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/xx
Corporate Governance Versicherer

Corporate Governance, Risikomanagement und internes Kontrollsystem bei Versicherern

Referenz:	FINMA-RS 17/xx " Corporate Governance Versicherer"
Erlass:	...
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 VAG Art. 14, 22, 27, 67, 68, 75, 76 AVO Art. 12–14, 16, 96–98*a*, 191, 195–196, 204

Adressaten																					
BankG			VAG			BEHG		KAG								GwG			Andere	
Banken	Finanzgruppen und -kongl.	Andere Intermediäre	Versicherer	Vers.-Gruppen und -Kongl.	Vermittler	Börsen und Teilnehmer	Effektenhändler	Fondsleitungen	SICAV	KG 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 16–28 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 der betroffenen Einheit 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 Entscheid- und Berichtslinien; 7
- Klare Trennung zwischen operativen Tätigkeiten und Kontrolltätigkeiten mittels geeigneter Massnahmen; 8
- Einrichtung von internen Berichterstattungs- und Kommunikationsprozessen 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
- Einrichtung von Grundsätzen, Prozessen und Strukturen zur Einhaltung von gesetzlichen, regulatorischen und internen Vorschriften; 12

- Festlegung von Grundsätzen, Prozessen und Strukturen zur Identifikation und Vermeidung oder Lösung 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 vertiefte Kenntnisse in der Geschäftsführung, im strategischen Management, in der Risikosteuerung und im Finanz- und Rechnungswesen verfügen. 16

Jedes Verwaltungsratsmitglied muss über Fachwissen oder Fähigkeiten verfügen, die im Zusammenwirken mit den anderen Mitgliedern für die Aufgabenerfüllung des Verwaltungsrates relevant sind. 17

Die Anzahl der Mitglieder des Verwaltungsrates beträgt mindestens drei und richtet sich nach Grösse, Komplexität und Risikoprofil des Versicherungsunternehmens. 18

Der Verwaltungsrat sollte mindestens zu einem Drittel aus Mitgliedern bestehen, welche die nachfolgenden Unabhängigkeitskriterien erfüllen. Die FINMA kann in begründeten Fällen Ausnahmen bewilligen. 19

Ein Mitglied des Verwaltungsrates gilt als unabhängig, wenn es mindestens die folgenden Kriterien erfüllt: 20

- nicht in anderer Funktion beim Versicherungsunternehmen beschäftigt ist und dies auch nicht innerhalb der letzten 2 Jahre gewesen ist; 21

- innerhalb der letzten 2 Jahre nicht bei der Prüfgesellschaft des Versicherungsunternehmens als für das Versicherungsunternehmen leitender Prüfer beschäftigt gewesen ist; und 22

- keine geschäftliche Beziehung zum Versicherungsunternehmen aufweist, welche aufgrund ihrer Art oder ihres Umfangs zu einem Interessenkonflikt führt. 23

Zudem sollte ein massgeblicher Teil des Verwaltungsrats nicht am Versicherungsunternehmen beteiligt oder, falls das Versicherungsunternehmen einer Unternehmensgruppe angehört, nicht bei einem anderen Unternehmen der Gruppe operativ tätig sein oder einen Beteiligten vertreten. 24

B. Verwaltungsratsausschüsse

Der Verwaltungsrat bildet falls zweckmässig Verwaltungsratsausschüsse zur effektiven Ausübung seiner Pflichten. 25

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. 26

Die Prüfungs- und Risikoausschüsse bestehen zu mindestens einem Drittel aus unabhängigen Mitgliedern (vgl. Rz 20–24). Der Verwaltungsratspräsident ist weder Vorsitzender des Prüfungsausschusses noch des Risikoausschusses. 27

Die Ausschüsse verfügen in ihrer Gesamtheit über die notwendigen Kenntnisse und Erfahrungen in ihrem jeweiligen Aufgabenbereich. Für den Vorsitzenden eines Ausschusses gelten höhere Anforderungen als für die Mitglieder. 28

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. 29

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. 30

Das Versicherungsunternehmen definiert Kontrollaktivitäten auf Unternehmens- und Prozessebene, um zu gewährleisten, dass die vom Verwaltungsrat und von der Geschäftsleitung angeordneten Massnahmen, mit welchen den wesentlichen Risiken der Geschäftsführung begegnet werden soll, eingehalten und ausgeführt werden. 31

Der Verwaltungsrat, die Geschäftsleitung sowie die übrigen Mitarbeiter erhalten alle notwendigen Informationen, damit sie ihre Verantwortlichkeiten betreffend das interne Kontrollsystem wahrnehmen können. 32

Das Versicherungsunternehmen hält sein internes Kontrollsystem in einer Dokumentation fest. Diese Dokumentation ist laufend zu aktualisieren und umfasst insbesondere: 33

- die unternehmensinternen Richtlinien zum internen Kontrollsystem und die damit verbundenen Prozesse; 34
- die Beschreibung der Aufbau- und Ablauforganisation inklusive die Aufgaben, Kompetenzen und Verantwortlichkeiten; 35
- die Anforderungen an das interne Kontrollsystem (unter anderem Ziele, Ausstattung mit Ressourcen, Sensibilisierung der Mitarbeiter); 36
- die Beschreibung der etablierten Kontrollaktivitäten. 37

C. Kontrollfunktionen

Das Versicherungsunternehmen stellt sicher, dass jede Kontrollfunktion frei von Einflüssen ist, die sie daran hindern, ihre Aufgaben objektiv und unabhängig wahrzunehmen. 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 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 stellt sicher, dass die wesentlichen rechtlichen und regulatorischen Verpflichtungen des Versicherungsunternehmens identifiziert werden und nimmt eine Einschätzung der Compliance-Risiken des Versicherungsunternehmens vor. Sie untersucht und beurteilt die Angemessenheit der vom Versicherungsunternehmen eingerichteten Richtlinien, Prozesse und Kontrollen zur Vermeidung von Compliance-Verstössen. 42

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

c) Interne Revision

Die interne Revision ist dem Verwaltungsrat 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 nationalen oder 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. Der Prüfungsplan deckt einen Planungszeitraum von mindestens einem Jahr ab und sollte einen Ausblick auf die mehrjährige Prüfungsplanung enthalten. Der Verwaltungsrat genehmigt den Prüfungsplan sowie wesentliche Änderungen daran. 46

Die interne Revision überprüft auf Grundlage der Prüfungsplanung in angemessenen Zeitabständen alle Bereiche der Geschäftstätigkeit und alle Funktionen des Versicherungsunternehmens. 47

Die interne Revision erstellt mindestens einmal jährlich einen Bericht an den Verwaltungsrat, welcher insbesondere die folgenden Punkte umfasst: 48

- die Erfüllung des vom Verwaltungsrat genehmigten Prüfungsplans sowie zusätzlich zum Prüfungsplan ausgeführte Tätigkeiten; 49
- den Stand der Umsetzung von verabschiedeten Verbesserungsmassnahmen; 50
- die Gegebenheiten, welche die Unabhängigkeit, Objektivität oder Effektivität der internen Revision negativ beeinträchtigen oder beeinträchtigen könnten. 51

Die interne Revision erstattet zeitnah und sachgerecht über alle wichtigen Feststellungen einer Prüfung schriftlich Bericht an den Verwaltungsrat. Gravierende Mängel müssen dem Verwaltungsrat unverzüglich gemeldet werden. 52

Die interne Revision stellt ihren Bericht an den Verwaltungsrat sowie ihre einzelnen Prüfberichte der Prüfgesellschaft nach Art. 28 VAG zur Verfügung. 53

Die Aufgaben der internen Revision oder Teile davon können, vorbehältlich der Zustimmung durch die FINMA, ausgelagert werden: 54

- auf die interne Revision des obersten Gruppenunternehmens, sofern das beaufsichtigte Versicherungsunternehmen in die gruppenweiten Kontroll- und Steuerungsprozesse einbezogen ist; 55
- auf eine von der Eidgenössischen Revisionsaufsichtsbehörde RAB zugelassene Prüfgesellschaft, welche von der vom Versicherungsunternehmen gemäss Art. 28 VAG bereits beauftragten Prüfgesellschaft unabhängig ist; 56
- auf einen externen Dienstleister, welcher von der vom Versicherungsunternehmen gemäss Art. 28 VAG bereits beauftragten Prüfgesellschaft unabhängig ist. 57

[1] Leitlinie zum Internal Audit des Schweizerischen Verbandes für Interne Revision (SVIR) oder Internationale Standards für die berufliche Praxis der internen Revision des Institute of Internal Auditors (IIA)

VI. Risikomanagement und internes Kontrollsystem bei Auslagerungen

Eine Auslagerung liegt vor, wenn ein Versicherungsunternehmen ein anderes Unternehmen (Dienstleister) beauftragt, selbständig und dauernd eine Funktion oder Aufgabe in Bezug auf die Geschäftstätigkeit des Versicherungsunternehmens wahrzunehmen. 58

Rz 60–66 sind für jede Art von Auslagerungen anzuwenden. 59

Die mit einer Auslagerung verbundenen Risiken sind systematisch zu identifizieren, zu überwachen, zu quantifizieren und zu steuern. 60

Vorgängig zu einer Auslagerung erstellt das Versicherungsunternehmen eine Risikoanalyse, welche die ökonomischen und operativen Überlegungen und die damit verbundenen Risiken nachvollziehbar darlegt. Bei wesentlichen Änderungen der Rahmenbedingungen der Auslagerung wird eine neue Risikoanalyse erstellt, um über die Fortführung oder Beendigung der Auslagerung zu entscheiden. 61

Werden mehrere Funktionen und/oder Aufgaben an den gleichen Dienstleister ausgelagert, so ist dem Konzentrationsrisiko im Besonderen Rechnung zu tragen. 62

Die mit der Auslagerung verbundenen Risiken sind in das interne Kontrollsystem des auslagernden Versicherungsunternehmens einzubinden. Datensicherheit, Datenschutz sowie Wirksamkeit der Geschäftsprozesse sind zusätzlich zu gewährleisten. 63

Das auslagernde Versicherungsunternehmen und die FINMA müssen die ausgelagerten Funktionen und/oder Aufgaben jederzeit prüfen können. 64

Das Versicherungsunternehmen definiert eine verantwortliche Person für die Überwachung und Kontrolle des Dienstleisters. 65

Das Versicherungsunternehmen sorgt für ein Reporting des Dienstleisters, um die ausgelagerten Funktionen und/oder Aufgaben angemessen überwachen zu können. 66

VII. Übergangsbestimmung

Die Umsetzung der Rz 18, 19–24 und 26–28 hat bis spätestens am 31. Dezember 2019 zu erfolgen. Die FINMA kann in begründeten Einzelfällen Ausnahmen gewähren. 67