Erfahrung nutzen, Zukunft sichern.

DIIR – Deutsches Institut für Interne Revision e.V. • Ohmstraße 59 • Frankfurt am Main

Email

Bundesanstalt für
Finanzdienstleistungsaufsicht
Referat BA 54
Graurheindorfer Str. 108
53117 Bonn

DIIR
Deutsches Institut für Interne Revision e.V.

Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 713769-0
Fax (069) 713769-69
www.diir.de
info@diir.de

Geschäftsführer:
Wilfried Fischenich
Volker Hampel
USt-ID DE 114235123
Vereinsregisternummer:
Amtsgericht Frankfurt
am Main VR 5326

GZ: BA 54-FR 2210-2012/0002
2012/0239859
Konsultation 01/2012 - Überarbeitung der MaRisk
Stellungnahme des DIIR – Deutsches Institut für Interne Revision e.V.

Sehr geehrte Damen und Herren,

am 26. April 2012 hatten Sie Ihr Konsultationspapier zur Überarbeitung der MaRisk veröffentlicht und den ersten Entwurf übersandt. Wir bedanken uns für die Möglichkeit einer Stellungnahme.

Das DIIR - Deutsches Institut für Interne Revision e.V. ist ein gemeinnütziges Institut zur Förderung und Weiterentwicklung der Internen Revision in Deutschland. Es wurde 1958 gegründet und hat mittlerweile über 2000 Mitglieder aus allen Bereichen der Wirtschaft, Wissenschaft und Verwaltung. Das DIIR ist Mitglied des The Institute of Internal Auditors (IIA). Unsere Stellungnahme wurde von dem Arbeitskreis „Mindestanforderungen an das Risikomanagement" (AK MaRisk) erstellt. Der Arbeitskreis ist mit Vertretern aus allen deutschen Kreditinstitutsgruppen besetzt und stellt die Schnittstelle des DIIR zum MaRisk-Fachgremium der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) dar. Er beschäftigt sich insbesondere mit den regulatorischen Anforderungen an die Interne Revision.

Mitglied des
Institute of Internal
Auditors (IIA), Inc.

Mitglied der
European Confederation
of Institutes of Internal
Auditing (ECIIA)

Mitglied im
Wuppertaler Kreis e.V. –
Bundesverband betriebliche
Weiterbildung

1. Grundsätzliche Anmerkungen

Nach KWG §25a und AT 1 Tz. 1 der MaRisk sind die einzurichtenden „Internen Kontrollverfahren" unterteilt in ein „Internes Kontrollsystem" (IKS) und die Interne Revision als unabhängige Überwachungsfunktion. AT 1 Tz. 1 nennt hier als Bestandteil des Internen Kontrollsystems insbesondere auch die Risikosteuerungs- und -controllingprozesse.

In der neuen Fassung KWG-E §25a (1) Satz 3 Nr. 3. sind die internen Kontrollverfahren unterteilt in das IKS, die Interne Revision und eine Compliance-Funktion. Das Risikocontrolling wird nicht explizit erwähnt.

Das BCBS-Papier „The Internal Audit Function in Banks, Nov 2011", das sich in der Konsultation befindet, reflektiert diese Differenzierung ebenfalls und hat die Position der Internen Revision als "3rd line of defence" besonders klar hervorgehoben.

> **Principle 13: Internal audit should both complement and assess operational management, risk management, compliance and other control functions.**
> 55. The Committee's document about corporate governance explicitly mentions that a bank should have a risk management function, a compliance function and an internal audit function. Each of these control functions, along with the bank's operational management, constitutes a line of defence against the risks the entity faces:
>
> 1st line operational management
> 2nd line risk management function, compliance function and other monitoring functions
> 3rd line internal audit function
>
> 56. Control failings by one line of defence should, in principle, be detected by another line of defence. However, responsibility for internal control does not transfer from one line to another.
> 57. Operational management has ownership, responsibility and accountability for identifying, assessing, controlling, mitigating and reporting on risks encountered in the course of a bank's business activities.
> 58. The risk management function facilitates and monitors the implementation of effective risk management practices by operational management. It assists operational management in defining risk exposures and reporting through the organisation. The compliance function monitors the risk of non-compliance with laws, regulations and standards. These functions are also control functions which ensure that policies and procedures with regard to risk-taking are enforced. Other monitoring functions may include human resources and the legal department.
> 59. The internal audit function employs a risk-based approach to assess the efficiency and effectiveness of the design and operation of internal control and periodically provides assurance to senior management and the board of directors.

Danach wären die Komponenten der „Internen Kontrollverfahren" wie folgt zu unterteilen:

- Erste Verteidigungslinie (Operatives Management):
  - prozessintegrierte Kontrollen und Funktionstrennungen
- Zweite Verteidigungslinie (Kontrolleinheiten):
  - Risikocontrolling
  - Compliance-Funktion
- Dritte Verteidigungslinie (Unabhängige Überwachung):
  - Interne Revision

Nach unserem Verständnis wären die erste und zweite Verteidigungslinie dem IKS zuzuordnen.

Wir gehen davon aus, dass die geplanten Veränderungen bzw. Ergänzungen der MaRisk im Rahmen dieser Differenzierung vorgenommen wurden, sehen dies jedoch im Regelungstext nicht klar genug herausgearbeitet. Daher empfehlen wir, die Komponenten des IKS bereits in AT 1 Tz. 1 zu verankern und auch in AT 4.3 und 4.4 entsprechend zu berücksichtigen.

Dementsprechend wäre auch eine Modifizierung des o. a. KWG-E § 25a in diesem Sinne erforderlich.

Insgesamt regen wir an, das in der Anlage 4 zu den MaRisk aus 2005 zuletzt verwendete Schaubild „Hierarchie der Begriffe in den MaRisk" entsprechend der aktuellen Regelungen zu überarbeiten und wieder als Anlage aufzunehmen.

2. Anmerkungen zu einzelnen Textziffern

Nr / Rdz	Wortlaut	Anmerkung / Empfehlung
AT 1 Tz. 1	Die internen Kontrollverfahren bestehen aus dem internen Kontrollsystem und der Internen Revision. Das interne Kontrollsystem umfasst insbesondere – Regelungen zur Aufbau- und Ablauforganisation ~~und~~ – Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation der Risiken (Risikosteuerungs- und -controllingprozesse) – das Risikocontrolling und – eine Compliance-Funktion. Das Risikomanagement schafft eine Grundlage für die sachgerechte Wahrnehmung der Überwachungsfunktionen des Aufsichtsorgans und beinhaltet deshalb auch dessen angemessene Einbindung.	Siehe grundsätzliche Anmerkungen oben. Ergänzung bzw. Klarstellung (wie nebenstehend rot/unterstrichen ergänzt), dass die Compliance-Funktion sowie das Risikocontrolling zum internen Kontrollsystem gehören. Damit deutliche Abgrenzung zur unabhängigen Revisionsfunktion als „dritte Verteidigungslinie".
AT 4.3 Tz. 1	In jedem Institut sind entsprechend Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten a) Regelungen zur Aufbau- und Ablauforganisation zu treffen ~~sowie~~ b) Risikosteuerungs- und -controllingprozesse einzurichten sowie c) ein Risikocontrolling und d) eine Compliance-Funktion zu implementieren.	Gesamthafte Beschreibung des IKS: Die einzurichtenden Funktionen des Internen Kontrollsystems (Risikocontrolling und Compliance) sollten diesem Abschnitt zugeordnet werden, um gesamthaft das Interne Kontrollsystem im respektiven AT 4.3. zu beschreiben und eine deutliche Abgrenzung von der Internen Revision als übergelagerter Überwachungsfunktion zu erreichen.

AT 4.4.1	**Risikocontrolling**	Siehe grundsätzliche Anmerkungen oben. Der gesamte Abschnitt sollte nach dem bereits vorhandenen „AT 4.3.2 Risikosteuerungs- und controllingprozesse" als AT 4.3.3 aufgeführt werden. Dies verdeutlicht die bereits gemäß AT 1 Tz. 1 vorgenommene Einordnung und führt die Passagen zum Risikocontrolling im Abschnitt zum Internen Kontrollsystem zusammen.
AT 4.4.2	**Interne Revision**	Siehe grundsätzliche Anmerkungen oben. Die alte Struktur „AT 4.4 Interne Revision" sollte erhalten bleiben, um die unabhängige Überwachungsfunktion (dritte Verteidigungslinie) deutlich zu machen.
AT 4.4.2 Tz. 6 (neu)	Wechselt die Leitung der Internen Revision, ist das Aufsichtsorgan vor der Entscheidung einzubeziehen.	Aufgrund des Auskunftsrechts des Vorsitzenden des Aufsichtsorgans (AT 4.4.2 Tz. 2) besteht eine besondere Schnittstelle der Internen Revision zum Aufsichtsorgan, die eine gleichartige Regelung wie für den Leiter des Risikocontrollings begründet.
AT 4.4.3	**Compliance**	Siehe grundsätzliche Anmerkungen oben. Wir empfehlen, den ganzen Abschnitt unter AT 4.3 als AT 4.3.5 nach den Stresstests einzuordnen. Dadurch wird deutlich, dass die ComplianceFunktion zum internen Kontrollsystem (AT 4.3) gehört. Dies wird auch bereits durch die Bezeichnung von Compliance und Risikocontrolling als „Kontrolleinheit" (4.4.3 Tz. 2) nahegelegt.

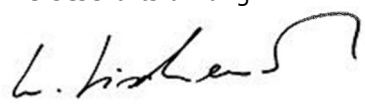
AT 4.4.3 Tz. 1	Jedes Institut muss über eine funktionsfähige Compliance-Funktion verfügen. Diese hat die institutsinternen Regelungen, die die Einhaltung der gesetzlichen Bestimmungen oder sonstigen Vorgaben gewährleisten, zu bewerten, deren Einhaltung zu überwachen sowie die Geschäftsleiter und die Geschäftsbereiche hinsichtlich der Einhaltung dieser Bestimmungen und Vorgaben zu unterstützen und zu beraten. Ferner hat sie die Risiken, die sich aus der Nichteinhaltung gesetzlicher Bestimmungen und sonstiger Vorgaben ergeben können, zu beurteilen.	Neu im Gegensatz zum bisherigen (deutschen) Verständnis ist der allumfänglich Ansatz der Compliance-Funktion, über WpHG- und GwG-Themen hinaus. Aus unserer Sicht ist die nebenstehende Formulierung zu unkonkret und weitgehend. Soll die Compliance-Funktion zukünftig z.B. auch hauptverantwortlich Basel-/KWG-Themen (wie Kreditrisiko/Kapitaladäquanz) überwachen? Es erfolgt eine Vermischung der Compliance-Funktion i.e.S. und der Verantwortung für Regelkonformität i.w.S. Die Pflichten der Tz. 1 sollten aufgrund des sehr weiten Umfanges der gesetzlichen und sonstigen Vorgaben auf Institutsebene gehoben bzw. von der Geschäftsleitung zugeordnet werden können. Den Banken sollte die Möglichkeit einer Selbstdefinition eingeräumt werden. Dies wäre auch in Übereinstimmung mit der Gesetzesbegründung zu § 25a KWG, die beispielhaft das GwG und das WpHG aufzählt und ermöglicht, die bereits in vielen Instituten seit längerem bestehenden Strukturen für Compliance im weiteren Sinne, also die allgemeine Sicherstellung der Gesetzeseinhaltung (z.B. Rechtsabteilung, Risikomanagement, Datenschutz, Personal-abteilung, Compliance-Funktion) beizubehalten. Dies erscheint auch im Sinne der EBA Guideline on Internal Governance GL 44 zu sein: siehe Feedbacktable on CP 44 Principle 25: Ergänzender Passus bzgl. Möglichkeit der Verlagerung von spezifischen Aufgaben zur Vermeidung von Interessenkonflikten. Alternativ könnte eine Konkretisierung vorgenommen werden, welche Regelungsgebiete mindestens umfasst sein sollten (siehe z.B. "Compliance and the Compliance-function in Banks" Baseler Ausschuss für Bankenaufsicht 2005).

AT 4.4.3 Tz. 2	Grundsätzlich ist die Compliance-Funktion unmittelbar der Geschäftsleitung unterstellt und berichtspflichtig. Sie kann auch an andere Kontrolleinheiten angebunden werden.	Die Unabhängigkeit der Compliance-Funktion ist bisher nicht im Entwurf explizit genannt. Die Möglichkeit zur Anbindung der Compliance-Funktion an andere Kontrolleinheiten sollte deutlich als Ausnahme formuliert werden (siehe Tz. 3: „Ausnahmefall"), wie auch in EBA Guideline CP 44 vorgegeben, um die Unabhängigkeit zu sichern. Außerdem verwenden die MaComp BT 1.1 Tz. 3 eine andere Formulierung, hier sollte eine Anpassung vorgenommen werden.
AT 8 Tz. 7	Für wesentliche Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen hat das Institut Prozesse zu etablieren, die die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität analysieren. Im Rahmen dieser Prozesse sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten. Im Rahmen ihrer Aufgaben sind auch die Interne Revision, das Risikocontrolling und die Compliance-Funktion zu beteiligen.	Der letzte Satz sollte um die dritte besondere Funktion des IKS, das Risikocontrolling, erweitert werden.
AT 9 Tz. 2	Das Institut muss auf der Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen). Die maßgeblichen Organisationseinheiten sind bei der Erstellung der Risikoanalyse einzubeziehen. Im Rahmen ihrer Aufgaben ~~ist~~ sind auch die Interne Revision, das Risikocontrolling sowie die Compliance-Funktion zu beteiligen. Soweit sich wesentliche Änderungen der Risikosituation ergeben, ist die Risikoanalyse anzupassen.	Das Risikocontrolling sowie die Compliance-Funktion sollten, wie auch beim Neue Produkte-Prozess, einbezogen werden.

Mit der Veröffentlichung dieser Stellungnahme sind wir einverstanden.

Mit freundlichen Grüßen

DIIR – Deutsches Institut für Interne Revision e.V.
Die Geschäftsführung



(W. Fischenich)