

Compliance Management: Grundlagen für eine effektive Compliance-Funktion

Einstieg in die Umsetzung

CHRISTOPH SCHMIDT, DR. MARTIN KINZELBACH

Leasing- und Factoring-Gesellschaften müssen aufgrund der 4. Novelle der MaRisk vom 14.12.2012 seit Januar 2014 eine Compliance-Funktion vorhalten. Gerade kleinere Gesellschaften haben oft nicht die Möglichkeit, hierfür separate Dienststellen oder Personal vorzuhalten. Deshalb stellt die Umsetzung der Regeltreue für sie inhaltlich wie organisatorisch eine Herausforderung dar. Dieser Beitrag beschreibt einige Modelle für die Aufbauorganisation einer Compliance-Funktion, gibt Hinweise zu Kommunikationswegen und zur Etablierung eines dafür verantwortlichen Beauftragten.

Nach § 25a Abs. 1 Kreditwesengesetz (KWG) muss ein Institut über eine ordnungsgemäße Geschäftsorganisation verfügen, die unter anderem die Einhaltung gesetzlicher Bestimmungen gewährleistet. Dieser Umstand erfordert ein angemessenes und effektives Risikomanagement. Hierzu gehört nach den Erläuterungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zu den Mindestanforderungen an das Risikomanagement (MaRisk), AT 4.4.2¹⁾, eine Compliance-Funktion. Demnach muss jedes Institut über wirksame Verfahren zur Einhaltung aller wesentlichen rechtlichen und vertraglichen Regelungen und Vorgaben sowie entsprechende Kontrollen verfügen.²⁾ Die Compliance-Funktion untersteht dabei direkt der Geschäftsleitung.³⁾

Ferner muss das Institut einen Compliance-Beauftragten benennen, der für die Erfüllung der Aufgaben der Compliance-Funktion verantwortlich zeichnet. In Ausnahmefällen kann in Anwendung des Proportionalitätsprinzips ein Geschäftsleiter die Aufgaben dieses Beauftragten überneh-

men.⁴⁾ Darüber hinaus besteht grundsätzlich die Möglichkeit einer Auslagerung.⁵⁾

Aufbauorganisation

Zur Umsetzung der aufsichtsrechtlichen Anforderungen in der Aufbauorganisation des Instituts eignen sich unterschiedliche Modelle, wie die einzelnen erforderlichen Kontrolleinheiten beziehungsweise Beauftragten eingerichtet und gegeben-

nenfalls zusammengefasst werden können. Dabei bezeichnet

- ▶ CoB den Compliance-Beauftragten,
- ▶ ZS die Zentrale Stelle für Geldwäsche- und Betrugsbekämpfung nach § 25h KWG, welche die Aufgaben des Geldwäschebeauftragten (GWB) umfasst, und
- ▶ DSB den Datenschutzbeauftragten nach Bundesdatenschutzgesetz.

In allen Modellen müssen Compliance und die Interne Revision voneinander organisatorisch und personell getrennt sein.⁶⁾

Im Modell 1 ist die Compliance-Funktion als Stabsstelle unter der Geschäftsleitung ausgeprägt und umfasst die anderen Kontrolleinheiten, wegen der Unabhängigkeitsanforderungen nicht jedoch die Interne Revision. In diesem Modell kann die In-

1) Vgl. BaFin: Erläuterungen zu den MaRisk in der Fassung vom 14.12.2012, S. 18.

2) Vgl. ebda. S. 18 Tz. 1.

3) Vgl. ebda. S. 19 Tz. 3.

4) Vgl. ebda. S. 19 Tz. 4.

5) Vgl. ebda. S. 28 Tz. 4.

6) Vgl. ebda. S. 19 Tz. 3.

DIE AUTOREN:

Christoph Schmidt LL.M.,
Viechtach,

ist Gründer und Inhaber von One More Consulting, einer auf Corporate Governance, Risikomanagement und Compliance spezialisierte Unternehmensberatung.

E-Mail:

christoph.schmidt@one-more.eu



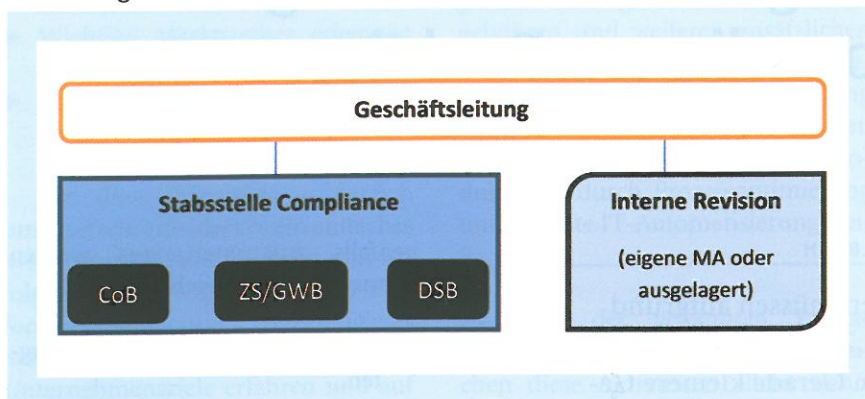
Dr. Martin Kinzelbach,
München,

ist Steuerberater und Wirtschaftsprüfer und hat gut 20 Jahre Erfahrung auf den Gebieten Interne Kontrollen, Risikomanagement, Revision und Controlling.

E-Mail: mk@mkinzelbach.de



Abbildung 1: Modell 1



Quelle: Eigene Darstellung

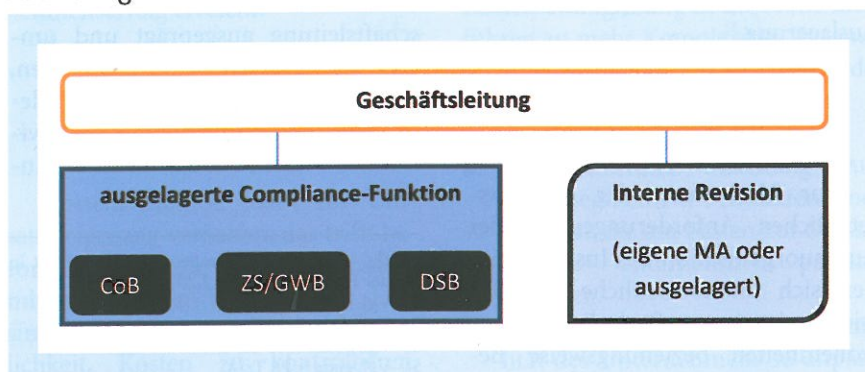
terne Revision ausgelagert sein (zum Beispiel an Konzern oder externe Dienstleister) oder von eigenem Personal ausgeübt werden. Die Stabsstelle ist mit einem Mitarbeiter der Gesellschaft besetzt, der direkt der Geschäftsleitung untersteht. Diese nimmt die Aufgaben als Compliance-Beauftragter, Geldwäschebeauftragter

und Datenschutzbeauftragter der Gesellschaft wahr.

Modell 1

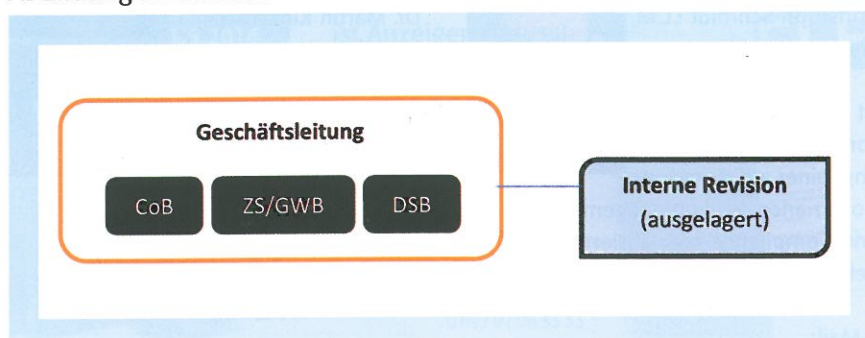
Das Modell 1 setzt eine gewisse Größe der Gesellschaft voraus, damit die Stabsstelle Compliance ausgeprägt

Abbildung 2: Modell 2



Quelle: Eigene Darstellung

Abbildung 3: Modell 3



Quelle: Eigene Darstellung

und personell besetzt werden kann. Für Gesellschaften, die diese Größe nicht erreichen oder aus anderen Gründen keine interne Stabsstelle schaffen möchten, bieten sich die folgenden Modelle an:

Im Modell 2 ist die Compliance-Funktion ausgelagert (etwa an Konzern oder externe Dienstleister). Neben der hier vorgestellten kompletten Auslagerung, sind Abwandlungen mit nur teilweiser Auslagerung derselben denkbar. In diesem Auslagerungsszenario nehmen externe Personen die Aufgaben des Compliance-Beauftragten, des Geldwäschebeauftragten und/oder Datenschutzbeauftragten der Gesellschaft wahr.

Modell 2

Bei der Auslagerung der Compliance-Funktion sind die allgemeinen Anforderungen an das Outsourcing zu beachten (MaRisk AT 9).⁷⁾ Insbesondere muss die Leistung klar spezifiziert sein, und der Gesellschaft sind entsprechende Weisungs-, Informations- und Prüfungsrechte einzuräumen.

Sollen sowohl die Compliance als auch die Interne Revision ausgelagert werden, kann dies nur dann an denselben Dienstleister erfolgen, wenn beim Dienstleister die erforderliche Funktionstrennung und wechselseitige Unabhängigkeit gewahrt bleibt. Nicht erlaubt ist eine Auslagerung beider Funktionen an einen Dienstleister, bei dem dieselbe Person oder ein einheitliches Team die Interne Revision und gleichzeitig die Compliance-Funktion der Gesellschaft ausübt.

Im Modell 3 nimmt ein Geschäftsleiter in Personalunion die Kontrollfunktionen Compliance, Geldwäsche und Datenschutz mit wahr, während die Interne Revision ausgelagert ist. Es funktioniert auch bei einer Geschäfts-

⁷⁾ Vgl. ebda. S. 27 ff.

leitung, die nur aus einer Person besteht.

Modelle 3 und 4

Das Modell 4 (siehe Abbildung 4) stellt eine Abwandlung des Modells 3 dar. Hier hat die Gesellschaft eine Geschäftsleitung, die aus mindestens zwei Personen besteht (GF, kurz für Geschäftsführer). Diese nehmen jeweils einzelne Kontrollfunktionen in Personalunion wahr. Die Interne Revision ist wieder ausgelagert.

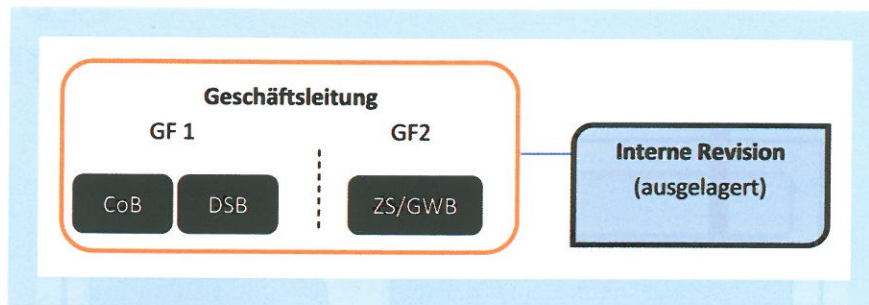
Die Modelle 3 und 4 sind durch eine Personalunion von Geschäftsleitung und Kontrollfunktionen charakterisiert. Sie kommen jedoch nur dann in Frage, wenn sie unter Berücksichtigung des Proportionalitätsprinzips im Verhältnis zur Größe, der Geschäftstätigkeit und zu den Risiken der Gesellschaften angemessen sind. Damit beschränken sich die beiden Modelle in der Regel auf Gesellschaften mit nur wenig Beschäftigten; höchstens Gesellschaften mit weniger als zehn Mitarbeitern (Außendienst nicht mitgezählt) sollten sie anwenden.

Unternehmensüberwachung

Neben der aufsichtsrechtlichen Notwendigkeit stellt eine Compliance-Funktion ein wichtiges Element der Unternehmensführung und -überwachung dar. Dies lässt sich gut im Kontext des sogenannten Three-Lines-of-Defense-Modell (kurz TLDM) darstellen.⁸⁾ Das TLDM bezeichnet Bausteine eines effektiven internen Kontrollsystems. Die Compliance kann dabei als Instrument der „zweiten Verteidigungslinie“ verstanden werden (siehe Abbildung 5).⁹⁾

Vergleicht man die dargestellten Modelle vor dem Hintergrund des TLDM, so lassen sich bei den Modellen 1 und 2 alle drei Verteidigungslinien erkennen. Dagegen führt im Modell 3 die Umsetzung der Compliance-Funktion in Personalunion be-

Abbildung 4: Modell 4



Quelle: Eigene Darstellung

züglich der betreffenden Risiken zu einer Reduzierung der Verteidigungslinien, nachdem die erste und zweite zusammenfallen. Im Modell 4 hängen die Verteidigungslinien von der konkreten Aufgabenzuordnung der Kontrollfunktionen ab: Sind bei den beiden Geschäftsführern die Fachverantwortung und die Kontrollverantwortung „über Kreuz“ zugeordnet, können wieder alle drei Verteidigungslinien wirksam werden.

Nachdem die Gesellschaft ein effektives internes Kontrollsystem benötigt, muss die Geschäftsleitung im Einzelfall abwägen, ob sich dieses Ziel erreichen lässt, wenn sie einzelne Kontrollfunktionen in Personalunion

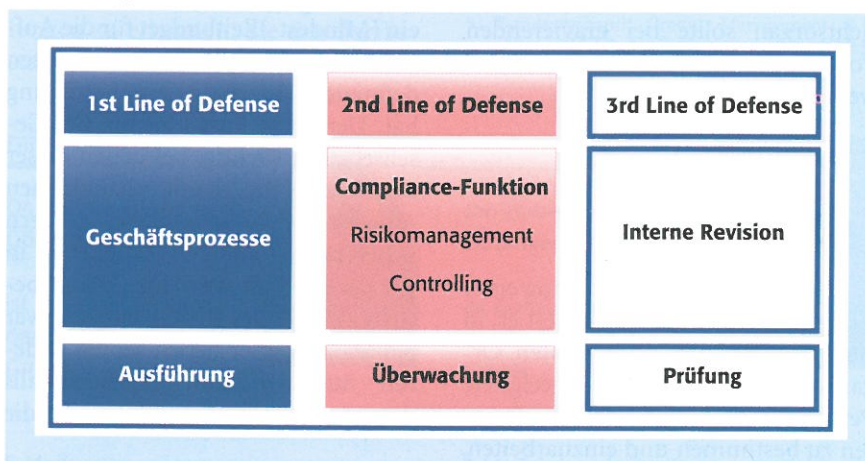
ausführt. Die ist ein weiterer Grund dafür, dass sich die Modelle 3 und 4 nur für kleine Gesellschaften mit sehr wenigen Mitarbeitern und überschaubaren Risiken eignen.

Kommunikation

Zu den Aufgaben der Compliance-Funktion gehört unter anderem die Kommunikation über ihre Tätigkeit und über relevante Vorgänge. Das Grundgerüst der Kommunikation bilden die regelmäßigen Berichte des CoB an die Geschäftsleitung. Diese Berichte stellen die Maßnahmen und Ergebnisse der laufenden Überwachung und Kontrolle der Einhaltung der relevanten rechtlichen Vorgaben und vertraglichen Regelungen dar.

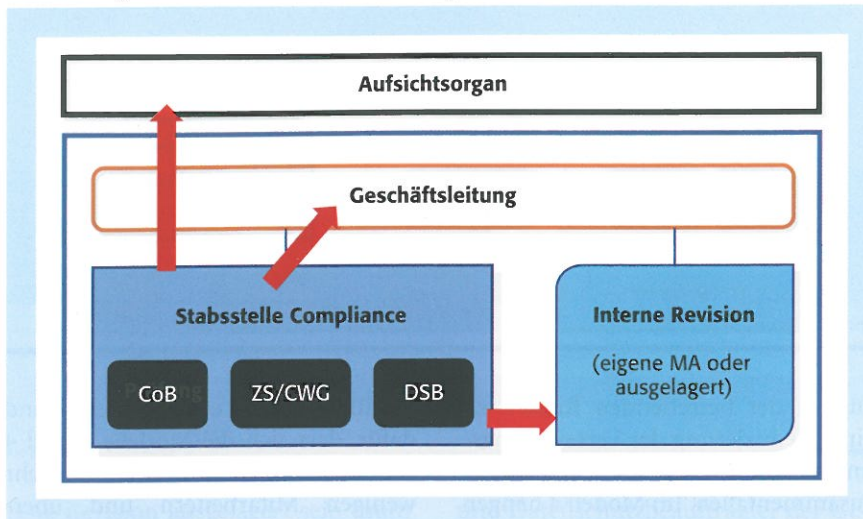
Der Bericht muss mindestens jährlich erstellt werden, bei entspre-

Abbildung 5: Three-Lines-of-Defense-Modell



Quelle: Eigene Darstellung

Abbildung 6: Kommunikationskonzept



Quelle: Eigene Darstellung

chender Größe und/oder Risikolage der Gesellschaft gegebenenfalls häufiger. Die regelmäßigen Berichte des CoB sind auch der Internen Revision und dem Aufsichtsgremium der Gesellschaft vorzulegen.¹⁰⁾ Damit bestehen grundsätzlich drei verschiedene Adressaten der Berichterstattung (hier in Abbildung 6 dargestellt auf Basis von Modell 1).

Neben der regelmäßigen Berichterstattung informiert der CoB anlassbezogen über besondere Vorkommnisse, beispielsweise bei Hinweisen auf Gesetzesverstöße oder auf betrügerische Handlungen. Die anlassbezogene Berichterstattung richtet sich in erster Linie an die Geschäftsleitung und die Interne Revision – das Aufsichtsorgan sollte bei gravierenden Vorkommnissen ebenfalls informiert werden.

Etablierung des Beauftragten

Die erfolgreiche Einrichtung einer Compliance-Funktion erfordert es, in Abhängigkeit vom angestrebten Organisationsmodell eine geeignete Person für die Aufgabe des Beauftragten zu bestimmen und einzuarbeiten. Im Falle der Auslagerung wird der Dienstleister oder das Konzernunter-

nehmen fachlich geeignetes Personal bereitstellen.

In allen anderen Fällen muss zunächst eine Mitarbeiterin oder ein Mitarbeiter identifiziert werden. Dabei sind insbesondere drei Voraussetzungen erfolgskritisch:

- Zum einen sollte die Person das Geschäft der Gesellschaft gut kennen;
- des Weiteren sollte sie über gute analytische Fähigkeiten verfügen und
- eine Affinität zu internen Kontrollsystemen oder Überwachung besitzen.

Schließlich muss die Gesellschaft ein (Mindest-)Zeitbudget für die Aufgabe des Compliance-Beauftragten definieren, die dieser zur Verfügung hat. Der letzte Punkt ist für alle Gesellschaften wichtig, bei denen dieser Beauftragte die damit verbundenen Aufgaben nicht in Vollzeit, sondern neben seinen anderen Tätigkeiten in der Gesellschaft verrichtet. Dann besteht ein latentes Risiko, dass er zwar benannt ist, aber neben seinen anderen Aufgaben und gegebenenfalls drängendem Tagesgeschäft nicht die

nötige Zeit und Konzentration für die Compliance-Themen findet.

Fundierte Einarbeitung

Hat die Gesellschaft eine Person als (künftigen) CoB identifiziert, sollte eine spezifische Einarbeitung stattfinden. Zur Einarbeitung gibt es am Markt verschiedene Literatur und diverse Seminarangebote. Dem Beauftragten sollte hierfür ein angemessenes Budget an Zeit und Sachkosten zur Verfügung stehen. Darüber hinaus kann es sehr nützlich sein, einen Erfahrungsaustausch mit anderen Gesellschaften oder den Kontakt zu Beratern zu suchen. Dies vor allem, wenn der CoB nach seiner persönlichen Einarbeitung beginnt, die Compliance-Funktion in der Gesellschaft mit ihren Vorkehrungen, Maßnahmen und Abläufen auszugestalten.

Es gibt verschiedene Modelloptionen zur organisatorischen Umsetzung der seit 2014 explizit vorgeschriebenen Compliance-Funktion. Das „klassische“ Modell ist eine separat ausgeprägte Stabsstelle. Diese untersteht direkt der Geschäftsleitung und bündelt zweckmäßigerweise die verschiedenen Kontrollfunktionen. Als Alternative bietet sich an, die Compliance-Funktion oder Teile davon auszulagern. Für kleine Leasing- und Factoring-Gesellschaften, die nur über eine geringe Personalstärke verfügen, kann es sinnvoll sein, dass ein Geschäftsführer Kontrollfunktionen in Personalunion mit ausführt. Die Gesellschaft sollte über ein effektives, aufsichtskonformes internes Kontrollsystem verfügen, was bei der Wahl des Modells unbedingt zu beachten ist.

Der CoB berichtet regelmäßig an die Geschäftsleitung. Seine Berichte stehen der Internen Revision und dem Aufsichtsgremium zur Verfügung. Bei der Etablierung des Beauftragten sollten die Gesellschaften darauf achten, für diese Aufgabe ausreichend Zeit zur Verfügung zu stellen und eine fachlich fundierte Einarbeitung zu ermöglichen. ◀

¹⁰⁾ Vgl. BaFin: Erläuterungen zu den MaRisk in der Fassung vom 14.12.2012, S19 Tz 6.