

Gerd Waschbusch / Sabrina Kiszka

Neue aufsichtsrechtliche Anforderungen an die Risikosteuerung

Obgleich die aufsichtsrechtlichen Bemühungen aufgrund der Erfahrungen aus der Finanz- und Wirtschaftskrise der Jahre 2007/08 die Resilienz des Bankensektors gestärkt haben, beweist die Pandemie, dass ergänzende Maßnahmen erforderlich sind, um Banken besser noch als bisher in die Lage zu versetzen, externe Schocks wie Pandemien, Cybervorfälle, technologische Ausfälle oder Naturkatastrophen zu bewältigen sowie daraus folgende weitreichende Störungen auf den Finanzmärkten zu vermeiden.¹⁾ In den vergangenen Jahren ließen sich prädominante operationelle Risiken im Banken-

vermehrt Cyberbedrohungen zu verzeichnen. Als Folge hat das Potenzial operationeller Risikoereignisse in den letzten Monaten stark zugenommen.

Um die anfänglichen Lehren aus der Corona-Pandemie zu nutzen und auf die neuen Risikopotenziale einzugehen, veröffentlichte der Baseler Ausschuss (BA) am 6. August 2020 nicht nur eine überarbeitete Version seiner Prinzipien zum Umgang mit operationellen Risiken (Revisions to the principles for the sound management of operational risk).²⁾ Er präsentierte darüber hinaus auch einen

Prinzipien zur Stärkung der operationellen Widerstandsfähigkeit einer Bank aufgezeigt.

Schwachstellen sollen geschlossen werden

Die im Jahr 2003 vom BA eingeführten Praxisempfehlungen zur Handhabung operationeller Risiken wurden zuletzt 2011 überarbeitet, um die Erfahrungen aus der Finanz- und Wirtschaftskrise zu berücksichtigen. Aufgrund der mittlerweile erkannten besonderen Risikopotenziale, die den Banken aus dem Einsatz der Informations- und Kommunikationstechnologien (IKT) erwachsen, beabsichtigt der Baseler Ausschuss, den bisherigen Katalog der Prinzipien zum Management operationeller Risiken um ein neues Prinzip zu erweitern, das sich dieser Problematik widmet.⁶⁾ Weitere geplante Änderungen an dem ursprünglichen Katalog sind auf eine durch den BA im Jahr 2014 durchgeführte Studie zum damaligen Umsetzungsstand der Prinzipien zurückzuführen, deren Ergebnisse ernüchternd ausfielen.⁷⁾

So waren die Prinzipien nur unzureichend implementiert. Neben der nicht adäquaten Nutzung der Instrumente zur Risikoidentifikation und -bewertung stellte der Baseler Ausschuss allerdings noch weitere Schwachstellen fest, die nach seiner Auffassung zusätzliche Leitlinien erforderlich machen: Die Implementierung der drei Verteidigungslinien, die Beaufsichtigung des Managements operationeller Risiken durch den Vorstand und die erste Führungsebene unterhalb des Vorstands, die Formulierung des Risi-

„Das Potenzial operationeller Risikoereignisse hat in den letzten Monaten stark zugenommen.“

sektor vor allem auf Schwachstellen in den Informations- und Kommunikationstechnologien aufgrund einer vorschleunigten Einführung neuartiger Systeme und der wachsenden Abhängigkeit von diesen Systemen sowie von Drittanbietern bei der Bereitstellung von Finanzdienstleistungen zurückführen.

Lehren aus Pandemie nutzen

Corona hat nicht nur diese Risiken verstärkt, sondern auch die allgemeine ökonomische und betriebliche Unsicherheit erhöht. So haben sich pandemiebedingte Störungen und die steigende Abhängigkeit von virtuellen Arbeitsvereinbarungen auf die bestehenden Systeme, Mitarbeiter, Einrichtungen und Beziehungen zu Drittanbietern ausgewirkt. Zusätzlich sind

neuen prinzipienorientierten Ansatz zur Verbesserung der operationellen Widerstandsfähigkeit der Banken (Principles for operational resilience).³⁾ Diese wird definiert als die Fähigkeit einer Bank, kritische Operationen trotz Störungen durch externe Schocks weiterhin gewährleisten zu können.⁴⁾ Als kritische Operationen gelten Aktivitäten, Prozesse und Dienstleistungen, deren Aufrechterhaltung für den weiteren Betrieb der Bank oder ihre Rolle im Finanzsystem wesentlich sind.⁵⁾

Beide Publikationen des BA befinden sich bis zum 6. November 2020 in Konsultation. Nachfolgend werden zunächst die wichtigsten zu erwartenden Änderungen in den aufsichtsrechtlichen Anforderungen an die Handhabung operationeller Risiken dargestellt. Im Anschluss daran werden die vom Baseler Ausschuss vorgestellten

koappetits der Bank, das Veränderungsmanagement und die Offenlegung der Risiken.⁸⁾

Vor allem in den vorgenannten Bereichen ergibt sich aus Sicht des BA die Notwendigkeit von Ergänzungen im Katalog der Prinzipien zum Management operationeller Risiken. Die wesentlichsten Inhalte dieses Katalogs werden in der Abbildung 1 dargestellt. Hierbei werden die wichtigsten Änderungen aufgrund des vom Baseler Ausschuss im August 2020 veröffentlichten Konsultationspapiers separat hervorgehoben. Soweit inhaltlich erforderlich, werden diese Änderungen im Nachhinein weiter erläutert.

Ein Hauptaugenmerk bei dem Vorschlag des BA wird auf das Modell der drei Verteidigungslinien gelegt. Dieses Modell teilt Banken in drei Verantwortungsbereiche auf.⁹⁾ Die erste Verteidigungslinie stellen Geschäftseinheiten dar, denen die operative Kontrolle der Risiken des täglichen Bankgeschäfts zufällt. Die zweite Verteidigungslinie überwacht als zentrale Risikomanagementeinheit die von der ersten Verteidigungslinie durchgeführten internen Kontrollen; sie entwickelt zudem Regelwerke zum Umgang mit den Risiken. Die dritte Verteidigungslinie – die interne Revision – übernimmt hingegen die unabhängige und objektive Prüfung der Effektivität des aus den beiden vorgelagerten Verteidigungslinien bestehenden internen Kontrollsystems.

Drei Verteidigungslinien

Für die Etablierung eines Managementrahmenwerks für operationelle Risiken (Prinzip 2) bedeutet dies, dass es durch die erste Verteidigungslinie in den gesamten Risikomanagementprozess der Bank zu integrieren, durch die zweite Verteidigungslinie zu überwachen und gegebenenfalls anzufechten sowie durch die dritte Verteidigungslinie unabhängig und objektiv zu überprüfen ist.¹⁰⁾ Der BA betont hierbei, dass jede Verteidigungslinie adäquate personelle, technische und finanzielle Ressourcen erhalten muss.¹¹⁾ Zusätzlich sind nach Ansicht des Baseler Ausschusses die Rollen und Verantwort-

lichkeiten der einzelnen Verteidigungslinien klar zu definieren. Denn wenn der BA auch anerkennt, dass die Banken das Modell der drei Verteidigungslinien in der Vergangenheit weitestgehend übernommen haben, wird dessen Effektivität nach seiner Erkenntnis bisher häufig durch unklare Zuständigkeiten eingeschränkt.

Um dieses Problem in den Griff zu bekommen und zugleich eine angemessene Risikokultur innerhalb der Bank zu fördern, sind die Mitarbeiter der einzelnen Verteidigungslinien kontinuierlich in Fragen des Risikomanagements und der Ethik weiterzubilden. In Prinzip 1 wird dies nun ausdrücklich festgehalten. Für die Gewährleistung einer umfassenden Steuerung der operationellen Risiken wird zudem vom BA ein Austausch zwischen den Verteidigungslinien als unverzichtbar angesehen. In dem vom BA überarbeiteten Prinzipienkatalog wird weiterhin die Bedeutung einer regelmäßigen Überprüfung des Managementrahmenwerks zur Handhabung operationeller Risiken betont (Prinzip 2). Nicht zuletzt werden auch die Dokumentationsanforderungen hinsichtlich des Aufbaus und der Ausgestaltung des Managementrahmenwerks für operationelle Risiken, beispielsweise durch die Erstellung eines Katalogs aller bankbetrieblichen Risiken und der diesbezüglich implementierten Kontrollen, verschärft (Prinzip 2).¹²⁾

Die Erklärung einer Bank zu ihrer Risikoneigung beziehungsweise Risikotoleranz (Prinzip 4), bei deren Formulierung nun explizit die Interessen der Bankkunden und Shareholder sowie regulatorische Anforderungen zu berücksichtigen sind, muss für alle Adressaten leicht verständlich und zukunftsorientiert ausgerichtet sein sowie wichtige Hintergrundinformationen und Annahmen enthalten, die die Geschäftspläne der Bank zum Zeitpunkt ihrer Genehmigung beeinflusst haben.¹³⁾ In diese Erklärung sind ferner Begründungen für das Eingehen beziehungsweise Vermeiden von bestimmten Risikoarten aufzunehmen, die mit der Überwachung entsprechender Risikolimits in jeder Geschäftseinheit einhergehen. Wichtige Inhalte dieser Erklärung sind aber auch Szenarioanalysen und Stresstests, um vor



Univ.-Prof. Dr.
Gerd Waschbusch

Lehrstuhl für Betriebswirtschaftslehre, insbesondere Bankbetriebslehre, Universität des Saarlandes, Saarbrücken



 
Sabrina Kiszka

M. Sc., Doktorandin, Lehrstuhl für Betriebswirtschaftslehre, insbesondere Bankbetriebslehre, Universität des Saarlandes, Saarbrücken

Anders als bei der Finanz- und Wirtschaftskrise 2007/08 sind Banken nicht der Auslöser der Rezession, die dieser Tage viele Länder in ihrem Griff hat. Dennoch: Banken sind nicht vor den operationellen Risiken gefeit, die die Coronapandemie bereithält. Sollten die wirtschaftlichen Auswirkungen einer ersten Pandemie-Welle sich hinziehen und die einer zweiten noch hinzukommen, könnten Banken, die von vielen gegenwärtig als Teil der Lösung des Problems angesehen werden, mit in den Sog der schlechten Wirtschaftslage geraten. Aber auch andere externe Schocks wie Naturkatastrophen und Cyberbedrohungen könnten an der momentan guten Stellung der Banken etwas verändern. Die Autoren des vorliegenden Beitrags begrüßt daher die aufsichtsrechtlichen Bemühungen, Banken zu einer besseren Steuerung ihres operationellen Risikos zu verpflichten. Teilweise bestehe Aufholbedarf, trotz der Erfahrungen der letzten Krisen. (Red.)

alle diejenigen Szenarien zu identifizieren, die die aktuelle Risikoneigung beziehungsweise Risikotoleranz der Bank übersteigen.

Erweiterter Instrumentenkatalog

Neben den Szenarioanalysen und Stresstests gibt der BA den Banken eine Vielzahl weiterer Steuerungsinstrumente an die Hand (Prinzip 6).¹⁴⁾ Er betont, dass alle Instrumente auf genauen Daten basieren müssen, deren Integrität durch solide

Abbildung 1: Prinzipien zum Management operationeller Risiken*

Bereich	Inhalt
1 Grundprinzipien	Aufbau einer starken Risikomanagementkultur durch den Vorstand – Betonung der hohen Bedeutung von Mitarbeiterschulungen im Hinblick auf das Risikomanagement und das Erfordernis ethischen Verhaltens
2	Etablierung eines Managementrahmenwerks für operationelle Risiken und dessen Einbettung in die Gesamtrisikosteuerung – stärkere Betonung des Modells der drei Verteidigungslinien, höhere Dokumentationsanforderungen hinsichtlich des Aufbaus und der Ausgestaltung des Managementrahmenwerks für operationelle Risiken, regelmäßige Überprüfung des Managementrahmenwerks für operationelle Risiken
3 Unternehmensführung	seitens des Vorstands Überwachung der materiellen operationellen Risiken, der Effektivität der Schlüsselkontrollen sowie der Art und Weise der Implementierung des Managementrahmenwerks für operationelle Risiken durch die erste Führungsebene auf allen Entscheidungsebenen der Bank – Betonung der Vorstandsverantwortung, regelmäßige Überprüfung der Kontrollen durch den Vorstand
4	regelmäßige Überprüfung der Risikoneigungs- und Risikotoleranzklärung – Betonung der Vorstandsverantwortung, gestiegene Anforderungen an den Inhalt der Risikoneigungs- und Risikotoleranzklärung
5	Entwicklung einer klaren, effektiven und robusten Governance-Struktur mit klaren Verantwortlichkeiten
6 Risikomanagementumfeld	Identifikation und Bewertung operationeller Risiken bei allen Produkten, Aktivitäten, Prozessen und Systemen durch die erste Führungsebene – Erweiterung der Steuerungsinstrumente um die Analyse von Schlüsselkontrollen sowie eingetretener operationeller Risikoereignisse (sog. Ereignismanagement)
7	Etablierung eines Prozesses bei unternehmerischen Veränderungen – Erweiterung des Betrachtungsgegenstands von Produkten, Aktivitäten, Prozessen und Systemen hin zu jeglichen unternehmerischen Veränderungen, ganzheitliche Betrachtung der entstehenden Risiken, regelmäßige Überprüfung des Veränderungsmanagements (gepaart mit klaren Verantwortlichkeiten innerhalb der drei Verteidigungslinien), Dokumentation aller Produkte und Dienstleistungen (inkl. Auslagerungen)
8	Implementierung regelmäßiger Überwachungsprozesse für operationelle Risiken, Einführung von Reportingstrukturen – kontinuierliche Verbesserung des Risikoreportings, Erweiterung der Berichtsinhalte
9	Etablierung eines strengen Kontrollumfelds – institutsweit einheitliche Vorgehensweise bei Klassifizierungen, Methodik und Verfahren innerhalb des Managements operationeller Risiken
10 Informations- und Kommunikationstechnologien (IKT)	Implementierung einer soliden IKT-Governance, die sicherstellt, dass die vorhandenen Informations- und Kommunikationssysteme die Geschäftstätigkeit der Bank vollständig unterstützen beziehungsweise erleichtern sowie Risiken reduzieren
11 Geschäftsführungspläne	Erstellung von Geschäftsführungsplänen – Widerstandsfähigkeitsbetrachtung nunmehr behandelt in einem separaten Papier des Baseler Ausschusses (siehe Kapitel 3)
12 Offenlegung	Offenlegung des Managements operationeller Risiken gegenüber den Stakeholdern – Erweiterung der Berichtsinhalte an die Stakeholder um Aussagen zur aktuellen operationellen Risikolage, regelmäßige Überprüfung der Offenlegungsgrundsätze

* einschließlich der wichtigsten Änderungen durch das aktuelle Konsultationspapier des Baseler Ausschusses
Quelle: Modifiziert entnommen aus Angermüller, Niels Olaf: Operationelle Risiken, in: Handbuch MaRisk und Basel III, hrsg. von Axel Becker; Walter Gruber und Dirk Wohler, 2. Aufl., Frankfurt am Main 2012, S. 596; Hänel, Corinna: Fraud-Prävention in Kreditinstituten, Wiesbaden 2016, S. 203–204, Kiszka, Sabrina: Die Steuerung operationeller Risiken in Kreditinstituten, Wiesbaden 2018, S. 137–138, erweitert um Inhalte aus BCBS 508.

Überprüfungs- und Validierungsverfahren sichergestellt werden muss. Die Ergebnisse der laufenden Risikosteuerung müssen bei der Überwachung von Aktions- sowie Sanierungsplänen Berücksichtigung finden. Der den Banken zur Verfügung stehende Instrumentenkatalog wurde vom Baseler Ausschuss durch die Analyse von Schlüsselkontrollen und das Ereignismanagement erweitert. Letzteres beinhaltet die Analyse und Auswertung eingetretener operationeller Risikoereignisse. Dahin gehend weist der BA explizit darauf hin, dass die erste Verteidigungslinie sicherstellen muss, dass alle verbleibenden operationellen Risikoereignisse, alle Kontroll- und Prozessmängel sowie alle Überschreitungen von Risikotoleranzgrenzen gemeldet werden (Prinzip 8).¹⁵⁾ Denn das Ziel der Banken soll es sein, die interne Berichterstattung über operationelle Risiken kontinuierlich zu verbessern, weshalb interne Berichte eine Darstellung der wichtigsten bestehenden sowie der neu auftretenden operationellen Risiken mitsamt einer Ursachenanalyse enthalten sollen. Ebenso sind mögliche Auswirkungen von regulatorischen Veränderungen in den internen Berichten darzulegen.

Bezüglich der externen Berichterstattung über die operationelle Risikolage der Bank fordert der BA die Offenlegung von für die Stakeholder relevanten Risikoinformationen (Prinzip 12). Eine solche Offenlegung darf jedoch nicht dazu führen, dass sie selbst ein operationelles Risiko erzeugt (beispielsweise durch die Beschreibung von nicht adressierten, aber erkannten Schwachstellen innerhalb von implementierten Kontrollmechanismen).¹⁶⁾ Die externen Offenlegungsgrundsätze sind zudem regelmäßig einer unabhängigen Überprüfung zu unterziehen. Über den gesamten Managementprozess operationeller Risiken hinweg sollen Banken im Hinblick auf Klassifizierungen, Methodik und Verfahren einheitlich vorgehen.¹⁷⁾

Mit dem neu in den Prinzipienkatalog aufgenommenen Prinzip 10 wird das Risikopotenzial, das einer Bank aus den Informations- und Kommunikationstechnologien erwächst, adressiert.¹⁸⁾ Hintergrund ist die Erkenntnis, dass die Funktionsfähigkeit und Sicherheit der eingesetzten



Informations- und Kommunikationssysteme wesentliche Voraussetzungen dafür sind, dass die Banken ihre Geschäftstätigkeiten ordnungsgemäß abwickeln können. Von daher fordert der BA, zukünftig eine solide IKT-Governance zu implementieren, die im Einklang mit der Erklärung zur Risikoneigung und Risikotoleranz steht und sicherstellen soll, dass die vorhandenen Informations- und Kommunikationssysteme die Geschäftstätigkeit der Bank vollständig unterstützen beziehungsweise erleichtern sowie Risiken reduzieren.

Ergänzend dazu soll zukünftig strikt darauf geachtet werden, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gewährleistet ist. Die Informations- und Kommunikationssysteme sind zu diesem Zweck mit geeigneten Programmen zu überwachen und zu sichern. Weiterhin sind Wiederherstellungsprogramme zu implementieren. Die etablierten Schutzmechanismen sind regelmäßig zu testen und müssen dem Nutzer zeitnah relevante Informationen übermitteln. Der BA er-

weitert den bisherigen Prinzipienkatalog allerdings nicht nur um die zuvor genannten Maßgaben für die Banken selbst, sondern adressiert auch die Aufsichtsbehörden. Diese sollen die Implementierung der Prinzipien sowie die Beseitigung möglicher Defizite bei den zu beaufsichtigenden Banken regelmäßig überwachen.¹⁹⁾

Neue Aufgaben für die Aufsichtsbehörden

Die operationelle Widerstandsfähigkeit einer Bank, die bisher als Bestandteil der Prinzipien zum Umgang mit operationellen Risiken behandelt wurde, soll zukünftig aufgrund des gestiegenen Risikopotenzials extern auftretender, nicht vermeidbarer Ereignisse wie beispielsweise Pandemien, Cybervorfälle, technologische Ausfälle oder Naturkatastrophen in einem eigenen Prinzipienkatalog reglementiert werden.²⁰⁾ Hierbei betont der Baseler Ausschuss allerdings, dass die operationelle Widerstandsfähigkeit einer

Bank von einem effektiven Management operationeller Risiken profitiert, da ein solches Management operationelle Störfälle verringert und damit vor allem auch die Aufrechterhaltung kritischer Funktionen schützt.

Neben dem zuvor angesprochenen effektiven Management operationeller Risiken sind aber auch Geschäftsfortführungspläne, Auslagerungsvereinbarungen und die Systeme, auf denen diese Vereinbarungen beruhen, wichtige Aspekte, die bei der Stärkung der operationellen Widerstandsfähigkeit einer Bank betrachtet werden müssen. Die Inhalte des Konsultationspapiers zur operationellen Widerstandsfähigkeit einer Bank sind in der Abbildung 2 im Überblick dargestellt.

Das Risikopotenzial, mit dem Banken konfrontiert werden, ist in der Vergangenheit kontinuierlich angestiegen. Nicht nur, aber auch die Corona-Pandemie offenbart dies für jeden spürbar in aller Deutlichkeit. Von daher kann es kaum

 Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

Vertriebsjob, meinen Erfolg selbst steuern

- DZ BANK Gruppe**
- Zweitgrößte **FinanzGruppe** Deutschlands
- Partner** der Kunden
- Vielfältige** Karrierechancen
- Umfassendes** Vertriebsnetzwerk
- Unterstützung durch **starkes Team**



Jetzt bewerben!

Wenn auch Sie im Job mehr bewirken wollen: Willkommen im Team. Bewerben Sie sich jetzt: www.karriere.dzbankgruppe.de



 **DZ BANK Gruppe**

Abbildung 2: Prinzipien zur operationellen Widerstandsfähigkeit einer Bank

Bereich	Inhalt
1 Unternehmensführung	Aufbau eines Ansatzes zur Bewertung der operationellen Widerstandsfähigkeit der Bank auf Basis des bestehenden Führungssystems durch die Analyse von Störfällen und die Durchführung von Szenarioanalysen, Einführung von Reportingstrukturen
2 Management operationeller Risiken	Nutzung der für das operationelle Risiko bestehenden Managementstrukturen zur Identifizierung von internen oder externen Bedrohungen für kritische Geschäftsprozesse sowie von Schwachstellen auf der personellen, prozessualen oder technischen Ebene
3 Geschäftsfortführungspläne	Erstellung von Geschäftsfortführungsplänen und Durchführung von Betriebsfortführungsübungen unter Einbeziehung der Mitarbeiter für plausible Szenarien mit schwerwiegenden Folgen
4 Verflechtungen und Abhängigkeiten	Abbildung der notwendigen Ressourcen zur Durchführung kritischer Operationen (beispielsweise Mitarbeiter, Systeme, Informationen, Gebäude) sowie der Verflechtungen und Abhängigkeiten zwischen diesen Operationen und Ressourcen sowie zu Drittanbietern
5 Abhängigkeitsmanagement	Steuerung der Abhängigkeit von Drittanbietern bei der Erbringung von kritischen Operationen, Durchführung einer Risikoanalyse vor dem Eingehen einer solchen Abhängigkeit
6 Ereignismanagement	Implementierung und kontinuierliche Verbesserung von Wiederanlaufplänen für Vorfälle, die die Bereitstellung kritischer Operationen gefährden könnten
7 Informations- und Kommunikationstechnologien	Sicherstellung belastbarer Informations- und Kommunikationstechnologien, auch im Hinblick auf die Cybersicherheit (im Einklang mit Prinzip 10 der Prinzipien zum Management operationeller Risiken)

Quelle: eigene Darstellung G. Waschbusch/S. Kiszka entsprechend den Inhalten aus BCBS 509, Seite 4–9

verwundern, dass auch das Management operationeller Risiken und die Stärkung der operationellen Widerstandsfähigkeit der Banken stark an Bedeutung gewonnen haben. Es ist deshalb durchaus positiv zu bewerten, dass der Baseler Ausschuss die in den vergangenen Jahren identifizierten Schwachstellen und die sich neu abzeichnenden Risiken in seinen Empfehlungen zum Umgang mit operationellen Risiken berücksichtigt und damit die Wahrnehmung der Banken und der Aufsicht für die in diesem Bereich bestehenden Gefahren schärft.

Banken werden nicht überfordert

Da die vom BA vorgesehenen Erweiterungen der Prinzipien zum Umgang mit operationellen Risiken und die von ihm neu vorgeschlagenen Prinzipien zur operationellen Widerstandsfähigkeit einer Bank größtenteils auf bereits zuvor veröffentlichten Orientierungshilfen beruhen,²¹⁾ sollten in den beiden im August vorgelegten Konsultationspapieren letztlich keine Anforderungen enthalten sein, welche die Banken überfordern. Dies setzt aller-

dings voraus, dass die bisherigen Empfehlungen und Orientierungshilfen des Baseler Ausschusses zur Handhabung der operationellen Risiken von den Banken weitgehend umgesetzt wurden. Angesichts der enttäuschenden Ergebnisse der anfangs genannten Untersuchung zum weltweiten Umsetzungsstand der Prinzipien im Jahr 2014 sind diesbezüglich aber Zweifel angebracht. Für deutsche Institute hingegen ist ein Großteil der vom Baseler Ausschuss angestrebten Erweiterungen hinsichtlich der Behandlung operationeller Risiken bereits seit Jahren innerhalb der MaRisk und BAIT normiert.

Wie der Umsetzungsstand der Prinzipien derzeit tatsächlich aussieht, wird sich unter Umständen anhand der Rückmeldungen aus der Bankenbranche innerhalb der laufenden Konsultationsphase ablesen lassen, denn es ist nicht davon auszugehen, dass neue Anforderungen moniert werden, die von den Banken bereits vollumfänglich implementiert wurden. Die Vergangenheit hat indessen aber immer wieder gezeigt, dass in Konsultationsphasen vor allem solche Sachverhalte kritisch hervorgehoben wurden, die mit

einem Mehraufwand für die Banken einhergingen. Somit kann es durchaus sein, dass die Rückmeldungen und die Anzahl der darin enthaltenen Kritikpunkte einen Einblick in mögliche Umsetzungsdefizite bei den Baseler Empfehlungen zum Umgang mit operationellen Risiken geben.

Unabhängig davon ist der angestrebte Austausch des BA mit den Banken als förderlich zu betrachten. So bittet der Baseler Ausschuss die einzelnen Banken darum, ihre jeweiligen Stellungnahmen zu den Konsultationspapieren um die eigenen Erfahrungen während der Corona-Krise zu erweitern, damit gegebenenfalls zusätzliche Ergänzungen bei den beiden Prinzipienkatalogen vorgenommen werden können, falls bisher nicht adressierte operationelle Problemstellungen erkannt werden sollten.²²⁾

Fußnoten

- 1) Vgl. auch nachfolgend Basel Committee on Banking Supervision: Consultative Document – Revisions to the principles for the sound management of operational risk – BCBS 508, S. 1–2. Zu notwendigen aufsichtsrechtlichen Lockerungen zur Sicherstellung der Kreditvergabe an die Realwirtschaft während der Corona-Pandemie siehe Waschbusch, Gerd; Kiszka, Sabrina: Die bremsende Wirkung der Corona-Krise auf die finale Umsetzung der Krisenregularien von Banken, abrufbar unter: <https://www.tax-legal-excellence.com/die-bremsende-wirkung-der-corona-krise-auf-die-finale-umsetzung-der-krisenregularien-von-banken/>, Stand: 11.09.2020.
- 2) Vgl. BCBS 508.
- 3) Vgl. Basel Committee on Banking Supervision: Consultative Document – Principles for operational resilience – BCBS 509.
- 4) Vgl. BCBS 508, S. 1, Fn. 4.
- 5) Vgl. BCBS 509, S. 4; Financial Stability Board: Recovery and Resolution Planning for Systemically Important Financial Institutions, abrufbar unter: https://www.fsb.org/wp-content/uploads/r_130716a.pdf, S. 7, Stand: 11.09.2020.
- 6) Vgl. BCBS 508, S. 1 i. V. m. S. 16–17.
- 7) Vgl. hierzu sowie nachfolgend Basel Committee on Banking Supervision: Review of the Principles for the Sound Management of Operational Risk – BCBS 292, S. 1–5; Kiszka, Sabrina: Die Steuerung operationeller Risiken in Kreditinstituten, Wiesbaden 2018, S. 132.
- 8) Vgl. BCBS 508, S. 1.
- 9) Vgl. zu den Ausführungen hinsichtlich des Modells der drei Verteidigungslinien Kiszka, Sabrina: Die Steuerung operationeller Risiken in Kreditinstituten, Wiesbaden 2018, S. 47 m. w. N.
- 10) Vgl. BCBS 508, S. 6.
- 11) Vgl. zu den erweiterten Anforderungen an das Modell der drei Verteidigungslinien BCBS 508, S. 3.
- 12) Vgl. BCBS 508, S. 6–7.
- 13) Vgl. zu den Inhalten der Erklärung zur Risikoneigung bzw. Risikotoleranz BCBS 508, S. 9.
- 14) Vgl. hierzu sowie nachfolgend BCBS 508, S. 12.
- 15) Vgl. hierzu sowie nachfolgend BCBS 508, S. 14.
- 16) Vgl. hierzu sowie nachfolgend BCBS 508, S. 18.
- 17) Vgl. BCBS 508, S. 16.
- 18) Vgl. zu dieser Thematik BCBS 508, S. 16–17.
- 19) Vgl. BCBS 508, S. 18–19.
- 20) Vgl. hierzu sowie nachfolgend BCBS 509, S. 1–2.
- 21) Vgl. BCBS 509, S. 3.
- 22) Vgl. hierzu BCBS 509, S. 9.