Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

# Rundschreiben 2017/2
# *Corporate Governance* – Versicherer

## *Corporate Governance*, Risikomanagement und internes Kontrollsystem bei Versicherern

| | |
|---|---|
| Referenz: | FINMA-RS 17/2 „*Corporate Governance* – Versicherer“ |
| Erlass: | 7. Dezember 2016 |
| Inkraftsetzung: | 1. Januar 2017 |
| Konkordanz: | vormals FINMA-RS 08/32 „*Corporate Governance* Versicherer“ und FINMA-RS 08/35 „Interne Revision Versicherer“, beide vom 20. November 2008 |
| Rechtliche Grundlagen: | FINMAG Art. 7 Abs. 1 Bst. b<br>VAG Art. 14, 22, 27, 67, 68, 75, 76<br>AVO Art. 12–14, 16, 96–98*a*, 191, 195–196, 204 |

| Adressaten | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BankG | | | VAG | | | BEHG | FinfraG | | | | | | KAG | | | | | | | | | | GwG | | | Andere | | | | | | |
| Banken | Finanzgruppen und -kongl. | Andere Intermediäre | Versicherer | Vers.-Gruppen und -Kongl. | Vermittler | Effektenhändler | Handelsplätze | Zentrale Gegenparteien | Zentralverwahrer | Transaktionsregister | Zahlungssysteme | Teilnehmer | Fondsleitungen | SICAV | KmG für KKA | SICAF | Depotbanken | Vermögensverwalter KKA | Vertriebsträger | Vertreter ausl. KKA | Andere Intermediäre | SRO | DUFI | SRO-Beaufsichtigte | Prüfgesellschaften | Ratingagenturen | | | | | | |
| | | | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Laupenstrasse 27, 3003 Bern
Tel. +41 (0)31 327 91 00, Fax +41 (0)31 327 91 01
**www.finma.ch**

# Inhaltsverzeichnis

## I. Zweck

Dieses Rundschreiben bezweckt die Konkretisierung der Bestimmungen des Versicherungsaufsichtsgesetzes (VAG; SR 961.01) betreffend *Corporate Governance*, Risikomanagement und internes Kontrollsystem (IKS). 1

## II. Geltungsbereich

Dieses Rundschreiben gilt für alle Versicherungsunternehmen nach Art. 2 Abs. 1 Bst. a und b VAG sowie für die der Gruppen- bzw. Konglomeratsaufsicht unterstellten Versicherungsgruppen und Versicherungskonglomerate nach Art. 2 Abs. 1 Bst. d i.V.m. Art. 65 und 73 VAG. 2

Auf Niederlassungen in der Schweiz von Versicherungsunternehmen mit Sitz im Ausland (Art. 2 Abs. 1 Bst. b VAG) und Versicherungsunternehmen mit Bewilligung zum Betrieb des Versicherungszweigs C3 (Rückversicherung durch *Captives*) ist das Rundschreiben sinngemäss anwendbar. 3

Rz 16–27 betreffend den Verwaltungsrat eines Versicherungsunternehmens gelten für das Verwaltungsorgan der Genossenschaft sinngemäss. 4

Bei der Anwendung dieser Bestimmungen ist auf die Besonderheiten, die Grösse und die Komplexität des betroffenen Versicherungsunternehmens Rücksicht zu nehmen und dem Prinzip der Verhältnismässigkeit Rechnung zu tragen. 5

## III. *Corporate-Governance*-Prinzipien

Das Versicherungsunternehmen setzt insbesondere folgende *Corporate-Governance*-Prinzipien unternehmensweit um: 6

- Klare Zuweisung und Dokumentation von Aufgaben, Kompetenzen, Verantwortungen sowie Berichtswegen; 7
- Klare Trennung zwischen operativen Tätigkeiten und Kontrolltätigkeiten mittels geeigneter Massnahmen; 8
- Einrichtung von internen Berichterstattungsprozessen zur Weitergabe von Informationen an alle relevanten Stellen im Unternehmen; 9
- Dokumentation wesentlicher Entscheidungen (inkl. Massnahmen); 10
- Einrichtung eines wirksamen unternehmensweiten Risikomanagementsystems und eines wirksamen internen Kontrollsystems (IKS) einschliesslich der Kontrollfunktionen (Risikomanagement, *Compliance*, interne Revision) und periodische Überprüfung auf deren Angemessenheit durch eine unabhängige (interne oder externe) Partei; 11
- Festlegung von Grundsätzen, Prozessen und Strukturen zur Einhaltung von gesetz- 12

lichen, regulatorischen und internen Vorschriften;

- Festlegung von Grundsätzen, Prozessen und Strukturen zur Identifikation und Behandlung von Interessenkonflikten und Missbräuchen; 13

- Festlegung von Grundsätzen zum von den Mitarbeitenden erwarteten Verhalten; 14

- Einrichtung von Prozessen, die gewährleisten, dass die für die Oberleitung, Aufsicht und Kontrolle sowie für die Geschäftsführung des Versicherungsunternehmens verantwortlichen Personen dauerhaft über die notwendige berufliche Erfahrung, das fachliche Wissen und die persönliche Eignung verfügen. 15

## IV. Verwaltungsrat

### A. Zusammensetzung

Der Verwaltungsrat muss in seiner Gesamtheit neben ausreichendem Versicherungswissen insbesondere über Berufserfahrungen und ausreichende Kenntnisse in der Geschäftsführung, im strategischen Management, in der Risikosteuerung und im Finanz- und Rechnungswesen verfügen. 16

Die Anzahl der Mitglieder des Verwaltungsrates beträgt mindestens drei und richtet sich nach Grösse, Komplexität und Risikoprofil des Versicherungsunternehmens. 17

Der Verwaltungsrat besteht mindestens zu einem Drittel aus Mitgliedern, welche die nachfolgenden Unabhängigkeitskriterien erfüllen. Die FINMA kann in begründeten Fällen, etwa bei Rückversicherungscaptives oder bei Tochtergesellschaften von unterstellten Versicherungsgruppen und Versicherungskonglomeraten, Ausnahmen bewilligen. 18

Ein Mitglied des Verwaltungsrates gilt als unabhängig, wenn es mindestens die folgenden Kriterien erfüllt: 19

- nicht in anderer Funktion beim Versicherungsunternehmen beschäftigt ist und dies auch nicht innerhalb der letzten 2 Jahre gewesen ist; 20

- innerhalb der letzten 2 Jahre nicht bei der Prüfgesellschaft des Versicherungsunternehmens als für das Versicherungsunternehmen leitender Prüfer beschäftigt gewesen ist; 21

- keine geschäftliche Beziehung zum Versicherungsunternehmen aufweist, welche aufgrund ihrer Art oder ihres Umfangs zu einem Interessenkonflikt führt; und 22

- nicht Beteiligter des Versicherungsunternehmens ist und keinen solchen vertritt. Als Beteiligte gelten Personen nach Art. 4 Abs. 2 Bst. f VAG. 23

### B. Verwaltungsratsausschüsse

Der Verwaltungsrat bildet, falls zweckmässig, Verwaltungsratsausschüsse zur effektiven Ausübung seiner Pflichten. 24

Versicherungsunternehmen der Aufsichtskategorien 2 und 3 richten einen Prüfungsausschuss und einen Risikoausschuss ein. Bei Versicherungsunternehmen der Aufsichtskategorie 3 kann ein kombinierter Risiko- und Prüfungsausschuss gebildet werden. 25

Die Prüfungs- und Risikoausschüsse bestehen zu mindestens einem Drittel aus unabhängigen Mitgliedern (vgl. Rz 19–23). Der Verwaltungsratspräsident soll grundsätzlich weder Mitglied des Prüfausschusses noch Vorsitzender des Risikoausschusses sein. 26

Jeder Ausschuss verfügt in seiner Gesamtheit über die notwendigen Kenntnisse und Erfahrungen im jeweiligen Aufgabenbereich. Der Vorsitzende eines Ausschusses verfügt über spezifische Kenntnisse in seinem Aufgabenbereich. 27

## V. Risikomanagementsystem und internes Kontrollsystem

### A. Risikomanagementsystem

Das Versicherungsunternehmen verfügt über ein Risikomanagementsystem nach Art. 96 AVO, welches nach Art. 97 AVO zu dokumentieren ist. Die in Art. 97 Abs. 2 Bst. e AVO erwähnten Limiten-Systeme für die Risikoexposition sowie die Kontrollmechanismen sollen sicherstellen, dass das Versicherungsunternehmen im Rahmen seiner Risikofähigkeit operiert. Die Grundsätze des Risikomanagements sind sowohl auf wesentliche Auslagerungen als auch auf übrige Beziehungen mit Drittpersonen anwendbar. 28

### B. Internes Kontrollsystem

Das Versicherungsunternehmen richtet ein internes Kontrollsystem ein, um eine angemessene Sicherheit bezüglich der Risiken der Geschäftsführung zu gewährleisten, insbesondere in Bezug auf die Wirksamkeit von Geschäftsprozessen, die Zuverlässigkeit der finanziellen Berichterstattung und die Befolgung von Rechtsnormen und internen Vorschriften. Die Grundsätze des internen Kontrollsystems sind sowohl auf wesentliche Auslagerungen als auch auf übrige Beziehungen mit Drittpersonen anwendbar. 29

Das Versicherungsunternehmen definiert hinreichende Kontrollaktivitäten auf Unternehmens- und Prozessebene, um zu gewährleisten, dass die vom Verwaltungsrat und von der Geschäftsleitung angeordneten Vorgänge, Methoden oder Massnahmen, mit welchen den wesentlichen Risiken der Geschäftsführung begegnet werden soll, eingehalten und ausgeführt werden. 30

Der Verwaltungsrat, die Geschäftsleitung sowie die übrigen Mitarbeitenden erhalten alle notwendigen Informationen, damit sie ihre Verantwortlichkeiten betreffend das interne Kontrollsystem wahrnehmen können. 31

Das Versicherungsunternehmen hält sein internes Kontrollsystem in einer Dokumentation fest. Diese Dokumentation ist laufend zu aktualisieren und umfasst insbesondere: 32

- die unternehmensinternen Richtlinien zum internen Kontrollsystem und die damit verbundenen Prozesse; 33

- die Beschreibung der Aufbau- und Ablauforganisation inklusive die Aufgaben, Kompetenzen und Verantwortlichkeiten; 34
- die Anforderungen an das interne Kontrollsystem (unter anderem Ziele, Ausstattung mit Ressourcen, Sensibilisierung der Mitarbeitenden); 35
- die Beschreibung der etablierten Kontrollaktivitäten. 36

## C. *Compliance*-Prozesse

Das Versicherungsunternehmen identifiziert seine wesentlichen rechtlichen und regulatorischen Verpflichtungen und nimmt eine Einschätzung seiner wesentlichen *Compliance*-Risiken vor. 37

## D. Kontrollfunktionen

Das Versicherungsunternehmen stellt sicher, dass jede Kontrollfunktion ihre Aufgaben objektiv und unabhängig wahrnimmt. 38

Die Vergütung der Mitarbeitenden der Kontrollfunktionen ist so auszugestalten, dass mögliche Interessenskonflikte mit den von ihnen überwachten oder kontrollierten Geschäftseinheiten minimiert werden. 39

Die Kontrollfunktionen haben uneingeschränkten Zugang zu allen Personen und Informationen, welche sie zur Erfüllung ihrer Aufgaben benötigen. 40

### a) Risikomanagement-Funktion

Der Leiter der Risikomanagement-Funktion nimmt regelmässig eine unabhängige Einschätzung der wesentlichen Risiken des Versicherungsunternehmens und der Angemessenheit des Risikomanagementsystems vor und berichtet darüber periodisch (mindestens jährlich) dem Verwaltungsrat. 41

### b) *Compliance*-Funktion

Die *Compliance*-Funktion beurteilt die Angemessenheit der vom Versicherungsunternehmen eingerichteten Grundsätze, Prozesse und (Kontroll-)Strukturen zur Einhaltung der rechtlichen, regulatorischen und internen Vorschriften sowie den Umgang des Versicherungsunternehmens mit *Compliance*-Verstössen. 42

Der Leiter der *Compliance*-Funktion nimmt periodisch (mindestens jährlich) eine unabhängige Einschätzung der wesentlichen *Compliance*-Risiken des Versicherungsunternehmens vor und berichtet darüber dem Verwaltungsrat. 43

### c) Interne Revision

Die interne Revision ist dem Verwaltungsrat oder dessen Prüfungsausschuss unmittelbar unterstellt. Sie ist organisatorisch und operativ von den anderen Kontrollfunktionen des Versicherungsunternehmens unabhängig. Sie verfügt über ein uneingeschränktes Einsichts-, Auskunfts- und Prüfungsrecht innerhalb des Versicherungsunternehmens. 44

Die interne Revision ist im Einklang mit internationalen Berufsstandards für die interne Revision[1] ausgestaltet und befolgt diese Standards in ihrer Tätigkeit. 45

Die interne Revision übt ihre Tätigkeiten auf der Grundlage einer periodischen, risikobasierten Prüfungsplanung aus. Sie bestimmt hierzu alle wesentlichen Geschäftsbereiche, Funktionen und Prozesse des Versicherungsunternehmens (die Prüfobjekte) und führt mindestens jährlich eine Risikobeurteilung der Prüfobjekte durch. Treten während der Prüfperiode wesentliche Änderungen im Risikoprofil des Versicherungsunternehmens ein, überprüft die interne Revision ihre Prüfungsplanung und passt diese nötigenfalls an. Der Verwaltungsrat oder sein Prüfungsausschuss genehmigt den Prüfungsplan sowie wesentliche Änderungen daran. 46

Die interne Revision erstellt mindestens einmal jährlich einen Bericht an den Verwaltungsrat, welcher insbesondere die folgenden Punkte umfasst: 47

- die Umsetzung des vom Verwaltungsrat genehmigten Prüfungsplans sowie zusätzlich zum Prüfungsplan ausgeführte Tätigkeiten; 48
- den Stand der Umsetzung von verabschiedeten Verbesserungsmassnahmen; 49
- die Gegebenheiten, welche die Unabhängigkeit, Objektivität oder Effektivität der internen Revision negativ beeinträchtigen. 50

Die interne Revision erstattet zeitnah und sachgerecht über alle wichtigen Feststellungen einer Prüfung schriftlich Bericht an den Verwaltungsrat oder an dessen Prüfungsausschuss. Gravierende Mängel müssen unverzüglich gemeldet werden. 51

Die interne Revision stellt ihren Bericht an den Verwaltungsrat sowie ihre einzelnen Prüfberichte der Prüfgesellschaft nach Art. 28 VAG zur Verfügung. 52

Die vollständige oder teilweise Auslagerung der Aufgaben der internen Revision ist nach Art. 4 Abs. 2 Bst. j VAG genehmigungspflichtig. Die Auslagerung kann erfolgen an: 53

- die interne Revision eines Gruppenunternehmens, sofern das beaufsichtigte Versicherungsunternehmen in die gruppenweiten Kontroll- und Steuerungsprozesse einbezogen ist; 54
- eine von der Eidgenössischen Revisionsaufsichtsbehörde RAB zugelassene Prüfgesellschaft, welche von der vom Versicherungsunternehmen gemäss Art. 28 VAG bereits beauftragten Prüfgesellschaft unabhängig ist; 55
- einen externen Dienstleister, welcher von der vom Versicherungsunternehmen gemäss Art. 28 VAG bereits beauftragten Prüfgesellschaft unabhängig ist. 56

[1] Internationale Standards für die berufliche Praxis der internen Revision des Institute of Internal Auditors (IIA)

## VI. Übergangsbestimmung

Die Umsetzung der Rz 17, 18–23 und 25–27 hat bis spätestens am 31. Dezember 2019 zu erfolgen. Die FINMA kann in begründeten Einzelfällen Ausnahmen gewähren. 57