisiko Dritter sowie zum IKT- und Cybersicherheitsmanagement setzen und somit den Schwerpunkt des Standards auf internationaler Ebene erweitern. Obwohl diese Themen implizit vom britischen Rahmen abgedeckt werden, stellen sie Bereiche dar, in denen Regulierungsbehörden in anderen Jurisdiktionen (insbesondere in der EU und den USA) möglicherweise auch explizitere Regeln für Unternehmen des Finanzsektors festlegen könnten. Gerade in Deutschland besteht sicherlich – auch im Vergleich zu anderen Ländern in Europa – bereits ein „Regulierungsvorsprung" (zumindest aus dem Blickwinkel der Bankenaufseher). In diesem Zusammenhang wird gerne auf die Mindestanforderungen für das Risikomanagement (MaRisk) und die Bankaufsichtlichen Anforderungen an die IT (BAIT) verwiesen.

Lokale Unterschiede

Aktuell ist daher davon auszugehen, dass einige Unterschiede bestehen bleiben und in der Folge könnte das durchaus bedeuten, dass Unternehmen aufgrund der jeweiligen lokalen Vorschriften unterschiedliche „wichtige Prozesse" in verschiedenen Regionen identifizieren und priorisieren müssen. Dies kann teurer und zeitaufwändiger sein, beeinträchtigt jedoch nicht die Logik eines global integrierten Ansatzes für Finanzdienstleistungsgruppen.

Bei der Fertigstellung ihres Rahmens gaben die britischen Behörden dann auch eine kurze Erklärung zur internationalen Rechtsangleichung ab, in der sie diesen Standpunkt akzeptierten und feststellten:[19] „Es ist realistisch anzunehmen, dass es lokale Unterschiede bei der Implementierung geben wird, und es ist vernünftig, dass verschiedene Gerichtsbarkeiten unterschiedliche Ansichten darüber haben, was sie für kritisch oder wichtig halten. Aber solange die Grundsätze aufeinander abgestimmt sind, ist die PRA der Ansicht, dass Firmen und ihre Aufsichtsbehörden effektiv über Grenzen hinweg arbeiten können."

In der Praxis ist zu beobachten, dass mehrere globale Banken vor diesem Hintergrund beschlossen haben, den britischen Ansatz zur operationellen Widerstandsfähigkeit konzernweit anzuwenden. Der Vorteil dieses Ansatzes besteht darin, dass er ihnen hilft, die Ausfallsicherheit ihrer wichtigen Dienste oder Prozesse unabhängig von ihrem geografischen Standort einheitlich zu behandeln und zu verbessern. Obwohl sie sich an die spezifischen regulatorischen Anforderungen in den einzelnen Gerichtsbarkeiten anpassen müssen, wird diese konzernweite Aktivität wahrscheinlich eine Schlüsselrolle dabei spielen, allen Aufsichtsbehörden eines Unternehmens zu zeigen, dass sie die erforderlichen Arbeiten durchgeführt haben, um viele ihrer sich abzeichnenden Erwartungen an die operationelle Widerstandsfähigkeit zu erfüllen.

Es ist zu erwarten, dass die meisten Aufsichtsbehörden den Banken einen gewissen Spielraum bei der Umsetzung der aufsichtsrechtlichen Anforderungen zugestehen werden. Wenn dies der Fall ist, muss eine gewisse regulatorische Fragmentierung nicht unbedingt zu einem wesentlichen Treiber für Kosten und Komplexität bei den Banken werden.

Konkrete Handlungsfelder

Es besteht mehr als je zuvor die Notwendigkeit, dass die Institute gegenüber ihren Aufsehern nachweisen, über eine entsprechende Belastbarkeit ihres Geschäftsbetriebs nicht nur nachgedacht, sondern auch einen Plan entwickelt zu haben, um Mängel zu identifizieren und zu beheben. Banken ist daher zweierlei zu empfehlen:

Zum einen sollten sie – falls nicht schon geschehen – dringend beginnen, sich des Themas Operational Resilience anzunehmen. Hierzu gehört eine Analyse, inwiefern eine Bank in verschiedenen Ländern von verschiedenen Aufsichtsregimen be-

troffen ist, eine für das Institut passende Festlegung kritischer Services, Toleranzen und Ambitionsniveaus, sowie eine erste Selbsteinschätzung zum Status quo. Auf dieser Basis kann ein Plan für die weitere Vorgehensweise ausgearbeitet werden.

Nachholbedarf bei deutschen Instituten

Zum anderen ist es für zielführend, konzernweit einen einheitlichen Ansatz für operative Resilienz zu verfolgen – trotz steigender Dynamik im Thema weltweit. Parallel bietet es sich an, die Diskussion rund um das Thema innerhalb von Verbänden oder vergleichbaren Interessenvertretungen von Banken zu beginnen beziehungsweise fortzuführen.

Die Entwicklungen rund um Operational Resilience sind in den letzten Monaten vorangeschritten, während Finanzinstitute weiterhin den Belastungen und Sorgen durch die Covid-19-Pandemie ausgesetzt sind. Der Fokus der Aufseher war bislang primär auf finanzielle Resilienz und Erleichterungen (zum Beispiel bei Meldungen) ausgerichtet. Doch nun überlegen die Finanzaufsichtsbehörden aktiv, was sie tun können, um das Finanzsystem und ihre wesentlichen Player auf noch schwerwiegendere operationelle Bedrohungen vorzubereiten, als sie Covid-19 mit sich gebracht hat.

Die Banken im Vereinigten Königreich und teilweise in den USA sind den Instituten in Europa einen Schritt voraus. Aus Kunden- und Projekterfahrungen ist bekannt, dass die Vorhaben zur dauerhaften Steigerung der operationellen Widerstandsfähigkeit langfristig – in der Regel über mehrere Jahre – angelegt sind. Komplexe und gruppenweite Programme mit dem Ziel einer strategisch angelegten Transformation unter enger Einbindung des Topmanagements sind in der Umsetzung. Im Wettbewerb ist eines also schon heute klar zu sehen: die Dekade operationeller Widerstandsfähigkeit hat begonnen – sind deutsche Institute bereit, die Herausforderung anzunehmen?

Fußnoten

1) Bank of England DP01/18, Prudential Regulation Authority DP01/18, Financial Conduct Authority DP18/04: „Building the UK financial sector's operational resilience", Juli 2018
2) Basel Committee on Banking Supervision: "Principles for Operational Resilience", März 2021
3) Europäische Kommission: „Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors", COM (2020) 595 final, September 2020
4) European Banking Association: „EBA Risk DashBoard Q4/2020", Seite 4: "Phishing attempts and other types of cyber-attacks are becoming more common."
5) Carnegie Mellon University's Software Engineering Institute (SEI): „CERT® Resilience Management Model Capability Appraisal Method (CAM)", Version 1.1, Oktober 2011, Seite 4
6) European Banking Association (EBA), EBA/GL/2019/02: „EBA Guidelines on outsourcing arrangements", Februar 2019
7) European Banking Association (EBA), EBA/GL/2017/11: „EBA Guidelines on internal governance under Directive 2013/36/EU", September 2017
8) European Banking Association (EBA), EBA/GL/2019/04: „EBA Guidelines on ICT and security risk management", November 2019
9) Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency: „Sound Practices to Strengthen Operational Resilience", Oktober 2020
10) Central Bank of Ireland: „Consultation on Cross Industry Guidance on Operational Resilience", Consultation Paper 140, April 2021
11) Basel Committee on Banking Supervision: „Revisions to the Principles for the Sound Management of Operational Risk", März 2021
12) Prudential Regulation Authority (PRA), Supervisory Statement I SS1/21: „Operational resilience: Impact tolerances for important business services", März 2021
13) Prudential Regulation Authority (PRA), PRA-2021/5: „PRA Rulebook: CRR Firms, Sovency II Firms: Operational Resilience Instrument 2021", März 2021
14) Financial Conduct Authority (FCA), Policy Statement I PS21/3: „Building operational resilience: Feedback to CP19/32 and final rules", März 2021
15) Prudential Regulation Authority (PRA), Draft Supervisory Statement „International banks: The PRA's approach to branch and subsidiary supervision" als Teil von Consultation PaperCP2/21nt business services", Januar 2021
16) Financial Conduct Authority (FCA): Our Approach to International Firms, Februar 2021
17) UK Statutory Instruments, 2018 No. 1149: „The EEA Passport Rights (Amendment, etc., and Transitional Provisions) (EU Exit) Regulations 2018"
18) European Central Bank, „Coordinated statement on operational resilience", SSM-2020-0741, Dezember 2020
19) Prudential Regulation Authority: „Operational resilience: Impact tolerances for important business services", Policy Statement I PS6/21, März 2021