Mindestanforderungen an das Risikomanagement (MaRisk)

Protokoll zur Sitzung des Fachgremiums MaRisk am 24.04.2013 in Bonn (BaFin)
Thema: Compliance-Funktion

1. Begrüßung

2. Allgemeine Anmerkungen zum Thema Compliance-Funktion

Die BaFin fasst zu Beginn der Sitzung kurz ihre Sichtweise zum Thema Compliance-Funktion zusammen, wie sie sie im Ansatz auch schon im Anschreiben zur Endfassung zur MaRisk-Novelle zum Ausdruck gebracht hat. Die neu in die MaRisk eingefügten Anforderungen zur Compliance-Funktion basieren schwerpunktmäßig auf einschlägigen Passagen in den EBA Guidelines on Internal Governance[1]. Weitere Aspekte hierzu, die in die gleiche Richtung zielen, lassen sich einem Papier des Baseler Ausschusses zum Thema Compliance[2] entnehmen. Mit der Compliance-Funktion soll nicht nur den Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können, begegnet werden. Sie ist vielmehr auch ein wichtiger Baustein zur Förderung einer einheitlichen Compliance-Kultur im Institut.

Beim Themenkomplex Compliance handelt es sich im Grunde nicht um eine neue Materie. Zunächst ist es natürlich eine Selbstverständlichkeit, dass Unternehmen – gleich welcher Branche – sicherzustellen haben, dass gesetzliche Regelungen und Vorgaben in Gänze befolgt und beachtet werden. Auch existierten schon vor der MaRisk-Überarbeitung Rechtsgebiete, die mit speziellen Compliance-Vorgaben belegt waren und sind. Namentlich sind hier die Vorgaben des WphG (MaComp), des § 25c KWG (Geldwäsche, sonstige strafbare Handlungen) und des Datenschutzgesetzes zu nennen. Die Tatsache, dass alle gesetzlichen Regelungen und Vorgaben zu beachten sind, bedeutet hingegen nicht, dass alle Rechtsbereiche gleichermaßen von einer speziell dafür eingerichteten Compliance-Funktion abgedeckt werden müssen. Diese wird sich aus Sicht der Aufsicht auf ganz bestimmte rechtliche Regelungen konzentrieren, nämlich auf solche, die mit Compliance-Risiken behaftet sind. In den einschlägigen internationalen Papieren wird weder der genaue Aufgabenumfang der Compliance-Funktion beschrieben noch eine abschließende Definition von Compliance-Risiken vorgenommen. Gleichwohl lässt sich konstatieren, dass die hier im Fokus stehenden Compliance-Risiken sich insbesondere dadurch „auszeichnen", dass bei einer Nichtbeachtung von rechtlichen Regelungen und Vorgaben vor allem (Geld-)Strafen/Bußgelder, Schadenersatzansprüche und/oder die Nichtigkeit von Verträgen drohen, die zu einer Gefährdung des Vermögens des Instituts führen können. So interpretiert lassen sich daraus Rückschlüsse ziehen, welche Art von rechtlichen Regelungen und Vorgaben (mindestens) von der Compliance-Funktion aufzugreifen sind. Neben jenen Rechtsbereichen, die schon aufgrund spezialgesetzlicher Anforderungen besonderen Compliance-Anforderungen unterliegen, sind weitere rechtlichen Regelungen und Vorgaben, die von der Compliance-Funktion abzudecken sind, eigenverantwortlich vom Institut zu identifizieren. Insofern wird eine vorgelagerte Identifizierung bzw. Analyse möglicher Compliance-Risiken eine wichtige Rolle einnehmen.

Was die organisatorische Anbindung betrifft, weist die BaFin darauf hin, dass unter der Einhaltung der Grundprämisse, nämlich der direkten Anbindung an die Geschäftsleitung, grundsätzlich mehrere Lösungen denkbar und möglich sind. Weitere Einzelheiten hierzu werden unter dem Themenpunkt „Organisatorische Einbindung" diskutiert.

---

[1] EBA Guidelines on Internal Governance (GL 44), 27.09.2011; abrufbar unter http://www.eba.europa.eu/Publications/Guidelines.aspx

[2] BCBS: Compliance and the compliance function in banks, 29.04.2005; abrufbar unter http://www.bis.org/publ/bcbs113.htm

3. Anwendungsbereich; Umfang der abzudeckenden rechtlichen Regelungen und Vorgaben

Anknüpfend an den einleitenden Ausführungen zeigt die BaFin auf, welche rechtlichen Regelungen und Vorgaben in jedem Fall in den Anwendungsbereich der Compliance-Funktion fallen. Hierzu gehören zunächst die Vorgaben des WphG, die schon Gegenstand der MaComp sind, weiterhin die Vorgaben zur Vermeidung von Geldwäsche und Terrorismusfinanzierung; Vorgaben zur Vermeidung sonstiger strafbarer Handlungen (die zusammen mit den Vorgaben zur Geldwäscheprävention in § 25c KWG geregelt sind), Vorgaben zum Datenschutz sowie weitere Vorgaben zum Verbraucherschutz (z.B. zu Verbraucherkrediten, AGB, Zahlungsverkehr; oftmals außerhalb des Aufsichtsrechts geregelt). Demgegenüber lassen sich aus Sicht der BaFin rechtliche Regelungen und Vorgaben nennen, deren Einhaltung zwar nicht weniger zwingend ist, die jedoch nicht unbedingt einer Adressierung durch die Compliance-Funktion unterliegen müssen. In vielen Fällen handelt es sich dabei um nicht-branchenspezifisches Recht: Arbeitsrecht/Personalrecht, Lohn-/Einkommensteuerrecht etc. Eine Ausklammerung solcher Rechtsbereiche aus dem Tätigkeitsbereich der Compliance-Funktion erscheint vor dem Hintergrund des Regulierungszwecks – Vermeidung oder zumindest Verminderung von Compliance-Risiken im beschriebenen Sinn – grundsätzlich nachvollziehbar. Explizit weist die BaFin auch auf den Umgang von rechtlichen Regelungen und Vorgaben hin, die die Bereiche Risikocontrolling und Rechnungslegung/Finanzen betreffen. Gerade für diese Bereiche kann eine Compliance-Funktion auf spezialisiertes Wissen der fachlich zuständigen Einheiten zurückgreifen und aufbauen. Insofern erscheint es aus Sicht der BaFin plausibel, bei entsprechenden rechtlichen Regelungen und Vorgaben, die das Risikocontrolling (z. B. solche zur Risikotragfähigkeit, zu Risikocontrollingprozessen, zur (regulatorische) Kapitalunterlegung) oder die Rechnungslegung (Bilanzrecht) betreffen, auf den Einschätzungen und Beurteilungen der jeweils zuständigen Einheiten aufzusetzen und auf eigene Aktivitäten der Compliance-Funktion (weitestgehend) zurückzustellen oder sogar im Wesentlichen zu verzichten.

Neben den rechtlichen Regelungen und Vorgaben, die zwingend von der Compliance-Funktion abzudecken sind, sind weitere Regelungen und Vorgaben, die von dieser aufgegriffen werden (sollen), letztendlich institutsindividuell zu identifizieren. Auf Fragen von Institutsvertretern, ob beispielsweise das Gesellschaftsrecht oder das Kartellrecht hierzu zu zählen haben, verweist die BaFin auf die Eigenverantwortlichkeit der Institute. Gleichzeitig macht die BaFin deutlich, dass eine vorgelagerte Bestandaufnahme/Risikoanalyse, die möglichst umfassend ausgestaltet ist und regelmäßig überprüft werden soll, in diesem Kontext von besonderer Bedeutung ist. Es besteht grundsätzlich Einigkeit, dass eine abschließende Aufzählung von Rechtsbereichen, die von der Compliance-Funktion zu adressieren sind und für alle Institute gleichermaßen zutreffend ist, nicht zielführend sein kann. Vielmehr ist die Thematik Compliance immer institutsindividuell vor dem Hintergrund der konkreten Geschäftsaktivitäten und der konkreten Märkte, auf dem sich das jeweilige Institut bewegt, zu sehen. Gleichermaßen wichtig ist jedoch auch eine möglichst umfassende Betrachtung aller Bereiche, um mögliche Compliance-Risiken zu identifizieren – dies betrifft grundsätzlich auch Rechtsbereiche, die später wieder aus dem Tätigkeitsfeld der Compliance-Funktion ausgeklammert werden.

4. Aufgaben der Compliance-Funktion

Aus der allgemeinen Aufgabe der Compliance-Funktion – des Hinwirkens auf die Implementierung wirksamer Verfahren zur Einhaltung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben und entsprechender Kontrollen – sowie der unmittelbaren Anbindung dieser Funktion an die Geschäftsleitung lassen sich aus Sicht der BaFin bestimmte konkrete Aufgaben ableiten. Zunächst wird damit deutlich, dass der Fokus nicht ausschließlich auf neuen Regelungen, sondern auch auf

schon bestehenden liegt. Daher muss die Compliance-Funktion nicht nur Neuregelungen im Auge haben, sondern auch die Rechtsprechung im Rahmen bestehender rechtlicher Regelungen und Vorgaben verfolgen, sofern diese Auswirkungen für das Institut haben könnte. Die Diskussion ergab, dass bei der Identifizierung von Handlungsbedarf aus Compliance-Sicht umfangreiche Unterstützungsleistungen aus den jeweiligen Fachbereichen und den Rechtsabteilungen der Institute geleistet werden. In Einzelfällen werden offenbar auch Projektteams gebildet, die sich aus unterschiedlichen Bereichen zusammensetzen (auch aus der Compliance-Funktion) und einzelne Themen, die sich aus Neuregelungen oder veränderter Rechtsprechung ergeben, sukzessive abarbeiten. Verbundangehörigen Institute werden bei der Informationsgewinnung zu Änderungen des rechtlichen Umfelds der Institute zusätzlich von den jeweiligen Verbänden unterstützt.

Die BaFin stellt klar, dass die Implementierung von wirksamen Verfahren zur Einhaltung wesentlicher gesetzlicher Regelungen und Vorgaben in der Verantwortung der jeweils betroffenen Fachbereiche liegt und nicht automatisch bei der Compliance-Funktion. Diese wiederum hat darauf zu achten, dass die betroffenen Fachbereiche ihrer Verantwortung auch tatsächlich nachkommen und dass keine Rechtsbereiche bestehen, in denen zwar Handlungsbedarf besteht, die mangels eindeutiger Zuständigkeiten jedoch gewissermaßen „brach liegen". So gesehen hat die Compliance-Funktion auch einen schwerpunktmäßig koordinierenden Charakter und – als Ausdruck der direkten Anbindung an die Geschäftsleitung – eine beratende Funktion gegenüber der Geschäftsleitung, welche auch weiterhin die Letztverantwortung für die Einhaltung rechtlicher Regelungen und Vorgaben im Institut trägt. Besonderheiten, die sich für bestimmte Rechtsbereiche aus spezialgesetzlichen Vorgaben ergeben können, bleiben jedoch unberührt. Dies ist schon in der Endfassung der neugefassten MaRisk ausdrücklich klargestellt. So weist die BaFin auf die Frage, inwieweit die Compliance-Funktion Überwachungshandlungen vorzunehmen hat, auf entsprechenden Vorgaben z.B. der MaComp hin, die mit Blick auf die WphG-Compliance explizit einen Überwachungsplan fordern und damit entsprechende Überwachungshandlungen erwarten. Auch unter MaRisk-Gesichtspunkten hält es die BaFin für erforderlich, dass die Compliance-Funktion Kontrollhandlungen zumindest durchführen können muss und insoweit auch entsprechende Kontrollrechte eingeräumt bekommt. Der tatsächliche Umfang vorzunehmender Kontrollhandlungen wird von BaFin-Seite nicht vorgegeben, sondern verbleibt in der Eigenverantwortung der Institute. Auch die Frage nach möglicherweise erforderlichen Weisungsrechten lässt sich nicht abschließend beantworten. Grundsätzlich erwartet die BaFin nicht, dass der Compliance-Funktion umfassende Weisungsrechte gegenüber den Fachbereichen eingeräumt werden, da sie eine „Eskalation" bei Mängeln in den Kontrollprozessen im Regelfall durch eine (Ad-hoc-)Berichterstattung an die Geschäftsleitung für zielführend erachtet. Dabei ist jedoch zu beachten, dass nach der spezialgesetzlichen Norm des § 25c KWG der Geldwäschebeauftragte mit einem solchen Weisungsrecht auszustatten ist, soweit geldwäscherelevante Fragen betroffen sind.

5. Organisatorische Einbindung

Die organisatorische Einbindung der Compliance Funktion wirft bei den Teilnehmern eine Reihe von Fragen auf, auf die die BaFin im Folgenden weiter eingeht. In der aufsichtlichen Praxis existieren bereits Vorgaben zur aufbauorganisatorischen Einbindung von Compliance-Einheiten (z.B. nach WphG/MaComp). Daher scheint es sowohl aus institutsinterner als auch aufsichtlicher Perspektive sinnvoll zu prüfen, inwieweit die Compliance-Funktion (nach MaRisk) in bereits bestehende Compliance-Strukturen integriert werden kann. Die Aufsicht hat daher bewusst in AT 4.4.2 Tz. 3 die Möglichkeit geschaffen, die Compliance-Funktion an andere Kontrolleinheiten anzubinden. Es ist unter Berücksichtigung des Proportionalitätsprinzips für kleinere Institute nicht notwendig, eine neue, eigenständige Stelle zu schaffen. Eine Einschränkung gilt jedoch für größere Institute – von diesen Instituten erwartet die Aufsicht, dass diese

eine eigenständige Organisationseinheit für die Compliance implementieren. Dies entspricht im Allgemeinen aber schon heute der gängigen Praxis.

Die BaFin hat noch einmal betont, dass die Compliance-Funktion, unabhängig davon, ob es sich um eine separate Organisationseinheit handelt oder eine Anbindung an eine andere Kontrolleinheit erfolgt, unmittelbar der Geschäftsleitung zu unterstellen ist. Weiterhin ist sie der Geschäftsleitung berichtspflichtig. Aus diesem Grund kann die Compliance-Funktion nicht als untergeordnete Stelle in der organisatorischen Struktur des Instituts angesiedelt werden. Nur eine unmittelbare organisatorische Zuordnung zur Geschäftsleitung verschafft ihr das notwendige Gehör auf Geschäftsleiterebene und fördert dadurch ihre Funktionsfähigkeit.
Im Hinblick auf die Anbindung an bereits bestehende Kontrolleinheiten – mit Ausnahme der Internen Revision - sind durchaus verschiedene Konstellationen denkbar. Wichtig ist hierbei, dass die organisatorische Zuordnung zu einem vom Markt und Handel unabhängigen Bereich erfolgt und die Compliance-Funktion der Geschäftsleitung unmittelbar unterstellt ist. Beispielhaft ist eine Bündelung beim Geldwäschebeauftragten ebenso möglich wie eine Anbindung an das Risikocontrolling. Die Bedeutung der Risikocontrolling Funktion (AT 4.4.1) wurde im Rahmen der MaRisk Novelle 2012 dahingehend unterstrichen, dass die Risikocontrolling-Funktion von großen, international tätigen Instituten von einem Geschäftsleiter in exklusiver Weise wahrzunehmen ist. Die BaFin stellt klar, dass bei einer exklusiven Wahrnehmung der Risikocontrolling-Funktion durch einen Geschäftsleiter einer Zuordnung der Compliance-Funktion beim Risikocontrolling nichts entgegensteht.

Sollte ein Institut eine eigenständige zentrale Organisationseinheit für alle Compliance-Bereiche vorhalten, ergäbe sich daraus zwangsläufig eine Personalunion des Leiters Compliance mit denen des WphG-Compliance-Beauftragten sowie des Geldwäschebeauftragten. Eine solche Lösung, wie sie bereits in der Praxis vorzufinden ist, wird von der BaFin durchaus als zulässig angesehen. Weiterhin möglich ist jedoch auch eine dezentral aufgestellte Compliance-Funktion, bei der die Beauftragten nach WphG/MaComp, nach § 25c KWG (Geldwäsche und sonstige strafbare Handlungen) sowie der Geldwäschebeauftragte separat agieren. Die diesbezüglichen Vorgaben der spezialgesetzlichen Regelungen – insbesondere auch zur Berichterstattung – sind auch dabei weiterhin zu beachten. Besonderheiten können sich hinsichtlich des Datenschutzbeauftragten gemäß BDSG ergeben. Dieser hat in seiner Funktion u.a. darauf zu achten, dass den Grundsätzen der Datenvermeidung und Datensparsamkeit Rechnung getragen wird. Dies könnte zu Interessenkonflikten führen, sollte der Datenschutzbeauftragte in einer zentral aufgestellten Compliance-Funktion integriert werden.

6. Schlussbemerkungen

Die Diskussion im Fachgremium zeigt, dass die Thematik Compliance durchaus sehr unterschiedlich in den Instituten gehandhabt wird. Dies soll auch in Zukunft nicht per se in Frage gestellt werden, sofern die aufsichtlichen Vorgaben – auch auf Basis der speziellen aufsichtlichen Regelungen – weiterhin erfüllt werden. Aus den Diskussionen wird auch deutlich, dass unterschiedlichste Ansätze und Ausgestaltungen dem aufsichtlichen Ziel einer Stärkung der Compliance in den Instituten gleichermaßen gerecht werden können. Gerade im Hinblick auf die Ausgestaltung der Compliance-Funktion haben die Institute großen Gestaltungsspielraum, der aus Sicht der BaFin genutzt werden soll, um die schon vorhandenen Compliance-Vorkehrungen um noch nicht berücksichtigte Bereiche zu ergänzen und so die Anforderungen der MaRisk vollständig zu erfüllen. Dabei ist sich die BaFin im Klaren darüber, dass es auch in Zukunft keine einheitliche Vorgehensweise in der Praxis geben muss und kann, da die Anforderungen sehr unterschiedlich mit Leben gefüllt werden können.