KAYE | SCHOLER

12. Mai 2014

Compliance Alert

BaFin—Vorbereitung auf Solvency II: Allgemeine Governance-Anforderungen für die Versicherungsindustrie

Die BaFin konsultiert mit ihrem Rundschreiben vom 16. April 2014 im Rahmen der Vorbereitung auf Solvency II die sogenannten allgemeinen Governance-Anforderungen. Sie plant zudem, nach Finalisierung dieses Rundschreibens, weitere präzisierende Rundschreiben zu erlassen.

Das Rundschreiben enthält insbesondere Aussagen zu Aufbau- und Ablauforganisationen, interner Überprüfung des Governance-Systems und interner Leitlinien, Aussagen zum Verwaltungs-, Management- oder Aufsichtsorgan und zu Notfallplänen sowie Aussagen zu den Schlüsselfunktionen (z.B. der Compliance-Funktion) in der Versicherungsindustrie.

Die Veröffentlichung der BaFin richtet sich an alle inländischen Versicherungsunternehmen, auf welche ab 1. Januar 2016 die Solvency II-Richtlinie (2009/138/EG—die „Richtlinie“) angewendet wird, sowie an alle Versicherungsgruppen, für welche die BaFin unter der Richtlinie die für die Gruppenaufsicht zuständige Behörde sein wird.

Dies sind alle inländischen Erst- und Rückversicherungsunternehmen im Sinne des § 1 Abs. 1 Nr. 1 VAG, soweit sie nicht Sterbekassen im Sinne des Art. 10 der Richtlinie oder Pensionskassen sind, nach Artikel 4 der Richtlinie von deren Anwendungsbereich ausgeschlossen sind oder als Rückversicherungsunternehmen ihre Tätigkeit nach Art. 12 der Richtlinie eingestellt haben.

Außerdem sind dies alle Versicherungsgruppen, die ausschließlich aus inländischen Erst- und Rückversicherungsunternehmen bestehen, sowie Versicherungsgruppen mit Erst- oder Rückversicherungsunternehmen in anderen EWR-Staaten, über welche die BaFin nach den in Art. 247 Abs. 2 der Richtlinie genannten Kriterien die für die Gruppenaufsicht zuständige Behörde sein wird.

Bei der Umsetzung der allgemeinen Governance-Anforderungen spielt der Grundsatz der Proportionalität eine erhebliche Rolle. Die Anforderungen sind auf eine Weise zu erfüllen, welche der Wesensart, dem Umfang und der Komplexität der mit der Geschäftstätigkeit des jeweiligen Versicherungsunternehmens einhergehenden Risiken gerecht wird (Art. 29 Abs. 3 der Richtlinie). Der Proportionalitätsgrundsatz knüpft also an das individuelle Risikoprofil eines jeden Unternehmens an und verlangt daher eine Einzelfallbetrachtung.

Aufbau- und Ablauforganisation

Die Versicherungsunternehmen haben angemessene und transparente Organisationsstrukturen aufzubauen und zu erhalten. Bei der Ausgestaltung sind sie grundsätzlich frei. Allerdings müssen sie die Angemessenheit ihrer Aufbau- und Ablauforganisation bewerten. Bei dieser Bewertung müssen die Unternehmen vor allem die Wesensart, den Umfang und die Komplexität ihrer Geschäftstätigkeit sowie die daraus resultierenden unternehmensindividuellen Risiken berücksichtigen. Aufbau- und Ablauforganisationen sollten die strategischen Ziele und Geschäftstätigkeit des Unternehmens unterstützen.

Eine angemessene transparente Aufbauorganisation erfordert eine klare Definition von Aufgaben und Verantwortlichkeiten. Schnittstellen sind explizit zu berücksichtigen und Vertretungsregelungen sind zu implementieren.

Angemessene Trennung der Zuständigkeiten

Die BaFin erwartet eine Trennung von Zuständigkeiten. Vor allem sind potentielle Interessenkonflikte zwischen dem Aufbau wesentlicher Risikoposition einerseits und deren Überwachung/Kontrolle andererseits zu vermeiden. Zu den mit wesentlichen Risiken behafteten Geschäftsabläufen zählen zumindest das versicherungstechnische Geschäft, die Reservierung, das Kapitalanlagemanagement einschließlich des Asset Liability Managements und das passive Rückversicherungsmanagement.

Festlegung/Ablauf organisatorischer Regelungen

Um die sorgfältige und gewissenhafte Aufgabenwahrnehmung weiter zu unterstützen, sollten die Erstellung und Umsetzung eines Verhaltenskodex für das gesamte Personal, auch für die Geschäftsleitung, die Führungskräfte einschließlich der Verantwortlichen für Schlüsselaufgaben und ggf. den Aufsichtsrat, vom Unternehmen in Betracht gezogen werden. Das Unternehmen hat seine Aufbau- und Ablauforganisation für Dritte nachvollziehbar zu dokumentieren.

Spezielle Gruppenaspekte

Die BaFin erwartet von der Geschäftsleitung des für die Erfüllung der Governance-Anforderung auf Gruppenebene zuständigen Unternehmens eine angemessene Kenntnis der internen Organisation der Gruppe, der Geschäftsmodelle der verschiedenen Unternehmen und der Verbindungen und Beziehungen zwischen ihnen und den aus der Gruppenstruktur resultierenden Risiken. Zudem haben Unternehmen Zuständigkeiten und Richtlinien auch in Bezug auf die Gruppenstruktur festzulegen.

Interne Überprüfung des Governance-Systems

Das Governance-System ist einer regelmäßigen internen Überprüfung zu unterziehen. Diese Überprüfung geht über die in Abschnitt 7.5 der MaRisk (VA) geforderte jährliche Überwachung der Funktionsfähigkeit der internen Kontrollen hinaus, da diese nur einen Teil des Governance-Systems darstellen.

Als Grundlage für die interne Überprüfung können neben den von der internen Revision bei der Überprüfung des Governance-Systems gewonnenen Erkenntnissen insbesondere auch Informationen dienen, welche die weiteren Schlüsselfunktionen (interne Revision, Compliance, Risikomanagement sowie versicherungsmathematische Funktion) bei der Durchführung ihrer Aufgaben erhalten. So hat beispielsweise die Risikomanagementfunktion—hierbei handelt es

sich um die unabhängige Risikocontrolling-Funktion im Sinne von § 64 a Abs. 7 Nr. 3 b cc VAG—unter anderem die Aufgabe, das Risikomanagement zu überwachen und zu überprüfen. Im Regelfall ist eine jährliche Überprüfung ausreichend.

Interne Leitlinien

Das Versicherungsunternehmen hat für die mit wesentlichen Risiken behafteten Geschäftsabläufe innerbetriebliche Leitlinien aufzustellen. Diese haben die rechtlichen, satzungsmäßigen und strategischen Grenzen der Geschäftstätigkeit sowie die organisatorischen Rahmenbedingungen zu berücksichtigen.

Die BaFin geht insoweit davon aus, dass Leitlinien, die auf Gruppenebene beschlossen werden, nicht automatisch für rechtlich selbstständige Einzelunternehmen gelten. Dies gilt auch, wenn Beherrschungsverträge bestehen. Damit die schriftlich festgelegten Leitlinien in der Praxis wirksam umgesetzt werden, haben die Unternehmen für die Einrichtung entsprechender Prozesse und Arbeitsabläufe Sorge zu tragen. Die schriftlich festgelegten Leitlinien sollen helfen, Handlungsvorgaben für Mitarbeiter und Mitarbeiterinnen zu geben. Dabei müssen die schriftlich festgelegten Leitlinien die mit ihnen verfolgten Ziele, Aufgaben und Verantwortlichkeiten der Geschäftsbereiche klar darstellen. Die BaFin erwartet auch, dass zu den vier Schlüsselfunktionen schriftliche Leitlinien erstellt werden, in denen u.a. die Befugnisse der Schlüsselfunktionen klar definiert werden.

Damit die Geschäftsstrategie wirksam umgesetzt werden kann, müssen zumindest alle zum Governance-System gehörenden Leitlinien auf die Geschäftsstrategie abgestimmt und mir ihr abgeglichen werden. Alle schriftlichen Leitlinien müssen auf einheitliche Art und Weise vollständig überprüft werden. Die Unternehmen sollen den Turnus dieser Überprüfung festlegen. Dabei sollte berücksichtigt werden, dass Änderungen einer schriftlich festgelegten Leitlinie oder der Geschäftsstrategie direkte Auswirkungen auf die anderen schriftlich festgelegten Leitlinien haben können. Die BaFin geht davon aus, dass die (mindestens vorhandenen) schriftlichen Leitlinien zu Risikomanagement, interner Kontrolle, interner Revision und Outsourcing zumindest einmal jährlich überprüft werden. Die Überprüfungen der schriftlich festgelegten Leitlinien müssen angemessen dokumentiert werden. Auch sind die Entscheidungen der Geschäftsleitung aufgrund der Überprüfung der Leitlinien nachvollziehbar zu begründen und zu dokumentieren.

Aus den Leitlinien sollten sich dementsprechend Arbeitsprozesse herausbilden. Diese sind klar zu kommunizieren, und den relevanten Mitarbeitern und Mitarbeiterinnen ist damit vorzugeben, auf welche Geschäftsabläufe sich diese schriftlichen Leitlinien beziehen.

Verwaltungs-, Management- oder Aufsichtsorgan

Hiermit ist national regelmäßig zunächst die Geschäftsleitung angesprochen. Dies bedeutet aber nicht, dass das Governance-System für den Aufsichtsrat nicht relevant ist. Nach dem nationalen Aktienrecht hat der Aufsichtsrat bei Unternehmen mit dualistischer Struktur keine nur reaktive Funktion. Bspw. ist er es, der die Mitglieder des Vorstands bestellt, deren Vergütung beschließt und deren Tätigkeiten überwacht. Zudem dürfen bestimmte Arten von Geschäften nicht ohne die Zustimmung des Aufsichtsrats vorgenommen werden. Zur Erfüllung von Pflichten werden ihm gesetzliche Informations-, Einsichts- und Prüfungsrechte eingeräumt.

Den Mitgliedern beider Organe (Geschäftsleitung und Aufsichtsrat) kommt innerhalb des Governance-Systems eine aktive Rolle zu. Beide haben in eigener Verantwortung zu überlegen, ob eine—und falls ja welche—Ausschuss-Struktur für das Unternehmen geeignet ist. In größeren Unternehmen mit komplexem Risikoprofil, bei denen Geschäftsleitung und/oder Aufsichtsrat ein größeres Gremium bilden, kann die Schaffung von Ausschüssen bzw. die Verteilung von Ressortzuständigkeiten zur Beschlussvorbereitung und zur Entlastung der Sitzung empfehlenswert sein. Beispiele hierfür sind die Bildung eines Risiko-, Prüfungs-, Anlage- oder Vergütungsausschusses auf Ebene des Aufsichtsrats. Für Unternehmen, die im Erst- und Rückversicherungsbereich tätig sind bzw. auch eine Holding-Funktion haben, kann sich die Einrichtung eines Ausschusses für Angelegenheiten des Geschäftsfeldes Rückversicherung anbieten.

Die Geschäftsleitung kann die ihren Governance-Systemen zugewiesene Rolle nicht insgesamt auf einzelne Mitglieder oder einen Ausschuss oder anderweitig delegieren. Eine Verlagerung der gesetzlich geregelten Verantwortung ist also nicht möglich.

Gruppenebene

Auf Gruppenebene muss die Geschäftsleitung des zuständigen Unternehmens in angemessener Interaktion mit der Geschäftsleitung aller Unternehmen innerhalb der Gruppe stehen. Sofern diese Anforderungen in einem Spannungsverhältnis zwischen gesellschafts- oder kapitalmarktrechtlichen Möglichkeiten stehen, erwartet die BaFin, dass die künftig nach den Bestimmungen der Gruppenaufsicht verpflichteten Unternehmen und die zur Gruppe gehörigen Versicherer sich dessen bewusst werden und im eigenen Interesse geeignete Maßgaben

ergreifen, um die Erfüllung aufsichtsrechtlicher Anforderungen sicherzustellen. Dies kann bspw. bedeuten, dass das gesellschaftsrechtlich bestehende Spannungsverhältnis transparent gemacht wird und soweit als möglich prüferisch nachvollziehbar eigene Maßnahmen einzuleiten sind.

Notfallpläne

Die Notfallplanung hat zum Ziel, die Widerstandsfähigkeit von Bereichen und Prozessen im Unternehmen zu erhöhen. Sie soll in möglichen Krisensituationen die Fortführung der Geschäftstätigkeit durch im Vorfeld definierte Verfahren gewährleisten. Alle Unternehmen haben sich fortlaufend mit einer Notfallplanung auseinanderzusetzen.

Schlüsselfunktion

Die BaFin gibt hier übergeordnete, vornehmlich organisatorische Aspekte vor, die für alle Schlüsselfunktionen Bedeutung haben. In weiteren Veröffentlichungen wird die BaFin sich speziell zur internen Revisionsfunktion und Compliance-Funktion, zur Risikomanagement-Funktion und zur versicherungsmathematischen Funktion äußern.

Die Unternehmen haben die Schlüsselfunktionen in angemessener Weise einzurichten. Dabei sind Artikel 44, 46, 47 und 48 der Richtlinie zu beachten, in denen die Aufgaben dieser Funktionen und z.T. auch deren Stellung im Unternehmen vorgegeben sind. Alle unter die Richtlinie fallenden Unternehmen müssen bis zum 1. Januar 2016 über diese vier Schlüsselfunktionen verfügen.

Im Vergleich zum geltenden § 44 VAG ist nur die versicherungsmathematische Funktion ganz neu. Die Schaffung einer internen Revision in einer unabhängigen Risikokontroll-Funktion ist bereits gesetzlich vorgeschrieben (§ 64 a Satz 4 Nr. 4, Abs. 7 Nr. 4 und § 64 a Abs. 7 Nr. 3 b cc VAG).

In Sachen Compliance ist zu unterscheiden: Es gibt bisher zwar keine organisatorische Vorgabe (wie bei Banken), eine Compliance-Funktion einzurichten. Jedes Unternehmen muss jedoch schon jetzt „compliant“ sein, also alle auf seinen Geschäftsbetrieb anwendbaren Gesetze und sonstigen Vorgaben einhalten. Außerdem unterliegt der Vorstand und damit die Geschäftsleitung einer Aktiengesellschaft der Pflicht, gesetzeskonformes Verhalten der Gesellschaft und ihrer Mitarbeiter gegenüber Dritten sowie der eigenen Belegschaft sicherzustellen (so genannte Legalitätspflicht).

Den Unternehmen steht es grundsätzlich frei, zunächst die Compliance-Funktion oder die versicherungsmathematische Funktion oder beide Funktionen gleichzeitig einzurichten. Wichtig ist, dass die Unternehmen sich bereits in der Vorbereitungsphase mit diesen organisatorischen Fragen beschäftigten und dann hierfür eine nachvollziehbare Entscheidung treffen.

Den Ausführungen der BaFin ist zu entnehmen, dass als Vorbild die Compliance-Organisation von Kreditinstituten, hier insbesondere die Vorgaben des KWG und der MaRisk sowie des WpHG und der MaComp gedient haben. Hieran können sich die Versicherungsunternehmen bei ihrer Umsetzung orientieren.

Die Schlüsselfunktionen sind auf angemessene Weise in der Aufbauorganisation des Unternehmens abzubilden. Dabei sind die Unternehmen grundsätzlich frei darin, wie sie diese Schlüsselfunktionen organisieren. Sie haben gleichermaßen das Recht und die Pflicht, insoweit die erste Einschätzung zu treffen, eigeninitiativ und individuell vorzugehen. Diese Ersteinschätzung ist zu begründen. Die Aufsichtsbehörde kann diese jedoch in Frage stellen.

Soweit die Größe eines Unternehmens im Rahmen der Einzelfallbetrachtung eine Rolle spielen kann, kommt es nicht auf die Mitarbeiteranzahl, sondern auf den Mitarbeiterbedarf an. Das heißt, auch Mitarbeiterkapazitäten, die sich das Unternehmen im Wege der Ausgliederung zu Nutze macht, sind in die Betrachtung miteinzubeziehen.

Der Begriff „organisatorische Einheit“ (wie er in Erwägungsgrund 32 der Richtlinie 2 verwendet wird) umfasst die Abbildung einer Schlüsselfunktion durch eine Person oder eine Personenmehrheit. Die Formulierung „von einer Person oder einer organisatorischen Einheit“ könnte missverstanden werden, weil auch unipersonale organisatorische Einheiten denkbar sind.

Mit Ausnahme der internen Revisionsfunktion kommen neben zentralen/stabstellenartigen auch dezentrale/integrierte Gestaltungsformen sowie—gruppenbezogene—Mischformen in Betracht.

In allen—auch dezentralen—Gestaltungsformen muss es ungeachtet der nicht delegierbaren letzten Verantwortung der Geschäftsleitung eine natürliche Person geben, welche die operative Verantwortung dafür trägt, dass die jeweilige Schlüsselfunktion ihre Aufgaben ordnungsgemäß erfüllt („verantwortlicher Inhaber“ einer Schlüsselfunktion). Es ist nicht zulässig, diese operative Verantwortung ganz oder teilweise mehreren natürlichen Personen zuzuordnen.

Personen, die für die Schlüsselfunktion tätig sind, ihr also zuarbeiten, kann es hingegen viele geben.

Unter Proportionalitätsgesichtspunkten kann es angemessen sein, eine Geschäftsleiterin oder einen Geschäftsleiter zum verantwortlichen Inhaber einer Schlüsselfunktion zu bestimmen.

Im Modell der „Three Lines of Defense" bildet die interne Revisionsfunktion die dritte Verteidigungslinie, die anderen Schlüsselfunktionen gehören zur zweiten Verteidigungslinie. Unabhängig von dieser Einordnung stehen die Schlüsselfunktionen unter der Richtlinie gleichrangig und gleichberechtigt nebeneinander, ohne untereinander weisungsbefugt zu sein. Die Geschäftsleitung bildet die Eskalationsinstanz im Falle von kontroversen Schlüsselfunktionen.

Alle Schlüsselfunktionen müssen direkt und unmittelbar an die—letztverantwortliche—Geschäftsleitung berichten. Hierzu muss die Geschäftsleitung eigeninitiativ und angemessen mit den Schlüsselfunktionen interagieren.

Die Schlüsselfunktionen müssen in der Lage sein, eigeninitiativ mit allen anderen Unternehmen zu kommunizieren. Sie benötigen uneingeschränkten Zugang zu den für die Erfüllung ihrer Aufgaben relevanten Informationen und müssen über die relevanten Sachverhalte zeitnah, ggf. ad hoc, informiert werden.

Neben angemessenen Ressourcen und Befugnissen bedarf es einer hervorgehobenen Stellung der Schlüsselfunktionen innerhalb des Unternehmens, die nicht alleine durch die internen Leitlinien erzeugt werden kann, sondern eine entsprechende Unternehmenskultur bedingt. Der „tone at the top" hat hier erhebliche Bedeutung.

Man sieht auch an dieser Stelle, dass das Vorbild für die BaFin eindeutig die Entwicklung der Compliance-Funktion in Kreditinstituten und Wertpapierdienstleistungsunternehmen war und sich die Beantwortung der Fragen zu der Ausgestaltung der Compliance-Funktion und der Entwicklung einer Compliance-Kultur an diesem bereits vorhandenen System für Banken orientieren soll. Die Versicherungsbranche ist somit gut beraten, sich an den sich bereits positiv zeigenden Effekten der Entwicklung der Governance- und Compliance-Strukturen in der Kreditwirtschaft zu orientieren, insofern diese Strukturen für die Versicherungsbranche sinnvoll sind.

Die weiteren Äußerungen der BaFin zur Entwicklung von Governance-Anforderungen an die Versicherungsbranche im Rahmen der Umsetzung von Solvency II sind damit sorgfältig zu beobachten.

Kontaktdaten

Hartmut T. Renz
+49 69 25494 230
hartmut.renz@kayescholer.com

George M. Williams jr
+1 212 836 8840
george.williams@kayescholer.com

Ingrid Kalisch
+49 69 25494 250
ingrid.kalisch@kayescholer.com

Sandra Pfister
+49 69 25494 240
sandra.pfister@kayescholer.com