Bernd Michael Lindner / Dorit Schroeren

Neueste Entwicklungen von **Compliance** in Banken durch die 4. MaRisk-Novelle[1)]

Die Bedeutung von Compliance ist in den letzten Jahren über alle Branchen hinweg stetig gestiegen, damit einhergehend auch das Compliance-Verständnis in der Bankenwelt. Wohingegen man anfangs in der deutschen Bankenbranche nur die Wertpapier-Compliance[2)], die Einhaltung von Vorschriften des WpHG und damit zusammenhängenden Verordnungen, unter den Begriff der Compliance gefasst hat, hat sich dieses Verständnis im Verlauf der Zeit stark geändert. Zunächst kam den Finanzsanktions- und Embargo-Regelungen beginnend mit den Terroranschlägen 2001 eine größere Bedeutung zu. Ein weiterer großer Schritt nach vorne ging 2008 von der 3. EG-Geldwäscherichtlinie aus, die dazu beigetragen hat, die bis dahin bereits bestehenden Regelungen zur Geldwäscheprävention von einem regelbasierten hin zu einem risikobasierten Ansatz weiterzuentwickeln.

Entwicklung zur integrierten Compliance

Die Compliance in Banken hat durch die erste Veröffentlichung der MaComp[3)] (2010), welche unter anderem die Compliance-Funktion für Wertpapierdienstleistungsunternehmen regelt, und die Einführung der zentralen Stelle durch den geänderten § 25c KWG wesentlich an Bedeutung gewonnen. Durch diese Regelungen, die nur exemplarisch genannt seien, hat sich in Banken als breiter Standard ein integrierter Compliance-Begriff entwickelt, der in der Compliance-Organisation die Themengebiete Wertpapier-Compliance, Geldwäscheprävention, Einhaltung von Finanzsanktions- und Embargobestimmungen und Prävention sonstiger strafbarer Handlungen (Betrugsprävention) umfasst.

Spätestens seit der Finanzkrise und dem damit einhergehenden Vertrauensverlust der Banken hat sich die Erwartungshaltung der Öffentlichkeit, vor allem der Investoren und Kunden, gegenüber Banken geändert. Dies hat das Compliance-Verständnis durchaus gestärkt.

Anfang Dezember 2012 erfolgte die Veröffentlichung der Neufassung der MaComp, die neben dem überarbeiteten allgemeinen Teil und neuen Modul BT 7 zur Geeignetheitsprüfung auch eine Weiterentwicklung und Konkretisierung der Compliance-Funktion nach BT 1 MaComp für Banken vorsieht, die gleichzeitig Wertpapierdienstleistungsunternehmen sind. Insbesondere wird dabei auf die Förderung und Stärkung der Compliance-Kultur Wert gelegt.

Mit der am 14. Dezember 2012 veröffentlichten Novellierung der MaRisk, die vor allem auf der überarbeiteten EU-Bankenrichtlinie[4)] und deren Verordnung[5)] sowie den EBA Guidelines of Internal Governance[6)] basieren, und der damit zusammenhängenden Forderung nach Einrichtung einer Compliance-Funktion (AT 4.4.2), soll ebenfalls die Compliance-Kultur in Banken gefestigt werden. Mit der Ausgestaltung der Compliance-Funktion nach MaRisk verfolgt die BaFin ein neues, weitergefasstes Compliance-Verständnis, dem ein risikoorientierter Ansatz, der mittlerweile auch in anderen Compliance-Themen existiert, zugrunde liegt.

Im Rahmen dieses Artikels werden aktuelle Fragestellungen im Zusammenhang mit der Compliance-Funktion nach MaRisk mit möglichen Lösungsansätzen diskutiert. Zunächst erfolgt allerdings eine kurze Darstellung der neuen Anforderungen durch AT 4.4.2 MaRisk.

Anforderungen nach AT 4.4.2 MaRisk im Überblick

Die Novellierung der MaRisk sowie des KWG sieht erstmalig die Etablierung der Compliance-Funktion vor, die als wesentliches Element neben der Risikocontrolling-Funktion als Bestandteil des internen

Bernd Michael Lindner, Partner, München, und Dorit Schroeren, RA, Senior Manager, Düsseldorf, beide Bereich Consulting Financial Services, KPMG AG Wirtschaftsprüfungsgesellschaft

Mit der Veröffentlichung der Mindestanforderungen an die Compliance-Funktion im Jahre 2010 und den relevanten Anpassungen im Dezember 2012 registrieren die Autoren ein weitergefasstes Compliance-Verständnis der Aufsicht, dem ein risikoorientierter Ansatz zugrunde liegt. Vor diesem Hintergrund diskutieren und bewerten sie aktuelle Fragestellungen im Zusammenhang mit der Compliance-Funktion nach MaRisk mit möglichen Lösungsansätzen. Als zentrale Herausforderung formulieren sie die Entwicklung eines individuellen Zielbildes und dessen effiziente und schlanke Umsetzung in einem strukturierten und systematischen Ansatz. Von einem methodischen Vorgehen versprechen sie sich dabei die Möglichkeit einer kompletten und nachvollziehbaren Dokumentation des gesamten Umsetzungsprozesses und die Schaffung eines Rahmens für die spätere regelmäßige Anwendung. (Red.)

Kontrollsystems im Kontext eines wirksamen und angemessenen Risikomanagements anzusehen ist (Abbildung 1).

Von der Compliance-Funktion wird eine kontinuierliche Beratung und Unterstützung der Geschäftsleitung hinsichtlich der Einhaltung der rechtlichen Regelungen und Vorgaben erwartet. Zu den Kernaufgaben der Compliance-Funktion nach AT 4.4.2 TZ 2 zählen die Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Vermögens des Instituts führen kann, und das Hinwirken auf die Implementierung wirksamer Verfahren zur Einhaltung dieser Regelungen und Vorgaben und entsprechender Kontrollen (AT 4.4.2 TZ 1). Des Weiteren hat die Compliance-Funktion auf die Angemessenheit und Wirksamkeit der Verfahren zur Einhaltung der identifizierten Regelungen und Vorgaben im Rahmen einer regelmäßigen Berichterstattung an die Geschäftsleitung einzugehen (Abbildung 2).

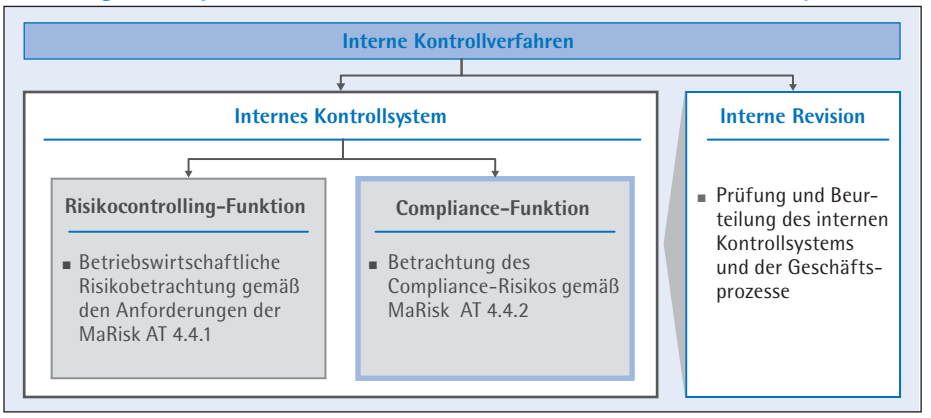
Für ihre Aufgabenerfüllung ist der Compliance-Funktion ein uneingeschränkter Zugang zu allen Informationen einzuräumen, die dafür erforderlich sind (AT 4.2.2 TZ 5). Dazu zählt auch die Bekanntgabe von Weisungen und Beschlüssen der Geschäftsleitung. Unter anderem ist hierfür notwendig, die Compliance-Funktion in den Neu-Produkt-Prozess einzubinden, wie nach AT 8.1 TZ 4 gefordert.

Wesentlichkeits- und Risikoanalyse

Eine der weit verbreiteten Diskussionen beschäftigt sich mit der Fragestellung der Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Vermögens des Instituts führen kann. Von einer Eingrenzung auf bestimmte Bereiche oder Spezialthemen ist in der MaRisk nicht die Rede, sodass zunächst alle rechtlichen Regelungen und Vorgaben (im Folgenden auch als Teilrechtsgebiete bezeichnet) in Betracht gezogen werden sollten, die nach Compliance-Gesichtspunkten mit besonderen Risiken behaftet sein können.

Die BaFin veröffentlichte in ihrem ergänzenden Schreiben „Neue MaRisk für Banken" vom 15. März 2013 eine erste Stellungnahme dazu, welche Themen sie in diesem Zusammenhang zwingend als wesentlich ansieht, nämlich die Bereiche

Abbildung 1: Compliance-Funktion als Bestandteil des internen Kontrollsystems



Wertpapierdienstleistungen, Geldwäsche, Verhinderung doloser Handlungen, Datenschutz und Verbraucherschutz. Sie weist aber im Weiteren auch deutlich darauf hin, dass Institute darüber hinaus eigenverantwortlich zu prüfen haben, welche weiteren rechtlichen Regelungen und Vorgaben Compliance-Risiken beinhalten, die von der Compliance-Funktion nach MaRisk aufzugreifen sind. Eine Beschränkung auf die durch die BaFin genannten Bereiche ohne weitergehende Betrachtungen ist dementsprechend nicht ausreichend.

Trotz der beschriebenen Eingrenzungen durch die BaFin ist das Thema für viele Institute nach wie vor wenig greifbar und lässt Interpretationsspielräume. Nachfolgend ist ein Vorgehensmodell dargestellt, mit dem die relevanten Regelungen und Vorgaben entsprechend spezifiziert werden können.

Zur Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben bedarf es einer systematischen, institutsspezifischen „Wesentlichkeits- und Risikoanalyse" (Abbildung 3). Ausgangspunkt dieser Analyse sollten alle nach dem Geschäftsmodell für das Institut relevanten rechtlichen Regelungen und Vorgaben sein. Dies reduziert die Grundgesamtheit auf diejenigen Vorschriften, die beispielsweise aufgrund der Rechtsform oder der vertriebenen Produkte Relevanz für das Institut haben. Im nächsten Schritt der Analyse erfolgt für die verbleibenden Teilrechtsgebiete eine Bewertung hinsichtlich der potenziellen Vermögensgefährdung bei Nichteinhaltung der Regelungen. Hierfür empfiehlt es sich, eine Bewertung hinsichtlich potenzieller Sanktionsrisiken, Reputationsrisiken und sonstigen finanziellen Risiken vorzunehmen. Für diese Bewertung können Ex-

Abbildung 2: Compliance-Regelkreis

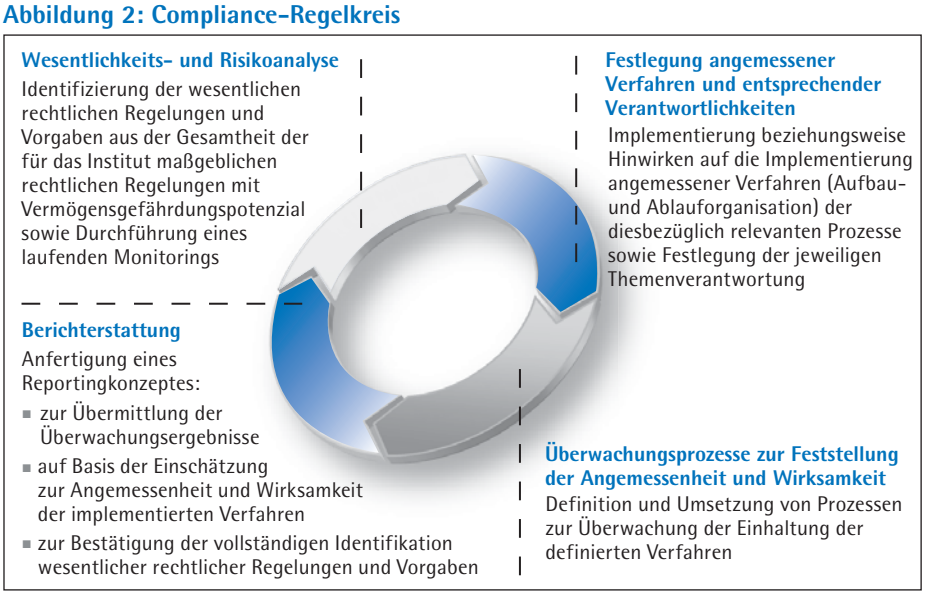
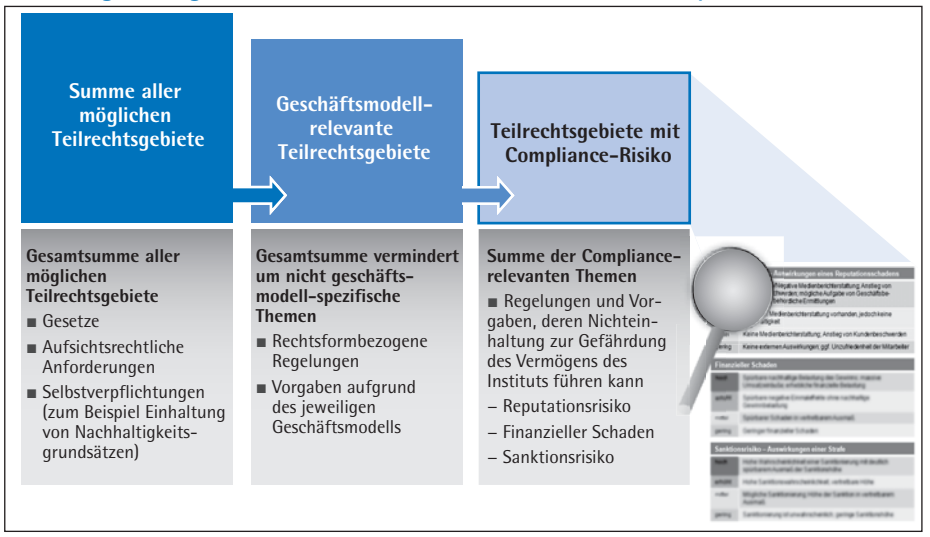


Abbildung 3: Vorgehensmodell Wesentlichkeits- und Risikoanalyse



perten des Instituts hinzugezogen werden (etwa aus dem Compliance-Bereich, dem Rechtsbereich, der Internen Revision, der Unternehmensstrategie), da die Compliance-Bereich allein nicht über alle Regelungen und deren Auswirkungen sowie über die zukünftige geschäftspolitische Ausrichtung urteilen sollte. Im Ergebnis ist das Compliance-Risiko für die relevanten Teilrechtsgebiete bestimmt.

In den nächsten Schritten kann geprüft werden, ob diese einerseits keine bankspezifischen Teilrechtsgebiete sind und daher aufgrund des Konsultationsverfahrens mit der BaFin[7)] ausgeschlossen werden können. Andererseits ist in jedem Fall zu prüfen, ob für die bis dahin identifizierten Teilrechtsgebiete bereits Verantwortliche benannt sind, sodass keine „weißen Flecken" existieren. Eine derartige Ausgestaltung hängt jedoch eindeutig vom Risikoappetit des Instituts und dem gewünschten Compliance-Zielbild ab, da hierdurch wieder Teilrechtsgebiete entfallen würden, denen grundsätzlich ein Compliance-Risiko innewohnt. Die für das Institut als wesentlich identifizierten rechtlichen Regelungen und Vorgaben bilden das Ergebnis dieses Analyseprozesses.

Kontinuierliches Monitoring neuer Regelungen und Vorgaben

Zu der Identifizierung zählt allerdings nicht nur eine initiale institutsspezifische Inventur, das heißt eine einmalige Durchführung der Wesentlichkeitsanalyse, sondern ein kontinuierliches Monitoring neuer Regelungen und Vorgaben, die das Institut betreffen, um insbesondere Änderungen der Geschäftsaktivitäten der Bank, ihren Prozessen und Zuständigkeiten Rechnung zu tragen. Die Wesentlichkeitsanalyse ist somit anlassbezogen und mindestens jährlich durchzuführen. Wichtig ist, dass der gesamte Prozess zur Herleitung der wesentlichen rechtlichen Regelungen und Vorgaben zu dokumentieren und jeweils getroffene Entscheidungen, insbesondere die im Rahmen der Risikoabwägung getroffene Eingrenzung, zu begründen ist.

„Hinwirken" – Festlegung angemessener Verfahren und Verantwortlichkeiten

Auch die Anforderung an die Compliance-Funktion, auf die Implementierung wirksamer Verfahren in Bezug auf diese Regelungen und Vorgaben sowie entsprechender Kontrollen hinzuwirken, wirft aktuell Fragen hinsichtlich der Umsetzung auf.

Die Verantwortung für die Umsetzung und Durchführung angemessener und wirksamer Verfahren liegt bei den jeweiligen Themenverantwortlichen beziehungsweise Sachzuständigen. Die Ausgestaltung der Compliance-Funktion kann sich somit lediglich auf eine Beratungs- und Koordinationsfunktion beschränken und somit einem generalistischen Ansatz folgen. Explizit nicht gewünscht ist ein „Super-Revisor". Das Ausmaß der durch die Compliance-Funktion angewendeten Verfahrenstiefe hinsichtlich dieser Anforderung variiert entsprechend dem Compliance-Zielbild, worauf nachfolgend näher eingegangen wird. Die BaFin unterstützt dabei den Ansatz, bestehende Prozesse durch die Compliance-Funktion im Rahmen von eigenen Überwachungshandlungen zu prüfen und, wo anwendbar, zu nutzen.

Um der Aufgabe der Compliance-Funktion angemessen nachzukommen, ist die Schaffung eines Rahmens durch diese empfehlenswert. Die Schaffung dieses Rahmens hängt vom Compliance-Zielbild ab und bestimmt damit, wie der „Schieberegler" (Abbildung 4) zu setzen ist. Für die „minimale Lösung" bedeutet dies, dass die Fachbereiche die dort verorteten, wesentlichen Teilrechtsgebiete selbst gestalten können, ohne dass die Compliance-Funktion Vorgaben zur Umsetzung aufzeigt. Sieht das Zielbild beispielsweise den „Schieberegler" im Mittelfeld verortet, empfiehlt sich eine Ausrichtung des „Hinwirkens" an den Grundelementen des Compliance-Management-Systems (CMS)[8)], sofern ein solches in der Bank bereits existiert.

Konkret kann dies bedeuten, dass für ein als wesentlich identifiziertes Teilrechtsgebiet, zum Beispiel FATCA, die Compliance-Funktion Empfehlungen zur Ausgestaltung der schriftlich fixierten Ordnung (Grundelement des CMS: Compliance-Programm) oder zu den Kontrollhandlungen (Grundelemente des CMS: Compliance-Risiken sowie Compliance-Überwachung und Verbesserung) ausspricht. Sofern ein CMS bereits implementiert ist, sind die Grundelemente ausgestaltet, und diese Standards können damit auf die relevanten Teilrechtsgebiete ausgeweitet werden. Ist allerdings ein intensives „Hinwirken" durch die Compliance-Funktion gewünscht („intensive Lösung"), unterstützt diese eng die Ausgestaltung der Maßnahmen in Bezug auf das relevante Teilrechtsgebiet. Egal wie die Intensität hinsichtlich der Compliance-Vorgaben ausgestaltet ist, obliegt die Verantwortung für deren Operationalisierung den Geschäftsbereichen. Die Compliance-Funktion ist jedoch Ansprechpartner der Bereiche und berät diese bei Fragestellungen zur Umsetzung der Vorgaben.

Überwachungsprozesse zur Feststellung der Angemessenheit und Wirksamkeit

Die Überprüfung der Angemessenheit und Wirksamkeit der Verfahren zur Einhaltung der wesentlichen rechtlichen Regelungen und Vorgaben ist eine weitere wichtige Aufgabe der Compliance-Funktion, deren Umsetzung in der Praxis zu Fragen führt.

In Abhängigkeit von dem bereits erwähnten Compliance-Zielbild und dem von der Geschäftsleitung vermittelten Compliance-Verständnis und der Compliance-Kultur der Bank sowie deren Risikoappetit können die Prozesse zur Überprüfung der Angemessenheit und Wirksamkeit unterschiedlich ausgestaltet sein. Grundsätzlich sei zu erwähnen, dass sich die Compliance-Funktion die Erkenntnisse aus den Prüfberichten der Internen Revision sowie den Risiko- und Gefährdungsanalysen (nach BT 1 MaComp und § 25c KWG) und den Ergebnissen der daraus folgenden Kontroll- und Überwachungshandlungen zunutze machen kann. Für die Ausgestaltung dieses Überprüfungsprozesses an sich sind im Wesentlichen drei Modelle vorstellbar.

Management-Testing durch die Fachbereiche: Zum einen ist denkbar, dass die Fachbereiche die Angemessenheit und Wirksamkeit ihrer implementierten Verfahren und Kontrollen zur Einhaltung der wesentlichen rechtlichen Regelungen und Vorgaben anhand von Vorgaben der Compliance-Funktion testen und deren Durchführung sowie deren Ergebnisse an die Compliance-Funktion berichten. Bei dieser Ausgestaltungsform findet keine inhaltliche Wertung durch die Compliance-Funktion statt.

Management-Testing durch die Fachbereiche mit anschließender Plausibilisierung durch Compliance: Zum anderen ist es möglich, dass die von den Fachbereichen durchgeführten und berichteten Kontrollhandlungen und deren Ergebnisse durch die Compliance-Funktion plausibilisiert werden. Im Rahmen dieser Ausgestaltung sollten eingangs genannte Erkenntnisse aus Prüfungsberichten et cetera verwertet werden.

Bewertung und Definition von Maßnahmen durch die Compliance-Funktion: In einer sehr stark ausgestalteten Compliance-Funktion bewertet diese selbst die Sicherungsmaßnahmen der Fachbereiche auf Angemessenheit und Wirksamkeit hinsichtlich der wesentlichen rechtlichen Regelungen und Vorgaben.

Unabhängig von der jeweiligen Umsetzung im Institut ist eine systematische Bewertung für jedes als wesentlich identifizierte Teilrechtsgebiet hinsichtlich bestehender Prozesse und Kontrollen zur Risikominimierung erforderlich. Sollte es hierbei an Prozessen oder Kontrollhandlungen diese nicht angemessen ausgestaltet oder wirksam sein, so hat die Compliance-Funktion darauf hinzuwirken, dass Maßnahmen zur Behebung des Defizits umgesetzt werden. Die Compliance-Funktion sollte bei Feststellung von Defiziten Maßnahmen zur Behebung dieser Defizite in Abstimmung mit den Fachbereichen einleiten. Die Compliance-Funktion sollte die eingeleiteten Maßnahmen in ihre nächsten Überwachungshandlungen einbeziehen. Die Ausgestaltung der Involvierung der Compliance-Funktion in diesen Prozess ist ebenfalls wiederum abhängig von dem im Institut gewünschten Compliance-Zielbild.

Berichterstattung

Zur Übermittlung der Überwachungsergebnisse hat die Compliance-Funktion mindestens jährlich sowie anlassbezogen einen Bericht an die Geschäftsleitung zu erstatten. Inhaltlich muss hierbei auf die Wirksamkeit der Verfahren und auf mögliche Defizite sowie Maßnahmen zu deren Behebung eingegangen werden.

Neben der Geschäftsleitung sind die Berichte auch an das Aufsichtsorgan und die Interne Revision weiterzuleiten. Je nach aufbauorganisatorischer Zuordnung der Compliance-Funktion kann die Berichtspflicht in die sonstigen Compliance-Berichte nach § 33 Abs. 1 S. 2 Nr. 5 WpHG und § 25c Abs. 4 S. 3 KWG integriert werden.

Ernennung des Compliance-Beauftragten

Neben den bereits dargestellten ablauforganisatorischen Fragestellungen soll nunmehr auf die aufbauorganisatorische Ausgestaltung der Compliance-Funktion eingegangen werden. Zunächst ist festzuhalten, dass der vom Institut zu benennende Compliance-Beauftragte nach MaRisk für die Erfüllung der Aufgaben der Compliance-Funktion verantwortlich ist und sein Wechsel dem Aufsichtsorgan laut AT 4.2.2. TZ 7 mitgeteilt werden muss.

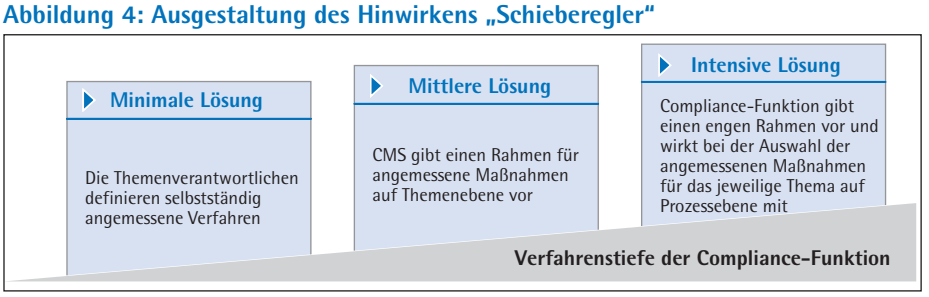
Darüber hinaus schreiben die MaRisk vor, dass die Compliance-Funktion unmittelbar der Geschäftsleitung zu unterstellen ist, und gehen im Grundsatz von einer unabhängigen Organisationseinheit aus. Denkbar könnte aber auch eine Anbindung an andere Kontrolleinheiten, beispielsweise an das Risikocontrolling sein.[9] Ausgeschlossen wird explizit eine Anbindung an die Interne Revision, um deren Unabhängigkeit zu wahren. Eine Anbindung an andere Organisationseinheiten sollte jedoch gut begründet sein und dokumentiert werden. Ein Baustein der Begründung könnte der Proportionalitätsgrundsatz[10] sein.

Die Autoren sehen allerdings die Anbindung an das Risikomanagement als kritisch an, da hierbei Interessenkonflikte aufgrund ihrer unterschiedlichen Ausrichtungen bestehen. Das Risikocontrolling ist verantwortlich für das Risikomanagement und damit sehr stark in Institutsaufgaben und -ziele eingebunden. Die Compliance-Funktion sollte auch den Institutsschutz im Fokus haben, vor allem hat sie jedoch die Markt- und Kundenschutzinteressen zu vertreten.

Der Vollständigkeit halber sei erwähnt, dass im Ausnahmefall bei sehr kleinen Instituten die Wahrnehmung der Compliance-Funktion durch einen Geschäftsleiter möglich ist.

Das ergänzende Schreiben „Neue MaRisk für Banken" der BaFin vom 15. März 2013 verweist ausdrücklich darauf, dass den Instituten hier keine weiteren Vorgaben gemacht werden und es sinnvoll erscheint, zu prüfen, inwieweit die neue Compliance-Funktion in bestehende Organisationsstrukturen eingebunden werden kann.

Abbildung 4: Ausgestaltung des Hinwirkens „Schieberegler"



Grundsätzlich kann die Ausgestaltung der Compliance-Funktion sowohl zentral als auch dezentral beziehungsweise in Mischformen organisiert sein.

Eine zentrale Organisation würde bedeuten, dass die Compliance-Funktion die wesentlichen rechtlichen Regelungen und Vorgaben und die damit einhergehenden Teilrechtsgebiete aufbauorganisatorisch in einer Einheit bündelt.

Beim dezentralen Modell verbleiben diese Teilrechtsgebiete in den bereits verantwortlichen Geschäftsbereichen. Eine Anbindung an die Compliance-Funktion kann in dieser Ausgestaltungsform beispielsweise durch die Einrichtung dezentraler Compliance-Officer oder ein MaRisk-Committee erfolgen. Wie auch immer die Ausgestaltung eines dezentralen Modells aussieht, ein besonderes Augenmerk ist auf die Einrichtung angemessener Kommunikationswege zwischen den Funktionen beziehungsweise Geschäftsbereichen zu legen.

Integration in den bestehenden Compliance-Bereich

Auch wenn sich noch kein Standard herausgebildet hat, so wird die Compliance-Funktion nach MaRisk in einer Vielzahl von Instituten weitestgehend zentral in der derzeitigen Compliance-Organisationseinheit angesiedelt, die häufig bereits für die eingangs erwähnten Compliance-Themengebiete verantwortlich ist. Damit folgt in vielen Fällen oft gleichzeitig eine Funktionszusammenlegung mit den anderen Compliance-Funktionen[11], welche zur Compliance-Funktion nach MaRisk in keinem Über- oder Unterordnungsverhältnis stehen. Gleichzeitig werden die weiteren als wesentlich identifizierten Teilrechtsgebiete dezentral in den bereits verantwortlichen Geschäftsbereichen belassen und mittels Schnittstellenregelungen an die Compliance-Funktion angebunden.

Aus Sicht der Autoren empfiehlt sich die eben beschriebene Ausgestaltung für eine Vielzahl von Instituten, da dies zum einen Synergien hebt, aber zum anderen vor allem der Markt- und Kundenschutz bereits heute zu den Aufgaben der Compliance-Funktion zählt. Insbesondere kann eine Integration in das CMS, das in einigen Häusern bereits aufgebaut ist, erfolgen. Im Speziellen hat die Compliance-Einheit bereits fachliche Kompetenzen und Erfahrungen mit relevanten Compliance-Themen und Prozessen wie beispielsweise Risikoanalysen und Überwachungshandlungen und übt bereits eine Beratungsfunktion aus. Insgesamt trägt diese Aufstellung zur Sichtbarkeit von Compliance deutlich bei und unterstützt die Stärkung des Compliance-Verständnisses.

Exkurs: Gruppenweite Umsetzung

Die Implementierung der auf Basis des Compliance-Regelkreises operationalisierten Compliance-Infrastruktur (Abbildung 2) muss auch auf Ebene der gesamten Institutsgruppe stattfinden. Hierzu müssen zunächst alle relevanten in- und ausländischen Konzerneinheiten gemäß § 25a Abs. 3 KWG-E identifiziert werden (sogenannter Compliance-relevanter Konsolidierungskreis). Maßgeblich ist hierfür der beherrschende Einfluss auf eine Tochtergesellschaft.

Zu erwähnen ist, dass der Geschäftsleiter des übergeordneten Unternehmens für die ordnungsgemäße Geschäftsorganisation der Institutsgruppe verantwortlich ist. Vor diesem Hintergrund sind im Rahmen der Wesentlichkeitsanalyse, der Feststellung der Angemessenheit und Wirksamkeit sowie der Berichterstattung aus Sicht der Autoren unbedingt Standards durch die Compliance-Funktion des übergeordneten Unternehmens zu setzen, nicht zuletzt um die Ergebnisse der nachgeordneten Unternehmen vergleichbar und somit für die Konzern-Compliance-Funktion aussagekräftig zu machen.

Eine anspruchsvolle Aufgabe

Die Anforderungen der MaRisk an die Compliance-Funktion von Banken mögen aufgrund ihres umfassenden Charakters auf den ersten Blick umsetzungsintensiv erscheinen und Raum für Interpretationen bieten. In der Tat handelt es sich dabei um eine anspruchsvolle Aufgabe, deren konkrete Ausgestaltung zudem von der Größe, Art und Ausgangssituation des Institutes abhängt. Es ist daher in jedem Fall entscheidend, ein individuelles Zielbild der Compliance-Funktion nach MaRisk zu entwickeln und dieses in einem strukturierten und systematischen Ansatz umzusetzen. Auf diese Weise können die Vorgaben der BaFin bei der Identifizierung und weiteren Berücksichtigung der für das Institut wesentlichen rechtlichen Regelungen und Vorgaben effizient und schlank umgesetzt werden.

Des Weiteren bietet ein solches methodisches Vorgehen die Möglichkeit einer kompletten und nachvollziehbaren Dokumentation des gesamten Umsetzungsprozesses und bildet einen Rahmen für die spätere kontinuierliche Anwendung als Compliance-Regelkreis.

An dieser Stelle sei noch darauf hingewiesen, dass die Einbettung der Umsetzung der Vorgaben der MaRisk in das Compliance-Management-System einem eventuell später vom Institut gewünschten Zertifizierungsprozess nach IDW PS 980 dienlich ist.

Erfahrungen der Autoren aus ersten Umsetzungsprojekten haben gezeigt, dass sich viele Themen der neuen Compliance-Funktion nach MaRisk an bestehende Funktionen und Prozesse anbinden lassen und so Synergien gehoben werden können.

Die Autoren danken Hannes Koch, Assistant Manager, für seine Unterstützung.

Fußnoten

[1] 4. Novelle der Mindestanforderungen an das Risikomanagement – Rundschreiben 10/2012 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk vom 14. Dezember 2012.

[2] Teilweise auch als Kapitalmarkt-Compliance bezeichnet.

[3] Rundschreiben 4/2010 (WA)-Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen zuletzt geändert am 7. Dezember 2012.

[4] CRD IV – Capital Requirements Directive – Veröffentlichung am 27. Juni 2013 und Inkrafttreten am 1. Januar 2014.

[5] CRR – Capital Requirements Regulation – Veröffentlichung am 27. Juni 2013 und Inkrafttreten am 1. Januar 2014.

[6] EBA Guidelines of Internal Governance – veröffentlicht am 27. September 2011.

[7] Sitzung des Fachgremiums MaRisk am 24. April 2013.

[8] Entsprechend IDW PS 980: Prüfungsstandard 980 des Instituts für Wirtschaftsprüfer; wichtig sind in diesem Zusammenhang vor allem die Elemente Compliance-Risiken, Compliance-Programm, Compliance-Organisation, Compliance-Kommunikation sowie Compliance-Überwachung und -Verbesserung.

[9] „Neue MaRisk für Banken", Markus Hofer, BaFin, 15. März 2013.

[10] Der Proportionalitätsgrundsatz besagt, dass die Anforderungen unter Berücksichtigung der unternehmensindividuellen Risiken, der Art und des Umfangs des Geschäftsbetriebes und der Komplexität des gewählten Geschäftsmodells des Unternehmens zu erfüllen sind.

[11] Compliance-Funktion nach § 33 Abs. 1 S. 2 Nr. 1 WpHG i. V. m. § 12 Abs. 4 S. 1 WpDVerOV und Geldwäschebeauftragter nach § 25c Abs. 4 S. 1 KWG.