Ausgestaltung und Auslagerung der MaRisk-Compliance-Funktion

Die Funktion des MaRisk[1]-Compliance-Beauftragten gibt es nun seit über zehn Jahren. Anlass für eine Bestandsaufnahme: Welche Aufgaben sind mit der MaRisk-Compliance-Funktion verbunden, wie grenzt sie sich zu anderen Funktionen ab und welche Anforderungen gibt es an die Auslagerbarkeit?

Grundlage der MaRisk-Compliance sind § 25a Kreditwesengesetz (KWG) und AT 4.4.2 MaRisk. Die Regelungen des § 25a KWG gehen auf die Leitlinien der Europäischen Bankenaufsichtsbehörde und Veröffentlichungen des Baseler Ausschusses für Bankenaufsicht zurück.

Bei den MaRisk selbst handelt es sich um normeninterpretierende Verwaltungsvorschriften zu § 25a KWG, die von der BaFin regelmäßig novelliert und veröffentlicht werden und eine Selbstbindung der Verwaltung darstellen. Die Einhaltung der MaRisk und somit des § 25a KWG wird regelmäßig vom Abschlussprüfer geprüft und kann auch Teil einer Sonderprüfung nach § 44 KWG sein.

Aufgaben

Die Aufgabe der MaRisk-Compliance-Funktion ist es zum einen, den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können, entgegenzuwirken, sowie zum anderen, rechtliche Regelungen und Vorgaben mit einem Compliance-Risiko zu identifizieren. Details ergeben sich überwiegend aus den Textziffern 1–7 der AT 4.4.2 MaRisk und teilweise aus anderen Regelungen der MaRisk wie folgt:

1. Implementierung wirksamer Verfahren, AT 4.4.2 Tz. 1, AT 5 Tz. 3 MaRisk

Die Compliance-Funktion hat auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben hinzuwirken. Durch die weiche Formulierung „hinzuwirken" bringt die Aufsicht zum Ausdruck, dass die primäre Verantwortung bei den entsprechenden Fachabteilungen verbleibt und die MaRisk-Compliance-Funktion eher eine koordinierende, beratende Aufgabe ausübt[2]. Klassische Tätigkeit der Compliance-Funktion ist die regelmäßige Überwachung des rechtlichen Umfeldes auf Veränderungen, um frühzeitig Änderungsbedarfe zu adressieren. Darüber hinaus ist darauf zu achten, dass im Institut für alle wesentlichen Regelungen und Vorgaben auch Zuständigkeiten bestehen. Verstößen gegen Vorgaben oder Regelungen ist nachzugehen.

2. Kontrollen, AT 4.4.2 Tz. 1 MaRisk

Gemäß Tz. 1 zu AT 4.4.2 MaRisk hat die MaRisk-Compliance-Funktion auf entsprechende Kontrollen hinzuwirken. Insofern ist strittig, ob die MaRisk-Compliance-Funktion auch selber eigene Kontrollen durchführen

muss. Die Einhaltung gesetzlicher Regelungen und die Implementierung wirksamer Verfahren zur Einhaltung der gesetzlichen Regelungen verbleiben auch gemäß den MaRisk primär in der Verantwortung des jeweiligen Fachbereichs.

Gleichwohl zeigt die Erfahrung, dass es für die Compliance-Funktion sinnvoll ist, eigene Kontrollen durchzuführen: Es gilt, das Risiko für die Bank zu mindern, indem Mängel (z. B. im Beschwerdewesen) frühzeitig erkannt werden. Aus unserer Sicht ist es für das Institut von Nutzen, wenn ein Mangel frühzeitig durch die Compliance-Funktion und deren Kontrollen aufgezeigt und abgestellt wird. Es ist besser, als wenn der Mangel Thema einer Jahresabschlussprüfung oder gar Sonderprüfung nach § 44 KWG ist.

3. Beratung und Unterstützung der Geschäftsleitung, AT 4.4.2 Tz. 1 MaRisk

Die Compliance-Funktion hat die Geschäftsleitung hinsichtlich der Einhaltung der rechtlichen Regelungen und Vorgaben zu unterstützen und zu beraten. Dementsprechend ist die Compliance-Funktion Ansprechpartner und Berater des Vorstandes zu Compliance-Themen.
Die Unterstützung des Vorstandes erfolgt durch

- die regelmäßige Berichterstattung,
- die regelmäßigen Kontroll- und Jahresberichte sowie
- ggf. durch Ad-hoc-Meldungen bei Feststellen schwerwiegender Mängel im Rahmen eigener Kontrollhandlungen.

Ein Beispiel aus unserer Praxis ist die Beratung zur Risikokultur und deren Implementierung im Institut.

4. Identifizierung wesentlicher Regelungen und Vorgaben, AT 4.4.2 Tz. 2 MaRisk

a. Risikoanalyse

Die Identifizierung der wesentlichen rechtlichen und institutsindividuellen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Vermögens des Institutes führen kann, ist eine der Hauptaufgaben der Compliance-Funktion und hat in regelmäßigen Abständen zu erfolgen. Darauf aufbauend ergeben sich dann die weiteren Schritte zur Risikoüberwachung und -reduzierung, z. B. durch Kontrollen, Schulungen etc.

Welche Regelungen und Vorgaben zu bewerten sind, ist mehrstufig zu prüfen. Zunächst müssen abhängig von dem Geschäftsmodell, den Produkten und Märkten etc. die Regelungen und Vorgaben herausgefiltert werden, die für das Institut nicht einschlägig sind. Darauf aufbauend sind die Regelungen und Vorgaben herauszufiltern, die nicht-finanzbranchenspezifisch sind und daher nicht unbedingt der Bewertung durch die MaRisk-Compliance-Funktion bedürfen. Schließlich gibt es auch Spezialzuständigkeiten bzw. Fachabteilungen mit besonderem Wissen, sodass die MaRisk-Compliance-Funktion hier hinter funktionierende Spezialzuständigkeiten zurücktritt.

Eine wesentliche Arbeitserleichterung ist die vom Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. (BVR) zur Verfügung gestellte und halbjährlich aktualisierte Muster-Bestandsaufnahme[3]. In dieser werden auf Grundlage des BaFin-Protokolls zur Sitzung des Fachgremiums MaRisk am 24. April 2013 bereits die unwesentlichen rechtlichen Regelungen und Vorgaben sowie auf etwaige Spezialzuständigkeiten eingegangen und aufgelistet.

Die Identifizierung der wesentlichen Regelungen und Vorgaben erfolgt üblicherweise in einer Risikoanalyse und hat mindestens jährlich sowie anlassbezogen zu erfolgen. Gründe für eine anlassbezogene Risikoanalyse können beispielsweise Fusionen, wesentliche eigene Feststellungen der Compliance-Funktion, der Internen Revision oder Erkenntnisse aus dem Prüfungsbericht des Jahresabschlussprüfers oder einer Sonderprüfung nach § 44 KWG sein.

b. Rechtsmonitoring

Darüber hinaus obliegt dem Institut die Überwachung der rechtlich-regulatorischen Regelungen und Vorgaben einschließlich deren Umsetzung. Damit soll sichergestellt werden, dass das Institut die aktuellen Vorschriften und Regelungen, z. B. Gesetze, Urteile, Vorgaben der Aufsicht, in der täglichen Praxis beachtet und umsetzt, wodurch eine Risikoreduzierung herbeigeführt wird.
Notwendig ist somit ein Rechtsmonitoring. Das Institut

selbst kann die entsprechenden einschlägigen Quellen auswerten und ein Rechtsmonitoring erstellen oder aber ein Rechtsmonitoring beziehen, das auf das Geschäftsmodell des Institutes abgestimmt sein sollte. Das heißt, die Rechtsmonitoring-Einträge nebst Handlungsempfehlungen sollten mit dem Geschäftsmodell der Bank korrespondieren und diese abdecken und nicht auch Themen enthalten, die für das Institut nicht einschlägig sind.

5. Berichtspflichten, AT 4.4.2 Tz. 7 MaRisk

In Tz. 7 zu AT 4.4.2 MaRisk ist normiert, dass die Compliance-Funktion mindestens jährlich sowie anlassbezogen über ihre Tätigkeit Bericht zu erstatten hat. Diese Berichterstattung erfolgt üblicherweise über den Jahresbericht und informiert die Geschäftsleitung über die erfolgten Tätigkeiten der MaRisk-Compliance-Funktion. Gleichzeitig wird eine Aussage zur Angemessenheit und Wirksamkeit des Compliance-Risikomanagementsystems getroffen. Damit wird der Vorstand in die Lage versetzt, die Compliance-Risiken zu beurteilen, zu steuern und etwaige Mängel abzustellen.

Ad-hoc-Berichte der Compliance-Funktion können in festgestellten und nicht beseitigten Mängeln, in Verstößen gegen wesentliche Regelungen und Vorgaben oder in wesentlichen Mängeln in Prozessen begründet sein.

Der (Compliance-)Bericht nach Tz. 7 MaRisk umfasst nur MaRisk-Compliance-relevante Themen. Die anderen Compliance-Funktionen, z. B. der WpHG-Compliance, Geldwäsche und Terrorismusfinanzierung, bzw. Datenschutz und Informationssicherheit erstellen eigene Berichte (soweit vorgeschrieben). Es ist nicht Aufgabe der MaRisk-Compliance-Funktion, einen „Gesamt-Compliance-Bericht“ zu erstellen.

Empfänger des MaRisk-Compliance-Berichtes ist zunächst der Vorstand. Die Berichte sind auch an die Interne Revision und das Aufsichtsorgan weiterzuleiten.

6. Einbindung in den Neu-Produkt-Prozess und Einbindung in die Änderung betrieblicher Prozesse oder Strukturen, AT 8.1 und AT 8.2 MaRisk

Die Compliance-Funktion ist auch bei Neu-Produkt-Prozessen und wesentlichen Änderungen einzubinden. Gegenstand der Compliance-Prüfung ist dann z. B.:

- ob die Risiken durch die Fachabteilungen bewertet wurden,
- ob die Produkt-Governance eingehalten wurde,
- ob der Produkt-/Märktekatalog angepasst werden muss bzw.
- ob die Ausführungen zur Wesentlichkeit der Änderung schlüssig und nachvollziehbar sind.

Damit verbunden ist jeweils die Frage, ob die Risikoanalyse unter Berücksichtigung der Bewertung nach AT 8 MaRisk die Risiken noch angemessen wiedergibt oder aber eine Ad-hoc-Risikoanalyse durchzuführen ist.

Befugnisse der Compliance-Funktion, AT 4.4.2 Tz. 3, 6 MaRisk

Die Compliance-Funktion muss schlagkräftig agieren können. Dementsprechend werden ihr spezielle Befugnisse eingeräumt. Sie kann auf andere Funktionen und Stellen zugreifen, sie hat Informationsrechte. Das heißt, sie hat einen uneingeschränkten Zugang zu allen Informationen, die sie für ihre Arbeit benötigt, und ihr gegenüber bestehen Mitteilungspflichten.

Nicht abschließend geklärt ist, ob die MaRisk-Compliance-Funktion auch Weisungs- oder Vetorechte hat, wie es beispielsweise bei anderen Funktionen der Fall ist. Die Aufsicht hat sich im Protokoll zur Sitzung des Fachgremiums MaRisk am 24. April 2013 in Abschnitt 4 dazu nicht abschließend geäußert.

Vor dem Hintergrund, dass die Compliance-Funktion lediglich auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen „hinwirken“ soll, ist es gut vertretbar, ein Veto- und Weisungsrecht zu verneinen. Dafür spricht auch, dass die Geschäftsleitung nach § 25c Abs. 4a Ziff. 3c KWG weiterhin die Gesamtverantwortung trägt und die Compliance-Funktion sich jederzeit an die Geschäftsleitung wenden kann.

1. Organisatorische Stellung der MaRisk-Compliance-Funktion, AT 4.4.2 Tz. 3 MaRisk

Die MaRisk-Compliance-Funktion ist grundsätzlich der Geschäftsleitung unterstellt. Eine Anbindung an andere Einheiten ist möglich, es muss aber immer eine direkte Berichtslinie an die Geschäftsleitung existieren.

Der Wechsel des MaRisk-Compliance-Beauftragten ist dem Aufsichtsorgan unter Angabe der Gründe mitzuteilen, eine Information der Aufsicht ist nicht notwendig.

2. Abgrenzung zu anderen Bereichen

Im Institut gibt es verschiedene Compliance- und Kontrollbereiche. Zu nennen ist u. a. die WpHG-Compliance-Funktion, die Funktion zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen, aber auch die Interne Revision.

Im Hinblick auf WpHG-Compliance und die Funktion des Geldwäschebeauftragten soll die MaRisk-Compliance-Funktion einerseits das Risiko reduzieren und weiße Flecken bzw. Regelungslücken im Institut verhindern und andererseits auf eine einheitliche Compliance-Kultur hinwirken. Daher hat die MaRisk-Compliance-Funktion einen generalistischen Ansatz und stellt keine Superkontroll- oder Superrevisionsinstanz für die anderen Compliance-Bereiche dar[4]. Sofern es spezialisiertes Compliance-Wissen im Institut gibt, sind diese speziellen Compliance-Funktionen primär für die einschlägigen Themen zuständig und nicht die MaRisk-Compliance-Funktion. Entsprechendes gilt auch für das Risiko-Controlling mit dem dort angesiedelten Fachwissen.

Das Verhältnis zur Internen Revision ist durch das Three-Lines-of-Defense-Modell gekennzeichnet. Compliance gehört der zweiten Verteidigungslinie an und prüft prozessabhängig beschränkt auf compliancerelevante Themen, während die Interne Revision der dritten Verteidigungslinie angehört und prozessunabhängig das gesamte Institut einschließlich der Compliance-Funktion prüft.

3. Herausforderungen der letzten Jahre

In den letzten Jahren haben sich das Aufgabenfeld des MaRisk-Compliance-Beauftragten und seine Wahrnehmung im Institut geändert.

Er trägt heute maßgeblich dazu bei, den Fachabteilungen und somit dem Institut Sicherheit zu geben. Die Compliance-Funktion ist bereits während des laufenden Prozesses in Entscheidungen eingebunden (anders als die Revision, die überwiegend nachgelagert und rückblickend tätig ist). Auch wird die Compliance-Funktion häufig als Gesprächs- und Sparringspartner gesucht, um Prozesse und Verfahren zu optimieren bzw. Sachverhalte frühzeitig zu besprechen.

Für den MaRisk-Compliance-Beauftragten ist das Aufgabenfeld umfassender geworden. Die BaFin hat z. B. die MaRisk-Compliance-relevanten Themen

- ESG AT 2.2, 3, 4.1 MaRisk und
- Immobilien BTO 3 MaRisk

in die MaRisk aufgenommen.

Auch sind durch die Bundesbank Finanzsanktionen nun eine Aufgabe des Compliance-Beauftragten, bei denen sogar eigenständige Kontrollen erwartet werden. Die Themen

- Risikokultur,
- Produktgovernance und leider auch
- die Kriege in der Ukraine und in Nahost

sind ebenfalls MaRisk-Compliance-relevant.

Auslagerung der MaRisk-Compliance-Funktion, AT 9 MaRisk

Die Auslagerung der Funktion des MaRisk-Compliance-Beauftragten ist grundsätzlich zulässig. In AT 9 Tz. 4 MaRisk ist geregelt, dass grundsätzlich alle Funktionen und Prozesse auslagerbar sind, wenn dadurch die Ordnungsgemäßheit der Geschäftsorganisation des Institutes nach § 25a Absatz 1 KWG nicht beeinträchtigt wird. Besondere Maßstäbe gelten für die vollständige oder teilweise Auslagerung der MaRisk-Compliance-Funktion. Nach AT 9 Tz. 5 MaRisk sind zwei Fallkonstellationen denkbar: zum einen bei einem Tochterinstitut innerhalb einer Gruppe und zum anderen bei „kleinen Instituten".

Bei kleinen Instituten ist die vollständige Auslagerung der MaRisk-Compliance-Funktion möglich, sofern deren Einrichtung vor dem Hintergrund der Institutsgröße sowie der Art und des Umfangs, der Komplexität und des Risikogehaltes der betriebenen Geschäftsaktivitäten nicht angemessen erscheint. Eine abschließende Festlegung der Aufsicht, wann ein Institut als klein gilt, gibt es nicht.

Während früher häufig allein auf die Bilanzsumme abgestellt wurde, so wird heute eine Kombination aus Bilanzsumme und Komplexität als Kriterium herangezogen. Bei Bilanzsummen bis zu 30 Mrd. Euro und einem wenig komplexen Geschäftsmodell ist eine Auslagerung der MaRisk-Compliance-Funktion zulässig. Ein wenig komplexes Geschäftsmodell liegt vor, wenn Standardgeschäfte betrieben werden, insbesondere die der Genossenschaftlichen FinanzGruppe. Der Risikogehalt der so betriebenen Geschäfte ist in der Regel gering.

Spätestens wenn ein Institut nicht mehr als „SNCI " (small and non-complex institution) privilegiert ist, dürfte die vollständige Auslagerung nicht mehr möglich sein, eine teilweise Auslagerung aber weiterhin. Vorteile einer vollständigen oder teilweisen Auslagerung der MaRisk-Compliance-Funktion sind

- umfassendes, spezialisiertes Fachwissen der Compliance-Funktion,
- modernes Compliance-Management-System, bei dem u. a. Risikoanalyse, Kontrollen und Rechtsmonitoring miteinander verknüpft sind,
- Reduzierung der Personalkosten im Institut,
- Sicherstellung der Abwesenheitsvertretung des Compliance-Beauftragten,
- Sicherstellung der Aus- und Fortbildung des Compliance-Beauftragten,
- Entfall der Kosten für den gesonderten Bezug eines Rechtsmonitorings, sofern dies im Rahmen der Auslagerung gestellt wird,
- Entfall von Prüfungsleistungen durch die Interne Revision des Institutes, sofern der Dienstleister über ein Testat nach IDW PS 951 Typ 2 verfügt. ▬

Jörg Scharditzky
Abteilungsleiter MaRisk-Compliance,
E-Mail: joerg.scharditzky@dz-cp.de

[1] Die Ausführungen im Text beziehen sich auf die aktuellen Mindestanforderungen an das Risikomanagement (MaRisk), BaFin-Rundschreiben 06/2024 (BA)
[2] Christoph Kunze, MaRisk-Compliance, BVR-Bankenreihe Band 4, 3. Auflage 2024
[3] Wie auch die weiteren Arbeitshilfen des BVR, z. B. Muster-Jahresbericht, Ad-hoc-Musterbericht
[4] Christoph Kunze, a.a.O., Ziff. 1.2.1