Point of View

RFC Professionals
SUSTAINABLE EXCELLENCE

Veröffentlichung der 5. MaRisk-Novelle

Nach zwei Konsultationsrunden im Jahr 2016 veröffentlichte die BaFin am 27. Oktober 2017 mit dem Rundschreiben 09/2017 die Neufassung der MaRisk.

In der 5. MaRisk-Novelle werden einerseits neue Anforderungen formuliert und andererseits Themenkomplexe weiter konkretisiert, was zu einem erheblichen Umsetzungsaufwand bei den betroffenen Instituten führt. Während die Klarstellungen direkt ab Veröffentlichung umzusetzen sind, gilt für die neuen Anforderungen eine Umsetzungsfrist bis zum 31. Oktober 2018. Davon abweichende Umsetzungsfristen ergeben sich für die Anforderungen des neuen Moduls AT 4.3.4: Ab dem Zeitpunkt der Einstufung als (anderweitig) systemrelevantes Institut beträgt die Umsetzungsfrist drei Jahre. Maßgeblichen Einfluss auf die Neufassung hatten die Grundsätze zur Datenaggregation und Risikoberichtserstattung (BCBS 239). Die Themengebiete Risikokultur in Banken sowie Auslagerungen bilden die weiteren Schwerpunkte der Novelle.

Point of View Branche:

Die Schwerpunktthemen, die in der 5. MaRisk-Novelle zu finden sind, ergeben sich vorwiegend aus internationalen Regelungsinitiativen. Die BCBS 239 zur Risikodatenaggregation und Risikoberichterstattung sowie die Bestrebungen der besseren Verankerung einer Governance und einer Risikokultur in Instituten (z.B. BCBS 328d und FSB „Guidance on Supervisory Interaction with financial institutions on Risk Culture") hatten einen wesentlichen Einfluss auf die Neufassung. Zudem haben die Erfahrungen aus der Aufsichtspraxis zu einer Konkretisierung der Auslagerungsvorgaben des AT 9 geführt.

- Datenmanagement, Datenqualität und Aggregation von Risikodaten (AT 4.3.4): Dieses neu hinzugefügte Modul richtet sich an systemrelevante Institute bspw. mit einer Bilanzsumme größer als 30 Mrd. Euro (systemrelevante Institute im Sinne der MaRisk sind gem. AT 1 Tz. 6 global systemrelevante Institute nach § 10f KWG und anderweitig systemrelevante Institute nach § 10g KWG). Um Banken besser auf künftige Krisenfälle vorzubereiten, hatte der Basler Ausschuss für Bankenaufsicht im Januar 2013 vierzehn Grundsätze hinsichtlich Risikodatenaggregation und Risikoberichterstattung veröffentlicht, die von den global systemrelevanten Banken bereits bis Ende 2015 umzusetzen waren. Ziel war die Verbesserung der IT-Infrastruktur der Institute in Bezug auf eine umfassende, genaue und aktuelle Aggregation der Risikopositionen und die zeitnahe Verfügbarkeit dieser Informationen für das Berichtswesen. Im Einzelnen werden die 14 Grundsätze von BCBS 239 vier verschiedenen Oberbegriffen zugeordnet:

  1) Gesamtunternehmensführung und Infrastruktur (Grundsatz 1 und 2)
  2) Risikodaten-Aggregationskapazitäten (Grundsatz 3-6)
  3) Risikoberichterstattung (Grundsatz 7-11)
  4) Aufsichtliche Überprüfungen, Instrumente und Zusammenarbeit (Grundsatz 12-14).

  Die wesentlichen Aussagen der Grundsätze sind nun in der 5. MaRisk Novelle wiederzufinden. Dabei sind die ersten beiden Themenblöcke „Gesamtunternehmensführung und Infrastruktur" sowie „Risikodaten-Aggregationskapazitäten" in AT 4.3.4 „Datenmanagement, Datenqualität und Aggregation von Risikodaten" zusammengefasst. Die Anforderungen beziehen sich u.a. auf Data-Governance, einheitliche Namenskonventionen,

Datenqualität und Datenvollständigkeit, Datenabgleich von Risiko mit Rechnungswesen und Meldewesen, Datenaktualität (auch in Stressphasen) sowie die Anpassungsfähigkeit der Datenaggregationen (Ad-hoc Informationen, Auswertungen nach unterschiedlichen Kategorien, Drilldown bis hinunter zur Einzelgeschäftsebene). Der dritte Themenblock „Risikoberichterstattung“ ist in das Modul BT 3 „Anforderungen an die Risikoberichterstattung“ eingeflossen und gilt für alle Institute. Risikoberichte müssen demnach nachvollziehbar und aussagefähig sein, d.h. sie müssen u.a. ein inhaltlich angemessenes Verhältnis zwischen quantitativen Informationen und qualitativer Beurteilung, zukunftsorientierte Risikoeinschätzungen, Aussagen über Risikokonzentrationen und Ergebnisse aus Stresstests beinhalten. Sie sollen auf vollständigen, genauen und aktuellen Daten beruhen, sind im zeitlich angemessenen Rahmen zu erstellen und müssen Ad-hoc-Auswertungen flexibel ermöglichen.

• Risikokultur (AT 3 und 5): Die Entwicklung, Förderung und Integration einer angemessenen Risikokultur soll - verantwortet durch die Geschäftsleitung - im Rahmen einer ordnungsgemäßen Geschäftsorganisation erfolgen. Diese, in der höchsten Hierarchieebene angesiedelte Aufgabe zeigt, dass die Risikokultur sich in allen Prozessen niederschlagen muss und innerhalb einer Unternehmenskultur langfristig zu verankern ist. Es dürfte ein langer Weg sein, Risikobewusstsein in allen Markt- und Marktfolgeabteilungen zu etablieren. Die Risikokultur ist zudem wesentlicher Bestandteil des SREP-Überprüfungsverfahrens.

• Auslagerungen (AT 9): Die Aufsicht hat mit den Änderungen in diesem Modul eine Klarstellung der aufsichtlichen Praxis geschaffen, verschärft aber auch Grenzen der Auslagerbarkeit, die sofort gültig sind. Die Voraussetzungen für Auslagerungen werden konkretisiert, vor allem für die Kontrollbereiche Risikocontrolling, Compliance und Interne Revision (eine Voll-Auslagerung ist nur für Tochterinstitute innerhalb einer Institutsgruppe zulässig). Kleine Institute können ggf. die Compliance-Funktion und die Interne Revision vollständig auslagern. Hier und in den Kernbankbereichen muss eine Rückführung der Aufgaben gewährleistet sein. Dazu müssen fundierte Kenntnisse und Erfahrungen weiterhin im Institut vorgehalten werden. Diese wesentlichen Auslagerungen müssen durch einen Auslagerungsbeauftragten überwacht werden. Bei größeren Instituten bzw. Instituten mit umfangreichen Auslagerungslösungen wird ein zentrales Auslagerungsmanagement gefordert, welches sowohl für die Kontrolle und die Überwachung der internen Anforderungen, der externen Dienstleister, der ordnungsgemäßen Dokumentation sowie für die Koordination und Überprüfung der Risikoanalyse der Auslagerungen zuständig ist. Ebenfalls werden nunmehr Weiterverlagerungen im Modul AT 9 (Tz. 8) thematisiert, deren explizite Ausgestaltungen im Auslagerungsvertrag festzuhalten sind.

Neben diesen Schwerpunkten sind weitere Änderungen mit größeren Prozess- oder Dokumentationsimplikationen zu beachten:

• Cooling-Off (AT 4.3.1): Ein Wechsel vom Markt in die Marktfolge oder in einen Kontrollbereich ist nur nach einer angemessenen Übergangsfrist möglich.

• Stresstest (AT 4.3.3): Die Aufsicht stellt klar, dass regelmäßige und einzelfallbezogene Stresstests auch für das Gesamtrisiko der Bank durchzuführen sind, welche marktweite und institutseigene Ursachen berücksichtigen müssen.

• Positionsverantwortung für das Risikocontrolling (AT 4.4.1): Ein Geschäftsleiter welcher für die Risikocontrollingfunktion verantwortlich ist, darf auch für die Marktfolge zuständig sein. Bei Instituten mit maximal drei Geschäftsleitern darf die Leitung für das Risikocontrolling und Marktfolge auch bei einer Person liegen, wobei hieraus keine Interessenkonflikte erkennbar sein dürfen.

• Technisch-organisatorische Ausstattung (AT 7.2): Es werden in diesem Modul angemessene Überwachungs- und Steuerungsprozesse für IT-Risiken gefordert, die in einem IT-Risikomanagement abzubilden sind. Hierzu hat die Aufsicht im November 2017 mit dem

Rundschreiben 10/2017 (BA) „Bankaufsichtliche Anforderungen an die IT“ aufgezeigt, welche konkreten Erwartungen sie hierzu hat.

• Produktkatalog und Neu-Produkt-Prozess (AT 8.1): Es ist zwingend ein Produkt- und Marktkatalog vorzuhalten. Die aufgenommenen Produkte und Märkte müssen regelmäßig überprüft werden, ob sie weiterhin Gegenstand der Geschäftstätigkeit sind. Sollten Veränderungen eingetreten sein, muss geprüft werden, ob ein NPP erneut zu durchlaufen ist. Die in den Konzepten getroffenen Annahmen sind dahingehend zu hinterfragen, ob diese im Hinblick auf die vorliegenden Risikoeinschätzungen und abgeleiteten Konsequenzen zutreffend waren. Nicht sachgerechte Handhabungen und Mängel sind umgehend zu beheben. Sollten bei dem NPP Unregelmäßigkeiten und Mängel auftreten, muss der NPP unverzüglich aktualisiert werden.

• Forbearance (BTO 1.2.4): In den Kriterien zur Zuordnung für die Intensivbetreuung sind Zugeständnisse, die an den Schuldner gemacht werden, zu berücksichtigen. Eine institutsindividuelle Festlegung soll an die EBA-Kriterien angelehnt erfolgen.

• Erfassung von Abwicklungserlösen (BTR 1, Tz. 7): Abwicklungserlöse und historische Sicherheitenwerte sind zu messen. Die Erkenntnisse aus dieser Erlösquotensammlung sind bei der Adressrisikosteuerung zu berücksichtigen.

• Liquiditätsrisiko (BTR 3): Es sind erhöhte Anforderungen an die Liquiditätsreserven und -diversifikation vorgesehen. Sie müssen so bemessen sein, dass sie auch in Stressphasen ausreichend sind. Die Liquiditätslage ist so darzustellen, dass der kurz-, mittel- und langfristige Bereich abgedeckt ist. Darüber hinaus haben Institute einen internen Refinanzierungsplan aufzustellen, der die Strategien, den Risikoappetit und das Geschäftsmodell angemessen widerspiegelt.

Point of View Kunde:

Die in der 5. MaRisk-Novelle aufgezeigten Klarstellungen gelten sofort, wodurch sich in der Praxis kurzfristig ein Handlungsbedarf ergibt, um Lücken regelkonform und nachhaltig zu schließen.

• Risikodatenaggregation und Risikoberichterstattung:

Aus dem Modul AT 4.3.4. resultiert ein massiver Anpassungsbedarf der in vielen Banken durch Datensilos und manuelle Reporting-Prozesse gekennzeichneten IT-Landschaften. Aus Sicht von RFC Professionals sollten sich Banken spätestens jetzt im Rahmen einer Gap-Analyse mit den Auswirkungen von BCBS 239 auf die Organisationsstruktur, Reporting-Prozesse und IT-Architektur ihres Hauses auseinandersetzen und eine Umsetzungsstrategie entwickeln. In vielen großen Häusern sind dazu bereits Programme aufgesetzt und gestartet worden. Auch wenn sich das Modul AT 4.3.4 explizit auf große und komplexe Institute bezieht, werden auch kleinere Banken nicht umhinkommen, ihre Reporting-Prozesse zu automatisieren, die Produktionszeiten zu verringern und die Datenaggregationskapazitäten zu modernisieren. Anders wird eine Umsetzung von BT 3 nur schwer möglich sein. So betont der Baseler Ausschuss immer wieder die Interdependenzen zwischen der Risikoberichterstattung und dem Datenmanagement. Und auch die Bafin weist explizit darauf hin, dass die Themen Risikodatenaggregation und der Ausbau der Aggregationskapazitäten nicht nur große, systemrelevante Institute betreffen.

• Risikokultur:

Auf der Risikokultur basiert das gesamte Risikomanagement. Risikolimits und die Risikoidentifikation sind Punkte, bei denen sich die Risikokultur am deutlichsten zeigt. Über die bislang schon sichtbare Verankerung der Risikokultur hinaus, muss nun im Unternehmen eine Haltung zum Risiko in Bezug auf die Geschäftstätigkeiten bei jedem Mitarbeiter geschaffen werden. Risikomanagement beginnt mit den Handlungen der Mitarbeiter. Jedem Mitarbeiter ist zu vermitteln, welches Handeln gewünscht und welches nicht gewünscht ist.

Risikokultur zeigt sich laut FSB in mindestens den folgenden vier Dimensionen:

- Eine, von der Unternehmensspitze, gelebte und vorgegebene Leitungskultur,
- festgelegte Verantwortlichkeiten der Mitarbeiter,
- eine offene und kritische Kommunikation sowie
- eine angemessene und langfristig angelegte Anreizstruktur.

Diese Punkte sind nicht nur mit festgeschriebenen Prozessen und Regelungen zu dokumentieren, sondern auch zu leben.

Im Risikomanagementhandbuch und auch für andere Abteilungen ist sichtbar ein Ethikkodex vorzugeben. Dieser Kodex sollte in den Handlungen und der Kommunikation der Führungsebene besonders berücksichtigt werden. Das ständige Bewusstmachen, auch durch regelmäßige Schulungen oder Seminare, ist bis zur untersten Mitarbeiterebene sicherzustellen. Der kritische Dialog ist jederzeit zu gewährleisten und bei Nichtermöglichung sollte eine Eskalationsstelle anrufbar sein. Die Herausforderung ist vor allem auch darin zu sehen, Risikokultur (auch in Reports) messbar und nachprüfbar zu machen.

Schlechte Risikokulturen schlagen sich nicht zuletzt in gehäuften und kostenintensiven Rechtsstreitigkeiten nieder.

• Auslagerung:

Eine Änderung mit erheblichen Auswirkungen ist die Einstufung des isolierten Bezugs von Software und den dazugehörigen Unterstützungsleistungen als sonstiger Fremdbezug, im Zusammenspiel mit den Anforderungen für den sonstigen Fremdbezug von IT-Dienstleistungen der BAIT. Als Auslagerung gilt hingegen der Bezug von Software zur Identifikation, Beurteilung, Steuerung, Überwachung und Kommunikation von Risiken (inkl. dazugehöriger Unterstützungsleitungen) sowie Software, welche für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist. Auch der Betrieb einer solchen Software durch externe Dritte qualifiziert als Auslagerung. In diesem Falle sind die Verträge sehr viel aufwendiger zu planen und umfangreicher zu managen. Die bestehenden Auslagerungsverträge und alle etwaigen Auslagerungen müssen auf notwendige Anpassungsbedarfe geprüft werden. Die Einrichtung eines zentralen Auslagerungsmanagements trägt zu dieser Aufgabe bei. Dort sollte auch die Überwachung und Dokumentation von eigenen, ausreichend fundierten Kenntnissen und Erfahrungen für die effektive Wahrnehmung der Steuerung und Kontrolle der ausgelagerten Funktionen liegen.

Eine Ausstiegsstrategie für jede wesentliche Auslagerung ist ebenfalls, unter Beachtung möglicher und zu identifizierender Handlungsoptionen, zu entwickeln.

Point of View Lösung:

Für alle Neuerungen in den MaRisk, bietet sich ein mehrstufiges Vorgehen an (siehe Abb.1). Zunächst sind die Abweichungen der bestehenden Prozesse zur finalen Fassung der MaRisk, den Vorgaben der bankaufsichtlichen Anforderungen an die IT (BAIT) und ergänzend auch zu entsprechenden Positionspapieren des Basler Ausschusses festzustellen. Dies erfolgt effizient und vollumfänglich über das **RFC MaRisk/BAIT-Check-up-Tool**.

In einem zweiten Schritt ist entsprechend der Kritikalität der Änderung bzw. den zu erwartenden Findings bei Nichterfüllung und den potentiellen wirtschaftlichen Folgen, eine Umsetzungsplanung inklusive Priorisierung zu erstellen. Wirtschaftliche Folgen zeigen sich nicht nur in Wettbewerbsnachteilen, deren Gründe über komparative Prozessschwächen hinausgehen, sie manifestieren sich auch in hohen Rückstellungen für juristische Auseinandersetzungen. Die vorhandenen Kapazitäten sind bei der Planung ebenfalls zu berücksichtigen.

Der dritte Schritt ist die Durchführung des Projekts und ist nachfolgend nur schematisch dargestellt: Der Inhalt ist so individuell wie das jeweilige Geschäftsmodell. Inhalte werden

hierbei Anpassungen im Rahmen des Daten(qualitäts)-managements, Änderungen des Managements von Auslagerungen oder auch die Umkehr von Auslagerungen sowie weitere Anpassungen der schriftlich fixierten Ordnung (SFO) sein.

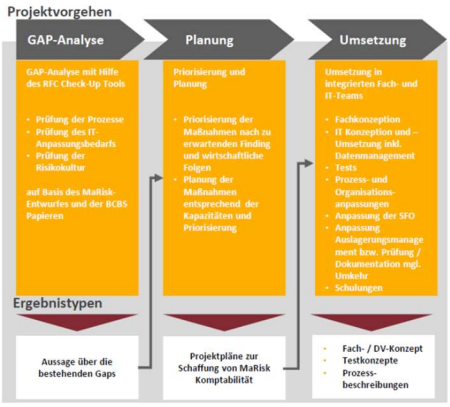

Abb. 1: mehrstufiges Projektvorgehen

Point of View Mehrwert:

Bei der Umsetzung der 5. MaRisk-Novelle begleiten wir unsere Kunden ganzheitlich von der toolunterstützten GAP-Analyse über die Planung der Roadmap bis hin zu den notwendigen Anpassungen der Prozesse und der IT-Landschaft.

Profitieren Sie dabei von der langjährigen Expertise unserer Berater in der gesamten Breite der neuen Anforderungen und greifen Sie auf unser profundes aufsichtsrechtliches Know-how bei Prüfungsvorbereitungen und -begleitungen zurück. Nutzen Sie die hohen Qualitätsstandards unserer zertifizierten Projekt- und Testmanager für eine erfolgreiche Durchführung Ihres MaRisk-Vorhabens. RFC Professionals verfügt über ein Beratungskonzept für die Umsetzung der neuen MaRisk und wird Ihr Institut hierbei nachhaltig unterstützen.

Ihre Ansprechpartner:

Volker Oostendorp Mobil: +49 151 4224 0774
Partner Mail: volker.oostendorp@rfc-professionals.com

Matthias Oßmann Mobil: + 49 151 4224 0784
Senior Manager Mail: matthias.ossmann@rfc-professionals.com

Daniel Jürgens Mobil: +49 171 569 4277
Manager Mail: daniel.juergens@rfc-professionals.com

www.rfc-professionals.com