5. MaRisk-Novelle

Erweiterung nationaler Vorgaben zu Risikomanagement und Auslagerung – Was lange währt wird endlich gut?

November 2017

Finale Fassung des neuen BaFin-Rundschreibens zu den „Mindestanforderungen an das Risikomanagement“

Zusammenfassung

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat am 27. Oktober 2017 die seit langem erwartete finale Fassung der MaRisk vorgelegt. Damit endet ein bereits am 18. Februar 2016 eingeleiteter Konsultationsprozess nach intensiven Abstimmungen mit der Kreditwirtschaft. Das Rundschreiben ist im Grundsatz für alle Institute gültig und tritt mit Veröffentlichung in Kraft. Während Klarstellungen umgehend anzuwenden sind, gilt für sogenannte Neuerungen eine Umsetzungsfrist bis 31. Oktober 2018.

Bezüglich der Anwendung ausgewählter Anforderungen der MaRisk, insbesondere der zu Datenmanagement, -qualität und –aggregation, erfolgt eine wichtige Festlegung: diese sind nur für global- und anderweitig systemrelevanten Institute (GSRI und ASRI) relevant. Dies gilt auch für bestimmte Vorgaben zur Geschäftsstrategie, Leitung der Risikocontrolling-Funktion, Organisation der Compliance-Funktion und zur Berichterstattung über Liquiditätsrisiken.

Materiell zielt die Überarbeitung des Rundschreibens vor allem auf die Umsetzung von weiterentwickelten internationalen und europäischen Vorgaben ab, insbesondere auf Standards der europäischen Bankenaufsicht EBA sowie des Basler Ausschusses für Bankenaufsicht (BCBS). Ferner sind Erkenntnisse der letzten Jahre aus der Aufsichtspraxis eingeflossen. Gegenüber einem inoffiziellen Zwischenentwurf wurden nur vereinzelt noch Änderungen vorgenommen, die die aufsichtliche Zielsetzung oder den Proportionalitätsgedanken stärker konkretisieren.

Wie erwartet betreffen die wesentlichsten Änderungen die Vorgaben vor allem zur Datenaggregation und Berichterstattung, zur Risikokultur sowie zur Auslagerung. Neben den oben genannten Schwerpunktthemen, bei denen

Inhalt

es sich häufig um Neuerungen mit entsprechend längeren Umsetzungsfristen handelt, ergeben sich zahlreiche Klarstellungen, die teilweise methodische, prozessuale oder organisatorische Auswirkungen haben und die die Institute je nach Komplexität des Geschäftsmodells in unterschiedlichem Ausmaß betreffen.

Diese befassen sich unter anderem mit Kreditprozessen, IT-Risiken, Liquiditäts- und Zinsänderungsrisiken im Bankbuch sowie der Ausgestaltung der Funktionentrennung, Risikotragfähigkeit und Revisionsplanung. Damit werden der unmittelbare Handlungsbedarf sowie die notwendige Einbindung unterschiedlichster Bereiche der Institute für die Umsetzung deutlich. Die BaFin weist darauf hin, dass sie Abweichungen von den genannten Umsetzungsfristen im begründeten Einzelfall für die Ausnahme hält.

Hinsichtlich der konkreten zeitlichen Umsetzungsfrist ist somit die Festlegung wichtig, ob es sich um eine Klarstellung oder Neuerung handelt. Im Anschreiben der BaFin an die Verbände der Kreditwirtschaft erfolgt zwar eine allgemeine Erläuterung zum Unterschied. Ansonsten werden aber zu den konkreten Änderungen analog zum Vorgehen bei der 4. Novelle nur vereinzelt Hinweise gegeben. Eine vollumfängliche Abgrenzung erfolgt bislang nicht. Diese wäre im Sinne der Planungs- und Umsetzungssicherheit aus Sicht der Kreditwirtschaft sicherlich zu begrüßen.

Der bisherige Mangel einer klaren Abgrenzung lässt den Schluss zu, dass die Aufsicht der Kreditwirtschaft entweder eine allgemeingültige Interpretation überlässt und sich somit Ermessensspielräume offen lässt oder eine institutsindividuelle Auslegung notwendig ist. Letztere kann sich neben der Prüfung der aktuell ggf. schon vorhandenen Regelungen auch daran orientieren, ob Änderungen der 5. Novelle beispielsweise bei einem größeren, international tätigen Institut bereits über internationale oder europäische Vorgaben zur Erwartungshaltung der Aufsicht Gegenstand der Weiterentwicklung des Risikomanagements sein sollten. Wie im Falle der Anforderungen an das Zinsänderungsrisiko im Bankbuch kann es sich dagegen für kleinere, national beaufsichtigte Institute sehr wohl um eine grundlegend „neue" Anforderung handeln.

Entstehung und Einordnung der 5. MaRisk-Novelle

Erstmals hatte die BaFin am 18. Februar 2016 einen neuen Entwurf der MaRisk der Kreditwirtschaft zur Konsultation überreicht. Nach Auswertung und Diskussion der Stellungnahmen der Kreditwirtschaft wurde am 24. Juni 2016 ein inoffizieller Zwischenentwurf zur Verfügung gestellt. Dieser enthielt bereits verschiedenste Anpassungen, die größtenteils im entsprechenden Fachgremium mit der Kreditwirtschaft besprochen wurden.

Die im Zwischenentwurf enthaltenen Anpassungen gingen oft mit Erleichterungen gegenüber der Ursprungsfassung einher und sollen eine praxisnahe Umsetzung durch die Institute sicherstellen. Dies betraf unter anderen Anforderungen im Kontext der Risikoberichterstattung, Anschaffung von Software, Gestaltung von Auslagerungsverträgen, Überprüfung des Neuen Produkte-Prozesses und der Sicherstellung einer unabhängigen Modellvalidierung.

Vor der nunmehr fünften Novellierung der MaRisk wurde die letzte grundlegend überarbeitete Fassung der MaRisk am 14. Dezember 2012 publiziert. Zwischenzeitlich hat das Aufsichtssystem in Europa fundamentale Änderungen erfahren:

- Mit der Schaffung der Bankenunion wurde eine einheitliche Beaufsichtigung mit der Europäischen Zentralbank (EZB) als neue Aufsichtsbehörde an der Spitze etabliert, deren Aufsichtspraxis sich von der deutschen unterscheidet und die Harmonisierung derselben in der Eurozone anstrebt.
- Sowohl die EZB als auch die Europäische Bankenaufsichtsbehörde (EBA) haben diverse Standards zur Ausgestaltung dieses neuen Aufsichtssystems veröffentlicht. Dazu gehören unter anderem das Aufsichtshandbuch der EZB sowie die Leitlinien zum SREP, zur Governance von Banken und die zum Management von IT-Risiken.
- Doch auch auf nationaler Ebene erfolgten aufgrund der Schaffung der Bankenunion und der Umsetzung von Basel III oder des Abwicklungs- und Sanierungsregimes zahlreiche Anpassungen der nationalen Rechtsgrundlagen.

Bezüglich der MaRisk wurde das Bundesministerium der Finanzen zwar durch § 25a Absatz 4 KWG ermächtigt, eine Verordnung zur Ausgestaltung eines angemessenen und wirksamen Risikomanagements auf Einzelinstituts- und Gruppenebene zu erlassen. Dennoch wurden die MaRisk wieder als Rundschreiben publiziert. Damit beschreiben die MaRisk weiterhin die Verwaltungspraxis der deutschen Aufsicht bei der Überprüfung der Ausgestaltung von §25a (Risikomanagement) sowie jetzt auch § 25b KWG (Auslagerung) durch die Institute.

Inhalte der 5. Novelle

Die wichtigsten inhaltlichen Neuerungen und Ergänzungen betreffen insbesondere folgende Themen:

Risikodaten und -berichtswesen

Die im Januar 2013 veröffentlichten „Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung" (BCBS 239) des Basel Committee on Banking Supervision werden durch die MaRisk nun auch in die deutsche Aufsichtspraxis übernommen.

Insgesamt entspricht die finale Fassung der MaRisk in Bezug auf die Risikodatenaggregation und –berichterstattung in wesentlichen Inhalten den Erwartungen und wurde nur punktuell bis auf die Konkretisierung der Umsetzungsfristen gegenüber den Konsultationsentwürfen angepasst.

Bei der Übernahme der in BCBS 239 veröffentlichten Grundsätze wurde zwischen Anforderungen, die ausschließlich von GSRI und ASRI zu erfüllen sind (Datenmanagement, Datenqualität und Aggregation von Risikodaten; **neues Modul AT 4.3.4**), und Anforderungen, die für **alle Institute** gelten (Risikoberichterstattung; neues **Modul BT 3**), unterschieden. Die Empfehlung, dass Institute, die nicht GSRI oder ASRI sind, ihre Risikodatenaggregationsfähigkeiten zumindest prüfen und weiter optimieren, bleibt im Anschreiben der BaFin zwar bestehen, fällt in der Formulierung aber vergleichsweise weich aus.

Für das neue Modul AT 4.3.4 gilt eine vom Grundsatz abweichende Umsetzungsfrist. Institute, die die Anforderungen des AT 4.3.4 erfüllen müssen, wird eine Umsetzungsfrist von drei Jahren gewährt. Diese gilt grundsätzlich ab dem Zeitpunkt der Einstufung als (anderweitig) systemrelevantes Institut. Ausgenommen von der Übergangsfrist sind global systemrelevante Institute, die die BCBS 239 Anforderungen schon seit Januar 2016 erfüllt haben müssen.

1. Anforderungen an systemrelevante Institute (AT 4.3.4):

Die Kernaussagen des BCBS 239 hinsichtlich Datenarchitektur bzw. -Aggregation[1] und Datenqualitätsmanagement[2] wurden weitgehend übernommen und punktuell ergänzt.

Enthalten sind auch die Anforderungen an den Abgleich und die Plausibilisierung von Risikodaten. So wird bei Verwendung mehrerer Namenskonventionen und Kennzeichnungen eine automatische Überleitbarkeit zwischen diesen Taxonomien gefordert. Darüber hinaus ist zur Identifikation von Datenschwächen eine Abstimmbarkeit und eine Plausibilisierung von Risikodaten mit anderen Informationen vorzusehen; als Beispiele für solche werden konkret die Daten aus dem Rechnungswesen und ggf. dem Meldewesen genannt. Dies trägt dem Umstand Rechnung, dass Institute in Deutschland vor dem Hintergrund oft mehrerer parallel anzuwendender Rechnungslegungsvorschriften (IFRS, HGB) besonderen Herausforderungen gegenüber stehen. Die explizite Nennung der Daten des Meldewesens ergänzt die bisherige Anforderung des BCBS 239.

Zudem sind für alle Prozessschritte in der Datenaggregation Verantwortlichkeiten und Kontrollen einzurichten. Daneben ist die Einhaltung der Anforderungen von einer unabhängigen Stelle (nicht den geschäftsinitiierenden bzw. geschäftsabschließenden Organisationseinheiten) regelmäßig zu überprüfen.

Nicht explizit in die neue MaRisk aufgenommen wurden die Anforderungen nach einer einheitlichen Datenquelle pro Risikoart sowie einem expliziten Management-Reporting über Datenqualitätsprobleme.

2. Anforderungen an sämtliche Institute (BT 3, teils AT 5, AT 7.2, AT 8.3):

Das neue Modul BT 3 umfasst neben den neuen Anforderungen zur Risikoberichterstattung aus BCBS 239 auch eine Bündelung der bestehenden Berichtspflichten, die zuvor in verschiedenen MaRisk-Modulen enthalten waren und richtet sich an alle Institute. Im Anschreiben wird von der BaFin betont, dass die Anforderungen aus AT 4.3.4, die sich ausschließlich an systemrelevante Institute richten, nicht, wie von vielen Instituten befürchtet, mit dem BT 3 „durch die Hintertür" für alle Institute gültig werden. Nicht-systemrelevante Institute können auch weiterhin die Ausgestaltung ihrer Risikoberichterstattung nach ihren individuellen Bedürfnissen und Notwendigkeiten zuschneiden (unter Beachtung der sonstigen Anforderungen der MaRisk und unter Berücksichtigung des Proportionalitätsprinzips).

Die Anforderungen des BCBS 239 an Inhalte, Zeitnähe, Ad-hoc-Fähigkeit und Flexibilität des Reportings wurden grundsätzlich übernommen (BT 3.1 und BT 3.2).

Die Berichte müssen auf vollständigen, genauen und aktuellen Da-

---

[1] Konsistente und granulare Datenstrukturen, einschließlich der Forderung nach einheitlichen Auswertungskategorien, Namenskonventionen bzw. einem Data Dictionary sowie hoher Automatisierungsgrad in den Datenaggregationsprozessen

[2] Kontrollen über die gesamte Verarbeitungskette vom Quellsystem bis zur Berichterstellung mit dem Ziel der Genauigkeit und Vollständigkeit

ten beruhen. Zudem sind neben einer Darstellung und Beurteilung der Risikosituation auch eine zukunftsorientierte Risikoeinschätzung abgeben und sich nicht ausschließlich auf aktuelle und historische Daten stützen.

Unverändert zum vorherigen Entwurf findet sich kein Hinweis in den MaRisk, in welcher Zeitdauer interne Berichte zu erstellen sind und die Erwartung des BCBS-Gremiums von t+10 wurde nicht übernommen. Gemäß den Diskussionen im Fachgremium sieht die Aufsicht hier eine Bandbreite von mehreren Wochen abhängig vom Institut als möglichen Industriestandard an.

Insgesamt sind die in BT 3 adressierten Teile des BCBS 239 vor dem zentralen Leitbild des Proportionalitätsprinzips als Mindestanforderungen formuliert (z.B. mindestens vierteljährlicher Gesamtrisikobericht). Sie sind vor dem Hintergrund des Risikogehalts und der Volatilität der jeweiligen Positionen auszugestalten – und die Erwartungen der Aufsicht gehen in der bereits heute gängigen Praxis häufig deutlich über diese Mindestanforderungen hinaus. Individuelle Zielbilder und damit einhergehende Frequenzen und Fristen sollten daher begründet, dokumentiert und mit der zuständigen Aufsicht abgestimmt werden.

Weiterhin wird die Notwendigkeit von hohen technisch-organisatorischen Standards beim Einsatz individueller Datenverarbeitung (AT 7.2), bei der Dokumentation von Regelungen zu Verfahren, Methoden und Prozessen der Risikodatenaggregation in Organisationsrichtlinien (bei systemrelevanten Instituten, AT 5) sowie die Berücksichtigung der Datenaggregationsfähigkeiten vor Übernahmen oder Fusionen (AT 8.3) betont.

Eine Konkretisierung der für die Umsetzung maßgeblichen Risikoberichte und -kennzahlen ist nicht erfolgt. Somit bleibt z.B. weiterhin offen, inwiefern Finanzberichte in den Gültigkeitskreis der Anforderungen vollständig einzubeziehen sind.

Weiterhin hat die EZB in jüngster Zeit Prüfungshandlungen zur Risikodatenaggregation und –berichterstattung vorgenommen. Ein regelmäßiges Nachhalten des Umsetzungsfortschritts durch die Aufsicht bzw. den Jahresabschlussprüfer bleibt somit wahrscheinlich.

Risikokultur und -governance

In Anlehnung an internationale bzw. europäische Vorgaben widmet die BaFin dem Thema Risikokultur und -governance größere Aufmerksamkeit. Dies gilt zunächst mit Blick auf die **Verantwortung der Geschäftsleitung**. Sowohl das FSB („Guidance on Supervisory Interaction with financial institutions on Risk Culture") als auch die EBA in ihrer Leitlinie zur Internal Governance haben basierend auf den Erfahrungen der Finanzkrise Verbesserungen angemahnt. Die Verantwortung der Geschäftsleitung wird in AT 3 explizit um die Entwicklung, Förderung und Integration einer angemessenen Risikokultur innerhalb des Instituts bzw. der Gruppe ergänzt. Die entsprechenden Vorgaben sind ggü. dem Erst- und Zwischenentwurf wie erwartet unverändert.

Für eine Verankerung von Risikobewusstsein auf **allen Ebenen der Organisation** ist zunächst eine klare Festlegung der Geschäftsleitung bzgl. Risikoappetit, strategischen Zielen und Werten des Unternehmens („tone at the top") notwendig. Diese Festlegung soll breit kommuniziert werden, Gegenstand eines offenen und kritischen Dialogs sein und ein risikobewusstes Verhalten aller Mitarbeiter bei sämtlichen Entscheidungsprozessen des täglichen Bankgeschäfts fördern. Entsprechende Anreizverfahren sowie ein **Verhaltenskodex** für Mitarbeiter (AT 5 Tz. 3) sollen entwickelt werden (mit Öffnungsklausel für kleinere und risikoarme Institute).

Im Anschreiben zu den MaRisk macht die BaFin deutlich, dass ein solcher Codex in größeren Instituten notwendig ist, die persönliche Ansprache und das „Vorleben" aber nicht minder von Bedeutung sind. Ebenso wird dort appelliert, die Risikokultur als ein wesentliches Werkzeug für ein angemessenes Risikomanagement zu begreifen und dieses auch zu nutzen. Die Herausforderung für Institute wird sein, eine „angemessene" Risikokultur zu definieren und die Einhaltung dieser zu beobachten bzw. zu überwachen. Die Erfahrungen z. B. holländischer Institute und Aufsicht zeigt, dass eine Bewertung bzw. Vermessung der Kultur durchaus möglich ist, und dass von diesem Startpunkt Maßnahmen wie Trainings etc. zur Verbesserung der Risikokultur beitragen können.

Im Bereich der Risikogovernance stellt die BaFin eine Reihe expliziter Anforderungen und präzisiert damit zum Teil ihre bisherige Erwartungshaltung: So ist die **Leitung der Risikocontrolling-Funktion** bei systemrelevanten Instituten durch einen Geschäftsleiter (CRO) zwingend; er darf dabei weder für den Bereich Finanzen/Rechnungswesen noch für den Bereich Organisation/IT verantwortlich sein. Für alle anderen Institute wird die Anforderung der „exklusiven" Wahrnehmung der Leitung der Risikocontrolling-Funktion spezifiziert.

Die **Compliance-Funktion** ist in jedem Fall unmittelbar der Geschäftsleitung zu unterstellen, in einem von Markt und Handel unabhängigen Bereich. Systemrele-

vante Institute haben dazu eine eigenständige Organisationseinheit einzurichten.

Bei einem Wechsel von Mitarbeitern der Handels- und Vertriebsbereiche in Kontrollbereiche wird eine angemessene **„Cooling-Off-Periode"** gefordert – für den Wechsel in die Interne Revision wird diese Anforderung auf alle Einheiten ausgedehnt.

In den Governance Themen erfolgt erstmals explizit die Erwähnung des **IT-Risikomanagements** als Teil der Risikosteuerungs- und -überwachungsprozesse der Institute. Sie umfassen vor allem die Feststellung des Schutzbedarfs, die Ableitung von Sicherheitsanforderungen sowie die Festlegung entsprechender Sicherheitsmaßnahmen. In die Anforderungen werden auch explizit die individuelle Datenverarbeitung („IDV") einbezogen.

Risikomanagement

Im Bereich der allgemeinen Vorgaben zum Risikomanagement gibt es nur kleinere Änderungen.

Zu einem wird für den Risikotragfähigkeitsansatz nun gefordert, dass die hierzu eingesetzten Verfahren sowohl das Ziel der Fortführung des Instituts als auch den Schutz der Gläubiger vor Verlusten aus ökonomischer Sicht angemessen zu berücksichtigen haben. Dies ist für sich genommen nur eine redaktionelle Änderung – wir verweisen allerdings auf den Entwurf des umfassend überarbeiteten Leitfadens zur aufsichtlichen Beurteilung bankinterner Risikotragfähigkeitskonzepte (für LSIs) sowie des entsprechenden Entwurfes einer ICAAP-Guideline der EZB (für SIs), die eine deutliche Änderung der aufsichtlichen Erwartungen zu den Ansätzen formulieren. Es werden zudem zeitnahe Schritte der EZB erwartet, den Risikotragfähigkeitsansatz auch bei LSIs zu harmonisieren.

Darüber hinaus wird konkretisiert, dass sofern aufgrund der Komplexität der Verfahren und Methoden zur Ermittlung der Risikotragfähigkeit eine umfassende Validierung durchzuführen ist, eine angemessene Unabhängigkeit zwischen Methodenentwicklung und Validierung zu gewährleisten ist. Damit ermöglicht die BaFin für LSIs eine proportionale Anwendung des Prinzips, während die EZB für SIs generell fordert, dass für die ICAAP-Modelle die gleichen Prinzipien wie für interne Modelle der Säule 1 anzuwenden sind.

Auslagerungen

Die Anforderungen an die Auslagerungen in AT 9 wurden in Teilen erneuert, konkretisiert und klargestellt. Festzustellen ist, dass mit den Ergänzungen im Wesentlichen Sachverhalte aufgenommen wurden, die von der Aufsicht in der Prüfungspraxis seit längerem gefordert bzw. empfohlen wurden. Ein Beispiel dafür ist die Einrichtung eines **zentralen Auslagerungsmanagements** mit Dokumentations-, Unterstützungs- und Koordinationspflichten bei größeren Instituten bzw. Instituten mit umfangreichen Auslagerungslösungen. Das zentrale Auslagerungsmanagement hat mindestens jährlich einen Bericht über die wesentlichen Auslagerungen zu erstellen.

Eine Neuerung ist die Definition der **Grenzen der Auslagerbarkeit von Kontroll-** (Risikocontrolling, Compliance und Interne Revision) **und Kernbankbereichen.** Hierbei ist sicherzustellen, dass eine Auslagerung nur dann wahrgenommen werden kann, wenn das auslagernde Institut bzw. die so genannte „retained organisation"[3] weiterhin über Kenntnisse und Erfahrungen verfügt, die eine wirksame Überwachung der vom Auslagerungsunternehmen erbrachten Dienstleistung gewährleistet. Im Vergleich zum inoffiziellen Zwischenentwurf vom 24. Juni 2016 wurde erleichternd gestrichen, dass das auslagernde Institut über „fundierte" Kenntnisse verfügen muss. Die vollständige Auslagerung ist für nicht wesentliche Tochterunternehmen zulässig und konkretisierend wird aufgenommen, dass sich die Nicht-Wesentlichkeit in der Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den Finanzsektor als auch der Bedeutung innerhalb der Gruppe widerspiegeln muss. Gleiches gilt für Gruppen, wenn das Mutterunternehmen kein Institut und im Inland ansässig ist.

Ferner stellt das Rundschreiben klar, dass eine Vollauslagerung der Risikocontrolling-Funktion bei kleinen Instituten nicht zulässig und eine vollständige Auslagerung der Compliance-Funktion sowie Internen Revision möglich ist. Bei einer Vollauslagerung dieser Bereiche ist zudem ein **Beauftragter** zu benennen, der die Durchführung der jeweiligen Aufgaben sicherstellen muss.

Die Abgrenzung des sonstigen Fremdbezugs bei **Software-Einsatz** wurde ggü. dem inoffiziellen Zwischenentwurf dahingehend noch weiter klargestellt, dass der reine Erwerb von Software in der Regel keine Auslagerung darstellt. Im Gegensatz dazu liegt bei oft umfangreichen Unterstützungsleistungen der Anbieter von Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder die für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist, immer ein Auslagerungssachverhalt vor. Der Betrieb der Software durch einen exter-

[3] Bei Auslagerungen in Unternehmen verbleibende Steuerungs- und Kontrolleinheit sowie Schnittstelle zum Dienstleister

nen Dritten ist regelmäßig als Auslagerung einzustufen.

Die Anforderung an **unbeabsichtigte und unerwartete Beendigungen von Auslagerungen** wurde dahingehend ergänzt, dass nunmehr Ausstiegsprozesse festzulegen sind. Ferner haben Institute Prozesse zu etablieren, welche die Handlungsoptionen regelmäßig und anlassbezogen überprüfen. Eine Berücksichtigung in der Notfallplanung ist dann erforderlich, wenn keine Handlungsoptionen existieren. Ziel ist es, die ausgelagerten Aktivitäten bzw. Prozesse aufrecht zu erhalten oder „in angemessener Zeit" wieder herstellen zu können.

Vertragliche Zustimmungsvorbehalte für **Weiterverlagerungen** sind nicht unbedingt erforderlich. Es wurde klarstellend aufgenommen, dass diese „möglichst" im Auslagerungsvertrag vereinbart werden sollen. Gefordert wird jedoch, vertraglich mindestens sicherzustellen, dass die Vereinbarungen des Auslagerungsunternehmens mit Subunternehmen im Einklang mit den vertraglichen Vereinbarungen des originären Auslagerungsvertrages stehen. In jedem Fall bleibt das ursprüngliche Auslagerungsunternehmen in der Berichtspflicht.

Weiterhin sind bereits bei Vertragsanbahnung **Eskalationsprozesse** darüber festzulegen, welchen Grad einer Schlechtleistung das auslagernde Institut akzeptieren möchte. Zur Beachtung in den Auslagerungsvertrag aufgenommenen **„sonstigen Sicherheitsanforderungen"** zählen im Wesentlichen Zugangsbestimmungen zu Räumen und Gebäuden sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen.

Kreditprozesse

Die Endfassung der veröffentlichten MaRisk-Novelle beinhaltet keine wesentlichen Änderungen ggü. den beiden Entwurfsversionen.

Im Rahmen der Anforderungen an die Prozesse im Kreditgeschäft gibt es in BT 1.2 sowohl Konkretisierungen als auch Neuerungen in den Bereichen Intensivbetreuung, Behandlung von Problemkrediten, Kapitaldienstfähigkeit sowie Sicherheiten. Im Wesentlichen handelt es sich hierbei um Erfahrungen aus der Prüfungspraxis. Einige Aspekte führen jedoch zur Notwendigkeit einer Weiterentwicklung und Verzahnung von Kreditbearbeitung, Risikoklassifizierung, Früherkennung und Risikovorsorgebildung.

Konsequenterweise neu aufgenommen in den MaRisk sind die sog. **Forbearance**-Anforderungen („Berücksichtigung von Zugeständnissen zugunsten des Kreditnehmers"), welche bei IFRS-Instituten bereits im aufsichtlichen Meldewesen Berücksichtigung finden bzw. für HGB-Institute ebenfalls jetzt flächendeckend eingeführt wurden. Diese ziehen häufig Anpassungsbedarf an den Kreditprozessen nach sich. Bei der Festlegung der „Trigger-Events", die eine Überführung in die Intensivbetreuung oder Sanierung bzw. Abwicklung erfordern, können sich Institute künftig an der EBA-Definition orientieren oder diese institutsindividuell festlegen. Folgerichtig sind die Erkenntnisse aus Forebearance-Maßnahmen auch bei den Prozessen der Früherkennung, der Risikoklassifizierung sowie der Risikovorsorgebildung zu berück-sichtigen.

Die Anforderungen an die Betreuung von Kreditengagements in der Intensivbetreuung sind gestiegen. Die Prüfungspraxis hat in einigen Fällen in der Vergangenheit gezeigt, dass Engagements trotz vorliegender „Trigger-Events" nicht in die Sanierung bzw. Abwicklung überführt wurden. So sind künftig beim Verbleib in der **Intensivbetreuung** und bei Vorlage von wesentlichen Leistungsstörungen Maßnahmen aufzusetzen, die das Adressenausfallrisiko minimieren (z.B. zusätzliche Sicherheitenstellung). Zugleich sind diese Maßnahmen mit den Sanierungs- bzw. Abwicklungsmitarbeitern abzustimmen und rechtliche Risiken zu berücksichtigen.

Bei der Ermittlung der **Kapitaldienstfähigkeit** wurde die Ergänzung vorgenommen, dass die Risiken für die zukünftige Vermögens- und ggf. Liquiditätslage des Kreditnehmers zu berücksichtigen sind. Darüber hinaus sind bei Immobilien-Verbraucherdarlehen (vormals in der inoffiziellen Zwischenversion als Hypotheken an Verbraucher bezeichnet) künftige als wahrscheinlich anzusehende Einkommensschwankungen zu beachten. Die relevanten Informationen sind entsprechend zu dokumentieren und über die gesamte Kreditlaufzeit aufzubewahren. Diese Betonung der künftigen Kapitaldienstfähigkeit leitet sich u.a. aus der Wohnimmobilienkredit-Richtlinie ab.

Ein zentraler Aspekt bei der Wertermittlungs-Festlegung von **Sicherheiten** in der Entwicklungsphase von Objekt- und Projektfinanzierungen ist, dass in unter Risikogesichtspunkten festzulegenden Abständen eine Durchführung von Besichtigungen und Baustandskontrollen zu erfolgen hat. Dies kann unseres Erachtens als Konkretisierung gelebter Prüfungspraxis verstanden werden. Im Vergleich zum inoffiziellen Zwischenentwurf wurde „regelmäßig" in „unter Risikogesichtspunkten festzulegenden Abständen" konkretisiert.

Die grundsätzliche Wichtigkeit der Inaugenscheinnahme von physischen Sicherheiten wird auch dadurch untermauert, dass bei der Sicherheitenbewertung im Rahmen der Kreditgewährung bzw. -prolongation die Werthaltigkeitsüberprüfung auch eine Objektbesichtigung ab einer zu definierenden Grenze beinhalten muss. Diese Grenze muss das Institut unter Risikogesichtspunkten und in Abhängigkeit von der Sicherheitenart definieren. Der alleinige Einsatz von Marktschwankungskonzepten im Rahmen der Sicherheitenüberwachung wird damit ab einer gewissen Größenordnung als nicht geeignet angesehen.

Liquidität

Die Anforderungen zum Management und Controlling von Liquiditätsrisiken in BTR 3 wurden durch die 5. Novelle an einigen Punkten konkretisiert und teilweise deutlich erweitert. Inhaltlich berücksichtigt die MaRisk-Novelle regulatorische Entwicklungen, die in den letzten Jahren durch EBA-Leitlinien zum SREP und zur Meldung von Refinanzierungsplänen bzw. als Vorgaben im Rahmen der CRR veröffentlicht wurden.

Liquiditätspuffer

Diversifikations- bzw. Konzentrationsrisiken sind bei den Refinanzierungsquellen und in der Liquiditätspuffer stärker in den Fokus gerückt. Sie sind anhand geeigneter Kriterien, wie z.B. Emittenten, Produkte, Laufzeiten und Regionen zu überwachen und zu begrenzen. Darüber hinaus sind Liquiditätspuffer derart zu bemessen, dass diese sowohl in einem Normal- als auch in einem Stressszenario ausreichend Liquidität zuführen können.
Außerdem detailliert die MaRisk Anforderungen an die Identifikation und das Reporting von belasteten Vermögensgegenständen (Asset Encumbrance) in Orientierung an den entsprechenden Standards der EBA.

Im BTR 3.2, der nur für kapitalmarktorientierte Institute anwendbar ist, werden zusätzlich weitere operative und qualitative Anforderungen an die Liquiditätspuffer gestellt. Zum Beispiel muss ein Institut sicherstellen, dass der Liquidierungsweg tatsächlich im Stressfall zur Verfügung steht.

Liquiditätsübersichten

Die BaFin konkretisiert, dass Liquiditätsübersichten und die zugrundeliegenden Modelle alle relevanten zeitlichen Horizonte (kurz-, mittel- und langfristig) abdecken sollen. Liquiditätsstresstests, welche der Erkennung sich abzeichnender Liquiditätsengpässe dienen, sind mindestens jährlich auf Angemessenheit zu überprüfen.
Außerdem erwartet die BaFin die Ermittlung eines individuellen Überlebenshorizonts (Survival Period) und konkretisiert auch für nicht-kapitalmarktorientierte Unternehmen die Anforderungen an Stressszenarien; so sind neben institutseigenen und marktweiten Liquiditätsrisikoszenarien diese nun auch kombiniert zu betrachten.

Untertägige Liquiditätsrisiken

Institute haben neben einer untertägigen Liquiditätsrisikomessung nun auch Maßnahmen zu deren Steuerung zu ergreifen. Während die Risikomessung üblicherweise rückwirkend am Tagesende durchgeführt wird, sind aktive Steuerungsmaßnahmen ad hoc bzw. a priori vorzunehmen. Diese Anforderungen stellen viele Institute insbesondere aus IT-Sicht vor Herausforderungen, da die meisten Zahlungsverkehrssysteme ein manuelles oder regelbasiertes Verzögern, Verschieben oder Stoppen von Zahlungsaufträgen nicht ermöglichen. Passive Steuerungsmaßnahmen wie eine untertägige Zahlungsverkehrsreserve können allerdings zu einer Zunahme der Reservehaltungskosten der Bank führen. Insgesamt erhöht die BaFin somit ihre Anforderungen an das Management von untertägigen Liquiditätsrisiken.

Risikoberichterstattung

Mit BT 3 erweitert und konkretisiert die BaFin ihre Anforderungen an die Risikoberichterstattung im Allgemeinen, sowie an die Liquiditätsrisikoberichterstattung im Speziellen. Neben den bisher geforderten Berichten über Stresstestergebnisse und Änderungen des Liquiditätsnotfallplans ist neu auch über Fremdwährungspositionen, untertägige Liquiditätsrisiken, sowie Höhe, Qualität und Zusammensetzung der Liquiditätsreserve an die Geschäftsleitung zu berichten. Entsprechende Berichte sind mindestens vierteljährlich, bzw. für kapitalmarktorientierte und systemrelevante Institute monatlich, erforderlich.
Ebenfalls fordert die BaFin als Teil des Gesamtrisikoberichts neben aktuellen Liquiditätskennzahlen auch Prognosen über die zukünftige Entwicklung von Liquiditätskennzahlen und Refinanzierungspositionen. Insbesondere die Prognose entsprechender Kennzahlen stellt viele Institute vor neue Herausforderungen.

Refinanzierungspläne

Die BaFin fordert einen mehrjährigen internen Refinanzierungsplan, welcher Risikoappetit, Strategien und Geschäftsmodell angemessen berücksichtigt. Mögliche - auch adverse - Veränderungen der eigenen Geschäftstätigkeit oder der strategischen Ziele sowie Veränderungen des wirtschaftlichen Umfelds sind in ihrer Wirkung auf den Refinanzierungsbedarf zu betrachten. Es handelt sich hier gemäß den Erläuterungen explizit nicht um die Umsetzung der Vorgaben der Leitlinien der EBA zur standardisierten Meldung von Refinanzierungsplänen (EBA/GL/2014/04). Die Anforderungen nach institutsspezifisch ausgestalteten Refinanzierungs-

plänen kann jedoch durch diese Standardformate der EBA erfüllt werden.

Zinsänderungsrisiko im Bankbuch

Schließlich greift die BaFin eine Kernforderung aus den EBA-Leitlinien zum Zinsänderungsrisiko im Bankbuch (IRRBB) auf: der dualen Betrachtung von IRRBB in seiner Wirkung auf das handelsrechtliche Ergebnis einerseits und den Barwert der zinstragenden Positionen andererseits. Die BaFin gestattet zwar, ein primär steuerungsrelevantes Verfahren zu definieren. Bei Wesentlichkeit ist aber eine parallele Betrachtung beider Sichten in den Verfahren und Prozessen der Risikosteuerung-, des -controllings sowie der Beurteilung der Risikotragfähigkeit notwendig. Diese Klarstellung der BaFin kommt aufgrund der EBA-Leitlinien und der vorherigen MaRisk-Entwürfe nicht überraschend. Entsprechend arbeiten bereits viele Institute an einer Erfüllung der Anforderungen. Dabei müssen Institute zum einen **Herausforderungen** in Bezug auf Datenverfügbarkeit und -verarbeitbarkeit meistern, um Risikometriken für beide Sichten berechnen und Abgleiche gegen Daten des Rechnungswesens durchführen zu können. Zum anderen sind das Design und die Etablierung von dualen Limit- und Steuerungsverfahren für deutsche Institute meist sehr herausfordernd. Zur vollständigen Erfüllung der Anforderungen sind oft grundlegend neue Verantwortungen zu etablieren und neue Verfahren, Systeme und Prozesse aufzusetzen.

Anforderungen an die IT

An den grundsätzlichen Anforderungen an die IT haben sich nur geringere Änderungen ergeben.

Wesentlichste Änderungen in Bezug auf die Anforderungen an die IT betrifft die unter AT 4.3.1 dargestellte Regelung zur regelmäßigen Überprüfung von IT-Berechtigungen. Die bisher definierten Zeiträume (halbjährlich für kritische Berechtigungen, jährlich für alle weiteren Berechtigungen) wurden auf einen jährlichen bis 3-jährigen Zeitraum ausgeweitet. Ausnahme bilden dabei nur noch die besonders kritischen IT-Berechtigungen (zum Beispiel von Administratoren), die weiterhin halbjährlich zu überprüfen sind. Darüber hinaus werden unter AT 7.2 erstmals Anforderungen an die Steuerung und Überwachung von IT-Risiken gestellt.

Eine Konkretisierung der bereits bestehenden Regelungen erfolgt in den zum 6. November 2017 veröffentlichten „Bankaufsichtlichen Anforderungen an die IT“ (BAIT). Dieses Rundschreiben trägt der erhöhten Erwartungshaltung der Aufsicht in Bezug auf die IT-Sicherheit Rechnung. Die Anforderungen umfassen beispielsweise Anforderungen an die IT Strategie, IT Risikomanagement und Informationssicherheitsmanagement. Die Anforderungen der BAIT treten ebenfalls mit der Veröffentlichung in Kraft.

Würdigung und Implikationen

Weniger bedeutende Institute (LSI)

Für die **direkt von der nationalen Aufsicht überwachten Institute** („weniger bedeutende Institute“ – less significant institutions LSI) sind die MaRisk weiterhin der unmittelbare Maßstab. Die „großen Themen“ Auslagerung, IT-Risiken, Risikokultur und Datenqualität als pars pro toto für das Thema Risikodatenaggregation sollten dabei nicht den Blick verstellen, für die Vielzahl der Klarstellungen und deren Implikationen auf Organisation, Prozesse und oder Methoden im Reporting, im Risikomanagement, der Organisation, der IT-Infrastuktur oder im Markt und Marktfolge von Instituten. Es lohnt ein gesamtheitlicher Blick auf diese MaRisk-Novelle, um mögliche Interdependenzen der Themen frühzeitig zu erkennen und in die Umsetzung einfließen zu lassen.

Wichtig für den Kreis der weniger bedeutenden Banken ist zudem, dass auch der Leitfaden zur aufsichtlichen Beurteilung der Risikotragfähigkeit überarbeitet wird (hier wurde am 6. September 2017 ein Entwurf zur Konsultation und Stellungnahme bis 17. Oktober 2017 gestellt).

Bedeutende Institute (SI)

Die BaFin wendet sich mit den MaRisk, die auch mit der EZB abgestimmt wurden, auch an größere („bedeutende Institute“ – significant institutions SI) **Institute, die direkt von der EZB überwacht werden**.

Bei den betroffenen Instituten können die MaRisk als Orientierungshilfe der Joint Supervisory Teams der EZB herangezogen werden, wie der deutsche Gesetzgeber die Umsetzung der §25a Abs und § 25b KWG erwartet. Dies gilt vor allem für Themenbereiche, bei denen der Detailgrad vorliegender europäischer Anforderungen hinter denen der überarbeiteten MaRisk zurückbleibt (zum Beispiel bei den Regelungen zu Auslagerungen).

Ansonsten wird die EZB natürlich auch internationale Standards wie die Anforderungen der Leitlinien zum SREP, die Papiere zur Governance oder die zum Management des Zinsrisikos als Messlatte für eine in Europa insgesamt harmonisierte Aufsicht über die ca. 130 sogenannten bedeutenden Institute heranziehen.

Dementsprechend wird im Markt unter bedeutenden Institute diskutiert, welche Anforderungen (**MaRisk versus internationale bzw.**

europäische Standards) durch diese Institute zu erfüllen sind. Die beiden Regelungskreise sind jedoch nur scheinbar ein Widerspruch – sind doch die MaRisk mit dieser Novelle sehr „international" geworden. De facto beruhen eine Vielzahl von Änderungen in den MaRisk auf einschlägigen Veröffentlichungen der EBA, des Financial Stability Boards (FSB) oder des Baseler Ausschusses für Bankenaufsicht (BCBS).

Bereits in den Vorbemerkungen der MaRisk unter AT 1, Tz. 3, findet sich der ausdrückliche Hinweis, dass große und komplexe Häuser „auch die Inhalte einschlägiger Veröffentlichungen des Baseler Ausschusses für Bankenaufsicht und des Financial Stability Boards" einzubeziehen haben. Auch in vielen anderen Detailregelungsinhalten finden sich **internationale Vorgaben** wieder, auch wenn sich kein expliziter Hinweis auf Quellen in den MaRisk findet. Einige Beispiele:

- Zu allererst dient das Baseler Papier zur **Risikodatenaggregation** (BCBS 239) als Grundlage für die Neuerungen in der Datenarchitektur und IT-Infrastruktur sowie der Risikoberichterstattung dieser MaRisk-Novelle.
- Zu vielen der in dieser MaRisk Novelle aufgebrachten weiteren Themen wie der **(Risiko-) Governance** (Kultur, Funktionstrennung, Outsourcing, Berichterstattung) hat sich die EBA mit der Leitlinie 44 „Guideline on Internal Governance" bereits im Jahr 2011, neu gefasst im September 2017, eine Meinung gebildet. Auf der internationalen Ebene hat sich das FSB im speziellen zu Risikoappetit und Risikorahmenwerk geäußert.
- Mit der Messung und Steuerung von **Zinsänderungsrisiken im Bankbuch** – die MaRisk-Novelle nennt hier zum Beispiel die Berücksichtigung sowohl von barwertigen als auch periodischen Steuerungsimpulsen – haben sich ebenfalls die EBA mit einer spezifischen Guideline aber auch der BCBS bereits auseinander gesetzt. Ferner befassen sich die Reformwerke zur CRD V und CRR II mit diesem Thema. Daneben fordern die MaRisk Risikoarten-übergreifende Stresstests; solche Analysen im Kontext des Zinsänderungsrisikos im Bankbuch sind ebenfalls Teil der oben genannten internationalen Papiere.
- In den Neuerungen im **Liquiditätsrisikomanagement** finden sich Vorgaben zur Berücksichtigung von belasteten Vermögenswerten (Asset Encumbrance) oder zu Refinanzierungsplänen (Funding Plans). Auch hier können einschlägige Standards der EBA als Grundlage und Quelle herangezogen werden.
- Die Berücksichtigung (und Kapitalisierung) von mehrjährigen Risikoarten-übergreifenden **Stresstests** stellt ebenfalls ein wesentliches Element im europäischen SREP dar; dies insbesondere vor dem Hintergrund der früher in diesem Jahr publizierten Leitlinie der EZB zum „ICLAAP".

Liest man die Neuerungen dieser MaRisk unter dem Blickwinkel des hohen Umfangs an internationalen und europäischen Regulierungen, so bleibt der Schluss: die MaRisk haben neben der Berücksichtigung von weiteren Erfahrungen aus der Prüfungspraxis die Inhalte vieler europäischer und internationaler Standards für alle Institute in Deutschland nachgezogen.

Dass sowohl eine europäische als auch eine deutsche Aufsicht der Umsetzung dieser Standards große Bedeutung beimisst, zeigt diese Novelle genauso wie die gelebte Aufsichts- und Prüfungspraxis.

Sprechen Sie uns gerne an!
Unsere Teams aus erfahrenen Experten in Regulatorik, Risk Banking und Business Technology unterstützen Sie gerne dabei, sich optimal auf die Anforderungen der MaRisk und die Querbeziehungen zu Prozess- und IT-Themen einzustellen.

Dr. Heiko Carstens
Partner, Financial Services
T +49 89 9282-4715
hcarstens@kpmg.com

Thilo Kasprowicz
Partner, Financial Services
T +49 69 9587-3198
tkasprowicz@kpmg.com

Marco Lenhardt
Partner, Financial Services
T +49 69 9587-3403
mlenhardt@kpmg.com

Dr. Matthias Mayer
Partner, Financial Services
T +49 89 9282-1433
matthiasmayer@kpmg.com

Daniel Quinten
Partner, Financial Services
T +49 89 9282-4910
dquinten@kpmg.com

Dr. Arvind Sarin
Partner, Financial Services
T +49 69 9587-2968
arvindsarin@kpmg.com

Dr. Daniel Sommer
Partner, Financial Services
T +49 69 9587-2498
dsommer@kpmg.com

Dr. Holger Spielberg
Partner, Financial Services
T +49 89 9282-4870
hspielberg@kpmg.com

Markus Quick
Partner, Financial Services
T +49 69 9587- 4687
markusquick@kpmg.com

Impressum

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Dr. Matthias Mayer **(V.i.S.d.P.)**
Partner, Financial Services
T +49 89 9282-1433
MatthiasMayer@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia