Erfahrung nutzen, Zukunft sichern.

DIIR

Deutsches Institut für
Interne Revision e.V.

Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 71 37 69 - 0
Fax (069) 71 37 69 - 69
www.diir.de
info@diir.de

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

Konsultation 4/2010 – Entwurf eines Rundschreibens zur Verhinderung betrügerischer Handlungen zu Lasten der Institute gemäß § 25c Abs. 1 des Kreditwesengesetzes

Geschäftszeichen: GW 1-FR 1903-2010/0001

Frankfurt am Main
28. Mai 2010

Stellungnahme des DIIR - Deutsches Institut für Interne Revision e.V.

1. Allgemeine Anmerkungen

Das Schreiben enthält sowohl konkrete Hinweise zur Umsetzung des § 25c Abs. 1 KWG als auch Hintergründe, Überlegungen und Empfehlungen der Aufsicht. Wir empfehlen, das Rundschreiben auf konkrete Maßgaben zu beschränken, die von den betroffenen Gesellschaften in Abhängigkeit von der jeweiligen Größe und Risikosituation angemessen umzusetzen sind (Proportionalität). Dabei sollte insbesondere der Ressourcensituation in kleineren Häusern Rechnung getragen werden. Insbesondere bei Formulierungen mit empfehlendem Charakter (Umsetzungsbespiele etc.) bleibt letztlich unklar, inwieweit die Aufsicht eine Umsetzung in den betroffenen Gesellschaften erwartet und welche Rolle diesen bei den einschlägigen Prüfungen von Interner und Externer Revision beizumessen ist. Wie auch bei anderen Rundschreiben (z.B. RS 15/2009 MaRisk Banken), sollten diese daher der Praxis überlassen bleiben.

Generell fällt auf, dass zentrale und dezentrale, in den Prozessen der betroffenen Gesellschaften verankerte Kontrollen vermischt werden. Maßnahmen zur Verhinderung von betrügerischen Handlungen sind üblicherweise im prozessimmanenten Internen Kontrollsystem verankert. Das implementierte Management operationeller Risiken umfasst selbstverständlich auch die Steuerung von "Betrugsrisiken". Insofern empfehlen wir insbesondere die Rolle der zentralen Stelle (ergänzend zu den bereits vorhandenen aufsichtsseitigen Regelungen) zu gestalten. Eine Verantwortung der zentralen Stelle für die Normengebung und die Überwachung sowie Eingriffsbefugnisse im Eskalationsfall sind sicher sinnvoll, eine konkrete Einbindung der zentralen Stelle in die Geschäftsprozesse führt jedoch zu unklaren Zuständigkeiten, da die Verantwortung für das Interne Kontrollsystem jeweils mit der Verantwortung für den Geschäftsprozess einhergehen sollte.

2. Anmerkungen zu I. Regelungsinhalt und -zweck

Die Ausführungen dieses Abschnittes passen teilweise nicht recht zur Überschrift „Regelungsinhalt und -zweck". Wir empfehlen, die Herleitung des §25c KWG n.F. und die Zitate internationaler Vorgaben zu streichen.

Insbesondere der Absatz:

> „Die Verpflichteten müssen u. a. über **Richtlinien, Grundsätze und Verfahren in Bezug auf die interne und externe Revision** verfügen sowie Verfahren zur (...), **Auswahl und Einstellung geeigneter Mitarbeiter** (insbesondere in Compliance-Funktion auf Managementebene) unter Beachtung hoher ethischer und professioneller Standards sowie **geeignete Managementinformationssysteme** vorhalten."

sollte gestrichen werden. Die Konkretisierung ist an dieser Stelle nicht erforderlich. Der Inhalt ist teilweise fehlerhaft bzw. unvollständig. So kann die Externe Revision nicht Gegenstand von Richtlinien der geprüften Gesellschaft sein. Es sollte daneben nicht der Eindruck erweckt werden, dass die Auswahl und Einstelllung geeigneter Mitarbeiter nur auf die „Compliance-Funktion auf Managementebene" beschränkt ist.

Der Satz

> „Dies bedeutet, dass soweit keine speziellen gesetzlichen oder untergesetzlichen Regelungen und Vorgaben eingreifen **und im nachfolgenden keine abweichenden Aussagen getroffen werden**, die allgemeinen Anforderungen an die Angemessenheit und die Wirksamkeit des Risikomanagement, wie sie sich aus § 25a Abs. 1 Satz 3 KWG sowie den Mindestanforderungen an das Risikomanagement (MaRisk [BA]) ergeben, hiervon unberührt bleiben."

impliziert, dass bei Abweichung der Aussagen dieses Rundschreibens zu § 25a Abs. 1, Satz 3 KWG und MaRisk die Aussagen dieses Rundschreibens gelten. Damit würde das Rundschreiben über dem Gesetz stehen. Wir empfehlen, die Formulierung anzupassen.

3. Anmerkungen zu II. Anwendungsbereich

Die hier getroffene Eingrenzung der betrügerischen Handlung auf den Zusammenhang mit den vom Institut erbrachten Dienstleistungen bedeutet, dass z.B. Korruption (außerhalb des Bankgeschäftes wie z.B. bei Bautätigkeit oder im Einkauf) nicht umfasst wäre. Wir empfehlen, den Punkt **„und im Zusammenhang mit den vom Institut erbrachten Dienstleistungen** steht" zu streichen oder weiter zu fassen.

Redaktionell:

„a) Diese können ~~entweder~~ in **unmittelbar gegen das Institut gerichteten Handlungen** bestehen. Hierzu zählen u.a. die nachfolgenden Fälle:"

Der Abschnitt

„c) **Nicht umfasst** sind dagegen – allerdings nur zur Vermeidung von Abgrenzungsschwierigkeiten - folgende Handlungen: **Geldwäsche, Terrorismusfinanzierung** sowie **Insiderhandel** und **Marktmanipulation**."

sollte so umformuliert werden, dass für die genannten Delikte auf die hierfür einschlägigen Regelungen verwiesen wird.

4. Anmerkungen zu III. Zuständigkeit

Wir empfehlen, größeren Häusern sowie kleinen Häusern, die die Geldwäschefunktion ausgelagert haben, die Möglichkeit zu eröffnen, neben dem Bereich zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, eine eigene Stelle für die Betrugsbekämpfung einzurichten. Diese wäre entweder dem Geldwäschebeauftragten oder direkt dem Vorstand zu unterstellen.

Wir empfehlen, den Absatz:

> „Zu den Aufgaben der Zentralen Stelle gehört daneben insbesondere die Implementierung von Sicherungsmaßnahmen (siehe dazu im Folgenden unter V.) sowie der Kontakt zu Strafverfolgungsbehörden sowie der BaFin."

zu streichen. Es wird der Eindruck erweckt, dass nur diese Stelle Sicherungsmaßnahmen implementiert sowie Kontakt zu Strafverfolgungsbehörden und BaFin hält. Dies ist nicht praxisgerecht. Die Zentrale Stelle sollte Grundsätze und Vorgaben zur Implementierung von Sicherungsmaßnahmen entwickeln, die von den Verantwortlichen für die Geschäftsprozesse umzusetzen sind. Die Umsetzung wäre wieder von der Zentralen Stelle zu überwachen. Daneben sollten z.B. auch Kontakte der Internen Revision, der Rechtsabteilung sowie des Managements zu Strafverfolgungsbehörden und BaFin weiter möglich sein.

Doppelzuständigkeiten können sinnvoll sein, wenn Aufgaben im Rahmen der Betrugsbekämpfung z.B. durch die Rechtsabteilung oder Ombudsleute wahrgenommen werden. Wie empfehlen, den Punkt „**keine Doppelzuständigkeiten** bestehen" zu streichen.

5. Anmerkungen zu IV. Gefährdungsanalyse

Der Satz:

> „Mit dem Erfordernis der Angemessenheit sind reine „Alibi-Maßnahmen" ausgeschlossen."

ist eine Selbstverständlichkeit und daher entbehrlich.

Redaktioneller Vorschlag:

„Die institutsinterne Gefährdungsanalyse muss **für ~~die interne und externe Revision~~ Dritte nachvollziehbar schriftlich fixiert** werden."

Die Absätze:

> „Die Kategorisierung bzw. Gewichtung der identifizierten Risiken hat sich auf der einen Seite an der **Schadenseintrittswahrscheinlichkeit** und auf der anderen Seite an der **potentiellen Schadenshöhe der jeweiligen betrügerischen Handlung** im untersuchten Bereich des Instituts zu orientieren.
>
> Neben dem **Erfahrungswissen der eigenen Mitarbeiter** des Instituts sind hierbei auch die **Expertise der internen und externen Prüfer, öffentlich verfügbare Informationen** über Betrugspraktiken im Finanzbereich, Typologienpapiere der Strafverfolgungsbehörden und anderer nationaler und internationaler Stellen sowie ggf. externer Berater einzubeziehen. Eine weitere wertvolle Hilfe für eine Bewertung stellen zudem die in vielen Instituten vorhandenen **Schadensfalldatenbanken** dar.

Hierbei kann es hilfreich sein, sowohl die Schadenseintrittswahrscheinlichkeit als auch die potentielle Schadenshöhe für die jeweiligen betrügerischen Handlungen sowie die untersuchten Bereiche mittels so genannter **Scoringwerte** einzustufen.

Empfehlenswert kann auch ein sog. „Risk-Mapping" sein, mit dem zugleich auch Prioritäten für den Handlungsbedarf festzulegen sind. Die identifizierten hohen Risiken erfordern Maßnahmen, die ebenfalls in der Analyse festzuhalten sind."

sollten gestrichen werden.

Werden derartige Beispiele in einem Rundschreiben der Aufsicht aufgeführt, so stellt sich für die Institute und deren interne und externe Prüfer die Frage, inwieweit Abweichungen von diesen Beispielen überhaupt möglich sind. Damit wird der Grundsatz der Proportionalität in Frage gestellt. Die angemessene Ausgestaltung der Gefährdungsanalyse sowie die Auswahl der mitwirkenden internen und externen Stellen sollten daher den Instituten und Empfehlungen der Verbände überlassen bleiben.

6. Anmerkungen zu V. Angemessene Sicherungsmaßnahmen

Redaktionell:

Sicherungsmaßnahmen müssen sowohl kundenbezogen, geschäftsbezogen als auch mitarbeiterbezogen sein.

Der Absatz:

„Je höher die Schadenseintrittswahrscheinlichkeit oder die Höhe des möglichen Schadens für das Institut ist, je umfangreicher müssen sich die vom Institut getroffenen Maßnahmen darstellen".

kann entfallen, da er redundant zu den voranstehenden Absätzen ist.

Die Definition der Sicherungsmaßnahmen bedarf einer Konkretisierung (siehe auch unsere einleitende Anmerkung unter 1.):

„aa) Zu den **allgemeine Sicherungsmaßnahmen** zählen für § 25c Abs. 1 KWG dabei insbesondere:

- Die Erstellung einer **Gefährdungsanalyse** (vgl. vorstehend unter IV.)
- Die Schaffung von Verfahren und Leitlinien, z.B.:
  - Klare **Berichts-~~Linien~~Pflichten**
  - Klare **Regelung der Verantwortlichkeiten und Genehmigungsbefugnisse** im Rahmen der Aufbau und Ablauforganisation
  - **Einbindung der** für die Verhinderung betrügerischer Handlungen zuständigen **Zentralen Stelle in ~~das operative Geschäft~~ in die Organisation der Geschäftsprozesse.**
  - Systematische und strukturierte **Aufdeckung von kriminellen Handlungen**
  - **Konsequente ~~Verfolgung~~ Untersuchung** aufgedeckter betrügerischer Handlungen"

Die Interne Revision ist gemäß § 25a (1) KWG nicht Bestandteil des Internen Kontrollsystems und kann demnach nicht als Bestandteil der internen (i.S.v. laufenden) Kontrollen aufgeführt werden. Weiterhin ist ein Hinweisgebersystem kein integraler Bestandteil des Internen Kontrollsystems. Der folgende Absatz sollte daher anpasst werden:

- „Die Durchführung von **internen Kontrollen** (Bestandsaufnahme/ Kassenkontrolle; Zutrittskontrolle/ Gebäudesicherheitskonzept; „Vier-Augen-Prinzip"; ~~Hinweisgebersystem („Whistleblowing")~~, statistische Überprüfungen; ~~Zuständigkeit der internen Revision auch in Bezug auf Risiken durch betrügerische Handlungen;~~ keine Ausnahmen für „Management-Override")."

Ggf. sind beide Punkte separat aufzuführen:

- Einbindung der Internen Revision bei der Untersuchung und Aufarbeitung betrügerischer Handlungen.
- Hinweisgebersystem („Whistleblowing")

Zu den konkreten mitarbeiterbezogenen Sicherungsmaßnahmen bleibt festzuhalten, dass die Maßnahme "know your colleague" u.E. die Persönlichkeitsrechte verletzen kann und eine Misstrauenskultur fördert. Besser ist die Formulierung „know your employee".

Wir bitten, die Beispiele zu den Kundenbezogenen Sicherungsmaßnahmen, z.B. „Abgleich mit Schurkenliste" und „Schufa-Anfragen" auf datenschutzrechtliche Zulässigkeit zu prüfen und ggf. zu spezifizieren.