D 7465

Zeitschrift für das gesamte
KREDITWESEN

77. Jahrgang · 1. Februar 2024

3-2024

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

Digitaler Sonderdruck

Foto: Adobe Stock (PX Media)

Regulatorische Agenda 2024 für Vorstand und Aufsichtsrat

Martin Neisen / Peter Büttel / Wiebke Sawahn

Martin Neisen / Peter Büttel / Wiebke Sawahn

Regulatorische Agenda 2024 für **Vorstand** und **Aufsichtsrat**

Das makrofinanzielle Umfeld, in dem sich Banken aktuell bewegen, ist herausfordernd: Neben dem deutlichen Zinsanstieg in Reaktion auf die anhaltend hohe Inflation befinden sich Realwirtschaft und Finanzsystem in einer Transitionsphase, geprägt vom klimapolitisch vorgegebenen Übergang zu einer kohlenstoffarmen Wirtschaft und anstehenden Strukturveränderungen bedingt durch demografischen Wandel und die tiefgreifende Digitalisierung aller Lebensbereiche.[1)]

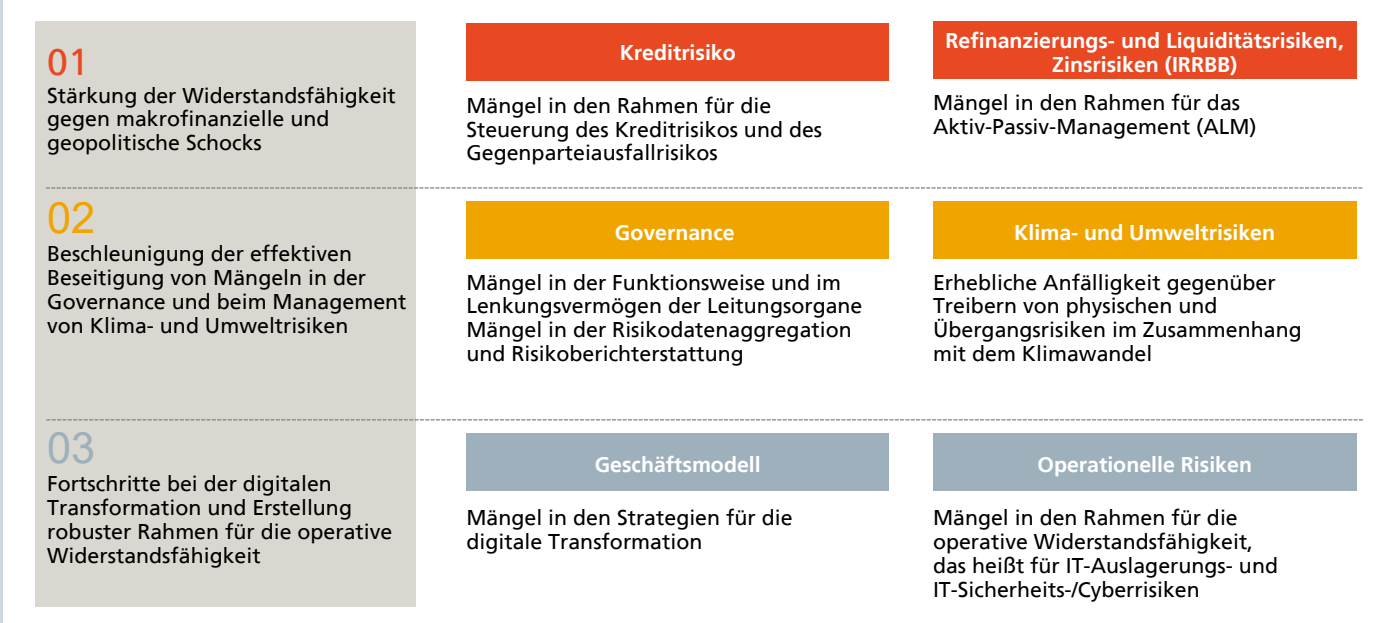
Damit nicht genug – das anhaltend unsichere geopolitische Umfeld mit immer neuen Krisenherden und Naturkatastrophen als „most anticipated crisis ever" wirkt sich auf das Verhalten der Marktteilnehmer aus, die von wirtschaftlichen Konsequenzen, Lieferengpässen und Ausfallwahrscheinlichkeiten betroffen sind.

Europäische Banken mit solider Kapitalausstattung

Gegenüber diesen Unwägbarkeiten müssen die Institute stark und widerstandsfähig sein. Im Rahmen der 2023 durchgeführten Stresstests von Europäischer Zentralbank (EZB) und Europäischer Bankenaufsichtsbehörde (European Banking Authority, EBA) zeigen die Ergebnisse, dass der deutsche Bankensektor insgesamt Krisenszenarien aufgrund der soliden Kapital- und Liquiditätspositionen gut bewältigen konnte.[2)] Die SREP-Ergebnisse 2023 bestätigen, dass die europäischen Banken im Hinblick auf die quantitativen Messgrößen für Kapital und Liquidität den makroökonomischen Herausforderungen 2023 gewachsen waren, sodass keine signifikanten Änderungen der Scorewerte und Säule-2-Anforderungen folgen.[3)]

Allerdings bestehen die eingangs erwähnten Unwägbarkeiten und Abwärtsrisiken weiter und dürften in Zukunft angesichts der vielen schwelenden Konflikte (China/Taiwan, Israel, Wahlen USA) sogar zunehmen, sodass die positiven quantitativen Kennzahlen in Relation zur Qualität von Risikomanagementverfahren und Governance zu sehen sind. Die zunehmend schlechten Risikoaussichten erfordern ein umsichtiges Risikomanagement

Abbildung 1: Aufsichtsprioritäten der EZB für 2024 bis 2026



Quelle: PwC

sowie eine stringente, vorausschauende Aufsicht. Fehlt beides, kann dies Krisen begünstigen, wie die Bankenturbulenzen im Frühjahr 2023 gezeigt haben.[4] Entsprechend haben sich die Schwerpunkte der EZB-Aufsicht für 2024 bis 2026 leicht verlagert. Im Fokus stehen drei Aufsichtsprioritäten, mit denen identifizierte Schwachstellen der Banken mit speziellen strategischen Zielen und Arbeitsprogrammen angegangen werden.

Stärkung der Widerstandsfähigkeit

Vor dem Hintergrund der (weiterhin) unsicheren makrofinanziellen Lage müssen die Institute darauf vorbereitet sein, dass die Refinanzierungsquellen volatiler werden, die Refinanzierungskosten steigen und Risiken auch kurzfristig und häufiger neu zu bewerten sind. Inwieweit die Banken diesen Herausforderungen mit diversifizierten Refinanzierungsquellen und zuverlässigen, soliden Refinanzierungsplänen begegnen, wird die Europäische Zentralbank gezielt überprüfen.

Angesichts des Umfelds höherer Zinsen und unsicherer Zinsentwicklung steht das Management von Zinsänderungsrisiken im Anlagebuch (Interest Rate Risk in the Banking Book – IRRBB) ebenfalls im Fokus der EZB-Aufsicht.[5] Zu den bereits 2022 überarbeiteten EBA-GL und RTS zum IRRBB, die Ausreißertests zu spezifischen aufsichtsrechtlichen Schock-Szenarien und Bewertungskriterien für den Nettozinsertrag und den wirtschaftlichen Wert des Eigenkapitals enthalten, kommen mit den ab 30. September 2024 anzuwendenden ITS (EBA/ITS/2023/03) umfangreiche Berichtsanforderungen für die Bewertung und Überwachung des IRRBB hinzu.

Die Meldeanforderungen gelten für alle europäischen Banken – mit vereinfachten Meldepflichten für kleinere Institute. Die Institute werden prüfen müssen, ob ihre IRRBB-Risikosimulationen die zur Erfüllung der Meldepflicht erforderlichen granularen Daten zu Zinsbindungsbilanzen, Modellparametern und Marktwertveränderungen in Stressszenarien aktuell liefern können. Hinzu kommt, dass die Daten aus den Bereichen Meldewesen, Risikomanagement und Controlling konsistent unter einen Hut zu bringen sind.

CRR III

Resilienz gegenüber einem volatilen Marktumfeld schafft vor allem eine angemessene Kapitalausstattung der Banken verbunden mit den entsprechenden Aufsichtsstandards. Nach der Einigung von EU Council und EU Parlament zum Bankenpaket sind im Dezember 2023 die (vorläufig) finalen CRR III/CRDVI-Vorschriften vorgelegt worden. Damit geht die Umsetzung von Basel III in der Europäischen Union durch CRR III/CRDVI auf die Zielgerade. Letzte Anpassungen kurz vor Abschluss der Einigung umfassen Korrekturen und Ergänzungen zu den Anforderungen an SA-CVA sowie das regulatorische CVA-Modell.

Darüber hinaus steht nun fest, dass die Anwendung des Output Floors sowohl auf konsolidierter als auch auf individueller Ebene erfolgen muss.[6] Bereits zu Jahresbeginn soll die finale Zustimmung von Rat und Parlament erfolgen, um noch im ersten Halbjahr 2024 als finale Rechtstexte im Amtsblatt der Europäischen Union offiziell veröffentlicht zu werden.[7] Substanzielle inhaltliche Änderungen werden dabei im Rahmen des endgültigen Verabschiedungsprozesses nicht mehr erwartet.

Höchste Zeit also, sich intensiv mit den weitreichenden Änderungen, insbesondere bei der Berechnung der risikogewichteten Aktiva, vertraut zu machen, denn die CRR III wird zum 1. Januar 2025 in Kraft treten. Am 12. Mai 2025 ist bereits die Einreichung der ersten Meldungen nach den Vorgaben der CRR III bei den zuständigen Aufsichtsbehörden fällig (zum Stichtag 31. März 2025). Die vorläufigen Ergebnisse der Internationalen PwC-Benchmark-Studie zum CRR-III-Umsetzungsstand zeigen, dass vor allem die Änderungen in Bezug auf den Kreditrisikostandardansatz (insbesondere Forderungsklasse Real Estate, Verwendung externer Ratings sowie die Floor-Regelungen) größere Umsetzungsherausforderungen darstellen. Wenig überraschend sehen die Institute auch die ESG-Offenlegungsanforderungen als schwierig an.[8] Insgesamt zeigen die Ergebnisse, dass viele Institute noch einen längeren Weg bis


Foto: PwC

Martin Neisen

Partner FS Governance, Risk and Compliance, Head of EBA/SSM Office – Global Basel IV Leader, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Frankfurt am Main


Foto: PwC

Peter Büttel

StB/WP, Partner FS Governance, Risk and Compliance, Regulatory Audit Lead, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Frankfurt am Main


Foto: PwC

Wiebke Sawahn

Senior Associate, FS Governance, Risk and Compliance Knowledge, Training and Media, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Stuttgart

Über einen Mangel an regulatorischen Aufgaben können sich Banken nicht beklagen. Die Herausforderungen werden nicht weniger – im Gegenteil! Grund genug, auch in diesem Jahr – nun zum 13. Mal – mit dem Überblick über die laufende Aufsichtspraxis der zuständigen nationalen, europäischen und internationalen Instanzen die traditionelle Vorschau auf die regulatorische Agenda für das frisch begonnene Jahr zu veröffentlichen. Die Dynamik der Neuerungen lasse es dabei zunehmend schwerfallen, auf Erfahrungswerte zurückzugreifen. Aber auch die Aufseher sehen die Autoren vor einer großen Aufgabe, Antworten auf teilweise unbekannte und schwer zu prognostizierende Herausforderungen zu finden. (Red.)

zur Implementierung aller Anforderungen der CRR III vor sich haben.

Parallel dazu hat die EBA ihren Umsetzungsfahrplan für die rund 140 technischen und regulatorischen Umsetzungsstandards, Guidelines und Reports veröffentlicht.[9)] In vier Phasen wird das umfangreiche Arbeitspaket, abgestuft nach Umsetzungsfristen, ausgerollt. Phase 1 und 2 umfassen die CRR-III-Mandate in Bezug auf Kredit-, Markt- und operationelles Risiko, die Bereiche zu ESG-Risiken und Governance aus der CRD VI, sowie die ersten technischen Standards (aufsichtliche Berichterstattung und die Offenlegung der Säule 3, Markt- und Gegenparteiausfallrisiko). Mit den technischen Standards für das aufsichtliche Meldewesen und für die Pillar-3-Offenlegung liegen die ersten Konsultationen schon vor – mit vielen zusätzlichen Berichts- und Offenlegungspflichten, die direkt in die aktuellen Umsetzungsprojekte einfließen sollten.[10)]

Insgesamt stehen die Institute vor der Herausforderung, dass sie ihre Vorbereitungen zur Umsetzung der CRR III auf Annahmen und eigene Auslegungsentscheidungen stützen müssen, solange die finalen EBA-Vorgaben (noch) nicht vorliegen. Umso wichtiger wird es sein, bei den laufenden Konsultationen sowohl den Überblick als auch den Einblick zu behalten, um die Umsetzungskonzepte direkt mit den richtigen Vorgaben und Variablen anzugehen beziehungsweise innerhalb des Konsultationsverfahrens entsprechend anzupassen. Angesichts des schieren Umfangs des Arbeitspakets und den damit zusammenhängenden zusätzlichen Anforderungen jedenfalls keine leichte Aufgabe.

Die MaRisk-Novelle

Bereits 2023 stand die 7. Novellierung der Mindestanforderungen an das Risikomanagement (MaRisk) auf der regulatorischen Agenda. Ende Juni 2023 wurden die finalen MaRisk veröffentlicht und müssen im Wesentlichen bis zum 1. Januar 2024 umgesetzt werden. Die zentrale Änderung der 7. MaRisk Novelle ist die Umsetzung der im Mai 2020 veröffentlichten EBA-Leitlinien für die Kreditvergabe und Überwachung in deutsches Aufsichtsrecht. Viele Institute haben bereits im vergangenen Jahr Vorstudien zum Erfüllungsgrad durchgeführt und die Implementierung abgeschlossen. Die Anforderungen des neuen BTO 3 an das Immobiliengeschäft wurden von den betroffenen Instituten in der Regel gut und zeitgerecht umgesetzt, da eine Vielzahl der Anforderungen aus vergleichbaren Regelungen des BTO 1 bekannt war.[11)]

Größere Herausforderungen ergeben sich für die Institute bei der Umsetzung der ESG-/Nachhaltigkeitsrisiken. Die Ableitung von plausiblen ESG-Szenarien und die Quantifizierung der ESG-Risiken stellen die Institute – auch bedingt durch fehlende Best Practices vonseiten der Aufsicht – vor größere Herausforderungen. Die Implementierung der komplett neuen Anforderungen an Modelle des AT 4.3.5 fordert von den Instituten eine Inventarisierung und Bewertung/Quantifizierung des Modellrisikos. Vielfach fehlen Instituten die – zur korrekten Identifizierung und Bewertung notwendigen – Zulieferungen von zentralen IT-Dienstleistern, sodass diese neuen Anforderungen flächendeckend den geringsten Umsetzungsstand aufweisen und für das Jahr 2024 bei den Instituten eine deutliche Priorisierung – auch vor dem Hintergrund der aufsichtlichen Erwartungshaltung – erfahren wird.[12)]

„Beim Thema Governance sieht die EZB noch deutliche Mängel bei den Banken."

Zahlungs- und E-Geldinstitute erhalten mit den noch in der Konsultation befindlichen Mindestanforderungen an das Risikomanagement von ZAG-Instituten (ZAG-MaRisk) einen eigenen, auf ihr Geschäftsmodell zugeschnittenen Rahmen zur Ausgestaltung der Risikomanagementprozesse.[13)] Im Fokus stehen operationelle Risiken (einschließlich IT-Risiken), aber auch Adressausfallrisiken, Marktpreisrisiken, Geschäftsmodellrisiken und Liquiditätsrisiken, soweit diese für das Businessmodell wesentlich sind.

Diese Risiken müssen unter Berücksichtigung von Risikokonzentrationen und des Gesamtrisikoprofils durch Risikodeckungspotenzial abgeschirmt sein. Damit wird eine an das Geschäftsmodell angepasste „Risikotragfähigkeitsrechnung" künftig auch von ZAG-Instituten gefordert.[14)] Da die Konsultationsphase erst Mitte Januar 2024 endet, dürfte mit einem Inkrafttreten der ZAG-MaRisk wohl nicht mehr im ersten Quartal 2024 zu rechnen sein. Allerdings zeigen die Erfahrungen mit den MaRisk für Banken, dass hier eher ein „Dauerlauf" bevorstehen könnte, mit künftigen Ausweitungen der Anforderung, die stets im Blick zu behalten sind, um auch auf kurzfristige Änderungen der aufsichtsrechtlichen Vorgaben reagieren zu können.

BCBS 239 – Mängel bei Risikodaten und Berichterstattung

Beim Thema Governance sieht die EZB noch deutliche Schwächen der Banken, wenn es um die Einhaltung der Grundsätze zur Risikodatenaggregation und Risikoberichterstattung (BCBS 239) sowie die Umsetzung der damit verbundenen aufsichtlichen Erwartungen geht. Ähnliche Beobachtungen gelten auch für die global systemrelevanten Institute: Nur zwei von 31 bewerteten global systemrelevanten Banken konnten volle Compliance mit den Grundsätzen sicherstellen.[15)]

Neben Schwachstellen in der Datenarchitektur, fragmentierten, nicht zusammenpassenden IT-Landschaften sind geringe Kapazitäten für die Datenaggregation und ineffektive Governance-Rahmen die größten Problemfelder, die es (endlich) anzugehen gilt. Immerhin liegen die BCBS-Grundsätze bereits seit 2013 vor. Im neuen Leitfaden „Guide on effective risk data aggregation and risk reporting" (final geplant für 2024) legt die EZB daher

nochmals ihre aufsichtlichen Erwartungen fest – als „Weckruf" und „Ermahnung" an die Institute, der Umsetzung der BCBS-Grundsätze die erforderliche Aufmerksamkeit einzuräumen.

Um dem Thema mehr Nachdruck zu verleihen, ist vorgesehen, die Leitungsorgane für die Fortschritte ihrer Bank bei der Umsetzung zur Verantwortung zu ziehen.

> „Ab 2025 gelten die umfangreichen qualitativen und quantitativen Offenlegungsanforderungen der Säule III."

Darüber hinaus sollen ab 2024 zunehmend Eskalations- und Sanktionsmechanismen Anwendung finden, ergänzt durch gezielte (Vor-Ort-)Überprüfungen und einen jährlichen Managementbericht zur Datengovernance und Datenqualität. Damit erhöht die EZB für die von ihr beaufsichtigten Institute den Druck, zügig Compliance mit BCBS 239 zu erreichen. Es ist also ratsam, die laufenden Umsetzungsprojekte zu priorisieren und bereits an den aufsichtlichen Erwartungen des Konsultationsentwurfs zu messen und bei Bedarf anzupassen beziehungsweise zu erweitern.

Darüber hinaus sollten sich die Institute auf aufsichtliche Prüfungen einstellen und entsprechend vorbereiten – zum Beispiel durch den Aufbau der notwendigen Ressourcen mit ausreichender Kenntnis und Erfahrung im Hinblick auf Datenmanagement, IT und Risikomanagement innerhalb des Leitungsorgans oder die Überarbeitung der internen Dokumentation. Es ist zu erwarten, dass die Anforderungen – auch wenn in geringerem Umfang – für LSIs und kleinere Institute als Maßstab herangezogen werden.

Schwachstelle Management von Klima- und Umweltrisiken

Um Klima- und Umweltrisiken gemäß der „Aufsichtsprio 2" weiter zu begrenzen und offenzulegen, erwartet die Aufsicht, dass die Banken diese angemessen sowohl in ihre Geschäftsstrategie als auch in ihre Governance- und Risikomanagementrahmenwerke einbeziehen. Die Europäische Zentralbank drückt aufs Tempo: Nur noch bis Ende 2024 läuft die Frist für die Banken, um die aufsichtlichen Erwartungen aus ihrem Leitfaden für Klima- und Umweltrisiken[16] vollständig zu erfüllen, darunter auch die Integration in den bankinternen Prozess zur Sicherstellung einer angemessenen Kapitalausstattung (Internal Capital Adequacy Assessment Process – ICAAP) und in die Stresstests.

Entsprechend werden Schwachstellen der Banken bei der strategischen und operativen Planung sowie mangelnde Kenntnisse der Leitungsorgane in den Bereichen Umwelt, Soziales und Unternehmensführung im SREP 2023 mit qualitativen Maßnahmen adressiert. Darüber hinaus stellt die EZB in Aussicht, ihr gesamtes Arsenal an Sanktions- und Eskalationsmaßnahmen auszuschöpfen (Kapitalaufschläge, Geldbußen, Zwangsgelder und so weiter), um sicherzustellen, dass die aufsichtlichen Erwartungen rechtzeitig erfüllt werden.[17]

Auch die Institute unter BaFin-Aufsicht, müssen sich (noch) intensiver mit dem Umweltrisiken und ihren besonderen Eigenschaften als Risikotreiber auseinandersetzen, denn die Berücksichtigung von Nachhaltigkeitsaspekten in der Aufsicht ist ein Mittelfristziel der BaFin und Schwerpunkt für die kommenden Jahre.[18] Dabei schlagen sich finanzielle Klimarisiken in den bekannten Risikokategorien nieder und werden hier im Risikomanagement (mit-)berücksichtigt – zum Beispiel in den MaRisk oder zuletzt im Rahmen der CRD VI. Bestimmungen zu ESG-Risiken wurden hier verschärft: Die Banken müssen spezifische Pläne und quantifizierbare Ziele zur Bewältigung kurz-, mittel- und langfristiger Risiken aus ESG-Faktoren entwickeln, einschließlich Übergangsplänen, die mit den ESG-Anforderungen aus anderen regulatorischen Zielen/Rechtsakten der EU übereinstimmen, wie zum Beispiel der Richtlinie über die Nachhaltigkeitsberichterstattung von Unternehmen (CSRD).[19]

Nach wie vor stehen die Institute aber vor der Aufgabe, herauszufinden, wie sie ihre spezifischen Umweltrisiken besser erkennen können, wo sie den größten Konzentrationsrisiken ausgesetzt sind, wie sie diese messen können und wo ihnen noch zuverlässige Daten hierfür fehlen. Mehr Transparenz und Verlässlichkeit bei der Datengrundlage sowohl für die Institute als auch für Anleger und Marktteilnehmer wird sukzessive mit europäischen Offenlegungsanforderungen geschaffen: Ab 2025 gelten die umfangreichen qualitativen und quantitativen Offenlegungsanforderungen der Säule III für alle CRR-Institute (bislang sind nur große kapitalmarktorientierte Institute zur Offenlegung ihrer ESG-Risiken verpflichtet).

Im Rahmen einer aktuellen PwC-Studie hat sich gezeigt, dass dort durchaus noch Lücken in den Offenlegungsberichten bestehen – zum Beispiel bei den qualitativen Informationen zu ESG-Risiken sowie bei den Angaben zu sozialen und governancebezogenen Aspekten.[20]

Schritt zur Verbesserung der Informationslage

Ein weiterer Schritt zur Verbesserung der Informationslage wird mit der EU-Richtlinie zur Nachhaltigkeitsberichterstattung im Lagebericht getan (Corporate Sustainability Reporting Directive, CSRD). Abhängig von Größe sowie Kapitalmarktorientierung werden Unternehmen nach und nach berichtspflichtig – beginnend für das Geschäftsjahr 2024 mit Unternehmen, die bereits der Pflicht zur nichtfinanziellen Erklärung unterliegen. Bis zum Jahr 2028 werden dann rund 50 000 Unternehmen in der Europäischen Union von den neuen Anforderungen betroffen sein und müssen über die Nachhaltigkeitsdatenpunkte berichten, die für sie aus finanzieller Sicht und im Hinblick auf die Auswirkungen wesentlich sind.

Dabei bringt die Nachhaltigkeitsberichterstattung viele neue Anforderungen: Die Daten müssen rechtzeitig erhoben und auf Wesentlichkeit analysiert werden, Reporting-Strategien und Systeme der Finanzberichterstattung werden sich nur bedingt auf die Nachhaltigkeitsberichterstattung übertragen lassen.[21)] Die Geschäftsführung wird auch die Nachhaltigkeitsberichterstattung überwachen und mit Blick auf den Anwendungszeitpunkt vorantreiben müssen, denn die BaFin prüft künftig die Nachhaltigkeitsberichterstattung als Teil des Lageberichts von kapitalmarktorientierten Unternehmen im Rahmen der Bilanzkontrolle.

Schwachstelle operative Resilienz

Die operative Widerstandsfähigkeit der Institute bei fortschreitender Digitalisierung des Geschäftsbetriebs und ihres Leistungsangebots ist für 2024 ein weiteres Fokusthema. Die EZB testet seit dem 2. Januar 2024 im Rahmen eines Stresstests zur Cyberresilienz, inwieweit die Institute in der Lage sind, auf einen erfolgreichen Cyberangriff, der Störungen im Tagesgeschäft verursacht, zu reagieren und sich davon zu erholen.[22)] In diesen qualitativen Test sind 109 direkt beaufsichtigte Institute einbezogen, 28 davon werden im Testverlauf eingehender geprüft. Rund 500 Fragen müssen von allen betroffenen Instituten beantwortet werden: Es geht um das Security-Incident-Response-Verfahren, also um die Meldung eines simulierten Cybervorfalls, die Nachweisbarkeit der Reaktionsfähigkeit im Rahmen der internen Richtlinien, Wiederherstellungsprozesse und Notfallpläne. Darüber hinaus werden auch potenzielle Auswirkungen und quantitative Bewertungen der Risiken im operationellen Bereich gefragt.

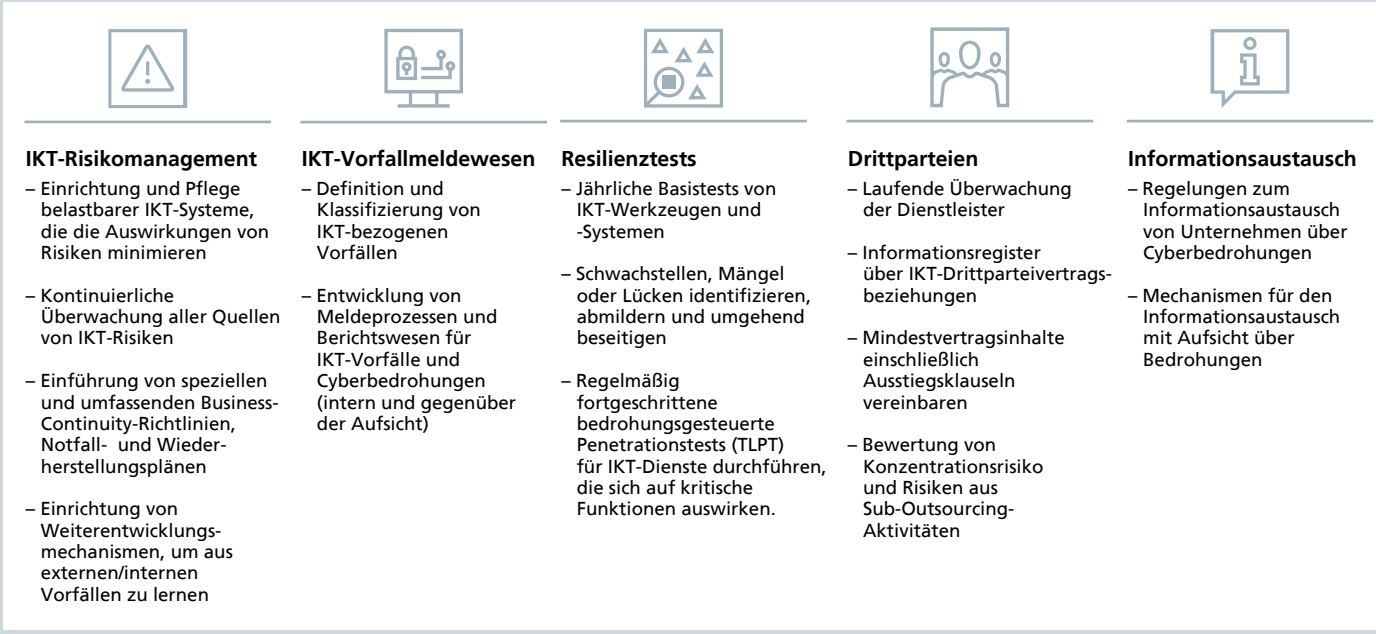
Beide Themenkomplexe erfordern eine detaillierte, umfangreiche und vollständige Dokumentation aller Verfahren, Methoden und Verantwortlichkeiten. Bis zum 29. Februar 2024 haben die Institute Zeit, den Fragenkatalog zu beantworten. Für die 28 Institute im vertieften Testverfahren geht es weiter: Sie müssen einen umfassenden IT-Recovery-Test durchführen. In beiden Testläufen müssen sich Institute auf Nachfragen, Validierungen und vor allem Nachbesprechungen mit der Aufsicht einstellen, denn die gewonnen Erkenntnisse sollen 2024 in die allgemeine aufsichtliche Beurteilung des SREP einfließen und die Ergebnisse beziehungsweise die daraus gezogenen Lehren mit den einzelnen Banken besprochen werden.

Nicht nur eine rein regulatorische Aufgabe

Letztlich sollten die Institute also die Chance nutzen, den Cyberresilienztest nicht nur als rein regulatorische Übung zu sehen, sondern ihre Widerstandsfähigkeit tatsächlich auf ein neues Level zu heben, zumal im aktuellen geopolitischen Umfeld die Zahl der gemeldeten Cyberangriffe zuletzt sprunghaft angestiegen ist.[23)] Darüber hinaus dürften alle Anstrengungen, die über Standardverfahren zur Quantifizierung von operationellen Risiken hinausgehen, ein lohnendes Investment für zukünftige regulatorische Anforderungen und aufsichtliche Erwartungen sein, die in diesem Bereich eher steigen werden.

Institute, die nicht unter EZB-Aufsicht stehen, dürfen sich beim Thema Cyberresilienz kaum entspannt zurücklehnen, denn auch die deutsche Aufsicht läuft sich schon mal warm für kommende Aufgaben: Im Rahmen einer Cyberkrisenübung probten BaFin zusammen mit Behörden und Banken, Versicherern,

Abbildung 2: Regulatorische Schwerpunkte von DORA



Quelle: PwC

Wertpapierhäusern, Zahlungsinstituten und IT-Dienstleistern wie das deutsche Finanzsystem einem schweren Cyberangriff effektiv und abgestimmt begegnen und im Ernstfall schnell und vor allem koordiniert entscheiden könnte.[24] Aufsichtsrechtlich steckt der EU Digital Operational Resilience Act (DORA) den regulatorischen Rahmen ab, auf dessen Grundlage die BaFin dafür sorgt, dass die Finanzunternehmen in Deutschland zur Abwehr von Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologie (IKT) künftig besser aufgestellt und widerstandsfähiger sind – ab 17. Januar 2025 wird die EU-Verordnung für mehr als 3 500 Unternehmen im deutschen Finanzsektor verbindlich.[25]

„Aufsichtsrechtlich steckt der DORA den regulatorischen Rahmen ab."

Die regulatorischen Schwerpunkte von DORA sind in Abbildung 2 dargestellt.

Neben den Anforderungen an die internen Unternehmensbereiche und -verfahren stehen vor allem die Risiken aus IT-Dienstleistungen Dritter im Fokus, denn Unzulänglichkeiten in den komplexen IT-Auslagerungsvereinbarungen bei zunehmender Abhängigkeit von externen Anbietern können zu neuen Konzentrationsrisiken führen – eine wesentliche Schwachstelle, die auch die EZB unter anderem mit der Analyse von Auslagerungsregistern zur Ermittlung von Verflechtungen zwischen beaufsichtigten Instituten und externen Anbietern sowie gezielten Überprüfungen von Auslagerungsvereinbarungen in Angriff nehmen wird.

Gerade was die Überwachung von kritischen Dienstleistern und den Einfluss auf große internationale Cloud-Anbieter angeht, erwartet die BaFin durch DORA jedenfalls eine deutliche Verbesserung: künftig dürften Verflechtungen und Marktkonzentrationen bei Dienstleistern viel besser erkannt und gemeinsam europäisch überwacht werden. Um eine vorausschauende und effektive Aufsicht sicherzustellen, sieht der Entwurf des Finanzmarktdigitalisierungsgesetzes vor, die Einhaltung der Vorschriften von DORA im Rahmen der Jahresabschlussprüfung zu prüfen. Offen ist aktuell noch, inwieweit es durch diese geplanten Gesetzesänderungen zu Überschneidungen in den Jahresabschlussprüfungen durch Prüfungshandlungen zur Einhaltung der Anforderungen aus BAIT, KAIT und ZAIT kommen wird.[26]

Die Institute werden die Zeit bis Januar 2025 auf jeden Fall gut nutzen müssen: Das gesamte IKT-Risikomanagement muss einer Reifegradprüfung unterzogen werden und gegebenenfalls auf ein neues Level gehoben werden, um die Vielzahl der (auch technischen Vorgaben) umzusetzen. Dies betrifft insbesondere die Dienstleistungen Dritter, denn auch dort müssen Risiken bekannt, analysiert und überwacht werden beziehungsweise darüber nachgedacht werden, wie Exit-Maßnahmen und -Strategien aussehen können. Nicht zu vergessen, dass hier noch umfangreiche Level-2-Dokumente der EBA in Form von RTS, Leitlinien und Empfehlungen ausstehen. Dabei ist der Weg zur digitalen operationellen Resilienz nicht nur Aufgabe der IT, sondern auch des Risikomanagements – und damit Chefsache.[27]

Krisenmanagement für den Ernstfall

Mit überarbeiteten Rundschreiben und Konsultationen geht die BaFin die Verbesserung der Abwicklungsfähigkeit der Institute an.[28] Dabei werden die bereits auf europäischer Ebene für Institute unter Zuständigkeit des Single Resolution Board (SRB) überarbeiteten EBA/GL/2023/05 (anwendbar ab dem 1. Januar 2024) berücksichtigt. Die Institute sind dazu aufgefordert – basierend auf den vorab festgelegten Abwicklungsstrategien – ihre Abwicklungsfähigkeit herzustellen oder zu verbessern. Dabei erhöht sich der Umfang und Detaillierungsgrad der aufsichtlichen Anforderungen und macht eine intensive Auseinandersetzung mit den unterschiedlichen Dimensionen der Abwicklungsfähigkeit unerlässlich.

Die BaFin erwartet von den Instituten, dass sie ihre Abwicklungsfähigkeiten testen und wird ebenfalls Tests mit den Instituten durchführen, die später in ein mehrjähriges Testprogramm der Abwicklungsplanung überführt werden. Mögliche (auch kombinierbare) Testmethoden sind dabei: Selbsteinschätzung, Walkthrough, Prüfung durch die Interne Revision, Dry Run (Testlauf), Bestätigung durch einen unabhängigen Dritten, Vor-Ort-Besuch oder Krisenübung.

Abwicklung erleichtern

Die Abwicklung von kleineren und mittelgroßen Banken in Schieflage zu erleichtern, steht im Fokus eines Vorschlags der EU-Kommission zur Anpassung und Stärkung des bestehenden EU-Rahmens für das Krisenmanagement im Bankensektor.[29] Gerade mittelgroße und kleinere Banken würden bei Ausfall häufig nicht abgewickelt, sondern andere Lösungen zulasten der Steuerzahler zum Einsatz kommen.

„Die BaFin erwartet von den Instituten, dass sie ihre Abwicklungsfähigkeiten testen."

Der Kommissionsvorschlag soll die Behörden in die Lage versetzen, ausfallende Banken unabhängig von ihrer Größe und ihrem Geschäftsmodell in einen geordneten Marktaustritt zu führen, und gibt ihnen diesbezüglich eine breite Palette von

Instrumenten an die Hand. Vorgesehen ist, dass die von den Banken selbst finanzierten Einlagensicherungsfonds einspringen, wenn nicht genügend Eigenkapital und verlusttragende Verbindlichkeiten da sind. Bislang stoßen diese Pläne auf wenig Gegenliebe, die Diskussion ist aber jedenfalls angestoßen.

Künstliche Intelligenz (KI) als Schlüsseltechnologie für die digitale Transformation ist längst im Bankensektor angekommen, zum Beispiel bei Kreditvergabeprozessen, die auf algorithmenbasierte Rating-, Scoring- oder Entscheidungsverfahren setzen. Harmonisierte Vorschriften und Standards für KI-Systeme soll der neue EU AI Act schaffen.[30)]

Er beinhaltet einen Regulierungsansatz, der KI-Systeme anhand ihrer Risiken klassifiziert und darauf aufbauend Qualitäts-, Dokumentations- und Transparenzstandards fordert.[31)] Die Anforderungen sind komplex und stellen die Institute vor neuartige Herausforderungen, müssen aber bereits jetzt in die Planungen und Überlegungen zum Einsatz von Künstlicher Intelligenz einbezogen werden.

Äußerst dynamisches regulatorisches Umfeld

Nach wie vor ist das Umfeld, in dem die Banken sich bewegen, von großen Unsicherheiten und Risiken mit hoher Dynamik geprägt: geopolitische Spannungen, die plötzlich in politische, wirtschaftliche und humanitäre Krisensituationen umschlagen, unvorhersehbare disruptive Klimakatastrophen und fragile Lieferketten. Banken müssen auf das „Unerwartete" immer schneller und flexibler mit tragfähigen Konzepten und Strategien reagieren.

Die Methoden, die dabei für die Risikomodellierung beziehungsweise -messung zum Einsatz kommen, sind alles andere als Standardformate. Datensätze, Variablen, Betrachtungshorizonte, Schätz- und – zunehmend weniger verlässliche – Erfahrungswerte sowie die passenden Prozesse müssen (neu) implementiert werden. Neue Risikodimensionen erfordern auch neue Aufsichtsmaßnahmen – entsprechend dynamisch muss auch die Bankenaufsicht agieren, um die neuen Risikofelder einzudämmen.

Gleichzeitig sind die Institute einer „neuen" regulatorischen Welle ausgesetzt – viele der schon länger in der Pipeline befindlichen umfangreichen Gesetzespakete (CRR III, CRD VI, DORA, AML et cetera) kommen innerhalb der nächsten Monate zur Anwendung. Auch wenn die Grundlagen der anstehenden regulatorischen

> „KI als Schlüsseltechnologie für die digitale Transformation ist längst im Bankensektor angekommen."

„Großprojekte" durch lange Konsultations- und Beratungsphasen bekannt sind, kommt eine Vielzahl von Begleitbestimmungen wie RTS, ITS, Guidelines, Empfehlungen und Auslegungsentscheidungen mit enormer Detailtiefe hinzu.

Große Herausforderungen

Aufgrund der neuartigen Dynamik fällt es zunehmend schwer, auf Erfahrungswerte zurückzugreifen. Aufseher stehen vor großen Herausforderungen, eine möglichst präventive Antwort auf teils unbekannte und schwer zu prognostizierende Risiken zu finden. Auch die Banken müssen sich auf dieses äußerst dynamische regulatorische Umfeld einstellen und den jeweiligen Entwicklungsstand sowohl bei den gesetzlichen Vorgaben als auch bei den aufsichtlichen Erwartungen stets im Blick behalten. Natürlich müssen dabei die unterschiedlichen Auswirkungen auf das individuelle Geschäftsmodell begleitend zu den Änderungen laufend analysiert werden.

Vorstand und Aufsichtsrat der Institute stehen in der Verantwortung und vor der Herausforderung, eine wirksame strategische Steuerung zu betreiben beziehungsweise zu überwachen und die Verfahren stetig weiterzuentwickeln, um die damit verbundenen Risiken angemessen zu bewerten, zu überwachen und zu steuern – inbesondere wenn es darum geht, die Geschäftsmodelle an stetig wechselnde Risikofelder, neue Trends bei der Digitalisierung und einen schnellen ökologischen Wandel anzupassen.

Fußnoten

1) Deutsche Bundesbank, Finanzstabilitätsbericht 2023
2) https://www.bafin.de/ref/19615732
3) bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp231219~421bbae836.de.html
4) Deutsche Bundesbank, Finanzstabilitätsbericht 2023
5) bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp231219~421bbae836.de.html
6) blogs.pwc.de/de/regulatory/article/241002: Die finale Phase der CRR III Veröffentlichung der endgültigen Fassungen von CRR III und CRD VI
7) EU Commission: https://finance.ec.europa.eu/news/latest-updates-banking-package-2023-12-14_en
8) PwC: CRR III Benchmarking Study, geplant für Februar 2024
9) eba.europa.eu/publications-and-media/press-releases/eba-publishes-roadmap-implementation-eu-banking-package
10) blogs.pwc.de/de/regulatory/article/: EBA Roadmap to implement the EU Banking Package
11) Maifarth/Thurmann/Heesen: 7. MaRisk-Novelle: Herausforderungen bei der Umsetzung, ZfgK 13/2023
12) Thurmann/Schröder: 7. MaRisk-Novelle und die neuen Anforderungen an Modelle, BankPraktiker 3/2023
13) https://www.bafin.de/ref/19677746
14) blogs.pwc.de/de/risk/article/239649: Mindestanforderungen an das Risikomanagement von ZAG-Instituten - ZAG-MaRisk
15) blogs.pwc.de/de/risk/article/240875: BCBS veröffentlicht 7. Fortschrittsbericht zur Umsetzung von BCBS 239
16) EZB-Leitfaden zu Klima- und Umweltrisiken, November 2020
17) bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp231207~10204b8b70.de
18) https://www.bafin.de/ref/19641124
19) finance.ec.europa.eu/news/latest-updates-banking-package-2023-12-14_en
20) PwC-Studie: „Zwischen Nachhaltigkeit und Transparenz – Die ESG Säule III Offenlegungsstudie", September 2023
21) pwc.de/de/audit-assurance/csrd-berichterstattung-und-pruefung.html
22) bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240103~a26e1930b0.de.html
23) bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory_priorities202312~a15d5d36ab.de.html
24) https://www.bafin.de/ref/19677678
25) pwc.de/de/im-fokus/cyber-security/digital-operational-resilience-act.html
26) blogs.pwc.de/en/trust-and-technology/article/240850: Kommt in Deutschland die Prüfungspflicht für die Anforderungen von DORA
27) https://www.bafin.de/ref/19617466
28) https://www.bafin.de/ref/19650828
29) https://ec.europa.eu/commission/presscorner/detail/de/ip_23_2250
30) https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473
31) www.pwc.de/de/risk-regulatory/responsible-ai/europaeische-ki-regulierung-und-ihre-umsetzung.html