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 2017/1
# *Corporate Governance* - Banken

## *Corporate Governance*, Risikomanagement und interne Kontrollen bei Banken



| | |
|---|---|
| Referenz: | FINMA-RS 17/1 „*Corporate Governance* – Banken“ |
| Erlass: | 22. September 2016 |
| Inkraftsetzung: | 1. Juli 2017 |
| Letzte Änderung: | … [Änderungen sind mit * gekennzeichnet und am Schluss des Dokuments aufgeführt] |
| Konkordanz: | vormals FINMA-RS 08/24 „Überwachung und interne Kontrolle Banken“ vom 20. November 2008 |
| Rechtliche Grundlagen: | FINMAG Art. 7 Abs. 1 Bst. b<br>BankG Art. 3 Abs. 2 Bst. a und c, 3*b*–3*f*, 4[quinquies], 6<br>BankV Art. 11 Abs. 2, 12<br>BEHG Art. 10 Abs. 2 Bst. a und Abs. 5, 14<br>BEHV Art. 19, 20<br>ERV Art. 7–12 |

| 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 | | | | | X | | | | | | | | | | | | | | | | | | | | | | | | | | |

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

# Inhaltsverzeichnis

## I. Gegenstand

Das vorliegende Rundschreiben erläutert die Anforderungen an die *Corporate Governance*, das Risikomanagement, das interne Kontrollsystem (IKS) und die interne Revision bei Banken, Effektenhändlern, Finanzgruppen (Art. 3*c* Abs. 1 BankG) und bank- oder effektenhandelsdominierten Finanzkonglomeraten (Art. 3*c* Abs. 2 BankG). Diese werden nachfolgend als Institute bezeichnet. 1

## II. Begriffe

Unter *Corporate Governance* werden im folgenden die Grundsätze und Strukturen verstanden, anhand derer ein Institut durch seine Organe gesteuert und kontrolliert wird. 2

Das Risikomanagement umfasst die organisatorischen Strukturen sowie die Methoden und Prozesse, die der Festlegung von Risikostrategien und Risikosteuerungsmassnahmen sowie der Identifikation, Analyse, Bewertung, Bewirtschaftung, Überwachung und Berichterstattung von Risiken dienen. 3

Die Risikotoleranz beinhaltet sowohl quantitative wie qualitative Überlegungen hinsichtlich der wesentlichen Risiken, die das Institut zur Erreichung seiner strategischen Geschäftsziele sowie in Anbetracht seiner Kapital- und Liquiditätsplanung einzugehen bereit ist. Die Risikotoleranz wird sowohl pro jeweilige Risikokategorie als auch auf Institutsebene festgelegt, sofern relevant. 4

Das Risikoprofil fasst auf Institutsebene und pro jeweilige Risikokategorie für einen bestimmten Zeitpunkt die jeweils eingenommenen Risikopositionen des Instituts zusammen. 5

Das IKS umfasst die Gesamtheit der Kontrollstrukturen und -prozesse, welche auf allen Ebenen des Instituts die Grundlage für die Erreichung der geschäftspolitischen Ziele und für einen ordnungsgemässen Institutsbetrieb bilden. Dabei beinhaltet das IKS nicht nur Aktivitäten der nachträglichen Kontrolle, sondern auch solche der Planung und Steuerung. Ein wirksames IKS umfasst u.a. in die Arbeitsabläufe integrierte Kontrollaktivitäten, geeignete Risikomanagement- und *Compliance*-Prozesse sowie der Grösse, Komplexität und dem Risikoprofil des Instituts entsprechend ausgestaltete Kontrollinstanzen, insbesondere eine unabhängige Risikokontrolle und *Compliance*-Funktion. 6

Als *Compliance* gilt die Einhaltung von gesetzlichen, regulatorischen und internen Vorschriften sowie die Beachtung von marktüblichen Standards und Standesregeln. 7

## III. Geltungsbereich (Proportionalitätsprinzip)

Das Rundschreiben gilt für alle Institute gemäss Rz 1. Die Anforderungen sind im Einzelfall unter Berücksichtigung der Grösse, der Komplexität, der Struktur und des Risikoprofils des 8

Instituts umzusetzen. Die FINMA kann im Einzelfall Erleichterungen bewilligen oder Verschärfungen anordnen.

## IV. Oberleitungsorgan

### A. Aufgaben und Verantwortlichkeiten

Die Aufgaben des Organs für die Oberleitung, Aufsicht und Kontrolle, nachfolgend „Oberleitungsorgan“, umfassen insbesondere: 9

**a) Geschäftsstrategie und Risikopolitik**

Das Oberleitungsorgan legt die Geschäftsstrategie fest und erlässt Leitsätze zur Unternehmenskultur. Es ~~genehmigt das Rahmenkonzept für das~~ verabschiedet die Risikopolitik sowie die Grundzüge des institutsweiten Risikomanagements und trägt die Verantwortung für die Reglementierung, Einrichtung und Überwachung eines wirksamen Risikomanagements sowie die Steuerung der Gesamtrisiken. 10 *

**b) Organisation**

Das Oberleitungsorgan ist verantwortlich für eine angemessene Unternehmensorganisation und erlässt die dafür notwendigen Reglemente. 11

**c) Finanzen**

Das Oberleitungsorgan trägt die oberste Verantwortung für die finanzielle Lage und Entwicklung des Instituts. Es genehmigt bzw. verabschiedet die Kapital- und Liquiditätsplanung sowie den Geschäftsbericht, das Jahresbudget, die Zwischenabschlüsse und die finanziellen Jahresziele. 12

**d) Personelle und weitere Ressourcen**

Das Oberleitungsorgan ist verantwortlich für die angemessene Ausstattung des Instituts mit personellen und weiteren Ressourcen (z.B. Infrastruktur, IT) sowie die Personal- und Vergütungspolitik. Es entscheidet über die Wahl und Abberufung seiner Ausschussmitglieder, der Mitglieder der Geschäftsleitung, deren Vorsitzender sowie des *Chief Risk Officer* (CRO) und des Leiters der internen Revision[1]. 13

**e) Überwachung und Kontrolle**

Das Oberleitungsorgan übt die Oberaufsicht über die Geschäftsleitung aus. Es ist verantwortlich für ein geeignetes Risiko- und Kontrollumfeld innerhalb des Instituts und sorgt für ein wirksames IKS. Es bestellt und überwacht die interne Revision, bestimmt die aufsichtsrechtliche Prüfgesellschaft und würdigt deren Berichte. 14

[1] Die Wahl des Leiters der internen Revision kann auch vom Prüfausschuss wahrgenommen werden.

### f) Wesentliche Strukturveränderungen und Investitionen

Das Oberleitungsorgan entscheidet über wesentliche Änderungen der Unternehmens- und Gruppenstruktur, wesentliche Veränderungen bei bedeutenden Tochtergesellschaften und andere Projekte von strategischer Bedeutung. 15

## B. Mitglieder des Oberleitungsorgans

### a) Allgemeine Voraussetzungen

Das Oberleitungsorgan verfügt in seiner Gesamtheit über hinreichende Führungskompetenz sowie die nötigen Fachkenntnisse und Erfahrung im Bank- und Finanzbereich. Es ist genügend diversifiziert, damit nebst den Hauptgeschäftsfeldern sämtliche zentralen Bereiche wie das Finanz- und Rechnungswesen sowie das Risikomanagement kompetent vertreten sind. 16

### b) Unabhängigkeit

Das Oberleitungsorgan besteht mindestens zu einem Drittel aus unabhängigen Mitgliedern. Die FINMA kann in begründeten Fällen, etwa bei inländischen Finanzgruppen, Ausnahmen bewilligen. 17

Ein Mitglied des Oberleitungsorgans gilt als unabhängig, wenn es: 18

- nicht in anderer Funktion beim Institut beschäftigt ist und dies auch nicht innerhalb der letzten 2 Jahre gewesen ist; 19
- innerhalb der letzten 2 Jahre nicht bei der Prüfgesellschaft des Instituts als für das Institut verantwortlicher leitender Prüfer beschäftigt gewesen ist; 20
- keine geschäftliche Beziehung zum Institut unterhält, welche aufgrund ihrer Art oder ihres Umfangs zu einem Interessenkonflikt führt; und 21
- nicht qualifizierter Beteiligter (im Sinne von Art. 3 Abs. 2 Bst. c$^{bis}$ BankG und Art. 10 Abs. 2 Bst. d BEHG) des Instituts ist und auch keinen solchen vertritt. 22

Von Kantonen, Gemeinden oder anderen kantonalen oder kommunalen Anstalten des öffentlichen Rechts in das Oberleitungsorgan von Kantonal- oder Kommunalbanken entsandte bzw. gewählte Mitglieder gelten im Sinne von Rz 18–22 als unabhängig, sofern sie: 23

- nicht der kantonalen oder kommunalen Regierung oder Verwaltung, bzw. einer anderen kantonalen oder kommunalen Körperschaft des öffentlichen Rechts angehören, und 24
- von ihrem Wahlorgan keine Instruktionen für die Tätigkeit als Mitglied des Oberleitungsorgans entgegennehmen. 25

## C. Grundsätze der Mandatsführung

Jedes Mitglied des Oberleitungsorgans widmet seinem Mandat genügend Zeit und wirkt aktiv an der strategischen Unternehmensführung mit. Es hat das Mandat persönlich auszuüben und sich über den ordentlichen Sitzungsrhythmus hinaus für Krisensituationen oder Notfälle dauernd bereitzuhalten. 26

Das Oberleitungsorgan legt das Anforderungsprofil seiner Mitglieder, seines Präsidenten und allfälliger Ausschussmitglieder sowie des Vorsitzenden der Geschäftsleitung fest. Es genehmigt und beurteilt periodisch das Anforderungsprofil der übrigen Mitglieder der Geschäftsleitung, des CRO und des Leiters der internen Revision. Es stellt die Nachfolgeplanung sicher. 27

Das Oberleitungsorgan beurteilt mindestens einmal jährlich, allenfalls unter Beiziehung eines Dritten, kritisch seine eigene Leistung (Zielerreichung und Arbeitsweise) und hält die Ergebnisse schriftlich fest. 28

Das Oberleitungsorgan regelt den Umgang mit Interessenkonflikten. Bestehende und frühere Interessenbindungen sind offenzulegen. Lässt sich ein Interessenkonflikt nicht vermeiden, trifft das Institut geeignete Massnahmen zu dessen wirksamer Begrenzung oder Beseitigung. 29

## D. Arbeitsteilung und Ausschüsse

### a) Rolle des Präsidenten

Der Präsident übt den Vorsitz über das Gesamtgremium aus und vertritt das Oberleitungsorgan nach innen und aussen. Er prägt die Strategie, Kommunikation und Kultur des Unternehmens massgeblich mit. 30

### b) Ausschüsse

Institute der Aufsichtskategorien 1–3 haben einen Prüf- und einen Risikoausschuss einzurichten. Institute der Aufsichtskategorie 3 dürfen diese auch in einem gemischten Ausschuss vereinen. Systemrelevante Institute haben mindestens auf Gruppenebene einen Vergütungs- und Nominationsausschuss einzusetzen. Die Ausschüsse sorgen für eine angemessene Berichterstattung an das gesamte Oberleitungsorgan. 31

Der Prüfausschuss soll sich von andern Ausschüssen personell hinreichend unterscheiden. 32

Die Mehrheit der Mitglieder des Prüf- und Risikoausschusses soll grundsätzlich unabhängig (vgl. Rz 18–25) sein. Der Präsident des Oberleitungsorgans soll grundsätzlich weder Mitglied des Prüfausschusses noch Vorsitzender des Risikoausschusses sein. Die Ausschüsse verfügen in ihrer Gesamtheit über hinreichende Kenntnisse und Erfahrung im Aufgabenbereich des entsprechenden Ausschusses. 33

**c) Aufgaben des Prüfausschusses**

Die Aufgaben umfassen insbesondere: 34

- die Ausarbeitung von allgemeinen Richtlinien zur internen Revision und zur finanziellen Berichterstattung zuhanden des gesamten Oberleitungsorgans; 35
- die Überwachung und Beurteilung der finanziellen Berichterstattung und der Integrität der Finanzabschlüsse, einschliesslich deren Besprechung mit dem für das Finanz- und Rechnungswesen verantwortlichen Geschäftsleitungsmitglied, mit dem leitenden Revisor sowie dem Leiter der internen Revision; 36
- die Überwachung und Beurteilung der Wirksamkeit der internen Kontrolle, namentlich auch der Risikokontrolle und der *Compliance*-Funktion, und der internen Revision, soweit diese Aufgabe nicht durch den Risikoausschuss wahrgenommen wird; 37
- die Überwachung und Beurteilung der Wirksamkeit und Unabhängigkeit der Prüfgesellschaft sowie deren Zusammenwirken mit der internen Revision, einschliesslich Besprechung der Prüfberichte mit dem leitenden Prüfer; 38
- die Würdigung des Prüfplans, des Prüfrhythmus und der Prüfergebnisse der internen Revision und der Prüfgesellschaft. 39

**d) Aufgaben des Risikoausschusses**

Die Aufgaben umfassen insbesondere: 40

- die Erörterung des Rahmenkonzepts für das institutsweite Risikomanagement und Unterbreitung der entsprechenden Empfehlungen an das gesamte Oberleitungsorgan; 41
- die Würdigung der Kapital- und Liquiditätsplanung und die diesbezügliche Berichterstattung an das gesamte Oberleitungsorgan; 42
- eine mindestens jährliche Beurteilung des Rahmenkonzepts für das institutsweite Risikomanagement und die Veranlassung der notwendigen Anpassungen; 43
- die Kontrolle, ob das Institut ein geeignetes Risikomanagement mit wirksamen Prozessen unterhält, die der jeweiligen Risikolage des Instituts gerecht werden; 44
- die Überwachung der Umsetzung der Risikostrategien, insbesondere im Hinblick auf deren Übereinstimmung mit der vorgegebenen Risikotoleranz und den Risikolimiten gemäss Rahmenkonzept für das institutsweite Risikomanagement. 45

Der Risikoausschuss erhält vom CRO und andern relevanten Funktionsträgern regelmässig aussagekräftige Berichte zu den jeweiligen Aspekten des Rahmenkonzepts für das institutsweite Risikomanagement (gemäss Rz 52–59) und dessen Einhaltung. 46

## V. Geschäftsleitung

### A. Aufgaben und Verantwortlichkeiten

Die Geschäftsleitung ist zuständig für die operative Geschäftstätigkeit im Einklang mit der Geschäftsstrategie sowie den Vorgaben und Beschlüssen des Oberleitungsorgans und ist insbesondere verantwortlich für: 47

- die Führung des Tagesgeschäfts, die operative Ertrags- und Risikosteuerung, einschliesslich das Bilanzstruktur- und Liquiditätsmanagement, sowie die Vertretung des Instituts gegenüber Dritten im operativen Bereich; 48
- die Antragstellung betreffend Geschäfte, die in die Zuständigkeit oder unter den Genehmigungsvorbehalt des Oberleitungsorgans fallen sowie den Erlass von Vorschriften zur Regelung des operativen Geschäftsbetriebs; 49
- die Ausgestaltung sowie den Unterhalt zweckmässiger interner Prozesse, eines angemessenen Managementinformationssystems und eines IKS sowie einer geeigneten Technologieinfrastruktur. 50

### B. Anforderungen an die Mitglieder der Geschäftsleitung

Die Geschäftsleitungsmitglieder verfügen als Gesamtorgan und als Funktionsverantwortliche über hinreichende Führungskompetenzen, die nötigen Fachkenntnisse und Erfahrungen im Bank- und Finanzbereich, um die Einhaltung der Bewilligungsvoraussetzungen im Rahmen der operativen Geschäftstätigkeiten angemessen sicherzustellen. 51

## VI. ~~Rahmenkonzept für das~~ Risikopolitik und Grundzüge des institutsweiten Risikomanagements

~~Das Rahmenkonzept für das~~ Die Risikopolitik und die Grundzüge des institutsweiten Risikomanagements ~~wird~~ werden von der Geschäftsleitung ausgearbeitet, ~~und~~ durch das Oberleitungsorgan verabschiedet und in geeigneter Form dokumentiert. 52*

~~Das Rahmenkonzept beinhaltet d~~Die Risikopolitik~~,~~ und die Grundzüge des institutsweiten Risikomanagements regeln den Umgang mit den wesentlichen Risiken, die Risikotoleranz und die darauf basierenden Risikolimiten in allen wesentlichen Risikokategorien. 53*

Institute der Aufsichtskategorien 1–3 haben namentlich f~~F~~olgenden Aspekten ~~ist im Rahmenkonzept~~ Rechnung zu tragen: 54*

- einheitliche Kategorisierung[2] der wesentlichen Risiken zur Gewährleistung der Konsistenz mit den Zielsetzungen im Risikomanagement; 55

[2] Nach Art, Typ und Ebene sowie in Anlehnung an die aufsichtsrechtlichen Definitionen gemäss ERV.

- Präzisierung des möglichen Verlusts aus diesen wesentlichen Risikokategorien; 56

- Definition und Einsatz der Instrumente sowie der organisatorischen Strukturen zur Identifikation, Analyse, Bewertung, Bewirtschaftung, Überwachung der wesentlichen Risikokategorien und der Berichterstattung; 57

- Ausgestaltung einer Dokumentation, die eine angemessene Überprüfung der Festlegung der Risikotoleranz sowie der entsprechenden Risikolimiten ermöglicht; 58

- Bestimmungen zur Risikodatenaggregation und -berichterstattung bei Instituten der Aufsichtskategorien 1–3. Bei systemrelevanten Instituten müssen diese Bestimmungen insbesondere Angaben über die Datenarchitektur und IT-Infrastruktur beinhalten, die eine aggregierte und zeitnahe Risikoanalyse und -bewertung sowie Risikodatenaggregation und -berichterstattung über sämtliche wesentlichen Risikokategorien des Instituts sowohl unter normalen Bedingungen wie auch in Stressperioden erlaubt. 59

## VII. Internes Kontrollsystem

Im Rahmen des IKS bestehen mindestens zwei Kontrollinstanzen: die ertragsorientierten Geschäftseinheiten und die von ihnen unabhängigen Kontrollinstanzen. 60

### A. Ertragsorientierte Geschäftseinheiten

Die ertragsorientierten Geschäftseinheiten nehmen ihre Kontrollfunktion im Rahmen des Tagesgeschäfts durch die Bewirtschaftung der Risiken, insbesondere durch deren direkte Überwachung, Steuerung und Berichterstattung wahr. 61

### B. Unabhängige Kontrollinstanzen

Die unabhängigen Kontrollinstanzen überwachen die Risiken sowie die Einhaltung gesetzlicher, regulatorischer und interner Vorschriften. Institutsspezifisch können verschiedene unabhängige Kontrollinstanzen eingerichtet werden, die aber mindestens die Aufgaben und Verantwortlichkeiten der Risikokontrolle (Rz 69–76) und der *Compliance*-Funktion (Rz 77–81) abdecken. 62

Das Vergütungssystem für unabhängige Kontrollinstanzen darf keine Anreize setzen, die zu Interessenkonflikten mit den Aufgaben dieser Instanzen führen. 63

#### a) Einrichtung und Unterstellung

Die unabhängigen Kontrollinstanzen verfügen im Rahmen ihrer Aufgaben über uneingeschränkte Auskunfts-, Zugangs- und Einsichtsrechte und sind von den ertragsorientierten Geschäftseinheiten unabhängig in die Gesamtorganisation bzw. in das IKS einzugliedern. Sie sind mit angemessenen Ressourcen und Kompetenzen auszustatten. 64

Das Institut bestimmt innerhalb der Geschäftsleitung eine Person bzw. mehrere Personen, die für die unabhängigen Kontrollinstanzen zuständig ist bzw. sind. 65

Es stellt sicher, dass die unabhängigen Kontrollinstanzen über einen direkten Zugang zum Oberleitungsorgan verfügen. 66

Die Institute der Aufsichtskategorien 1–3 verfügen über eine eigenständige Risikokontrolle und *Compliance*-Funktion als unabhängige Kontrollinstanzen. Sie bestimmen einen CRO, der neben der Risikokontrolle auch für andere unabhängige Kontrollinstanzen zuständig sein kann. 67

Systemrelevante Institute bestimmen einen CRO, der Mitglied der Geschäftsleitung ist. 68

**b) Aufgaben und Verantwortlichkeiten der Risikokontrolle**

Die Risikokontrolle stellt die ~~umfassende und~~ systematische Überwachung und Berichterstattung von einzelnen wie auch aggregierten Risikopositionen sicher. Dies beinhaltet als Teil der quantitativen und qualitativen Analysen die Durchführung von Stresstests und Szenarioanalysen unter ungünstigen Geschäftsbedingungen. Banken im Kleinbankenregime haben mindestens Szenarioanalysen durchzuführen. 69*

Bei Instituten der Aufsichtskategorien 1–3 stellt die Risikokontrolle zudem die angemessene Umsetzung der Bestimmungen zu Risikodatenaggregation und -berichterstattung gemäss Rz 59 sicher. 70

Die Risikokontrolle überwacht insbesondere in Abstimmung mit dem im Rahmenkonzept für das institutsweite Risikomanagement festgelegten Risikotoleranz und den Risikolimiten das Risikoprofil des Instituts. 71

In die Verantwortung der Risikokontrolle fallen zudem die Ausarbeitung und der Betrieb von adäquaten Risikoüberwachungssystemen, die Vorgabe und Anwendung von Grundlagen und Methoden für die Risikoanalyse und -bewertung (z.B. Bewertungs- und Aggregationsmethoden, Validierung von Modellen) sowie die Überwachung von Systemen für die Einhaltung von aufsichtsrechtlichen Vorschriften (insbesondere Eigenmittel-, Risikoverteilungs- und Liquiditätsvorschriften). 72

Die Risikokontrolle wird bei der Entwicklung von neuen oder erweiterten Produktekategorien, Dienstleistungen, Geschäfts- oder Marktbereichen sowie bei wesentlichen oder komplexen Transaktionen angemessen einbezogen. 73

Die Risikokontrolle nimmt aktiv am Prozess der Festlegung der Risikolimiten teil und stellt dabei sicher, dass die Risikolimiten insbesondere im Einklang mit der Risikotoleranz stehen und mit den Ergebnissen aus den Stresstests abgestimmt und so gesetzt sind, dass sie für die Geschäftsleitung ein operativ wirksames Steuerungsinstrument darstellen. 74

Die Risikokontrolle erstattet der Geschäftsleitung mindestens halbjährlich und dem Oberleitungsorgan mindestens jährlich Bericht über die Entwicklung des Risikoprofils des 75

Instituts und seine Tätigkeit gemäss Rz 69–78. Eine Kopie dieser Berichte ist der internen Revision und der Prüfgesellschaft zur Verfügung zu stellen.

Bei besonderen Entwicklungen informiert die Risikokontrolle zeitgerecht die Geschäftsleitung und die interne Revision und bei Sachverhalten von grosser Tragweite zusätzlich das Oberleitungsorgan. 76

**c) Aufgaben und Verantwortlichkeiten der *Compliance*-Funktion**

Die Aufgaben und Verantwortlichkeiten der *Compliance*-Funktion umfassen mindestens die folgenden Tätigkeiten: 77

- jährliche Einschätzung des *Compliance*-Risikos der Geschäftstätigkeit des Instituts und Ausarbeitung eines risikoorientierten Tätigkeitsplans, der durch die Geschäftsleitung zu genehmigen ist. Der Tätigkeitsplan ist auch der internen Revision zur Verfügung zu stellen; 78

- zeitgerechte Berichterstattung an die Geschäftsleitung über wesentliche Veränderungen in der Einschätzung des *Compliance*-Risikos; 79

- jährliche Berichterstattung an das Oberleitungsorgan über die Einschätzung des *Compliance*-Risikos und die Tätigkeit der *Compliance*-Funktion. Eine Kopie der Berichterstattung ist der internen Revision und im Weiteren der Prüfgesellschaft zur Verfügung zu stellen; 80

- zeitgerechte Berichterstattung an die Geschäftsleitung und das Oberleitungsorgan über schwerwiegende Verletzungen der *Compliance* bzw. Sachverhalte von grosser Tragweite und Unterstützung der Geschäftsleitung bei der Wahl der zu treffenden Anordnungen oder Massnahmen. Die interne Revision ist entsprechend zu informieren. 81

## VIII. Interne Revision

### A. Einrichtung

Jedes Institut hat grundsätzlich eine interne Revision einzurichten. 82

Erscheint die Einrichtung einer betriebseigenen internen Revision als nicht angemessen, können die Aufgaben der internen Revision übertragen werden: 83

- der internen Revision der Muttergesellschaft oder der internen Revision einer anderen Gruppengesellschaft, sofern diese eine Bank, ein Effektenhändler oder ein anderer staatlich beaufsichtigter Finanzintermediär (z.B. Versicherungsunternehmen) ist (für ausländische Banken im Rahmen von Art. 4$^{quinquies}$ BankG); 84

- einer zweiten Prüfgesellschaft, welche von der Prüfgesellschaft des Instituts unabhängig ist; oder 85

- an eine Gruppengesellschaft oder einen unabhängigen Dritten, vorausgesetzt die Prüfgesellschaft bestätigt dessen professionelle Kompetenzen und angemessene technische und personelle Ressourcen. 86

## B. Unterstellung und Organisation

Die interne Revision ist dem Oberleitungsorgan oder dessen Prüfausschuss unterstellt und nimmt die ihr übertragenen Prüf- und Überwachungsaufgaben in unabhängiger Art und Weise wahr. Sie verfügt über ein uneingeschränktes Einsichts-, Auskunfts- und Prüfungsrecht innerhalb des Instituts und dessen konsolidierungspflichtigen Unternehmen gemäss Rz 98. 87

Die interne Revision ist der Grösse, Komplexität und dem Risikoprofil des Instituts entsprechend auszugestalten und bildet organisatorisch eine selbständige und vom Geschäftsbetrieb unabhängige Einheit. 88

Die interne Revision hat die qualitativen Anforderungen des Schweizerischen Verbandes für interne Revision (SVIR) zu erfüllen. Die Arbeit der internen Revision richtet sich nach den International Standards for the Professional Practice of Internal Auditing des Institute of Internal Auditors (IIA). 89

Das Entschädigungssystem für Mitarbeiter der internen Revision darf keine Anreize setzen, die zu Interessenkonflikten führen. 90

## C. Aufgaben und Verantwortlichkeiten

Die interne Revision erbringt unabhängige Prüfungen und Beurteilungen bezüglich der Angemessenheit und Wirksamkeit der Unternehmensorganisation und Geschäftsprozesse sowie insbesondere bezüglich des IKS und des Risikomanagements des Instituts. 91

Sie führt mindestens jährlich eine umfassende Risikobeurteilung der wesentlichen Risikokategorien des Instituts gemäss Rz 53 durch, wobei sie externe Entwicklungen (z.B. wirtschaftliches Umfeld, regulatorische Änderungen) und interne Faktoren (z.B. wesentliche Projekte, Geschäftsausrichtung) angemessen berücksichtigt. Banken im Kleinbankenregime können die Beurteilung alle zwei Jahre durchführen, sofern sich das Risikoprofil des Instituts nicht wesentlich verändert hat. 92*

Ausgehend von dieser Risikobeurteilung und sich anderweitig ergebenden Prüfbedürfnissen legt die interne Revision die Prüfziele und -planung für die nächste Prüfperiode fest und lässt diese sowie wesentliche Änderungen durch das Oberleitungsorgan oder dessen Prüfausschuss genehmigen. 93

Die interne Revision veranlasst, dass die Geschäftsleitung und die Prüfgesellschaft über die Risikobeurteilung und die Prüfziele informiert ist. 94

Die interne Revision erstattet zeitgerecht über alle wichtigen Feststellungen einer Prüfung schriftlich Bericht an das Oberleitungsorgan oder dessen Prüfausschuss und an die Geschäftsleitung. 95

Mindestens jährlich erstellt die interne Revision einen schriftlichen Bericht über die wesentlichen Prüfergebnisse und wichtigen Tätigkeiten in der Prüfperiode und unterbreitet diesen mit den entsprechenden Schlussfolgerungen dem Oberleitungsorgan oder dessen Prüfausschuss, der Geschäftsleitung und der Prüfgesellschaft zur Kenntnisnahme. 96

Im Weiteren informiert die interne Revision oder eine andere unabhängige Instanz im Institut (z.B. *Compliance*-Funktion oder Risikokontrolle) das Oberleitungsorgan oder dessen Prüfausschuss mindestens halbjährlich über die Beseitigung wesentlicher Mängel bzw. den Stand der Umsetzung von Empfehlungen der internen Revision und der Prüfgesellschaft. 97

## IX. Gruppenstrukturen

Dieses Rundschreiben gilt für Finanzgruppen und -konglomerate („Gruppen“) sinngemäss. 98

Die Gruppen müssen die Aufgaben und Verantwortlichkeiten der Einheiten mit Gesamtverantwortung für die Gruppenführung regeln. Die Vorgaben müssen unter Berücksichtigung der Geschäftstätigkeit und der wesentlichen Risiken auf Gruppen- und Einzelinstitutsebene die effiziente und einheitliche Steuerung der Gruppe gewährleisten, den entsprechenden Informationsaustausch erlauben, den rechtlichen und organisatorischen Strukturen Rechnung tragen und die Aufgaben und Verantwortlichkeiten sowie die erforderliche Unabhängigkeit der jeweiligen Führungsebenen definieren. Dabei sind im Besonderen die Risiken zu berücksichtigen, welche sich aus dem Zusammenschluss mehrerer Unternehmen zu einer wirtschaftlichen Einheit ergeben. 99

## X. Übergangsbestimmungen

Die Umsetzung folgender Anforderungen hat bis spätestens ein Jahr nach Inkrafttreten zu erfolgen: 100

- Die Umsetzung der Drittelsregel zur Unabhängigkeit des Oberleitungsorgans gemäss Rz 17. 101
- Die Einführung eines Prüfausschusses und eines davon separaten Risikoausschusses für Institute der Aufsichtskategorien 1–3 gemäss Rz 31. 102
- Die Erstellung und Genehmigung eines Rahmenkonzepts für das institutsweite Risikomanagement gemäss Rz 52–59. 103
- Das Führen einer separaten CRO-Position, u.a. als Teil der Geschäftsleitung für systemrelevante Institute gemäss Rz 67 und 68. 104

Für die Erfüllung der weiterführenden Bestimmungen zu Risikodatenaggregation und -berichterstattung gemäss Rz 59 für systemrelevante Banken gilt der jeweils spätere Zeitpunkt aus: 105

- der Inkraftsetzung dieses Rundschreibens, oder
- einer dreijährigen Übergangsfrist nach Bezeichnung als systemrelevante Bank gemäss Art. 8 Abs. 3 BankG.

# Verzeichnis der Änderungen

**Das Rundschreiben wird wie folgt geändert:**

Diese Änderungen wurden am … 2019 beschlossen und treten am … in Kraft

Geänderte Rz