Regulatorische Agenda im ersten Halbjahr 2019:

Wesentliche Neuerungen und Umsetzungsprioritäten für deutsche und österreichische Banken

Schlagworte: PSD II, Third-Party-Provider, Open Banking, FMA Leitfäden IT-Sicherheit, Cyber Sicherheit Plattform, Netz- und Informationssicherheitsgesetz, Betreiber wesentlicher Dienste, schwerwiegende Betriebs- oder Sicherheitsvorfälle

Dr. Patrik Buchmüller
ist freiberuflicher Unternehmensberater und Hochschuldozent (u.a. Lehrbeauftragter für die Fachhochschule Worms und Duale Hochschule Baden-Württemberg, Ravensburg) mit langjähriger Erfahrung als Risikomanager bei privaten und öffentlichen Banken in Deutschland sowie als BaFin-Mitarbeiter mit Zuständigkeit für das operationelle Risiko.
patrik.buchmueller@marisk.academy

Mag. Georg Puntus, LLM
ist Referent bei der österreichischen Finanzmarktaufsicht (FMA), in der Abteilung für Horizontale Bankaufsichtsangelegenheiten.

Mag. Dr. Georg Tuder
ist Referent bei der österreichischen Finanzmarktaufsicht (FMA), in der Abteilung für die Aufsicht über Aktienbanken, Zahlungsinstitute und Einlagensicherungen. Davor war er als Universitätsassistent und Lektor am Institut für Recht der Wirtschaft an der Universität Wien tätig.

Dieser Beitrag gibt einen Überblick über wichtige regulatorische Umsetzungsthemen für Banken in Deutschland und Österreich mit Fokus auf die Fortentwicklung von Säule I und Säule II sowie die regulatorischen Anforderungen zu IT-Risikomanagement und Cybersecurity. Neben der Vorstellung der Aufsichtsplanungen für 2019 und aktueller Vorgaben zum Stresstesting wird auf die Arbeiten zur Umsetzung von Basel III sowie die Fortentwicklung von bankaufsichtlichen und branchenübergreifenden IT-Rechtsnormen eingegangen. Die im Februar 2019 veröffentlichten EBA-Leitlinien zum Outsourcing und Vorgaben PSD II Umsetzung werden detaillierter vorgestellt. Abschließend wird die aktuelle Risikolage im Bankensektor mit Fokus auf Konjunkturrisiken, Immobilienmarkt und Brexit kommentiert. Im Gegensatz zu den üblichen Darstellungen der regulatorischen Agenda setzt dieser Beitrag bewusst Schwerpunkte auf wenige, wichtige Themen und berücksichtigt die Risikosituation der Institute. [1]

1. Einführung

Jedes Jahr stellt sich für die Risikomanager in den Instituten die Frage, wie sie ihre knappe Zeit auf die Umsetzung der regulatorischen Neuerungen aufteilen sollen. Dieser Beitrag möchte hierzu eine Hilfestellung geben. Abbildung 1 gibt einen Überblick über die aus Sicht der Autoren wichtigsten regulatorischen Entwicklungen sowie Hauptrisiken für die Banken in Deutschland und stellt diese nach Wichtigkeit und zeitlicher Dringlichkeit entsprechend dem üblichen „Eisenhower-Diagramm“ dar.

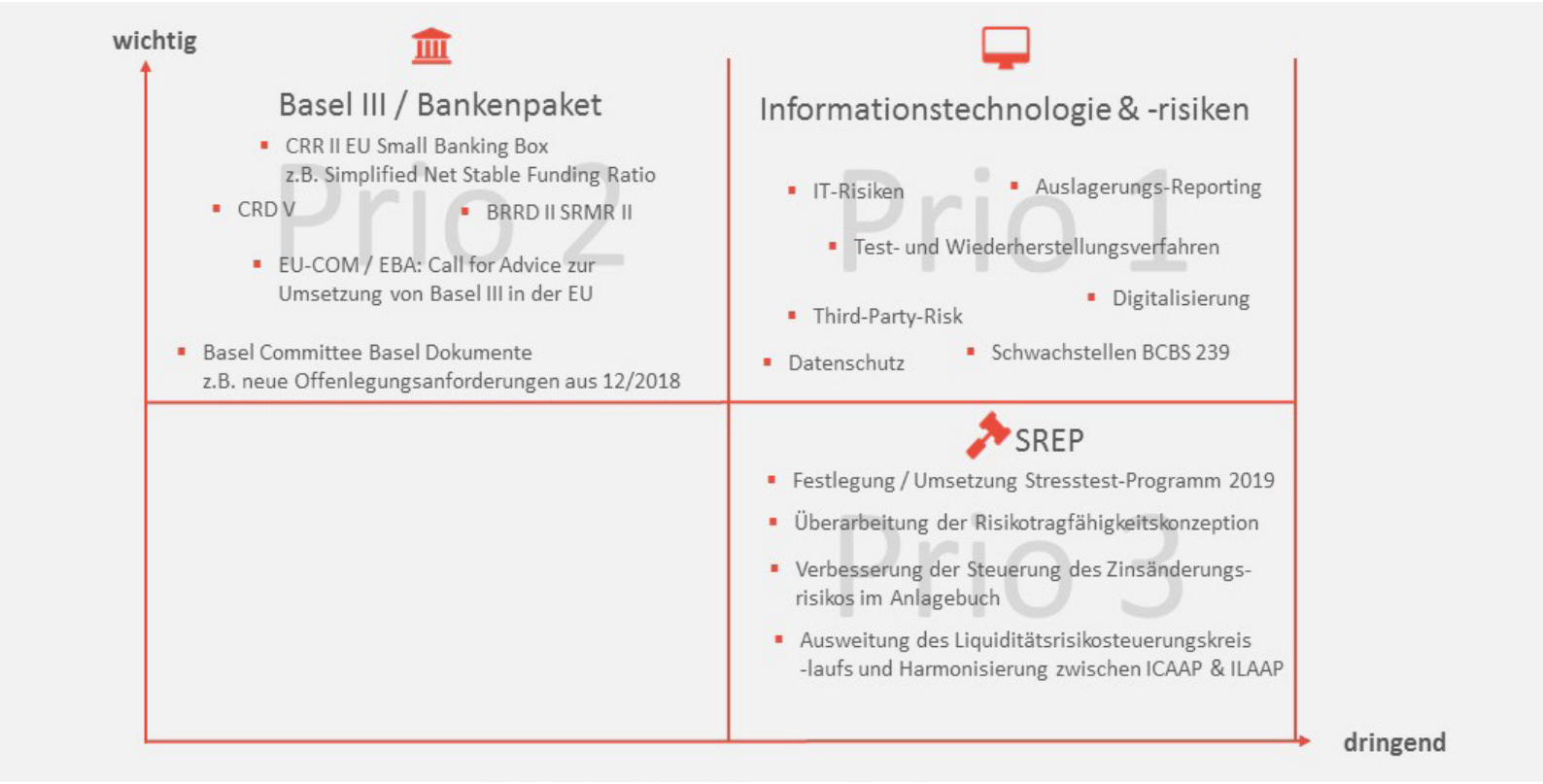

Abb. 1 Potentielle Schwerpunktthemen für die Institute in 2019

Quelle: Buchmüller/Mährle/Rambock (2019) [76]

Im Folgenden konzentrieren wir uns auf die bereits visuell dargestellten Themenbündel und erweitern unseren Blick auf Umsetzungsfragen in Österreich, die sehr ähnlich zu Deutschland sind. In den Abschnitten 2-4 möchten wir insbesondere kleineren Instituten einen Kurzüberblick über die wichtigsten Entwicklungen zu geben. Abschließend geben wir in Abschnitt 5 auf Basis einer kurzen Sichtung der Hauptrisiken in 2019 aus betriebswirtschaftlicher Perspektive unsere Empfehlungen zur Priorisierung der konkreten Umsetzungshandlungen.

2. Agenda von BaFin / Bundesbank, FMA, EBA und EZB im Überblick

2.1 Prioritätensetzung von EBA, EZB-Bankenaufsicht und BaFin

Die Europäische Bankenaufsichtsbehörde (EBA) hat im Oktober 2018 ein 32-Seiten starkes Arbeitsprogramm für 2019 veröffentlicht.[2] Als strategische Prioritäten nennt sie dabei in dieser Reihenfolge:

1. Basel III Umsetzung in der EU
2. Stärkung ihres Verständnisses der Finanzinnovationen
3. Datensammlung & -analyse
4. Umzug nach Paris
5. Stärkung der Verlustabsorptionskapazität im EU-Bankensystem.

Abschnitt 4 dieses Beitrags erläutert die Arbeiten von EBA und EU-Kommission zum CRR II / CRD V / BRRD II Paket sowie zur Umsetzung der neuen Baseler Rahmenvereinbarung. Diese Aktivitäten wurden seitens der EBA als wichtigste strategische Priorität für das laufende Jahr eingewertet.

Die EZB-Bankenaufsicht hat dagegen eine eher knappe Auflistung ihrer aufsichtlichen Prioritäten veröffentlicht [3]. Diese wurden aus den Risikoeinschätzungen der Aufsicht abgeleitet, die v.a. die geopolitischen und IT-Risiken neben non-performing loans und Preisverwerfungen auf den Finanzmärkten als wichtigste Risikofaktoren identifizieren.[4] Die EZB hat folgende konkrete Aufsichtsmaßnahmen angekündigt: Im Bereich Kreditrisiko u.a. Nacharbeiten zur NPL Guidance und on-site Prüfungshandlungen zu Immobilienkrediten und Leveraged Finance. Im Bereich Risikomanage-

ment u.a. die Finalisierung des TRIM Guide, Prüfungshandlungen zur Verbesserung des ICAAP & ILAAP der Banken sowie on-site Prüfungen zu IT-Risiken & Fortsetzung des Cyberincident Reporting. Zu beachten ist, dass der jährliche aufsichtliche Stresstest der EZB 2019 mit besonderem Fokus auf das Liquiditätsrisiko durchgeführt wird. Unter dem Schlagwort „Multiple Risk Dimensions" hat die EZB-Bankenaufsicht zudem die besondere Überwachung der Brexit-Vorbereitungen der ihrer Aufsicht unterstehenden Institute, einen aufsichtlichen Dialog zur Umsetzung der Vorgaben zum Zinsänderungsrisiko im Anlagebuch sowie intensivere Prüfungen zum Handel und Marktrisiko bei einzelnen Instituten avisiert. Zuletzt hat der neue Vorsitzende der EZB-Bankenaufsicht, Andrea Enria bei der Vorstellung des Jahresberichtes der EZB-Bankenaufsicht im Europäischen Parlament am 21.03.2019 diese Prioritäten bekräftigt und gleichzeitig neue Maßnahmen zur besseren Beaufsichtigung von IT- & Cyberrisiken angekündigt. Auf Grundlage des seit 2017 bestehenden Cyber Incident Reporting und v.a. des Self Assessments der beaufsichtigten Institute zu ihren IT-Risiken hat die EZB-Bankenaufsicht eine Reihe horizontaler Analysen durchgeführt. Die Ergebnisse werden nun in die EZB-Prüfungskampagne zu IT-Risiken im Rahmen der Vor-Ort-Prüfungen im laufenden Jahr einfließen.

Die BaFin hat am 18.12.2018 erstmals die zusammen mit der Bundesbank festgelegten Schwerpunkte ihrer Aufsicht über die weniger bedeutenden Institute (less significant institutions) in Deutschland für das Jahr 2019 veröffentlicht. [5].

Dabei wurden folgende sechs Risiken genannt:

1) Ertragsrisiken;
2) Zinsrisiken,
3) Digitalisierung/IT-Risiken,
4) Kreditrisiken (darunter Entwicklungen im Immobiliensektor),
5) Länderrisiken
6) Rechts- und Reputationsrisiken.

Für die Institute ist es besonders interessant zu wissen, dass sich die deutsche Bankenaufsicht einerseits fokussiert auf den LSI-Stresstest 2019 mit Überprüfung der Auswirkungen auf Ertragslage und Zinsänderungsrisiken und andererseits auf die Prüfung von IT-Systemen und der dazugehörigen IT-Prozesse. Ergänzend hat die BaFin auch Schwerpunkte ihrer gesamten Tätigkeit über die Bankenaufsicht hinaus veröffentlicht und dabei insbesondere die Themen Digitalisierung und Brexit genannt.[6]

2.2 Prüfschwerpunkte der FMA & rechtliche Entwicklungen in Österreich

Die FMA hat am 28.11.2018 ihre Prüfschwerpunkte für das Jahr 2019 veröffentlicht.[7] Dabei wurde mit Hilfe einer mittelfristigen Risikoanalyse (2019 – 2024) versucht, jene Bereiche des Finanzmarktes zu identifizieren, welche die Regulierung und Aufsicht in den kommenden Jahren vor besonders große Herausforderungen stellen werden. Auf Grundlage dieser Analyse wurden im Wesentlichen folgende sechs Themenbereiche als Prüfungs- und Aufsichtsschwerpunkte für das Jahr 2019 von der FMA festgelegt:

- Digitalisierung am Finanzmarkt: digitalen Wandel unterstützen, Risiken managen
- Einsatzbereitschaft für künftige Krisenfälle: Fitness der FMA und des Finanzplatzes für schwerere Zeiten verbessern
- Nachhaltigkeit der Geschäftsmodelle im Wirtschaftsaufschwung: vorausschauend denken, antizyklisch handeln
- Governance der Unternehmen: die Widerstandsfähigkeit in einem sich ändernden Risikoumfeld stärken
- Umfassende Risikobetrachtung: mit starker Compliance und konsequenter Geldwäscheprävention die Stabilität der beaufsichtigten Unternehmen erhöhen
- Kollektiver Verbraucherschutz: mehr Risikobewusstsein durch gezielte Information, mehr Vertrauen durch Produkttransparenz, mehr Fairness durch höchste Qualität im Vertrieb [8]

> Entsprechend des § 107v Abs. 99 BWG trat diese BWG-spezifische Compliance Funktion mit 01.01.2019 in Kraft

Zu jedem dieser Schwerpunkte hat die FMA eine Reihe konkreter Maßnahmen definiert, mit welchen eine entsprechende Operationalisierung sichergestellt werden soll. So wird etwa die Einsatzbereitschaft der österreichischen Banken bei Eintritt eines Krisenfalles (z.B. Hackerattacke auf das Kernbankensystem) unter anderem durch eine „Cyber Incident Simulation" überprüft. Ziel dieser Simulation ist u.a. die Sensibilisierung des österreichischen Bankensektors auf die gesteigerten Sicherheitsrisiken, welche sich aus der zunehmenden Bedeutung von Informationstechnologien und ausgelagerten IT-Services ergeben. Zudem soll die Übung dazu dienen, eine bessere Einschätzung des Grades der Vorbereitung der österreichischen Kreditinstitute hinsichtlich der Behandlung von Cyberattacken zu erlangen.

Ein weiterer Schwerpunkt wird überdies auf die Einhaltung der Wohlverhaltensregeln zum Schutz der Verbraucher beim Einsatz digitaler Instrumente und Techniken, wie etwa Robo-Advise, gelegt. Überdies ist eine zielgerichtete Informationsoffensive zu den spezifischen Risiken digitaler Finanzprodukte, insbesondere zu Krypto-Assets, von Seiten der FMA geplant.

Bereits im September 2017 veröffentlichte die EBA die Final Reports ihrer überarbeiteten Guidelines on internal Governance [9] und die in Kooperation mit der ESMA überarbeitenden Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU.[10] Diese Guidelines sind seit dem 30.06.2018 bereits anwendbar und lösten auch korrespondierende Umsetzungsschritte des Gesetzgebers und der zuständigen Behörden aus. Der Anwendungsumfang der Guidelines richtet sich gemäß Art. 16 Abs. 3 der EBA-Verordnung [11] nach der jeweiligen Compliance-Erklärung der zuständigen Behörde.[12] Signifikante Kreditinstitute, die der direkten Aufsicht der EZB unterliegen, müssen die Guidelines in dem Umfang anwenden, indem sich die EZB als „compliant" zu den neuen Guidelines erklärt hat. Weniger bedeutende Institute im Sinne der SSM-VO, die der Aufsicht der FMA unterliegen, richten sich nach der Erklärung der FMA. Grundsätzlich ist die Implementierung dieser Leitlinien aufgrund des Inkrafttreten Datums bereits Mitte 2018 erfolgt. Jedoch sehen die Guidelines eine Umsetzungsfrist vor, da die Überprüfung der Eignung bestehender Leitungsorganmitglieder erst im Rahmen der ordentlichen, regelmäßigen Überprüfung erfolgen muss. Darüber hinaus ergeben sich auch aufgrund nationaler Bestimmungen weitere Übergangsfristen.

In diesem Zusammenhang ist nicht zu übersehen, dass ein Teilbereich der Guidelines Einzug in das Bankwesengesetz (BWG) genommen hat.[13] Der Gesetzgeber hat sich damit zum Ziel gesetzt, die Vorgaben der Guidelines, angepasst an den österreichischen gesetzlichen Rahmen, zu präziseren und gleichzeitig Rechtsicherheit für die Aufsichtsbehörden (EZB und FMA) sowie die Kreditinstitute zu schaffen.[14] Im Zuge dieser Normierung wurde auch eine Implementierungsfrist für diverse Vorgaben vorgesehen, die sicherstellen sollen, dass die Institute die neuen strikten Regularien effektiv umsetzen können. Dies umfasst auch die Einführung einer neuen umfassenden „BWG-Compliance-Funktion", die für alle Institute von erheblicher Bedeutung ist.[15] Eine solche getrennte BWG-Compliance-Organisationseinheit, die sich auf diese Aspekte bezieht, war dem österreichischen Aufsichtsrecht bisher nicht immanent, da sich die organisatorischen Vorgaben auf die Aufgaben des„WAG-Compliance Beauftragten" [16] beschränkten. [17] Entsprechend des § 107w Abs. 99 BWG [18] trat diese BWG-spezifische Compliance- Funktion mit 01.01.2019 in Kraft. In ihrem Zuständigkeitsbereich obliegt, „die ständige Überwachung und regelmäßige Bewertung der Angemessenheit und Wirksamkeit der [Compliance] Grundsätze und Verfahren" [19]. Im Weiteren beurteilt sie die Mängelbehebungen in den Compliance relevanten Prozessen und berät dabei auch die Geschäftsleitung.[20]

Praxistipp

Auch die kleineren Institute sollten bei der Fortentwicklung ihrer Risikotragfähigkeitskonzeptionen und ihres ILAAP die Leitlinien der EBA zum SREP, Stresstesting und Zinsänderungsrisiko im Anlagebuch sichten ebenso wie die neuen EZB ICAAP- und ILAAP-Leitfaden und die Methodik zum Liquiditätsrisikostresstest der EZB.

Auch die Änderungen der Vorgaben zur Aufsichtsrats- und Ausschussbesetzung mit unabhängigen Mitgliedern wurden in Österreich nicht mit 30.06.2018 vollständig implementiert. Vielmehr hat der österreichische Gesetzgeber eine Rechtsgrundlage geschaffen, und dabei die Anwendung der EBA Guidelines on internal Governance eingeschränkt. Grundsätzlich sind in die Aufsichtsräte aller Kreditinstitute [21] zumindest ein unabhängiges Mitglied zu bestellen. Alle Institute von erheblicher Bedeutung im Sinne des § 5 Abs. 4 BWG haben darüber hinaus zumindest noch ein weiteres unabhängiges Mitglied zu bestellen. Während die Unabhängigkeitsanforderungen für die Mehrheit der Risikoausschussmitglieder und dessen Vorsitzenden von systemrelevanten Kreditinstituten umgesetzt wurde, stellte die spiegelbildliche Vorgabe für den Nominierungsausschuss einen zu tiefen Einschnitt in die Rechte der Gesellschafter dar.[22] Weiters wurde eine Umsetzungsfrist bis 01.07.2019 gesetzt.[23] Sofern sich die personelle Zusammensetzung des Aufsichtsrates aber innerhalb dieses Zeitraums verändert, sind die Vorgaben hinsichtlich der Unabhängigkeit bereits zu berücksichtigen. Die unterliegende Ratio ist, dass die Institute eine gegebenenfalls notwendige Nominierung von unabhängigen Mitgliedern im Rahmen der ordentlichen Hauptversammlung, die in aller Regel im ersten Halbjahr stattfindet, durchführen können.[24]

2.3 Umsetzung der neuen Säule II Vorgaben

Leider hat die EZB-Bankenaufsicht die in den vergangenen Jahren jeweils im Dezember veröffentlichte Überblickspublikation zu den Ergebnissen des SREP Stand 31.03.2019 (noch) nicht auf ihrer Internetseite veröffentlicht. Stattdessen hat die EZB in ihrem Jahresbericht 2019 in Kurzform gängige Moniten aus den Vor-Ort-Prüfungen zu den einzelnen Risikoarten genannt.[25] So lagen beim IT-Risiko die besonders schwerwiegenden Prüfungsfeststellungen demnach mehrheitlich beim Management des IT-Betriebs (ungeeignete Störungsbehebungsverfahren, Fehlen umfassender und genauer Bestandsübersichten), der Verwaltung von Zugriffsrechten (ineffektive Rezertifizierungsverfahren, unzureichende Trennung der Verantwortlichkeiten), beim Datenqualitätsmanagement (Schwächen in den betrieblichen Prozessen zur Validierung manueller Eingaben) sowie beim IT-Sicherheitsmanagement (verzögerte und unangemessene Erkennungs- und Korrekturmaßnahmen). Beim Liquiditätsrisiko betreffen die Moniten am häufigsten die Risikomessung und das Stresstesting:

So nennt die EZB eine generell unzureichende Risikomessung, Schwächen bei der Schätzung des Run-off Profils der Finanzprodukte, Fehler bei der LCR-Berechnung oder dass die Stresstest-Szenarien für das Liquiditätsrisiko nicht zur Komplexität des Instituts passen. Abb. 2 gibt einen Überblick über die Vor-Ort-Prüfungen der EZB-Bankenaufsicht bei den ihrer direkten Aufsicht unterstehenden Instituten in den letzten beiden Jahren. Die einzelnen Risikokategorien, die im Prüfungsschwerpunkt lagen, verdeutlichen, dass neben den einzelnen Risikoarten zunehmend auch die anderen SREP Schwerpunkte wie Governance sowie das Geschäftsmodell und die Ertragskraft geprüft werden. Die Institute müssen sich darauf einrichten, dass die EZB zunehmend ganzheitlich prüft.

Neben den Bereichen IT und Auslagerungen, auf die wir noch besonders eingehen, sind über die Überarbeitung der Risikotragfähigkeitskonzeptionen hinaus in Säule II v.a. auch die Themen Stresstesting, Zinsänderungsrisiko und Liquiditätsrisiko von besonderer Bedeutung. Hierzu hilfreich als Orientierungshilfen sind die EBA-Leitlinien zum SREP, Zinsänderungsrisiko im Anlagebuch und Stresstesting, die nach ihrer Veröffentlichung am 19.07.2018 mittlerweile auch in deutscher Sprache auf der EBA-Homepage vorliegen.[26] Während die überarbeiteten SREP- und Stresstesting-Leitlinien bereits seit 01.01.2019 gültig sind, treten die IRRBB-Leitlinien erst zum 30.06.2019 in Kraft. Gerade aufgrund der sich drehenden Konjunktur enthält das mit

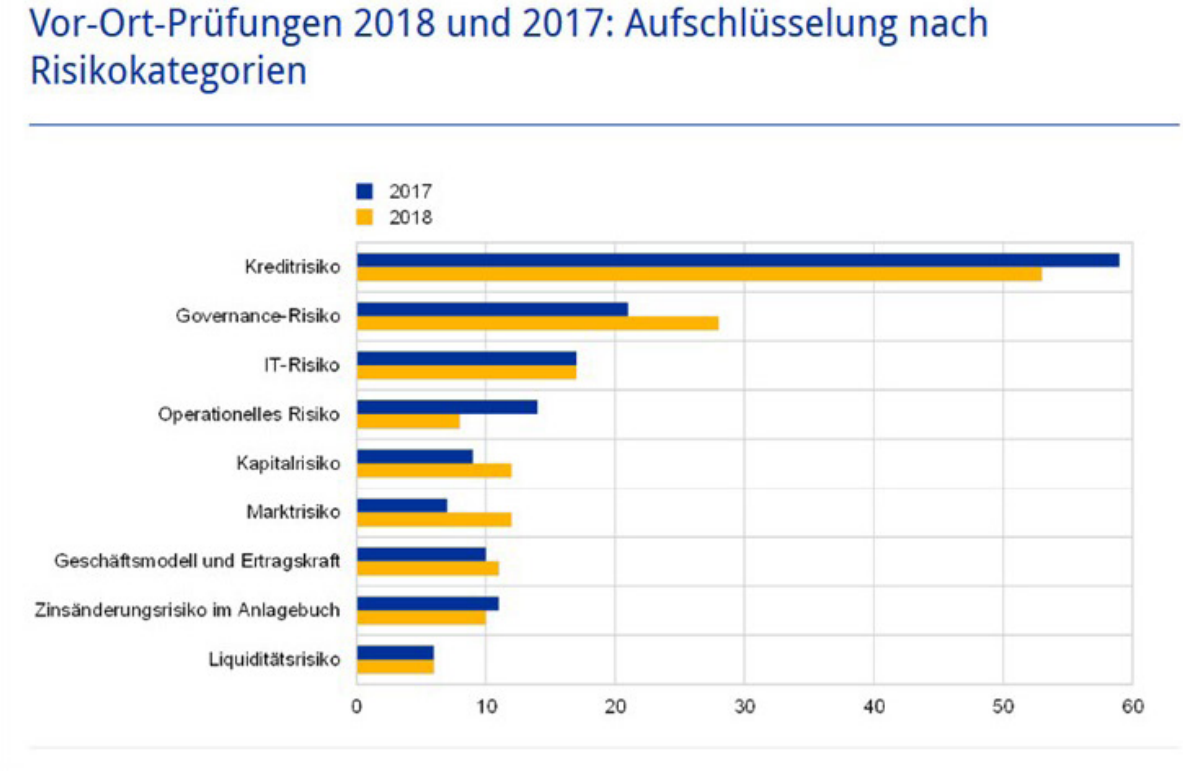

Abb. 2 Schwerpunkte der EZB bei Vor-Ort-Prüfungen

Quelle: EZB-Jahresbericht zur Aufsichtstätigkeit 2018, Kap. 1.6 [25]

Inkrafttreten der neuen EBA Stresstesting Guidelines geforderte Stresstesting-Programm eine neue Bedeutung: Es ist dringend zu empfehlen, dem Gesamtvorstand entsprechend der Abschnitte 4.1. und 4.2 der neuen EBA-Stresstest-Leitlinien jährlich die Liste der geplanten Stresstests zur Genehmigung vorzulegen.

Die Umsetzung zum Stresstesting und Zinsänderungsrisiko sollte mit den Anpassungen der Risikotragfähigkeitskonzeption verbunden werden. Zu beachten sind dabei in Deutschland der bereits im Mai 2018 von BaFin und Bundesbank veröffentlichte neue RTF-Leitfaden[27] sowie im gesamten Euro-Raum die im November 2018 von der EZB-Bankenaufsicht veröffentlichten finalen ICAAP- & ILAAP Guides.[28] Diese EZB-Leitfäden sollten auch die Banken unter direkter BaFin-Aufsicht sichten, da darin insbesondere zur Fortentwicklung des ILAAP wertvolle Hinweise enthalten sind.[29] In Deutschland hat die Bundesbank ein Überblickspapier zur „Range of Practice" der bisher von den LSI zwischen 2015 und 2017 verwendeten ICAAP-Ansätze veröffentlicht.[30] Diese Publikation, mit der die über das Säule II Meldewesen erhaltenen Informationen ausgewertet werden, kann gerade den kleinen Instituten helfen, bei der Analyse, wo sie vor der Anpassung ihrer Ansätze auf die neuen Vorgaben stehen. Am 06.02.2019 hat die EZB Bankenaufsicht auf 61 Seiten ihre methodische Vorgaben zur aufsichtlichen Sensitivitätsanalyse des Liquiditätsrisikos im EZB-Stresstest 2019 veröffentlicht.[31] Auch die Lektüre dieses Papiers ist für alle Institute lohnenswert zur Sichtung der aufsichtlichen Vorgehensweise, aus der möglicherweise Anleihen für das institutsinterne Stresstesting gezogen werden können. In Deutschland muss allerdings der Fokus der kleineren und mittleren Institute weiterhin primär auf dem Zinsänderungsrisiko liegen, zu dem BaFin und Bundesbank am 01.04.19 ihren mit der Niedrigzinsumfrage verbundenen LSI-Stresstest gestartet haben.[32]

3. Verstärkte Regulierung zu IT-Risiken und Auslagerungen

3.1. Neue EBA-Leitlinien zu Informations- und Kommunikationsrisiken

Wie eingangs erläutert, ist sowohl durch die nationalen Behörden als auch seitens der EZB-Bankenaufsicht mit nochmals verstärkten Prüfungshandlungen im Bereich IT zu rechnen. Dies kann neben den üblichen Feststellungen zur Nichterfüllung aufsichtsrechtlicher Vorgaben v.a. zu Kapitalaufschlägen im SREP führen. Im SREP wird die IT-Ausstattung einerseits unter dem Blickwinkel der Geschäftsmodellanalyse geprüft. Hierunter fällt auch die Prüfung der

Digitalisierungsanstrengungen der Institute. Andererseits beurteilt die Aufsicht die IT der Banken und deren Steuerung auch in den übrigen SREP-Prüfungsdimensionen wie Governance & Kontrollsystem, Angemessenheit der Kapitalausstattung in Relation zu den Risiken und Liquiditätsausstattung & -steuerung. Als Bewertungskriterien für die, von der EBA als Informations- und Kommunikationsrisiken (IKT-Risiken) bezeichneten IT-Risiken, sind die bereits gültigen EBA-Leitlinien für die IKT-Risikobewertung im Rahmen des SREP heranzuziehen.[33] Besonders wichtig in diesem Zusammenhang sind in 2019 nun die neuen EBA-Leitlinien zum Management operationeller und sicherheitsrelevanter Risiken aus der PSD II, die EBA-Leitlinien zu Auslagerungen sowie zu IT-Risiken (ICT and Security Risk Management).

Am 13.12.2018 hat die EBA die englischsprachigen Draft Guidelines on ICT and Security Risk Management veröffentlicht.[34] Mit einer Veröffentlichung der finalen Leitlinien ist bis Ende September 2019 zu rechnen. Nach der üblichen 6-Monatsfrist ist demnach mit einem Inkrafttreten im Frühjahr 2020 zu rechnen. Diese neuen EBA-Leitlinien fordern eine verstärkte Überwachung des Third Party Risk (u.a. durch Meldungen von IT-Sicherheitsvorfällen von Auslagerungsunternehmen an das auslagernde Institut) und eine Einbindung des Vorstandes durch explizite Vorlage der IT-Risikobewertungen und des Ad-hoc-Reportings des IT-Sicherheitsbeauftragten. Neu gegenüber den deutschen BAIT (bankaufsichtliche Anforderungen an die IT) sind spezifische Anforderungen an Informationssicherheitsrisiko-Szenarien, die sonst nur aus dem Sanierungsplan (auf Gruppenebene) bekannt sind und Vorgaben zur Krisenkommunikation. Zudem werden eine eigene „ICT project management policy“ und spezifische Schulungsmaßnahmen zum IT-Risiko gefordert. Zwar wird im Text des Leitlinienentwurfs darauf hingewiesen, dass die Umsetzung proportional sein soll, konkrete Öffnungsklauseln für kleinere Institute sind im Regelungstext bisher aber nicht enthalten. Nach den im letzten Jahr veröffentlichten Aussagen der BaFin werden alle EBA-Leitlinien auch ohne weitere rechtliche Umsetzung in Deutschland Gültigkeit besitzen, es sei denn die BaFin trifft anderslautende Entscheidungen im Einzelfall.[35]

3.2. EBA-Leitlinien zu Auslagerungen

Der finale Report der EBA Guidelines on Outsourcing wurde am 25.02.2019 in englischer Sprache veröffentlicht.[36] Die Leitlinien werden am 30.09.2019 in Kraft treten und zuvor nach Abschluss der Übersetzungsarbeiten in allen Amtssprachen der EU im EU-Amtsblatt veröffentlicht. Dies setzt auch den „Comply-or-Explain“- Prozess gem. Art. 16 Abs. 3 der EBA-Verordnung in Kraft. Bereits im Juni 2018 veröffentlichte die EBA einen Konsultationsentwurf [37] zu diesen Guidelines, der dazu diente, Rückmeldungen aus der Industrie zu erhalten.[38] Der Aufbau der Guidelines wurde dem Grunde nach überarbeitet, um den Fokus der Vorgaben auf die wesentlichen („critical or important“) Auslagerungen zu legen.[39] Somit wurde der Anwendungsbereich der Guidelines nochmals nachgeschärft und es ist nunmehr klargestellt, dass auch nicht wesentliche Auslagerungen der allgemeinen Steuerung von „third-party-risk“ unterliegen.[40] Im Weiteren finden sich noch vereinzelte Vorgaben zu allen Auslagerungsverträgen, wie beispielsweise hinsichtlich der Dokumentation [41] und den Prüf-, Zugangs- und Informationsrechten [42]. Im Vergleich zum Konsultationsentwurf wurden die Vorgaben jedoch deutlich eingeschränkt. So sah das Konsultationspapier[43] noch umfassende Mindestvertragsinhalte für nicht wesentliche Auslagerungen vor, während die finale Version sich damit begnügt, mit Ausnahme der Prüf-, Zugangs- und Informationsrechte, für diese Auslagerungsverträge lediglich die schriftliche Vertragsform zu verlangen.[44] Nachgebessert wurde auch im Bereich der Übergangsfristen. Diese sehen vor, dass die Dokumentation (Register) sowie die Anpassung der bestehenden Verträge grundsätzlich mit 31.12.2021 abgeschlossen sein müssen, während ab dem 30.09.2019 neue oder angepasste Verträge den neuen Vorgaben entsprechen müssen.[45]

Zusammenfassend bleibt festzuhalten, dass die neuen EBA Guidelines on Outsourcing zwar auf Basis der CEBS Guidelines on Outsourcing aus dem Jahr 2006 basieren, diese aber durch die deutlich granularere Ausgestaltung weiterentwickeln. Insbesondere die Vorgaben zur Führung eines Registers aller Auslagerungen (unerheblich von ihrer Wesentlichkeit) stellen eine bedeutende Neuerung dar.

> Zwar wird im Text des Leitlinienentwurfs darauf hingewiesen, dass die Umsetzung proportional sein soll, konkrete Öffnungsklauseln für kleinere Institute sind im Regelungstext bisher aber nicht enthalten. Nach den im letzten Jahr veröffentlichten Aussagen der BaFin werden alle EBA-Leitlinien auch ohne weitere rechtliche Umsetzung in Deutschland Gültigkeit besitzen, es sei denn die BaFin trifft anderslautende Entscheidungen im Einzelfall [35].

3.3. EBA Leitlinien zum Management operationeller und sicherheitsrelevanter Risiken

Mit der Payment Services Directive II (PSD II) [46], welche von den Mitgliedstaaten bis 13.01.2018 [47] in das jeweils nationale Recht zu implementieren war, ist es zu weitreichenden Änderungen am europäischen Zahlungsverkehrsmarkt gekommen. Einerseits durch die neu in den Anwendungsbereich aufgenommenen Third-Party-Provider (TPP), sprich den Zahlungsauslöse- und Kontoinformationsdienstleistern sowie des damit im Zusammenhang stehenden „Open Bankings“ und andererseits auch durch die neuen rechtlichen Anforderungen im Zusammenhang mit operationellen und sicherheitsrelevanten Risiken.[48] Mit diesem vollständig neuen Regelungskomplex innerhalb der PSD II möchte der europäische Gesetzgeber v.a. den Sicherheitsrisiken, welche sich aus der zunehmenden technischen Komplexität von elektronischen Zahlungen sowie deren stetig wachsenden Volumen ergeben, entgegentreten. Die in Art. 95 und 96 PSD II [49] vorgesehenen Bestimmungen haben dabei den Zweck, Schäden durch Betriebs- und Sicherheitsvorfälle für Nutzer, andere Zahlungsdienstleister oder Zahlungssysteme, in Zukunft auf ein Minimum zu reduzieren. Um den betroffenen Zahlungsdienstleistern ein besseres Verständnis darüber zu geben, welche Verpflichtungen für sie durch diese Bestimmungen in der Folge bestehen, hat die EBA mehrere Leitlinien veröffentlicht:

- EBA Guidelines on the Security Measures for Operational and Security Risks (EBA/GL/2017/17)
- EBA Guidelines on Major Incidents Reporting (EBA/GL/2017/1)
- EBA Guidelines on fraud reporting (EBA/GL/2018/05)

Die Zahlungsdienstleister sind nach Art. 95 Abs. 1 PSD II nunmehr dazu angehalten, angemessene Risikominderungsmaßnahmen und Kontrollmechanismen zur Beherrschung ihrer operationellen sowie sicherheitsrelevanten Risiken vorzusehen, welche im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten bestehen. Die dabei vorgesehenen Maßnahmen müssen dabei für die jeweils bestehenden Sicherheitsrisiken angemessen sein. Der von den Zahlungsdienstleistern festgelegte Rahmen von Maßnahmen soll insbesondere gewährleisten, dass operationelle sowie sicherheitsrelevante Risiken reduziert werden und dass bei Eintritt eines solchen Vorfalls ein wirksames Verfahren zu dessen Beseitigung besteht. Zusätzlich zu den hierbei auferlegten Verpflichtungen haben die Zahlungsdienstleister der zuständigen Aufsichtsbehörde zumindest einmal jährlich eine aktualisierte und umfassende Bewertung der operationellen und sicherheitsrelevanten Risiken zu übermitteln. Die Bewertung hat zudem auch Auskunft über die Angemessenheit der ergriffenen Risikominderungsmaßnahmen und Kontrollmechanismen zu geben. Damit die Regelungen des Art. 95 PSD II durch die Zahlungsdienstleister auch in entsprechender Weise umgesetzt werden, hat die EBA die Leitlinien on the Security Measures for Operational and Security Risks entwickelt. Diese legt u.a. die Anforderungen für die Festlegung, Anwendung sowie die Überwachung der Sicherheitsmaßnahmen fest.[50]

Praxistipp

Nach Redaktionsschluss dieses Beitrags hat die EZB-Bankenaufsicht am 08.04.2019 die Ergebnisse zum SREP 2018 veröffentlicht. Im neuen SREP Methodology Booklet der EZB sind nun auch erweiterte Informationen zum Vorgehen der EZB und den ergriffenen Maßnahmen enthalten.

Art. 96 Abs. 1 PSD II legt dagegen fest, dass über alle schwerwiegenden Betriebs- oder Sicherheitsvorfälle unverzüglich die zuständige Stelle zu informieren ist. Die Meldung des betroffenen Zahlungsdienstleisters hat hierbei gegenüber jener Behörde zu erfolgen, in welchem sich dessen (Haupt-) Sitz befindet. Damit die Zahlungsdienstleister leichter überprüfen können, ob es sich um einen mitteilungspflichtigen Vorfall handelt, hat die EBA die Leitlinien on Major Incidents Reporting ausgearbeitet. Die Leitlinien legen u.a. fest, wann ein schwerwiegender Vorfall besteht, den Inhalt, das Format (einschließlich Standartformblättern für die Meldungen) sowie das Verfahren für die Meldung derartiger Vorfälle.[51] Mittels dieses Frühwarnsystems wird insbesondere auch ein wichtiger Beitrag zum Schutz vor Cyberattacken geleistet, indem die entsprechenden Vorfälle identifiziert werden und die Ergebnisse der Analysen in das Risikomanagement der Institute einfließen.[52]

Nach Art. 96 Abs. 6 PSD II haben die Mitgliedstaaten schließlich sicherzustellen, dass Zahlungsdienstleister den für sie zuständigen Behörden mindestens einmal jährlich statistische Daten zu Betrugsfällen in Verbindung mit den unterschiedlichen Zahlungsmitteln vorlegen. Hierfür hat die EBA gemäß Art. 96 Abs. 3 PSD II die Leitlinien on Fraud Reporting herausgegeben. Die Leitlinien enthalten detaillierte Angaben zu den Berichtsperioden, wann eine betrügerische Zahlungstransaktion vorliegt, die Form der Datenaufschlüsselung sowie zu der Übermittlung dieser Daten.

3.4. BAIT & potenzielle EZB-Vorgaben

Wesentliche Impulse zur Fortentwicklung der bankinternen IT-Risikosteuerung setzen die neuen EBA-Leitlinien und die anhaltenden Prüfungen der Aufsicht. In Deutschland haben BaFin und Bundesbank bereits Schritte zur Ergänzungen der bankaufsichtlichen IT-Rechtsnormen angekündigt.[53] Hier ist zunächst über eine kommende BAIT-Novelle die Konkretisierung der Vorgaben des AT 7.3 MaRisk zum Notfallkonzept vorgesehen, wobei insbesondere die Test- und Wiederherstellungsverfahren für IT-Systeme und die dazugehörigen IT-Prozesse konkretisiert werden sollen. Dabei ist davon auszugehen, dass mit der kommenden BAIT-Novelle auch neue EBA-Anforderungen in das BaFin-Rundschreiben übernommen werden. Dies kann die neuen Leitlinien zu IT und Auslagerungen betreffen aber auch Aspekte aus den EBA-Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß PSD2.[54]

Inwiefern die EZB die von ihr angekündigten „Guidelines on IT Risk Management for Significant Institutions in 2019 veröffentlichen wird, ist offen. Interessant zu lesen, v.a. für die größeren Institute unter direkter EZB-Aufsicht, die unter AT 4.3.4 MaRisk fallen und die Baseler Vorgaben umsetzen müssen, ist der vom der EZB bereits im Mai 2018 veröffentlichte Report zum „Thematic Review" bezüglich Risikodatenaggregation und Risikoreporting.[55] Dieser listet detailliert neben den Schwachstellen der Umsetzung der BCBS-239-Vorgaben auch Best Practices auf. Abb. 3 stellt wesentliche Ergebnisse des EZB-Reports dar und kann als Checkliste für die Prüfungsvorbereitung genutzt werden. Die EZB hat bei den Instituten unter ihrer direkten Aufsicht zum Teil schwerwiegende Schwachstellen bei allen Baseler BCBS 239 Prinzipien beobachtet. Der Umsetzungsdruck hierzu dürfte für die großen Institute unverändert hoch bleiben, zumal der Baseler Ausschuss zu vergleichbaren Schlussfolgerungen kam.[56] Kleinere Institute unterliegen nicht zwar nicht den Anforderungen nach BCBS 239. Die Aussagen der EZB zum Risikoreporting sind aber dennoch lesenswert. So können sie z.B. in Deutschland hilfreich sein zur Erfüllung der Anforderungen an die Risikoberichterstattung in BT 3 MaRisk, die für alle Institute gleichermaßen gültig sind.

Abb. 3: Kernergebnisse des EZB Thematic Review zu Risikoaggregation und Risikoreporting

Wesentliche Schwachstellen	Wesentliche Best Practices
Governance und IT-Infrastruktur	
Rollen und Verantwortlichkeiten: ▪ Unzureichende Zuordnung von Rollen und Verantwortlichkeiten für Datenqualität ▪ Fehlende Verantwortlichkeiten („Ownership“) für Datenqualität in Fach-, IT- und überwachenden Einheiten Umsetzungsprojekte: ▪ Keine klare Definition von Scope und Roadmaps der Umsetzungsprojekte von BCBS 239 ▪ Nicht alle relevanten Konzernbereiche sind Teil des Projekts ▪ Unzureichende Aufmerksamkeit auf Executive und Senior Management Ebene Interne Prüfung des Umsetzungsstands: ▪ Mangelnde Unabhängigkeit und Ressourcenausstattung der Prüfeinheiten Qualität der umgesetzten Lösungen: ▪ Unzureichende Integration der IT-Systeme für Datenaggregation und Reporterstellung ▪ Keine homogene und integrierte Datentaxonomie auf Konzernebene ▪ Manuelle Prozessbrüche, die teilweise nicht ausreichend dokumentiert sind oder überwacht werden ▪ Keine Eskalationsprozesse bei fehlerhaften Daten ▪ Lückenhaftes Business Continuity Management der betroffenen IT-Systeme ▪ Unzureichende Drill-Down-Fähigkeiten	Rollen und Verantwortlichkeiten: ▪ Etablierung eines „Data Governance Office“ als „Second Line of Defence“ mit Verantwortlichkeiten wie z.B. Datenrichtlinien, Klassifizierung von Kernrisikodaten, Überwachung des Datenqualitätsprozesses ▪ Netzwerk von dezentralen „Data Ownern“ als „First Line of Defence“ Umsetzungsprojekte: ▪ Etablierung konzernweiter Steering Committees mit der Verantwortung für eine einheitliche Umsetzung der BCBS-239-Vorgaben in allen Konzerneinheiten zu sorgen Interne Prüfung des Umsetzungsstands: ▪ Regelmäßige Überprüfung der Umsetzungsqualität inkl. ausgelagerter Bereiche durch unabhängige Instanzen ▪ Etablierung eigener Einheiten, die für eine Konsistenz der Policies und Verfahren konzernweit verantwortlich sind ▪ Entwicklung von Datenqualitäts-Repositories für den Gesamtkonzern ▪ Einrichtung eigener operativer Budgettöpfe für die Umsetzung von BCBS-239-Vorgaben Qualität der umgesetzten Lösungen: ▪ Nutzung einer einheitlichen Datenquelle für das Risiko- und Finanzreporting sowie das Meldewesen ▪ Alle manuellen Eingriffe in die Daten (inkl. IDV-Lösungen) werden erfasst und nach Kriterien wie Komplexität und Relevanz eingestuft ▪ Etablierung automatisierter Konsistenzchecks vom Frontoffice- bis zum Reportingsystem sowie zwischen verschiedenen Datenquellen (z.B. Risiko- und Finanzdaten) ▪ Etablierung eines kontinuierlichen Verbesserungsprozesses für die permanente Weiterentwicklung der Datenqualität ▪ Nutzung des Legal Entity Identifier oder eines instituts- ▪ eigenen einheitlichen Kundenschlüssels

Wesentliche Schwachstellen	Wesentliche Best Practices
Risikodatenaggregation	
▪ Unvollständige oder nicht abgenommene Datenqualitätsrichtlinien ▪ Unzureichende Key Quality Indicators (z.B. unzureichende Abdeckung, nicht nachvollziehbares Setzen von Toleranzgrenzen) ▪ Keine nachvollziehbare Dokumentation bei der Anpassung von Daten ▪ Hoher manueller Aufwand führt zu verspäteter Bereitstellung der aggregierten Daten für das Reporting oder Adhoc-Anfragen Risikodaten von Tochtergesellschaften, Niederlassungen oder Business Lines ▪ Verfügbarkeit von Daten häufig in unstrukturierter Form (z.B. Ausdrucke, gescannte Dokumente)	▪ Regelmäßiger Review von Datenqualitätsrichtlinien ▪ Etablierung eines Datenqualitätszertifizierungsprozesses für die „golden source“ ▪ Logging von Datenveränderungen ▪ Definition von Metriken, die in Stresssituationen bereitgestellt werden müssen ▪ Schaffen von Voraussetzungen, dass diese Metriken in Stresssituationen auf wöchentlicher oder Tagesbasis bereitgestellt werden können
Risikoreporting	
▪ Unzureichende Plausibilitäts- und Konsistenzchecks der Reports ▪ Unzureichende Möglichkeiten der Datenrückverfolgung („Data Lineage“) aufgrund manueller Prozesse und infolgedessen auch unzureichende Kommentierung der Daten ▪ Abstimmungsfehler insbesondere bei regulatorischem Kapital aufgrund manueller Prozesse ▪ Intensive Nutzung von fehleranfälligen und komplexen IDV-Lösungen ▪ Fehlende Policies für den Umgang mit nicht verarbeiteten Daten ▪ Ineffektive Kontrollprozesse auf Konzernebene ▪ Probleme im Standard-Risikoreporting vorausschauende Aspekte zu berücksichtigen (z.B. Stresstesting, Szenario-analyse) ▪ Probleme beim Herunterbrechen von Risikodaten in Unterkategorien ▪ Fehlende formale Feedbackschleifen des Senior Managements zum Risikoreporting ▪ Fehlerhafte Interpretation der Risikoreports auf Seiten des Managements aufgrund fehlender einheitlicher Definitionen ▪ Kein adressatengerechtes Reporting (Reporting zu komplex, zu technisch etc.) ▪ Keine Dokumentation des Adressatenkreises der Reports sowie der Vertraulichkeit der Informationen ▪ Keine automatisierte Verteilung der Reports	▪ Dokumentation von Datenqualitätsanforderungen und aller Datenqualitätschecks ▪ Berücksichtigung ökonomischer Vorhersagen für die wichtigsten Volkswirtschaften und Regionen im Risikoreport (makroökonomische Daten wie Zinskurven) ▪ Einführung von Zufriedenheitsumfragen für Risikoreports sowie einer Arbeitsgruppe zur Verbesserung von Risikoreports ▪ Risikoreports enthalten eine Zusammenfassung wesentlicher Risiken sowie qualitative Aussagen ▪ Bereitstellung von internen Daten-Lexika zur Sicherstellung einer einheitlichen Nutzung und Interpretation von Fachbegriffen ▪ Etablierung von konzernweit einheitlichen Vorgaben für die Dokumentation ▪ Vorgaben werden von Leitungsgremien beschlossen und durchgesetzt ▪ Formale Definition aller Reportempfänger und automatisierte Verteilung ▪ Etablierung von Policies, in denen für jeden Report das „need to know“ definiert wird ▪ Bereitstellung der Reports über eine zentrale IT-Plattform mit sicheren Zugangsmechanismen

Quelle: Buchmüller/Mährle/Rambock (2019) [76]

Um dem Themenbereich IT-Risiken eine noch gewichtigere Rolle einzuräumen, hat die FMA zudem bereits im Jahr 2017 einen „IT-Security Circle“ (ISC) eingerichtet.

3.5. FMA Leitfäden zum Thema IT-Sicherheit

Um den gesteigerten Risiken in Zusammenhang mit der fortschreitenden Digitalisierung im Finanzsektor Rechnung zu tragen, hat die FMA mehrere Leitfäden mit Bezug auf IT-Sicherheit veröffentlicht:

- FMA Leitfaden IKT-Sicherheit in Kreditinstituten
- FMA-Leitfaden IT-Sicherheit in Versicherungs- und Rückversicherungsunternehmen
- FMA-Leitfaden zur IT-Sicherheit in Wertpapierdienstleistungsunternehmen und Wertpapieren
- FMA-Leitfaden zur IT-Sicherheit in Verwertungsgesellschaften
- FMA-Leitfaden zur IT-Sicherheit in Pensionskassen

In diesen Leitfäden stellt die FMA ihre Erwartungshaltung zur Governance und Steuerung sowie zur operativen Umsetzung und Ausgestaltung der IT-Sicherheitsmaßnahmen in den beaufsichtigten Unternehmen dar. Eine besondere Bedeutung kommt hierbei den Führungskräften des Unternehmens zu, da sie die IT-Strategie sowie die Vorgaben der IT-Aufbau- und Ablauforganisation zu verantworten haben. Hierbei ist insbesondere auf eine angemessene technisch-organisatorische Ausstattung sowie auf die Vermeidung von Interessenkonflikten zu achten. Weiters beinhalten die Leitfäden ein Rahmenwerk zur Identifikation und Begrenzung des IT-Verfügbarkeits- und Kontinuitätsrisikos samt präventiver Maßnahmen, Anforderungen an das Benutzerberechtigungsmanagement (Need-to-know-Prinzip), wie auch an das Schwachstellenmanagement.[57]

Die Ziele und Intentionen der Leitfäden sind deckungsgleich, wobei jedoch aufgrund von branchen- oder produktspezifischer Besonderheiten kleinere Unterschiede zwischen den einzelnen Leitfäden bestehen. Alle veröffentlichten Leitfäden folgen zudem dem Grundsatz der Proportionalität. Es gilt folglich Art, Umfang, Komplexität der Geschäfte sowie Risikostruktur des jeweiligen Unternehmens bei der Umsetzung des entsprechenden Leitfadens zu berücksichtigen. Anhand dieser Kriterien hat das jeweilige Unternehmen zu bestimmen, welche Methoden, Systeme und Prozesse in Bezug auf die IT-Sicherheit aufgrund der angebotenen Dienstleistungen angemessen sind.[58]

Um dem Themenbereich IT-Risiken eine noch gewichtigere Rolle einzuräumen, hat die FMA zudem bereits im Jahr 2017 einen „IT-Security Circle“ (ISC) eingerichtet. Zu den Zielen dieses Forums zählt insbesondere der Informations- und Erfahrungsaustausch zwischen den Fachbereichen. Zudem stellt der ISC eine Kontaktstelle für die Fachabteilungen zu IT-spezifischen Aufsichtsthemen dar.[59]

Auf nationaler Ebene beteiligt sich die FMA ferner an den Arbeiten der „Cyber Sicherheit Plattform“ (CSP), welche von der österreichischen Bundesregierung im Jahr 2015 ins Leben gerufen wurde und in welcher der private und öffentliche Sektor in Sachen Cybersicherheit und Schutz kritischer Infrastrukturen eng zusammenarbeiten.

3.6. Arbeiten auf globaler Ebene zum Thema IT-Risiko

Die Bedeutung des Themas IT-Risiko wurde von den Staats- und Regierungschefs auf Ebene der G20 zuletzt im Rahmen des Treffens in Buenos Aires im Dezember 2018 betont. Der Ausschuss für Finanzstabilität (Financial Stability Board, FSB) wurde hierzu mit Umsetzungsarbeiten betraut. Dies kann mittelfristig, ebenso wie zuvor im Bereich Sanierungs- & Abwicklungsplanung dazu führen, dass auf dieser Ebene Standards ausgearbeitet werden, die für global systemrelevante Institute sehr schnell direkt umsetzungsrelevant werden. Bisheriger FSB-Output ist ein im November 2018 veröffentlichtes Cyber Lexicon.[60] Dieses knapp 20-seitige Dokument ist insbesondere für Institute interessant, die Teil global operierender Bankengruppen sind, da neben der Definition grundlegender IT-Begrifflichkeiten auch die unterschiedlichen internationalen IT-Risikosteuerungsnormen genannt und unter Nennung aktueller Bedrohungspotenziale eingeordnet werden. Damit kann dieses Dokument ggf. für internationale Bankengruppen bei der Ausarbeitung der internen Handbücher hilfreich sein. Ansonsten hat sich das FSB im zweiten Halbjahr 2018 vermehrt mit dem Thema Conduct Risk beschäftigt. Auch diese Ausarbeitungen sollten die größten Institute zur Kenntnis nehmen und bei der Fortentwicklung ihres Instrumentariums zur Steuerung von operationellen Risiken berücksichtigen.

Ein ähnliches Dokument wie das FSB Cyber Lexicon ist das vom Baseler Ausschuss im Dezember 2018 veröffentlichte Range of Practice Dokument zum Thema „Cyber-Resilience". [61] Hier werden unterschiedliche Regulierungsansätze auf nationaler Ebene vorgestellt (u.a. die deutschen BAIT). Aktuell stehen über die bereits 2017 veröffentlichten Vorgaben zum Thema Step-in Risk [62] keine weiteren bindenden Regelungen des Baseler Ausschusses mit Bezug zum IT-Risiko kurzfristig vor der Implementierung. Deshalb empfehlen wir kleineren Instituten in Deutschland, sich auf die BAIT- & EBA-Vorgaben sowie die Fortentwicklung von DSGVO und Informationssicherheitsgesetz in 2019 zu konzentrieren. Größere Institute sollten allerdings durchaus im Sinne der gemäß MaRisk geforderten Proportionalität die Veröffentlichungen von FSB und Baseler Ausschuss weiter beobachten. Hierbei scheint weiterhin die BCBS-239-Umsetzung am dringendsten, wie dem Progress Report des Baseler Ausschusses vom Juni 2018 zu entnehmen ist. Für mittlere und große Institute, die noch keine IT-Prüfung durchlaufen haben, können die in diesem Bericht enthaltenen Mängelbeschreibungen ebenso wie der bereits genannte EZB-Bericht bei der Prüfungsvorbereitung zum Thema helfen.

Die Institute sowie IT-Dienstleister für den Bankensektor, wie z.B. Rechenzentrumsbetreiber können sich über die bereits genannten Texte hinaus auch an zwei aktuellen Veröffentlichungen der G7 Cyber Expert Group orientieren. Die von der Expertengruppe unter Mittwirkung von Vertretern des Bundesfinanzministeriums, der Bundesbank und der BaFin erstellten Berichte wurden durch die Finanzminister und Notenbankgouverneure der G7-Staaten am 11. Oktober 2018 in Bali verabschiedet und haben empfehlenden Charakter. Der erste Text, die sog. G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector [63] enthält rechtlich nicht bindende Risikomanagement-Bausteine zum Umgang mit Drittparteien, wie beispielsweise Cloud-Anbietern. Der zweite Text, die G7 Fundamental Elements for Threat-Led Penetration Testing [64] beinhaltet Hinweise, wie mittels simulierter Cyber-Attacken die Cyber-Widerstandsfähigkeit einer Bank inklusive ausgelagerter IT-Infrastrukturelemente beurteilt werden kann und Schwachstellen identifiziert werden können.

Wichtigstes Thema der EU-Datenschutzregulierung in 2019 dürfte die geplante ePrivacy-Verordnung sein, die auch das Online-Marketing der Banken betreffen dürfte. Im Mai 2020 wird die EU-Kommission dann einen Evaluierungsbericht zur DSGVO veröffentlichen, der dann auch weitere Vorschläge zur Fortentwicklung des Datenschutz-Rechtsrahmen in der EU enthalten dürfte.

3.7. Informationssicherheitsgesetz und weitere branchenübergreifende IT-Rechtsnormen in Deutschland

In Deutschland ist das seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz") die zentrale Rechtsnorm zur IT-Sicherheit. Das Bundesinnenministerium (BMI), hatte bereits im Sommer 2018 angekündigt, in 2019 mit einer Novelle des IT-Sicherheitsgesetzes („IT-Sicherheitsgesetz 2.0") die Meldepflicht von Unternehmen bei Angriffen auf ihre IT-Infrastruktur zu verschärfen. Damit würde die Meldepflicht von bisher sehr eng definierten Betreibern sogenannter „kritischer Infrastrukturen" potenziell auf mittelständische Unternehmen ausgeweitet. Dies könnte dann möglicherweise auch kleinere Banken treffen. Infolge des Anfang Januar aufgetretenen Falls der massenhaften Entwendung und Veröffentlichung personenbezogener Daten von Politikern und anderer Personen des öffentlichen Lebens, ist nun mit verstärkten gesetzgeberischen Aktivitäten zu rechnen. Diese dürften auch die Kreditinstitute treffen. Neben der Novelle des IT-Sicherheitsgesetzes, zu der das BMI noch in der ersten Jahreshälfte 2019 einen Entwurf vorlegen möchte, werden weitere Gesetzesänderungen diskutiert, wie z.B. die Erhöhung der Strafmaße für Datendiebstahl und andere Cybercrime-Delikte.

Ein wichtiges regulatorisches Umsetzungsthema im vergangenen Jahr war das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) zum 25.05.2018. Über die daraus folgenden Umsetzungspflichten herrscht weiterhin große Rechtsunsicherheit. Aus diesem Grund empfiehlt sich hierzu das regelmäßige Verfolgen der Auslegungen des Bundesdatenschutzbeauftragten und der Datenschutzkonferenz zur DSGVO bzw. der nachgelagerten Regulierungsinitiativen auf EU-Ebene. Nach den Europawahlen 2019 ist hier wahrscheinlich mit weiteren Initiativen auf EU-Ebene zu rechnen. Wichtigstes Thema der EU-Datenschutzregulierung in 2019 dürfte die geplante ePrivacy-Verordnung sein, die auch das Online-Marketing der Banken betreffen dürfte. Im Mai 2020 wird die EU-Kommission dann einen Evaluierungsbericht zur DSGVO veröffentlichen, der dann auch weitere Vorschläge zur Fortentwicklung des Datenschutz-Rechtsrahmen in der EU enthalten dürfte.

3.8. Netz- und Informationssicherheitsgesetz und weitere branchenübergreifende IT-Rechtsnormen in Österreich

Mit dem Netz- und Informationssicherheitsgesetz (BGBl I 2018/111), welches am 29.12.2018 in Kraft getreten ist, wurde die NIS-RL [65] in Österreich umgesetzt. Zu den Zielen dieses Gesetzes zählt u.a. die Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen sowie die verstärkte Zusammenarbeit zwischen den Mitgliedstaaten der EU in strategischer und operationeller Hinsicht. Weiters schreibt es bestimmte Mindeststandards hinsichtlich von Sicherheitsanforderungen, als auch gewisse Meldeverpflichtungen vor. Das Gesetz richtet sich dabei an verschiedene Sektoren (u.a. Energie, Verkehr, Bankwesen), welche als Betreiber wesentlicher Dienste (BwD) zusammengefasst sind, an Anbieter digitaler Dienste sowie an Einrichtungen der öffentlichen Verwaltung.[66] Dem Bundeskanzler kommt hierbei die Aufgabe zu, für jeden Sektor die entsprechenden Unternehmen zu ermitteln, welche als Betreiber wesentlicher Dienste anzusehen sind. Hierfür sind von diesem mehrere Faktoren zu berücksichtigen. Zu diesen zählen etwa die Zahl der Nutzer, die den vom jeweiligen Betreiber eines wesentlichen Dienstes angebotenen Dienst in Anspruch nehmen, aber auch die geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betrof-

fen sein könnte.[67] Sieht der Bundeskanzler die Anforderungen als erfüllt an, wird dem betreffenden Unternehmen ein Bescheid zugestellt. Nach dem Erhalt des Bescheides hat der Betreiber innerhalb von zwei Wochen eine Kontaktstelle für die Kommunikation mit dem Bundeskanzler, dem Bundesminister für Inneres oder den Computer-Notfallteams (Certs) zu nennen.[68] Zu den weiteren Verpflichtungen eines Betreibers eines wesentlichen Dienstes gehört es auch, dass er für geeignete und verhältnismäßige technische und organisatorische Sicherheitsanforderungen zu sorgen hat. Hat sich zudem ein Sicherheitsvorfall bei einem derartigen Betreiber ereignet, ist dieser grundsätzlich verpflichtet, dies unverzüglich an das nationale Computer-Notfallteam zu melden. Für den Bankensektor besteht in diesem Zusammenhang eine Besonderheit, da die Bestimmungen über Sicherheitsvorkehrungen sowie Meldeverpflichtungen auf sie nicht zur Anwendung gelangen. Dies hat den Hintergrund, dass eine lex specialis Regelung im Gesetz vorgesehen ist, wonach die Vorschriften der §§ 17 und 19 NISG nicht anzuwenden sind, wenn in anderen Materiengesetzen ebenfalls Bestimmungen über Sicherheitsvorkehrungen und Meldeverpflichtungen enthalten sind, die zumindest ein gleichwertiges Sicherheitsniveau für die Netz- und Informationssysteme sicherstellen.[69] Für den Bankensektor bestehen vergleichbare Regelungen in den §§ 85 ZaDiG 2018, wodurch die lex specialis Regelung in diesem Fall schlagend wird.

Das NISG stellt jedoch nicht die einzige Bestrebung dar, um die Sicherheit von Netz- und Informationssystemen zu stärken. So wurde nämlich von der österreichischen Bundesregierung bereits 2013 eine Strategie für Cybersicherheit in Österreich erstellt (Österreichische Strategie für Cyber Sicherheit [ÖSCS]).[70] Im Zuge dieser Strategie wurde auf nationaler Ebene eine Struktur zur Koordination auf der operativen Ebene geschaffen. Vorrangiges Ziel ist es dabei, einen regelmäßigen Informationsaustausch zwischen den entscheidenden Unternehmen in diesem Bereich sicherzustellen, die Situation im Cyberraum laufend zu beobachten, zu bewerten und diese Informationen in Form eines aktuellen Lagebilds festzuhalten. Weiters wurde im Rahmen dieser Strategie auch eine Cyber Sicherheit Plattform (CSP) ins Leben gerufen, welche konkrete Maßnahmen festlegt, um mit deren Hilfe die Cybersicherheit in Österreich weiter zu erhöhen und um eine hohe Resilienz kritischer Infrastrukturen gegen Cyberattacken sicherzustellen.

3.9. Fortentwicklung der branchenübergreifende IT-Sicherheitsnormen auf EU-Ebene

Auch auf EU-Ebene sind die Vorgaben zur IT-Sicherheit aktuell im Fluss. Zwar existiert die Europäische Agentur für Netz- und Informationssicherheit (ENISA, European Union Agency for Network and Information Security) mit Sitz in Athen mittlerweile bereits seit 15 Jahren. Mit dem von der EU-Kommission im September 2017 vorgelegten Reformpaket zur Stärkung der Cybersicherheit gewinnt dieses Politikfeld auf EU-Ebene allerdings stark an Bedeutung. Die Zielsetzungen die einer schlagkräftigeren EU-Agentur für Cybersicherheit und eines EU-weiten Zertifizierungssystems für Cybersicherheit hat der Rat der Staats- und Regierungschefs der Europäischen Union in seinem Treffen vom Oktober 2018 bekräftigt. Das Europäische Parlament hat mit seiner Beschlussfassung im März 2019 nun die politische Einigung über den „EU Cybersecurity Act" entscheidend vorangebracht. Damit werden Budget und Aufgaben der ENISA erweitert. Neu ist die Zertifizierung von Informations- und Kommunikationstechnologieprodukten, die EU-weit auf freiwilliger Ebene erfolgen soll. Generell verfolgt die EU-Initiative eine Bündelung der diesbezüglichen Anstrengungen, so dass einheitliche EU-Zertifikate anstelle national unterschiedlicher Vorgaben eine hinreichende IT-Sicherheit technischer Komponenten vor dem Hintergrund des rasant voranschreitenden Internet der Dinge (Internet-of-things (IoT)) sicherstellen sollen. Auch bei Krisenübungen und

Sicherheitswarnungen könnte die EU-Behörde ENISA zukünftig gegenüber den nationalen Behörden, wie dem BSI in Deutschland, an Bedeutung gewinnen und dann auch in den Fokus der Banken rücken.

4. Überarbeitung von CRR & CRD zur Umsetzung von Basel III

Das Basel III Rahmenwerk vom 07.12.2017 [71] ist einschließlich der vom Baseler Ausschuss im Dezember 2018 veröffentlichten neuen Offenlegungsanforderungen [72] bis zum 01.01.2022 umzusetzen. Hierzu wurde die EBA von der Europäischen Kommission bereits am 04.05.2018 beauftragt, Auswirkungsanalysen und Vorschläge zur EU-Umsetzung bis 30.06.2019 vorzulegen.[73] Gemäß dem Call for Advice der EU-Kommission muss die EBA u.a. Folgendes liefern:

- Granulare Auswirkungsschätzungen der Umsetzungskosten und Änderung der Kapitalanforderungen zum Ist-Stand nach Größe, Geschäftsmodell und Sitz der Banken
- Auswirkungsanalyse zum Kreditrisikostandardansatz inkl. administrativer Umsetzungskosten der verschärften Anforderungen an Due Dilligence und Immobilienbewertung
- Empfehlung zum Grad der Nutzung externer Ratings im Kreditrisikostandardansatz und Festlegung des Granularitätskriteriums für das Retail-Exposure
- Auswirkungsanalysen zur Überführung des Banken- & Großunternehmensportfolios aus dem IRBA in den Kreditrisikostandardansatz, Abschaffung des IRBA-Skalierungsfaktors und Änderung der aufsichtlichen LGD- & CCF Vorgaben
- Umsetzungsanalysen zu den neuen Vorgaben an das Credit Valuation Adjustment (CVA) Risiko und den Baseler Anforderungen im Rahmen des Fundamental Review of the Trading Book (FRTB). Diese Analysen kann die EBA ggf. auch außerhalb des bis 30.06. zu liefernden Haupt-Ergebnisdokuments separat bis zum 30.09.19 nachreichen.
- Umsetzungsanalyse zum neuen Säule I Ansatz für operationelle Risiken (inkl. Möglichkeit zur Einführung neuer Anforderungen zu IT- & Cybersecurity-Risiken und von Anreizen zur Verbesserung der bankinternen OpRisk-Steuerung im Zusammenspiel mit Säule II).

Sobald die EBA ihre (englischsprachigen) Ergebnisdokumente liefert, wird klarer werden, wie Basel III in der EU umgesetzt werden könnte. Bis Ende 2019 dürften auch erste Äußerungen zur allgemeinen Ausrichtung der Basel III Umsetzung vorliegen. Dies betrifft insbesondere die Frage von inhaltlichen Erleichterungen für kleine Institute (Stichwort: Small Banking Box) sowie eine potenzielle Verschiebung des Inkrafttretens der neuen Kapitalanforderungen vom 01.01.2022 um möglicherweise 2-3 Jahre. Die politische Rahmenfestlegung wird primär durch die neu zusammengesetzte EU-Kommission und das vom 23. bis 26.05.2019 neu gewählte EU-Parlament erfolgen. Wie schnell dies geschieht, hängt sehr stark vom Wahlverlauf und der allgemeinen europapolitischen Entwicklung ab.

Unabhängig von möglichen Verzögerungen im politischen Prozess sollte zumindest für die Drei-Jahresplanung 2020-2022 im vierten Quartal 2019 ein erster Projekt-Setup bzgl. Scope, grober (Zeit-)Planung und Budgetierung dieses ambitionierten Projektes erfolgen. Bis zum Inkrafttreten von Basel III müssen für die nach der bisherigen Basel II Methodik zugelassenen Modelle in Säule I weiterhin die von der Aufsicht geforderten Verbesserungen umgesetzt werden. Dies betrifft für die IRBA-Institute im Kreditrisiko sowie die internen Marktrisikomodelle die Ergebnisse des Targeted Review of Internal Models (TRIM) [74] und für die fortgeschrittenen Messansätze im operationellen Risiko (advanced measurement approaches, AMA) die Anforderungen der im Juli 2018 veröffentlichen delegierten Verordnung zur AMA-Beurteilung.[75]

Praxistipp

Unabhängig von möglichen Verzögerungen im politischen Prozess sollte zumindest für die Drei-Jahresplanung 2020-2022 im vierten Quartal 2019 ein erster Projekt-Setup bzgl. Scope, grober (Zeit-)Planung und grobe Kostenplanung zur Umsetzung der neuen Basel III-Vorgaben erfolgen

5. Risikolage im Bankensektor und Fazit

Inwiefern es tatsächlich in 2019 zu einem größeren Konjunktureinbruch kommen wird, ist gegenwärtig noch nicht absehbar. Ausschlaggebend dürften v.a. „geopolitische Risiken" insbesondere in Bezug auf den Brexit und die US-Handelspolitik sowie die generelle Entwicklung der internationalen Beziehungen (z.B. Russland) und Weltwirtschaftslage (z.B. China) sein. Für die deutsche Konjunktur bedeutet dies Gegenwind, sodass aktuell nicht zu erwarten ist, dass die BaFin antizyklischen Pufferanforderungen verhängen bzw. sonstige makroprudenzielle Maßnahmen (z.B. nach §48u KWG) ergreifen wird, um beispielsweise einer Überhitzung des Immobilienmarktes entgegenzuwirken (s. hierzu den Beitrag von Buchmüller/Igl in der gleichen Ausgabe der ZFF).

Vor diesem Hintergrund sollten sich die deutschen Institute auf zunehmende Kreditausfälle, erhöhte operationelle Risiken (v.a. durch Rechtsrisiken/ Conduct Risk sowie IT-Ausfälle und Cybercrime) und auf potenzielle Verwerfungen auf den Kapitalmärkten (z.B. Ansteigen der Risikoprämien für diverse EU-Staaten aufgrund zunehmender politischer Konflikte oder volatileres Refinanzierungsumfeld) einstellen und diese Entwicklungen angemessen in ihrer Risikosteuerung berücksichtigen. Die Auswirkungen der schlechter werdenden Gesamtkonjunktur sollten im Kredit- und Marktrisiko sowie hinsichtlich möglicher Effekte auf die Liquidität analysiert werden. Dies gilt, sowohl für die laufende Risikosteuerung / Frühwarnung, als auch für die Risikotragfähigkeitsrechnung und das Stresstesting. Für den inversen Stresstest könnte möglicherweise ein Großverlust aufgrund von schlagend gewordenen IT-Risiken (z.B. umfangreicher Datendiebstahl) simuliert werden. Für die operative Risikosteuerung sollten die spezifischen Haupttreiber der Konjunkturrisiken möglichst genau identifiziert werden, insbesondere hinsichtlich Konzentrationsrisiken. Im Kreditrisiko könnten möglicherweise Ausfälle von Großkreditnehmern mit einer gleichzeitigen Belastung im Retailportfolio aufgrund des konjunkturell verschärften Strukturwandels in Schlüsselindustrien über ein spezifisches Szenario analysiert werden. So könnten Institute regional z.B. durch den von Ford angekündigten massiven Jobabbau in europäischen Autowerken besonders betroffen sein.

Insgesamt schlagen wir vor dem Hintergrund der Risikolage und der aufsichtlichen Ankündigungen die folgenden, in Abb. 4 dargestellten Schwerpunkte für die bankinternen Umsetzungsmaßnahmen in 2019 vor.

> Vor diesem Hintergrund sollten sich die deutschen Institute auf zunehmende Kreditausfälle, erhöhte operationelle Risiken (v.a. durch Rechtsrisiken/ Conduct Risk sowie IT-Ausfälle und Cybercrime) und auf potenzielle Verwerfungen auf den Kapitalmärkten (z.B. Ansteigen der Risikoprämien für diverse EU-Staaten aufgrund zunehmender politischer Konflikte oder volatileres Refinanzierungsumfeld) einstellen und diese Entwicklungen angemessen in ihrer Risikosteuerung berücksichtigen

Q2 2019

Abarbeitung der neuen EBA-Vorgaben zu **Zinsänderungsrisiko** und **Stresstesting** sowie Anpassung des **Risikotragfähigkeit**skonzeptes an die neuen Vorgaben von EBA & EZB (und BaFin / Bundesbank in Deutschland)
Zentral sind hier die bessere Verknüpfung des **ICAAP** mit dem **ILAAP** sowie die **Konzeption aussagekräftiger Stresstests** zu den genannten spezifischen Risiken (zur Durchführung in Q2 oder Q3, bzw. im Zusammenhang mit dem Liquiditätsstresstest der EZB (bzw. der neuen Niedrigzinsumfrage / dem LSI-Stresstest von BaFin und Bundesbank) und die **Festlegung klarer Frühwarnkriterien**, ab denen Planungsanpassungen mit konkreten **Risikosenkungsmaßnahmen** erfolgen müssen.

Q3/Q4 2019

Beginn der **Umsetzung**sarbeiten zu **Basel III** durch **Sichtung des EBA-Ergebnisdokumentes zum Call for Advice** der EU-Kommission sowie ergänzend der Regelungstexte des Baseler Ausschusses (z.B. zur Offenlegung) sowie weiterer EBA-Papiere mit Meldewesenbezug (z.B. Outsourcing Guidelines).

Ganzjährig

Verbesserung der **IT-(Risiko-)Steuerung** mit Überprüfung der **IT-Governance** (insbesondere Berichterstattung an den Vorstand und spezifischer IT-Gremien), Anweisungswesen (in Deutschland Abarbeitung von **BAIT-Moniten** zusammen mit Umsetzung der EBA-Leitlinien) und gesonderten **Risikoanalysen** (z.B. Sichtung der jüngsten Schadenfälle bzw. Beauftragung von Penetrationstests sowie v.a. Intensivierung der geforderten **Schutzbedarfsanalysen**). Möglichweiser Verstärkung der **Vernetzung mit der Fach-Community** (in Deutschland z.B. durch Beitritt zur Allianz für Cyber-Sicherheit bzw. sonstigem Austausch mit BSI und weiteren Sicherheitsbehörden).

Abb. 4: Möglicher Umsetzungsfahrplan zur regulatorischen Agenda

Quelle: Eigene Darstellung in Anlehnung an Buchmüller/Mährle/Rambock (2019) [76]

Quellenverzeichnis

[1]	Die in diesem Beitrag getätigten Aussagen sind allein die persönliche Meinung der Autoren und stellen in keiner Weise offizielle Aussagen der FMA dar. Die zahlreichen Publikationen von Aufsichtsbehörden und weiteren Standardsetzern, die in diesem Beitrag genannt sind, finden Sie gebündelt im „Regulatorik-Tracker" auf der Internetseite www.marisk.academy
[2]	EBA (2018a): Work Programme 2019, London, 23.10.2018
[3]	EZB-Bankenaufsicht (2018): Aufsichtsprioritäten des SSM im Jahr 2019, Frankfurt am Main 30.10.2018
[4]	EZB-Bankenaufsicht (2018): Risikobewertung für 2019, Frankfurt am Main 30.10.2018
[5]	BaFin (2018): Schwerpunkte der Bankenaufsicht 2019, Bonn & Frankfurt am Main, 18.12.2018
[6]	BaFin (2018): Schwerpunkte der Aufsicht 2019, Bonn Frankfurt am Main, 18.12.2018
[7]	Siehe FMA, Pressemitteilung vom 28.11.2018, FMA veröffentlicht die Aufsichts- und Prüfschwerpunkte 2019 und präsentiert die Publikation „Fakten, Trends und Strategien 2019", https://www.fma.gv.at/fma-veroeffentlicht-die-aufsichts-und-pruefschwerpunkte-2019-und-praesentiert-die-publikation-fakten-trends-und-strategien-2019/ (abgefragt am 10.03.2019)
[8]	FMA (2018): Fakten, Trends und Strategien 2019, Wien, 28.11.2018
[9]	EBA (2017): Guidelines on internal Governance (EBA/GL/2017/11)
[10]	EBA (2017): Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (EBA/GL/2017/12)
[11]	Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission, ABl. L 331/2010, 12 (idF EBA-Verordnung)
[12]	Vgl. die Tabelle der Compliance-Erklärungen, zuletzt abgerufen am 10.03.2019 unter: https://eba.europa.eu/documents/10180/1972987/EBA+GL+2017+11-CT+GLs+on+internal+-governance.pdf/1c55bd94-4647-424f-a79a-fb5203f68439 (EBA/GL/2017/11) bzw https://eba.europa.eu/documents/10180/15718/EBA+GL+2017+12-CT+GLs+Consolidated+Joint+ESMA+EBA+on+assessment+of+the+s....pdf/09131720-6b13-408c-98ef-8b5ba8e63f22 (EBA/GL/2017/12)
[13]	Bundesgesetz, mit dem das Bankwesengesetz und das Investmentfondsgesetz 2011 geändert werden BGBl I 2018/36 und EB 106 BglNR 26. GP
[14]	EB 106 BglNR 26. GP, 1
[15]	Vgl § 5 Abs. 4 BWG idF BGBl I 2018/112
[16]	Vgl § 29 WAG 2018 idF BGBl I 2017/107107/2017
[17]	EB 106 BglNR 26. GP, 2
[18]	BWG idF BGBl I 2018/112
[19]	§ 39 Abs. 6 Z 2 BWG idF BGBl I 2018/112
[20]	§ 39 Abs. 6 Z 2 BWG idF BGBl I 2018/112
[21]	Ausgenommen sind hundertprozentige Töchter, die weder von erheblicher Bedeutung sind und keine Wertpapiere ausgegeben haben, die zum Handel am geregelten Markt zugelassen sind; Vgl. §28a Abs. 5a Z 2 BWG idF BGBl I 2017/107
[22]	EB 106 BglNR 26. GP, 3
[23]	§ 103w BWG idF BGBl I 2018/112
[24]	EB 106 BglNR 26. GP, 3
[25]	EZB-Bankenaufsicht (2019): EZB-Jahresbericht zur Aufsichtstätigkeit 2018, Frankfurt am Main, 21.03.2019 https://www.bankingsupervision.europa.eu/press/publications/annual-report/html/ssm.ar2018~927cb99de4.de.html#toc33 (zuletzt abgerufen am 29.04.2019)
[26]	EBA (2018b): Überarbeitete Leitlinien zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs- und Bewertungsprozess (Supervisory Review and Evaluation Process, SREP) sowie für die aufsichtlichen Stresstests, zur Änderung der EBA/GL/2014/13 vom 19. Dezember 2014, London, 19.07.2018 (EBA/GL/2018/03 – Hinweis: Dieses Dokument enthält lediglich die Änderungen der ursprünglichen Leitlinien, die neue konsolidierte Fassung der SREP-Guidelines liegt Stand 15.01.2019 nur in englischer Sprache vor); EBA (2018c): Leitlinien zu den Stresstests der Institute, London, 19.07.2018 (EBA/GL/2018/04); EBA (2018d): Leitlinien zur Steuerung des Zinsänderungsrisikos bei Geschäften des Anlagebuchs, London, 19.07.2018 (EBA/GL/2018/02); EBA (2018e): Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing, Final Report London, 19.07.2018 (EBA/GL/2018/03, final report bzw. EBA/GL/2014/13 consolidated version)
[27]	BaFin/Bundesbank (2018): Aufsichtliche Beurteilung bankinterner Risikotragfähigkeitskonzepte und deren prozessualer Einbindung in die Gesamtbanksteuerung („ICAAP") - Neuausrichtung, Bonn / Frankfurt am Main, 24.05.2018

[28]	Europäische Zentralbank (2018): Leitfaden der EZB für den bankinternen Prozess zur Sicherstellung einer angemessenen Kapitalausstattung (Internal Capital Adequacy Assessment Process – ICAAP), Frankfurt am Main, November 2018. Europäische Zentralbank (2018): Leitfaden der EZB für den bankinternen Prozess zur Sicherstellung einer angemessenen Liquiditätsausstattung (Internal Liquidity Adequacy Assessment Process – ILAAP), Frankfurt am Main, November 2018.
[29]	Eine umfassende Darstellung der neuen EZB-Vorgaben in den ICAAP & ILAAP Guides vor dem Hintergrund der bisherigen deutschen Ausprägung des SREP und dem neuen RTF-Leitfaden von BaFin und Bundesbank gibt der Sammelband Buchmüller/Igl (2019): Handbuch ICAAP/ILAAP. Die Neuen Vorgaben zur Risikotragfähigkeit von EZB und BaFin, Bank-Verlag, Januar 2019
[30]	Deutsche Bundesbank (2019): Sicherstellung der Risikotragfähigkeit bei weniger bedeutenden Instituten (LSI). Range of Practice 2015-2017, Frankfurt am Main, 06.02.2019
[31]	ECB Banking Supervision (2019): ECB Sensitivity Analysis of Liquidity Risk – Stress Test 2019. Methodological Note, Frankfurt am Main 06.02.2019
[32]	BaFin/Bundesbank (2019): BaFin und Bundesbank starten Stresstest für kleine und mittelgroße Institute, Gemeinsame Pressenotiz, Bonn / Frankfurt am Main, 01.04.19; https://www.bundesbank.de/de/presse/pressenotizen/bafin-und-bundesbank-starten-stresstest-fuer-kleine-und-mittelgrosse-institute-785226
[33]	EBA (2017): Leitlinien für die IKT-Risikobewertung im Rahmen des SREP, London, 11.09.2017 (EBA/GL2017/05)
[34]	EBA (2018): EBA Draft Guidelines on ICT and Security Risk Management (EBA/CP/2018/15), London, 13.12.2018
[35]	BaFin (2018): Europäische Aufsichtsbehörden BaFin übernimmt grundsätzlich alle Leitlinien sowie Fragen und Antworten in ihre Verwaltungspraxis, in: BaFin-Journal Februar 2018, S. 5 (ohne Verfasser).
[36]	EBA (2019): Revised Guidelines on Outsourcing Arrangements, London, 25.02.2019 (EBA/GL/2019/02)
[37]	EBA (2018): EBA Draft Guidelines on Outsourcing arrangements, London, 22.06.2018 (EBA(CP/2018/11))
[38]	Die nicht vertraulichen schriftlichen Stellungnahmen sind unter folgendem Link abrufbar: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements/-/regulatory-activity/consultation-paper. Darüber hinaus fand auch eine öffentliche Anhörung statt (vgl. EBA/GL/2019/02, 69)
[39]	EBA/GL/2019/02, 70
[40]	EBA/GL/2019/02, 30
[41]	EBA/GL/2019/02, 36 und 37
[42]	EBA/GL/2019/02, 47 und 48
[43]	EBA/CP/2018/11, 37 und 38
[44]	EBA/GL/2019/02, 44
[45]	EBA/GL/2019/02, 22; hinsichtlich Cloud-Outsourcing-Lösungen ist auf die Vorgaben der Empfehlungen EBA/Rec/2017/03 hinsichtlich der Dokumentation und Vertragsgestaltung zu verweisen, die bereits seit 30.06.2018 in Kraft sind
[46]	RL/2015/2366/EU
[47]	Der deutsche Gesetzgeber hat sich wie schon bei der PSD I dazu entschlossen, die zivilrechtlichen Regelungen in das Bürgerliche Gesetzbuch (dBGB) zu implementieren und die aufsichtsrechtlichen Regelungen im Zahlungsaufsichtsgesetz (ZAG) zu regeln. In Österreich erfolgte die Umsetzung wiederum wieder in einem eigenen Sondergesetz, dem ZaDiG 2018
[48]	Ausführlich zur PSD II siehe etwa Tuder, Grundsatzfragen des ZaDiG infolge der ZDRL II (2019)
[49]	Die Umsetzung der Art 95 und 96 PSD II erfolgte in Deutschland in §§ 53 und 54 ZAG und in Österreich in den §§ 85 und 86 ZaDiG 2018
[50]	Vgl. *Tuder*, Grundsatzfragen des ZaDiG infolge der ZDRL II, 160
[51]	Vgl. *Tuder*, Grundsatzfragen des ZaDiG infolge der ZDRL II, 160 f
[52]	Vgl. FMA, Fakten, Trends und Strategien 2019, 151
[53]	Paust, Michael/Essler, Renate (2018): Bankaufsichtliche Anforderungen an die IT (BAIT), Vortrag im Rahmen der BaFin-Konferenz, IT-Aufsicht bei Banken, Frankfurt am Main, 27.09.2018
[54]	EBA (2018): Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2), London, 12.01.2018 (EBA/GL/2017/17)
[55]	ECB Banking Supervision (2018): Report on the Thematic Review on effective risk data aggregation and risk reporting, 08.05.2018
[56]	Basel Committee on Banking Supervision (2018): Progress in adopting the principles for effective risk data aggregation and reporting, Basel, 21.06.2018
[57]	FMA, Fakten, Trends und Strategien 2019, 146 f
[58]	FMA, Fakten, Trends und Strategien 2019, 147
[59]	FMA, Fakten, Trends und Strategien 2019, 149 f
[60]	Financial Stability Board (2018): Cyber Lexicon, Basel, 12.11.2018
[61]	Basel Committee on Banking Supervision (2018): Cyber-Resilience. Range of Practices, Basel 04.12.2018

[62]	Basel Committee on Banking Supervision (2017): Identification and Management of Step-in Risk, Basel 25.10.2017
[63]	G7 (2018): Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector, Oktober 2018: https://www.bundesbank.de/de/aufgaben/themen/g7-staaten-verabschieden-berichte-zur-cyber-sicherheit-764580
[64]	G7 (2018): Fundamental Elements for Threat-Led Penetration Testing, October 2018: https://www.bundesbank.de/de/aufgaben/themen/g7-staaten-verabschieden-berichte-zur-cyber-sicherheit-764580
[65]	Zur NIS-RL siehe etwa Burgstaller, NIS – Netz- und Informationssicherheit, ZIR 2016, 139; Haslinger, Rechtliche und organisatorische Aspekte neuer Meldepflichten im Bereich der Netz- und Informationssicherheit, jusIT 2017, 218
[66]	Vgl. § 2 NISG
[67]	Vgl. § 16 Abs. 2 NISG
[68]	§ 16 Abs. 3 NISG
[69]	§ 20 Abs. 1 NISG
[70]	Siehe https://www.bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf (abgefragt am 10.3.2019)
[71]	Basel Committee on Banking Supervision (2017): Basel III. Finalising Post-Crisis Reform, Basel 07.12.2017
[72]	Basel Committee on Banking Supervision (2018): Pillar 3 Disclosure Requirements, updated framework, Basel, 11.12.2018
[73]	European Commission (2018): Call for advice to the EBA for the purposes of revising the own fund requirements for credit, operational, market and credit valuation adjustment risk, Brüssel 04.05.2018
[74]	ECB Banking Supervision (2018): ECB Guide to internal Models. General topics chapter, 15.11.2018
[75]	Delegierte Verordnung (EU) Nr. 529/2014 der Kommission vom 12. März 2014 zur Ergänzung der Verordnung (EU) 575/2013 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die Beurteilung der Wesentlichkeit von Erweiterungen und Änderungen des auf internen Beurteilungen basierenden Ansatzes und des fortgeschrittenen Messansatzes veröffentlicht im Amtsblatt der Europäischen Union, 20.05.2018
[76]	Buchmüller, Patrik / Mährle, Christine / Rambock, Oliver (2019): Agenda Bankrisikosteuerung: Hauptthemen für 2019, in: Risikomanager, 01/2019, S. 21-27