

## Compliance Alert

### BaFin—Vorbereitung auf Solvency II: Interne Kontrollen, Compliance und Interne Revision

---

Die BaFin konsultiert mit ihrer Veröffentlichung vom 9. Juli 2014 im Rahmen der Vorbereitung auf Solvency II die Anforderungen an interne Kontrollen im Rahmen der Compliance-Funktion und der internen Revision.

Die Veröffentlichung enthält insbesondere Aussagen zu den Aufgaben der Compliance-Funktion und der internen Revision bei Versicherungsunternehmen. Betroffene Unternehmen können bis zum 8. August 2014 Anmerkungen an die BaFin übermitteln. Auch die hier beschriebenen Anforderungen sind im Rahmen der Solvency II-Umsetzung bis zum 1. Januar 2016 insbesondere in allen inländischen Versicherungsunternehmen umzusetzen.

---

Dieser Compliance Alert ergänzt den Alert vom 12. Mai 2014 zu den allgemeinen Governance-Anforderungen für die Versicherungsindustrie. Der Fokus der BaFin-Veröffentlichung und damit dieses Alerts liegt auf den internen Kontrollen in Versicherungsunternehmen.

Bei der Umsetzung der Anforderungen an die internen Kontrollen spielt der Grundsatz der Proportionalität eine erhebliche Rolle. Die Anforderungen sind auf eine Weise zu erfüllen, die der Wesensart, dem Umfang und der Komplexität der mit der Geschäftstätigkeit des Unternehmens einhergehenden Risiken gerecht wird (Art. 29 Abs. 3 Solvency II-Richtlinie). Damit knüpft der Proportionalitätsgrundsatz an das individuelle Risikoprofil eines jeden Versicherungsunternehmens an und erfordert damit eine Einzelfallbetrachtung. Die Proportionalität betrifft aber nicht die Frage, ob die geltenden Anforderungen überhaupt zu

erfüllen sind, sie wirkt sich vielmehr nur darauf aus, auf welche Art und Weise diese Anforderungen erfüllt werden können.

Die BaFin legt in ihrer Veröffentlichung dar, dass das interne Kontrollsystem ein zentraler Bestandteil des Governance-Systems eines jeden Versicherungsunternehmens ist. Das interne Kontrollsystem dient vor allem dazu, die Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit zu unterstützen und sicherzustellen, dass Versicherungsunternehmen alle zu beachtenden Gesetze und Verordnungen, alle regulatorischen Anforderungen und auch alle internen Vorgaben tatsächlich einhalten.

## **Compliance-Funktion**

Ein wirksames internes Kontrollsystem erfasst nach Art. 46 Abs. 1 unter Abschnitt 2 Solvency II-Richtlinie zumindest Verwaltungs- und Rechnungslegungsverfahren, einen internen Kontrollrahmen, angemessene Melderegungen auf allen Unternehmensebenen und eine Funktion zur Überwachung der Einhaltung der Anforderungen an das Versicherungsunternehmen (Compliance-Funktion). Verantwortlich für die Einrichtung und Überwachung eines wirksamen internen Kontrollsystems ist die Geschäftsleitung. Diese Verantwortung kann nicht delegiert werden. Das interne Kontrollsystem umfasst alle Unternehmensebenen und ggf. auch ausgegliederte Bereiche und Prozesse.

Die BaFin betont, dass, sofern die Anforderungen in einem Spannungsfeld mit den gesellschaftsrechtlichen und kapitalmarktrechtlichen Möglichkeiten innerhalb von Versicherungsgruppen stehen, die künftig nach den Bestimmungen über die Gruppenaufsicht verpflichteten Unternehmen und die gruppzugehörigen Versicherungsunternehmen sich dessen bewusst werden und im eigenen Interesse angemessene Maßnahmen ergreifen, um die Erfüllung aufsichtsrechtlicher Anforderungen sicherzustellen. Dies kann bspw. durch den Abschluss von Beherrschungsverträgen erfolgen. Damit gesteht die BaFin zu, dass es in Gruppen- oder Konzernstrukturen aufgrund gesellschaftsrechtlicher Vorgaben schwierig sein kann, gruppen- oder konzernweite Compliance-Maßnahmen umzusetzen.

Der erforderliche interne Kontrollrahmen berücksichtigt das interne Kontrollumfeld, die interne Kontrolltätigkeit, die Kommunikation und die Überwachung. Damit umfasst das interne Kontrollumfeld die Gesamtheit aller Standards, Prozesse und Strukturen, die für die internen Kontrollen notwendig sind. Die Ausgestaltung des Kontrollumfelds wird maßgeblich durch die Unternehmenskultur bestimmt, etwa durch den Führungsstil und die Grundeinstellung der Geschäftsleitung und der nachgelagerten Führungsebenen sowie deren Integrität und fachlicher Kompetenz. Die BaFin zeigt damit nochmals auf, dass es von unschätzbarem Vorteil ist, eine positive Compliance-Kultur im Versicherungsunternehmen etabliert zu wissen. Dabei orientieren sich Art, Häufigkeit und Umfang der internen Kontrollen an der Wesentlichkeit der jeweiligen Bereiche und Prozesse. Die Wirksamkeit der internen Kontrollen ist mit Hilfe angemessener Verfahren fortlaufend zu überwachen und sicherzustellen. Die Geschäftsleitung hat sich regelmäßig über die Ergebnisse der Überwachung berichten zu lassen. In besonderen

Situationen, vor allem bei erheblichen Mängeln der internen Kontrollen, sind außerdem ad-hoc-Berichte erforderlich. Die Geschäftsleitung stellt durch geeignete Maßnahmen sicher, dass die notwendigen Anpassungen zeitnah umgesetzt werden.

Das interne Kontrollsystem umfasst auch eine angemessene und wirksame Compliance-Funktion zur Überwachung der Einhaltung der Anforderungen. Diese Compliance-Funktion ist spätestens zum *1. Januar 2016* einzurichten. Den Versicherungsunternehmen steht es grundsätzlich frei, wie sie die Compliance-Funktion ausgestalten und in die Aufbau-Organisation einbinden. Allerdings ist die Compliance-Funktion so einzurichten, dass sie jederzeit frei von Einflüssen ist, die eine objektive, faire und unabhängige Aufgabenerfüllung beeinträchtigen können.

Für die Compliance-Funktion müssen alle für ihre Arbeiten notwendigen Informationen uneingeschränkt zugänglich sein. Die Compliance-Funktion hat die Einhaltung aller zu beachtenden Gesetze und Verordnungen, aller regulatorischen (d.h. externen) Anforderungen und aller internen Vorgaben zu überwachen. Dabei muss die Compliance-Funktion nicht selbst die notwendigen Verfahren implementieren, sondern ggf. überwachen, dass die betroffenen Bereiche angemessene Verfahren eigenverantwortlich einrichten. Die Verantwortung liegt damit, wie durch die BaFin in der MaComp für Wertpapierdienstleistungsunternehmen festgelegt, bei den jeweiligen Fachbereichen. Die Compliance-Funktion beurteilt auch die möglichen Auswirkungen von Änderungen des Rechtsumfeldes, was nach Ansicht von EIOPA und BaFin nicht (mehr) durch die Rechtsabteilung erfolgen soll. Eine Zulieferung der Rechtsabteilung an die Compliance-Funktion bleibt nach unserer Interpretation aber möglich. Dies ist frühzeitig zu beobachten und zu analysieren. Dabei ist die Geschäftsleitung so zeitnah über die Folgen möglicher Änderungen des Rechtsumfeldes zu informieren, dass sie entsprechende Vorkehrungen und Maßnahmen ergreifen kann.

Die Compliance-Funktion identifiziert und bewertet die bestehenden Compliance-Risiken. Zu diesen gehören vor allem das Risiko rechtlicher oder aufsichtsbehördlicher Sanktionen, das Risiko wesentlicher finanzieller Verluste und das Risiko vor Reputationsverlusten, wenn und soweit diese Risiken auch aus Nichteinhaltung externer Anforderungen oder interner Vorgaben resultieren.

Die BaFin gibt vor, dass die Aktivitäten der Compliance-Funktion auf Basis eines sogenannten Compliance-Plans zu erfolgen haben. In diesem sind zumindest alle Tätigkeiten und Überwachungsmaßnahmen aufzuführen, die in den kommenden Geschäftsjahren vorgesehen sind. Der Compliance-Plan muss alle relevanten Geschäftsbereiche berücksichtigen. Die Auswahl der Aktivitäten hat risikoorientiert zu erfolgen. Die Aktualität des Compliance-Plans ist regelmäßig zu überprüfen. Im Gegensatz zur MaComp (für Wertpapierdienstleistungsunternehmen) scheint die BaFin nach derzeitiger Interpretation nicht davon auszugehen, dass alle relevanten Verfahren und Prozesse einmal jährlich geprüft werden müssen, sondern dass diese über mehrere Jahre verteilt werden und analysiert werden können.

Die Compliance-Funktion informiert die Geschäftsleitung regelmäßig über aktuelle Compliance-Themen. Dazu erstellt sie in angemessenen Zeitabständen, mindestens jedoch jährlich, einen Bericht. In besonderen Situationen können außerdem ad-hoc-Berichte erforderlich sein. Die Berichte informieren über bestehende Compliance-Risiken und die diese Risiken mindernden Maßnahmen. Ferner geben sie der Geschäftsleitung einen Überblick über die Angemessenheit der implementierten Verfahren zur Einhaltung der Anforderungen. Die BaFin empfiehlt, im Bericht die von der Compliance-Funktion durchgeführten Überwachungsmaßnahmen, die wesentlichen Vorfälle und die ergriffenen Gegenmaßnahmen aufzuführen, sowie mögliche Rechtsänderungsrisiken und den Umgang damit darzustellen.

## **Interne Revision**

Die Einrichtung einer funktionsfähigen, objektiv und unabhängig arbeitenden internen Revision ist national bereits vorgeschrieben (§ 64a Abs. 1 Satz 4 Nr. 4, Abs. 7 Nr. 4 VAG). Die Ausnahmeregelung des § 64a Abs. 5 VAG darf unter Solvency II nicht fortgeführt werden, da nach der Solvency II-Richtlinie alle ihr unterfallenden Versicherungsunternehmen über eine interne Revision verfügen müssen.

Die interne Revision darf keinen Einflüssen unterliegen, die ihre Unabhängigkeit und Unparteilichkeit bei der Erledigung ihrer Aufgaben beeinträchtigen können (unangemessene Einflüsse). Dies gilt für den verantwortlichen Inhaber der internen Revision sowie für alle Personen, die für die interne Revision tätig sind. Interessenkonflikte, auch persönlicher Natur, sind zu vermeiden. Dabei muss die interne Revision ihre Aufgaben eigenverantwortlich und ohne unangemessene Beeinflussung (Kontrollen, Einschränkungen oder sonstige Einflüsse), etwa durch andere Schlüsselfunktionen, die Geschäftsleitung oder den Aufsichtsrat, wahrnehmen können. Dies bedeutet auch, dass sie in der Lage sein muss, der Geschäftsleitung ihre Ergebnisse, Erkenntnisse, Bedenken, Verbesserungsempfehlungen usw. direkt mitzuteilen, und zwar ohne vorherige ändernde Einflussnahme. Eine begleitende Kommentierung ihrer Berichte durch andere Bereiche im Unternehmen ist hingegen zulässig.

Das Direktionsrecht der Geschäftsleitung in Bezug auf die Prüfungsplanung der internen Revision steht der Unabhängigkeit der internen Revision jetzt und auch künftig grundsätzlich nicht entgegen. Der internen Revision selbst steht das Recht zu, ad-hoc-Prüfungen außerhalb der Prüfungsplanung durchzuführen.

Die interne Revision darf keine revisionsfremden Aufgaben übernehmen, insbesondere keine operativen. Proportionalitätsaspekte spielen insoweit keine Rolle.

Bei kleineren Unternehmen wird allerdings derzeit auf europäischer Ebene diskutiert, ob es unter Anwendung des Proportionalitätsgrundsatzes möglich sein kann, die interne Revision mit anderen Schlüsselfunktionen zu bündeln. Diese Möglichkeit könnte für kleinere Unternehmen mit einem geringen Mitarbeiterbedarf und einem wenig komplexen Risikoprofil relevant sein.

Eine Bündelung mit operativen Funktionen steht jedoch z.Zt. nicht zur Diskussion, soll also weiterhin für alle Unternehmen ausgeschlossen sein. Diese Entwicklung gilt es mit Aufmerksamkeit 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

· Chicago      · Los Angeles      · Shanghai  
· Frankfurt    · New York        · Washington, DC  
· London        · Palo Alto        · West Palm Beach

**KAYE** | **SCHOLER**