

Rundschreiben 2016/xx

Corporate Governance - Banken

Corporate Governance, Risikomanagement und interne Kontrollen bei Banken

Referenz: FINMA-RS 16/xx „Corporate Governance – Banken“
 Erlass: ...
 Inkraftsetzung: 1. Juli 2016
 Konkordanz: vormals FINMA-RS 08/24 „Überwachung und interne Kontrollen Banken“ vom 20. November 2008
 Rechtliche Grundlagen: FINMAG Art. 7 Abs. 1 Bst. b
 BankG Art. 3 Abs. 2 Bst. a, 3b–3g, 4^{quinquies}
 BankV Art. 11 Abs. 2, 12
 BEHG Art. 10 Abs. 2 Bst. a und Abs. 5, 14
 BEHV Art. 19, 20
 ERV Art. 7–12
 Anhang: n/a

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	Vertreter	Vertreter ausl. KKA	Andere Intermediäre	SRO	DUF1	SRO-Beaufichtigte	Prüfungsgesellschaften	Ratingagenturen	
X	X						X															

I. Gegenstand	Rz	1-2
II. Begriffe	Rz	3-8
III. Geltungsbereich (Proportionalitätsprinzip)	Rz	9
IV. Oberleitungsorgan	Rz	10-52
A. Aufgaben und Verantwortlichkeiten	Rz	10-17
a) Geschäftsstrategie und Risikopolitik	Rz	12
b) Organisation	Rz	13
c) Finanzen	Rz	14
d) Personelle und weitere Ressourcen	Rz	15
e) Überwachung und Kontrolle	Rz	16
f) Strukturveränderungen und Investitionen	Rz	17
B. Mitglieder des Oberleitungsorgans	Rz	18-29
a) Allgemeine Voraussetzungen	Rz	18-19
b) Unabhängigkeit	Rz	20-29
C. Grundsätze der Mandatsführung	Rz	30-33
D. Arbeitsteilung und Ausschüsse	Rz	34-52
a) Rolle des Präsidenten	Rz	34-35
b) Ausschüsse	Rz	36-39
c) Aufgaben des Prüfausschusses	Rz	40-45
d) Aufgaben des Risikoausschusses	Rz	46-52
V. Geschäftsleitung	Rz	53-65
A. Aufgaben und Verantwortlichkeiten	Rz	53-63
B. Anforderungen an die Mitglieder der Geschäftsleitung	Rz	64-65
VI. Rahmenkonzept für das institutsweite Risikomanagement	Rz	66-78
VII. Internes Kontrollsystem	Rz	79-103
A. Ertragsorientierte Geschäftseinheiten	Rz	81
B. Unabhängige Kontrollinstanzen	Rz	82-103

a)	Einrichtung und Unterstellung	Rz	83-88
b)	Aufgaben und Verantwortlichkeiten der Risikokontrolle	Rz	89-98
c)	Aufgaben und Verantwortlichkeiten der Compliance-Funktion	Rz	99-103
VIII.	Interne Revision	Rz	104-124
A.	Einrichtung	Rz	104-109
B.	Unterstellung und Organisation	Rz	110-116
C.	Aufgaben und Verantwortlichkeiten	Rz	117-124
IX.	Gruppenstrukturen	Rz	125-127
X.	Offenlegung	Rz	128-143
XI.	Inkrafttreten und Übergangsbestimmungen	Rz	144-145

Anhörung

Farbliche Unterlegung zur Textherkunft:

Aus dem FINMA-RS 08/24 (mit sprachlichen Anpassungen)

Aus den FINMA-RS 08/21 und 08/32 (mit sprachlichen Anpassungen)

Internationale Richtlinien (insbesondere BCBS Corporate Governance Principles)

FAQ Oberleitungsorgan

I. Gegenstand

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

1

Unter Corporate Governance werden im folgenden die Grundsätze und Strukturen verstanden, anhand derer ein Institut durch seine Organe gesteuert und kontrolliert wird. Corporate Governance bezweckt ein funktionales Gleichgewicht zwischen den verschiedenen Organen des Unternehmens („checks and balances“), eine ausreichende Transparenz der unternehmensinternen Vorgänge sowie die Abstimmung der Zielsetzungen des Unternehmens mit den Erwartungen der verschiedenen Anspruchsgruppen.

2

II. Begriffe

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

3

Die Risikokontrolle überwacht als unabhängige Kontrollinstanz das Risikoprofil des Instituts und stellt die für die Risikoüberwachung notwendigen Risikoinformationen bereit.

4

Der Risikoappetit 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 bereit ist einzugehen. Der Risikoappetit wird sowohl pro jeweilige Risikokategorie als auch auf Institutsebene festgelegt.

5

Das Risikoprofil fasst auf Institutsebene und pro jeweilige Risikokategorie für einen bestimmten Zeitpunkt die jeweils eingenommenen Risikopositionen des Instituts zusammen. 6

Das Interne Kontrollsystem umfasst die vom Institut definierten Vorgänge, Methoden und Massnahmen, die dazu dienen, eine angemessene Sicherheit in Bezug auf die Wirksamkeit von operativen Geschäftsprozessen, die Zuverlässigkeit der finanziellen Berichterstattung, die Minderung von Risiken und die Befolgung von Gesetzen und Vorschriften zu gewährleisten. 7

Die Compliance-Funktion kontrolliert die Einhaltung regulatorischer und interner Vorschriften sowie die Beachtung marktüblicher Standards und Standesregeln. 8

III. Geltungsbereich (Proportionalitätsprinzip)

Das Rundschreiben gilt grundsätzlich für alle Institute gemäss Rz 1. Die Anforderungen sind im Einzelfall abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen. In den Randziffern wird vermerkt, wenn Institute der Aufsichtskategorien 4 und 5 generell von der Anwendung ausgenommen sind. Die FINMA kann im Einzelfall Erleichterungen oder Verschärfungen anordnen. 9

IV. Oberleitungsorgan

A. Aufgaben und Verantwortlichkeiten

Das Organ für die Oberleitung, Aufsicht und Kontrolle entwickelt die strategischen Ziele, legt die Mittel fest, um diese Ziele zu erreichen und kontrolliert die Geschäftsleitung im Hinblick auf die Verfolgung dieser Ziele. 10

Seine Aufgaben umfassen insbesondere: 11

a) Geschäftsstrategie und Risikopolitik

Das Oberleitungsorgan entscheidet auf Antrag der Geschäftsleitung über die Geschäftsstrategie, die wesentlichen Unternehmensziele und das Unternehmensleitbild und erlässt Leitsätze zur Unternehmenskultur und den Unternehmenswerten. Es genehmigt das Rahmenkonzept für das institutsweite Risikomanagement und trägt die Verantwortung für die Reglementierung, Einrichtung und Überwachung eines wirksamen Risikomanagements sowie die Steuerung der Gesamtrisiken. Es versteht die Unternehmensstrukturen und Risiken der einzelnen Geschäftsfelder des Instituts. 12

b) Organisation

Das Oberleitungsorgan ist verantwortlich für eine angemessene Unternehmensorganisation mit ausgewogenen „Checks and Balances“. Es erlässt die für 13

den Geschäftsbetrieb und die für die Kompetenzverteilung und Überwachung notwendigen Reglemente, insbesondere das Organisations- und Geschäftsreglement, und Weisungen.

c) Finanzen

Das Oberleitungsorgan trägt die oberste Verantwortung für die finanzielle Lage und Entwicklung des Instituts. Es sorgt für eine wirksame Ausgestaltung des Rechnungswesens und der Finanzkontrolle und genehmigt periodisch die von der Geschäftsleitung erstellte Kapital- und Liquiditätsplanung. Es verabschiedet den Geschäftsbericht, das Jahresbudget, die Zwischenabschlüsse sowie die finanziellen Jahresziele. 14

d) Personelle und weitere Ressourcen

Das Oberleitungsorgan ist verantwortlich für die angemessene Ausstattung des Instituts mit personellen und weiteren Ressourcen (z.B. Infrastruktur, IT). Es verabschiedet die Personal- und Vergütungspolitik und entscheidet über die Wahl und Abberufung ihrer Ausschussmitglieder, der Mitglieder der Geschäftsleitung, deren Vorsitzende sowie weiterer Personen in leitenden Kontroll- und Schlüsselfunktionen (z.B. Chief Risk Officer, Chief Compliance Officer, Head IT). 15

e) Überwachung und Kontrolle

Das Oberleitungsorgan übt die Oberaufsicht über die Geschäftsleitung aus und stellt die Compliance des Instituts sicher. Es sorgt für ein geeignetes Risiko- und Kontrollumfeld innerhalb des Instituts. Es richtet ein wirksames internes Kontrollsystem ein, bestellt und überwacht die interne Revision, bestimmt die aufsichtsrechtliche Prüfgesellschaft und würdigt deren Berichte. Das Oberleitungsorgan oder sein zuständiger Ausschuss überwacht und beurteilt die interne Revision und vergewissert sich periodisch, dass diese über angemessene Ressourcen und Kompetenzen sowie Unabhängigkeit und Objektivität verfügt, um ihre Prüfaufgaben beim Institut wahrzunehmen. 16

f) Strukturveränderungen und Investitionen

Das Oberleitungsorgan entscheidet über Änderungen der Unternehmensstruktur, Neugründungen und Schliessungen von bedeutenden Tochtergesellschaften und Niederlassungen, bedeutende Akquisitionen und Veräusserungen, Fusionen, Funktionsauslagerungen, wesentliche Veränderungen bei bedeutenden Tochtergesellschaften und andere Projekte von strategischer Bedeutung. 17

B. Mitglieder des Oberleitungsorgans

a) Allgemeine Voraussetzungen

Die Mitglieder des Oberleitungsorgans geniessen einen guten Ruf und bieten Gewähr für eine einwandfreie Geschäftstätigkeit. Sie sind integer und verfügen als Gesamtorgan über hinreichende Führungskompetenz sowie die nötigen Fachkenntnisse und Erfahrung im 18

Bank- und Finanzbereich. Das Oberleitungsorgan ist genügend breit aufgestellt, so dass neben den Hauptgeschäftsfeldern sämtliche weitere zentralen Bereiche wie Finanz- und Rechnungswesen, Risikomanagement, Controlling, Compliance und IT kompetent vertreten sind. Jedes einzelne Mitglied verfügt über mindestens eine vertiefte Kernkompetenz, welche zu einer ausgewogenen Strukturierung des Gesamtorgans beiträgt.

Das Oberleitungsorgan ist insgesamt je nach geographischer Geschäftsausrichtung mit den lokalen, regionalen, nationalen und internationalen Märkten und dem entsprechenden regulatorischen Umfeld hinreichend vertraut. 19

b) Unabhängigkeit

Die Mitglieder des Oberleitungsorgans ordnen ihre persönlichen und geschäftlichen Verhältnisse so, dass Interessenkonflikte mit dem Institut möglichst vermieden werden. Die Mitglieder des Oberleitungsorgans gehören nicht gleichzeitig der Geschäftsleitung an. Sie üben grundsätzlich keine operative Tätigkeit für das Institut aus. 20

Das Oberleitungsorgan verfügt über eine genügende Anzahl unabhängiger Mitglieder, die kein besonderes Näheverhältnis zum Institut aufweisen. Es besteht mindestens zu einem Drittel aus unabhängigen Mitgliedern. Die FINMA kann in begründeten Fällen Ausnahmen bewilligen. 21

Ein Mitglied des Oberleitungsorgans gilt als unabhängig, wenn es mindestens die folgenden Kriterien erfüllt: 22

- nicht in anderer Funktion beim Institut beschäftigt ist und dies auch nicht innerhalb der letzten 2 Jahre gewesen ist; 23
- innerhalb der letzten 2 Jahre nicht bei der Prüfgesellschaft des Instituts als für das Institut verantwortlicher leitender Prüfer beschäftigt gewesen ist; und 24
- keine geschäftliche Beziehung zum Institut aufweist, welche aufgrund ihrer Art oder ihres Umfangs zu einem Interessenkonflikt führt. 25

Zudem sollte ein massgeblicher Teil des Oberleitungsorgans nicht am Institut qualifiziert beteiligt sein oder einen qualifizierten Beteiligten vertreten. Die Gläubigerinteressen auf Ebene des Einzelinstituts haben gegenüber abweichenden Eigentümer- oder Gruppeninteressen Vorrang. 26

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 als unabhängig, sofern sie: 27

- nicht der kantonalen oder kommunalen Regierung oder Verwaltung, respektive einer anderen kantonalen oder kommunalen Körperschaft des öffentlichen Rechts angehört. 28

ren, und

- von ihrem Wahlorgan keine Instruktionen für die Tätigkeit als Mitglied des Oberleitungsorgans entgegennehmen. 29

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. Anzahl und Art weiterer Mandate und Tätigkeiten sind mit den konkreten Anforderungen des Oberleitungsmandats so abzustimmen, dass dieses mit der gebotenen Sorgfalt bewältigt werden kann. 30

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 sowie weiterer Schlüsselpersonen. Es stellt die Nachfolgeplanung sicher. 31

Das Oberleitungsorgan beurteilt mindestens einmal jährlich, allenfalls unter Beiziehung eines Dritten, kritisch seine eigene Leistung (Zielerreichung und Arbeitsweise) und hält die Ergebnisse schriftlich fest. Seine Mitglieder bilden sich gezielt weiter und sind über die laufenden Entwicklungen in den relevanten Bereichen, einschliesslich des regulatorischen Umfelds, informiert. Neue Mandatsträger werden in ihre Aufgaben und Pflichten eingeführt. 32

Das Oberleitungsorgan regelt den Umgang mit Interessenkonflikten und legt Ausstandspflichten fest. Bestehende und frühere Interessenbindungen sind offenzulegen und Interessenkonflikte wirksam zu beseitigen. Lässt sich ein Interessenkonflikt auf Dauer nicht vermeiden, ist das Mandat niederzulegen. 33

D. Arbeitsteilung und Ausschüsse

a) Rolle des Präsidenten

Der Präsident ist eine Persönlichkeit mit ausgewiesener Integrität, Führungsstärke und Urteilkraft. Er prägt die Strategie, Kommunikation und Kultur des Unternehmens entscheidend mit. 34

Er übt den Vorsitz über das Gesamtgremium aus und trägt die Verantwortung für dessen ordnungsgemässes Funktionieren. Er vertritt das Oberleitungsorgan nach innen und aussen. Er steht in regelmässigem Dialog mit dem Vorsitzenden und anderen Mitgliedern der Geschäftsleitung, den Personen in leitenden Kontrollfunktionen und ist für die Aufbereitung und Steuerung des Informationsflusses innerhalb des Oberleitungsorgans verantwortlich. 35

b) Ausschüsse

Zu seiner Unterstützung kann das Oberleitungsorgan aus seiner Mitte Ausschüsse einrichten oder Aufgaben einzelnen Mitgliedern übertragen. Institute der Aufsichtskategorien 1 - 3 müssen je einen separaten Prüfausschuss und Risikoausschuss einrichten. Systemrelevante Banken müssen über weitere Ausschüsse, jedoch zwingend über einen Vergütungs- und Nominationsausschuss verfügen, der das Oberleitungsorgan bei der Festlegung der Vergütungspolitik, der Erarbeitung von Grundsätzen zur Auswahl der obersten Führungskräfte, der Vorbereitung und Durchführung von Personalentscheiden sowie bei der Nachfolgeplanung unterstützt und im Weiteren die Umsetzung der Vergütungspolitik überwacht. Die Ausschüsse sorgen für eine angemessene Berichterstattung an das gesamte Oberleitungsorgan.

36

Der Prüfausschuss soll sich von andern Ausschüssen personell hinreichend unterscheiden.

37

Die Mehrheit der Mitglieder des Prüf-, Risiko- und Nominationsausschusses muss grundsätzlich unabhängig (vgl. Rz 20ff) sein. Die FINMA kann bei Finanzgruppen Erleichterungen gewähren. Der Präsident des Oberleitungsorgans soll grundsätzlich weder dem Prüfausschuss angehören noch Vorsitzender eines andern Ausschusses sein. Die Mitglieder sämtlicher Ausschüsse müssen insgesamt über ausgewiesene Kenntnisse und Erfahrung im Aufgabenbereich des entsprechenden Ausschusses verfügen.

38

Aufgaben und Funktionsweise von ständigen Ausschüssen sind vom Oberleitungsorgan in einem Organisationsreglement zu regeln.

39

c) Aufgaben des Prüfausschusses

Die Aufgaben umfassen insbesondere die:

40

- Ausarbeitung von allgemeinen Richtlinien zur internen Revision und zur finanziellen Berichterstattung zuhanden des gesamten Oberleitungsorgans;
- 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;
- Überwachung und Beurteilung der Wirksamkeit der internen Kontrolle, namentlich auch der Risikokontrolle und der Compliance-Funktion, und der internen Revision;
- Überwachung und Beurteilung der Wirksamkeit und Unabhängigkeit der Prüfgesellschaft sowie deren Zusammenwirken mit der internen Revision, einschliesslich Besprechung der Prüfberichte mit dem leitenden Prüfer;
- Würdigung des Prüfplans, des Prüfrhythmus und der Prüfergebnisse der internen Re-

41

42

43

44

45

vision und der Prüfgesellschaft.

d) Aufgaben des Risikoausschusses

Die Aufgaben umfassen insbesondere die:	46
• Erörterung des Rahmenkonzepts für das institutsweite Risikomanagement und Unterbreitung der entsprechenden Empfehlungen an das gesamte Oberleitungsorgan;	47
• Würdigung der Kapital- und Liquiditätsplanung und diesbezügliche Berichterstattung an das gesamte Oberleitungsorgan;	
• Mindestens jährliche Beurteilung des Rahmenkonzepts für das institutsweite Risikomanagement und Veranlassung der notwendigen Anpassungen;	48
• Kontrolle, ob das Institut ein geeignetes Risikomanagement mit wirksamen Prozessen unterhält, die der jeweiligen Risikolage des Instituts gerecht werden;	49
• Überwachung der Umsetzung der Risikostrategien, insbesondere im Hinblick auf deren Übereinstimmung mit dem vorgegebenen Risikoappetit und den Risikolimiten gemäss Rahmenkonzept für das institutsweite Risikomanagement.	50
Der Risikoausschuss erhält vom Chief Risk Officer (CRO) und andern relevanten Funktionsträgern regelmässig aussagekräftige Berichte zu den jeweiligen Aspekten des Rahmenkonzepts für das institutsweite Risikomanagement (gemäss Rz 66ff.) und dessen Einhaltung.	51
Zwischen Prüfausschuss und Risikoausschuss sind geeignete Informationsflüsse einzurichten, welche eine wirksame gegenseitige Abstimmung und eine angemessene Reaktion auf Veränderungen im Risikoprofil des Instituts ermöglichen.	52

V. Geschäftsleitung

A. Aufgaben und Verantwortlichkeiten

Die Geschäftsleitung ist zuständig für die operative Geschäftstätigkeit im Einklang mit der Geschäftsstrategie, dem Rahmenkonzept für das institutsweite Risikomanagement sowie den weiteren vom Oberleitungsorgan verabschiedeten Grundlagen, Geschäfts- und Organisationsvorschriften. Sie vollzieht die Beschlüsse des Oberleitungsorgans und ist für die Einhaltung der aufsichtsrechtlichen Vorschriften im Rahmen der operationellen Geschäftstätigkeit verantwortlich.	53
Die Geschäftsleitung ist insbesondere verantwortlich für:	54
• die Führung des Tagesgeschäfts und die Vertretung des Instituts gegenüber Dritten im operativen Bereich;	55

- die Antragstellung betreffend Geschäfte, die in die Zuständigkeit oder unter den Genehmigungsvorbehalt des Oberleitungsorgans fallen, namentlich die Ausarbeitung der Geschäftspolitik, des Rahmenkonzepts für das institutsweite Risikomanagement, des Unternehmensleitbildes und der Unternehmensziele; 56
- eine institutsweite Führungs- und Organisationsstruktur, in welcher Verantwortlichkeiten, Kompetenzen, Rechenschaftspflichten, Anordnungs- und Entscheidungsbefugnisse sowie eine geeignete Trennung von Funktionen sichergestellt sind; 57
- den Unterhalt eines Managementinformationssystems (MIS); hierbei sind Informationsflüsse festzulegen, um alle relevanten Informationen über das betriebliche Geschehen zu erheben und zu bearbeiten sowie dem Oberleitungsorgan in angemessener Form zur Verfügung zu stellen; 58
- die Ausgestaltung sowie den Unterhalt eines internen Kontrollsystems (IKS) gemäss Rz 79; 59
- die operative Ertrags- und Risikosteuerung, einschliesslich das Bilanzstrukturmanagement; 60
- den Erlass von Vorschriften zur Regelung des operativen Geschäftsbetriebs; 61
- eine Technologieinfrastruktur, deren Kapazitäten den aktuellen und längerfristigen Geschäftsbedürfnissen ausreichend Rechnung trägt und operationelle Risiken mindern kann, den üblichen Geschäftsbetrieb und Stresssituationen berücksichtigt sowie die Sicherheit, Integrität und Verfügbarkeit der Daten und Systeme gewährleistet; 62
- dass geplante Anpassungen der Geschäftstätigkeit, die sich namentlich durch die Errichtung von oder die Beteiligung an in- und ausländischen Gesellschaften oder Niederlassungen oder durch die Einführung von neuen Dienstleistungen, Finanzprodukten und -lösungen auszeichnen, den aufsichtsrechtlichen Vorschriften und internen Vorgaben entsprechen. 63

B. Anforderungen an die Mitglieder der Geschäftsleitung

Die Mitglieder der Geschäftsleitung geniessen einen guten Ruf und bieten Gewähr für eine einwandfreie Geschäftstätigkeit. Sie sind integer und verfügen als Gesamtorgan sowie als Funktionsverantwortliche über hinreichende Führungskompetenz, die nötigen Fachkenntnisse und Erfahrung im Bank- und Finanzbereich um die operative Geschäftstätigkeit angemessen sicherzustellen. Die Mitglieder der Geschäftsleitung tragen mit ihrem persönlichen Verhalten die Unternehmens- und Risikokultur des Instituts mit. 64

Die Geschäftsleitung ist insgesamt je nach geographischer Geschäftsausrichtung mit den lokalen, regionalen, nationalen und internationalen Märkten und dem entsprechenden regulatorischen Umfeld hinreichend vertraut. 65

VI. Rahmenkonzept für das institutsweite Risikomanagement

Das Rahmenkonzept für das institutsweite Risikomanagement wird von der Geschäftsleitung ausgearbeitet und durch das Oberleitungsorgan verabschiedet.	66
Es legt die Risikopolitik, den Risikoappetit sowie die Risikolimiten fest und hält dabei Art, Typ und Ebene der Risiken fest, welchen das Institut ausgesetzt ist und welche es einzugehen bereit ist.	67
Folgende Aspekte sind im Rahmenkonzept abzudecken:	68
<ul style="list-style-type: none"> • Einheitliche Kategorisierung der wesentlichen Risiken zur Gewährleistung von Konsistenz bei den Zielsetzungen im Risikomanagement, bei der Risikoidentifikation, Risikomessung, Risikobewirtschaftung, Risikoüberwachung und Risikoberichterstattung; 	69
<ul style="list-style-type: none"> • Präzisierung der institutsspezifischen Risiken und des möglichen Verlusts aus diesen Risiken, in Anlehnung an die aufsichtsrechtlichen Definitionen sowie Bestimmung und Einsatz der Instrumente, welche für die Identifikation, Messung, Bewirtschaftung und Überwachung sämtlicher Risikokategorien eingesetzt werden; 	70
<ul style="list-style-type: none"> • Festlegung des Risikoappetits und Risikolimiten in Bezug auf sämtliche Risikokategorien und Definition von Risikominderungsstrategien und -instrumenten; 	71
<ul style="list-style-type: none"> • Definition von Massnahmen, um Verletzungen der Risikolimiten rechtzeitig zu erkennen und zu beheben; 	72
<ul style="list-style-type: none"> • Einrichtung organisatorischer Strukturen für die Bewirtschaftung sämtlicher Risikokategorien, einschliesslich Kompetenzen, Rechenschaftspflichten und Berichtslinien; 	73
<ul style="list-style-type: none"> • Ausgestaltung einer Dokumentation, welche einen angemessenen unabhängigen Nachvollzug bzw. eine Überprüfung und Beurteilung der Festlegung des Risikoappetits sowie der Risikolimiten ermöglicht; 	74
<ul style="list-style-type: none"> • Unterhalt eines Risikoberichterstattungs- und Managementinformationssystems (MIS) für sämtliche Risikokategorien; 	75
<ul style="list-style-type: none"> • Pflicht zur zeitnahen und fortwährenden Überprüfung und allfälligen Anpassung des Rahmenkonzepts im Fall einer wesentlich veränderten Risikosituation durch eine eindeutig bezeichnete Organisationseinheit, die über genügend qualifiziertes Personal verfügt; 	76
<ul style="list-style-type: none"> • Vorgaben zur institutsweiten konsistenten Anwendung des Rahmenkonzepts, insbesondere alle neuen und wesentlichen bestehenden Produkte, Aktivitäten, Prozesse und Systeme betreffend; 	77
<ul style="list-style-type: none"> • Bestimmungen zur Risikodatenaggregation und Risikoberichterstattung bei systemrelevanten Banken. 	78

VII. Internes Kontrollsystem

Das Institut hat über ein adäquates, dokumentiertes internes Kontrollsystem, das auf Vorgaben, Prozessen und Systemen aufbaut, zu verfügen. Dieses soll namentlich die Identifikation, Messung, Bewirtschaftung und Überwachung der durch das Institut eingegangenen Risiken als integraler Bestandteil sämtlicher Arbeitsprozesse beinhalten. Im Weiteren sind Kontrollen vorzusehen, um insbesondere Verletzungen der Risikolimiten und Abweichungen von der festgelegten Risikopolitik frühzeitig zu erkennen. Im Rahmen dessen hat das Finanzinstitut angemessene Risikominderungs- und/oder Risikotransferstrategien zu implementieren.	79
Die Kontrollinstanzen umfassen mindestens drei verschiedene Bereiche des Instituts: die ertragsorientierten Geschäftseinheiten, die von den ertragsorientierten Geschäftseinheiten unabhängigen Kontrollinstanzen sowie die interne Revision.	80
A. Ertragsorientierte Geschäftseinheiten	
Die ertragsorientierten Geschäftseinheiten nehmen ihre Kontrollfunktion im Rahmen des Tagesgeschäfts durch die Bewirtschaftung von Risiken und insbesondere durch deren direkte Überwachung, Steuerung und Berichterstattung wahr.	81
B. Unabhängige Kontrollinstanzen	
Das Vergütungssystem für unabhängige Kontrollinstanzen darf keine Anreize setzen, die zu Interessenkonflikten mit den Aufgaben dieser Instanzen führen. Die Bemessung der variablen Vergütung dieser Personen darf nicht direkt vom Resultat der zu überwachenden Geschäftseinheiten, einzelner Produkte oder Transaktionen abhängen.	82
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 resp. in das interne Kontrollsystem einzugliedern.	83
Die unabhängigen Kontrollinstanzen sind mit angemessenen Ressourcen und Kompetenzen auszustatten. Jedes Institut hat zu gewährleisten, dass beruhend auf der Erfahrung und Qualifikation der Mitarbeiter eine effektive und risikoorientierte Beurteilung der ertragsorientierten Geschäftseinheiten sichergestellt wird. Die Mitarbeiter der unabhängigen Kontrollinstanzen sind diesbezüglich regelmässig aus- und weiterzubilden.	84
Das Institut bestimmt innerhalb der Geschäftsleitung eine Person bzw. mehrere Personen, die für die unabhängigen Kontrollinstanzen zuständig ist bzw. sind.	85

Das Institut stellt sicher, dass die unabhängigen Kontrollinstanzen über einen direkten und regelmässigen Zugang zum Oberleitungsorgan oder dessen Risikoausschuss verfügen.	86
Die Institute der Aufsichtskategorien 1 bis 3 verfügen über eine eigenständige Risikokontrolle und Compliance-Funktion als unabhängige Kontrollinstanzen. Sie bestimmen einen CRO, der für die Risikokontrolle zuständig ist.	87
Systemrelevante Banken bestimmen einen CRO, der Mitglied der Geschäftsleitung und ausschliesslich für die Risikokontrolle zuständig ist.	88
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.	89
Die Risikokontrolle überwacht insbesondere in Abstimmung mit dem im Rahmenkonzept für das institutsweite Risikomanagement festgelegten Risikoappetit und den Risikolimiten das Risikoprofil des Instituts.	90
Die Risikokontrolle stellt die für die Risikoüberwachung notwendigen Informationen bereit.	91
In die Verantwortung der Risikokontrolle fallen zudem die Ausarbeitung und Umsetzung von adäquaten Risikoüberwachungssystemen und deren Anpassung an neue Geschäftsaktivitäten und Finanzprodukte bzw. -dienstleistungen, die Vorgabe und Anwendung von Grundlagen und Methoden für die Risikomessung (z.B. Bewertungs- und Aggregationsmethoden, Validierung von Modellen) sowie die Überwachung von Systemen für die Einhaltung von aufsichtsrechtlichen Vorschriften (insbesondere Eigenmittel-, Risikoverteilungs- und Liquiditätsvorschriften).	92
Die Risikokontrolle nimmt bei der Entwicklung von neuen oder erweiterten Produkten, Dienstleistungen, Geschäfts- oder Marktbereichen sowie bei wesentlichen oder komplexen Transaktionen am Entwicklungsprozess bzw. an der Sorgfaltsprüfung (Due Diligence) teil.	93
Die Risikokontrolle setzt die Geschäftsleitung über wesentliche Annahmen und Mängel in den Risikomodellen und Risikoanalysen in geeigneter Form in Kenntnis.	94
Weiter gewährleistet die Risikokontrolle, dass die Risikolimiten insbesondere im Einklang mit dem Risikoappetit stehen und mit den Ergebnissen aus den Stresstests abgestimmt und so gesetzt sind, dass sie ein operativ wirksames Steuerungsinstrument darstellen. Zudem stellt die Risikokontrolle sicher, dass eindeutige und dokumentierte Abläufe im Umgang mit Berechtigungen für die Limitensetzung und -änderung sowie bei Verstössen existieren.	95

Bei systemrelevanten Banken prüft die Risikokontrolle die angemessene Umsetzung der Bestimmungen zur Risikodatenaggregation und Risikoberichterstattung, die Teil des vom Oberleitungsorgan genehmigten Rahmenkonzepts für das institutsweite Risikomanagement sind. Dabei stellt die Risikokontrolle insbesondere sicher, dass das Institut über eine Datenarchitektur und IT-Infrastruktur verfügt, die eine aggregierte sowie zeitnahe Risikomessung, Risikodatenaggregation und –berichterstattung über sämtliche wesentlichen Risikokategorien des Instituts sowohl unter normalen Bedingungen wie auch in Stressperioden erlaubt. Weiter prüft die Risikokontrolle, ob angemessene Ressourcen hierfür zur Verfügung stehen.	96
Die Risikokontrolle erstattet der Geschäftsleitung mindestens halbjährlich einen Bericht über die Risiken bzw. Risikopositionen. Bei besonderen Entwicklungen informiert sie unverzüglich die Geschäftsleitung und die interne Revision und bei Sachverhalten von grosser Tragweite das Oberleitungsorgan bzw. den Risikoausschuss.	97
Die Risikokontrolle berichtet dem Oberleitungsorgan mindestens jährlich über die Entwicklung des Risikoprofils des Instituts und seine Tätigkeit gemäss Rz 89ff. Im Weiteren unterrichtet die Risikokontrolle das Oberleitungsorgan unverzüglich über Verletzungen der Risikolimiten, die vom Oberleitungsorgan genehmigt wurden. Eine Kopie dieser Berichte ist der internen Revision und der Prüfgesellschaft zur Verfügung zu stellen.	98
c) Aufgaben und Verantwortlichkeiten der Compliance-Funktion	
Die Aufgaben und Verantwortlichkeiten der Compliance-Funktion als unabhängige Kontrollinstanz umfassen in der Regel folgende Tätigkeiten:	99
<ul style="list-style-type: none">• Mindestens 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;	100
<ul style="list-style-type: none">• Zeitgerechte Berichterstattung an die Geschäftsleitung über wesentliche Veränderungen in der Einschätzung des Compliance-Risikos, Feststellung und Untersuchung von schwerwiegenden Verletzungen der Compliance und Unterstützung der Geschäftsleitung bei der Wahl der zu treffenden Anordnungen oder Massnahmen. Die interne Revision ist entsprechend zu informieren;	101
<ul style="list-style-type: none">• 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.	102
Nebst den Aufgaben und Verantwortlichkeiten der Compliance-Funktion in ihrer Rolle als unabhängige Kontrollinstanz unterstützt und berätet die Compliance-Funktion die Geschäftsleitung sowie die Mitarbeiter bei der Ausarbeitung, Durchsetzung und	103

Überwachung der regulatorischen und internen Vorschriften und unterstützt die Geschäftsleitung bei der Ausbildung und Information der Mitarbeiter bezüglich Compliance.

VIII. Interne Revision

A. Einrichtung

Jedes Institut hat eine interne Revision einzurichten.	104
In besonderen Fällen kann die FINMA, nach Anhörung der Prüfgesellschaft, ein Institut von der Verpflichtung gemäss Rz 104 befreien.	105
Erscheint die Einrichtung einer betriebseigenen internen Revision als nicht angemessen, können die Aufgaben der internen Revision übertragen werden:	106
<ul style="list-style-type: none">• 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),	107
<ul style="list-style-type: none">• einer zweiten Prüfgesellschaft, welche von der Prüfgesellschaft des Instituts unabhängig ist, oder	108
<ul style="list-style-type: none">• einem unabhängigen Dritten, vorausgesetzt die Prüfgesellschaft bestätigt dessen professionelle Kompetenzen und angemessene technische und personelle Ressourcen.	109
<h3>B. Unterstellung und Organisation</h3>	
Die interne Revision ist dem Oberleitungsorgan oder dessen Prüfausschuss unterstellt und nimmt die ihr übertragenen Prüf- und Überwachungsaufgaben in unabhängiger Art und Weise wahr.	110
Die interne Revision ist der Grösse, Komplexität und dem Risikoprofil des Instituts entsprechend auszugestalten und bildet organisatorisch eine selbständige und vom Geschäftsbetrieb unabhängige Einheit. Sie muss personell ausreichend dotiert sein und über die nötigen Fachkompetenzen verfügen, damit sie ihr Mandat erfüllen kann.	111
Der Leiter der internen Revision wird vom Oberleitungsorgan ernannt.	112
Die interne Revision arbeitet unabhängig von den täglichen Geschäftsprozessen und sie verfügt über ein unbeschränktes Zugriffs- und Prüferecht innerhalb des Instituts und dessen konsolidierungspflichtigen Unternehmen gemäss Rz 125. Es sind ihr alle Auskünfte zu erteilen, die zur Erfüllung ihrer Prüfungsaufgaben erforderlich sind.	113
Die für die interne Revision notwendigen Grundlagen, wie z.B. ein Reglement mit Angaben zu Organisation, Aufgaben und Verantwortlichkeiten, sind vom Oberleitungsorgan oder von	114

dessen Prüfausschuss zu erlassen. Daneben legt die interne Revision ihre Arbeitsweise (z.B. Methodik, Revisionsarten, Aus- und Weiterbildungen) fest.

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 Standards for the Professional Practice des Institute of Internal Auditors (IIA). 115

Das Entschädigungssystem für Mitarbeiter der internen Revision darf keine Anreize setzen, die zu Interessenkonflikten führen. Insbesondere darf die Entschädigung (z.B. Löhne, Boni, Honorare, und Prämien) nicht vom Erfolg einzelner Produkte oder Transaktionen abhängen. 116

C. Aufgaben und Verantwortlichkeiten

Die interne Revision liefert wichtige Entscheidungsgrundlagen für die Beurteilung, ob das Institut ein seinem Risikoprofil angemessenes und wirksames internes Kontrollsystem besitzt. 117

Sie führt mindestens jährlich eine umfassende Risikobeurteilung des Instituts durch, wobei sie externe Entwicklungen (z.B. wirtschaftliches Umfeld, regulatorische Änderungen) und interne Faktoren (z.B. wesentliche Projekte, Geschäftsausrichtung) angemessen berücksichtigt. 118

Ausgehend von dieser Risikobeurteilung legt die interne Revision die Prüfziele und die Prüfplanung für die nächste Prüfperiode fest und lässt diese durch das Oberleitungsorgan oder dessen Prüfausschuss genehmigen. Treten während der Prüfperiode wesentliche Änderungen im Risikoprofil ein, passt die interne Revision die Prüfziele und die Prüfplanung an und lässt diese wiederum genehmigen. 119

Die interne Revision veranlasst, dass die Geschäftsleitung über die Risikobeurteilung und die Prüfziele informiert ist und die Prüfgesellschaft jeweils eine Kopie dieser Unterlagen erhält. 120

Im Weiteren stellt sie sicher, dass sämtliche risikorelevanten Geschäftsaktivitäten im Rahmen einer Mehrjahresplanung einer Prüfung durch sie selbst oder die Prüfgesellschaft unterliegen. 121

Die interne Revision erstattet zeitgerecht über alle wichtigen Feststellungen einer Prüfung schriftlich Bericht an das Oberleitungsorgan oder dessen Prüfausschuss und die Geschäftsleitung. 122

Mindestens jährlich erstellt die interne Revision einen schriftlichen Bericht über die wesentlichen Prüfergebnisse und wichtigen Tätigkeiten in der Prüfperiode und unterbreitet diesen und die entsprechenden Schlussfolgerungen dem Oberleitungsorgan oder dessen Prüfausschuss zur Kenntnisnahme. Der Bericht ist auch der Geschäftsleitung und der 123

Prüfgesellschaft zuzustellen.

Im Weiteren informiert die interne Revision das Oberleitungsorgan oder dessen Prüfausschuss mindestens halbjährlich über die Beseitigung festgestellter Mängel bzw. den Stand der Umsetzung von Empfehlungen der internen Revision und der Prüfgesellschaft. Diese Information und das entsprechende „Audit Tracking“ kann auch durch eine andere unabhängige Instanz im Institut erfolgen, beispielsweise durch die Compliance-Funktion oder die Risikokontrolle.

IX. Gruppenstrukturen

Die Grundsätze und Bestimmungen dieses Rundschreibens gelten für Finanzgruppen und -konglomerate („Gruppen“) sinngemäss.

Die Gruppen müssen die Aufgaben und Verantwortlichkeiten gemäss diesem Rundschreiben auf Oberleitungs- und Geschäftsführungsebene der Einheiten mit Gesamtverantwortung für die Gruppenführung regeln. Es ist sicherzustellen, dass Vorgaben bestehen, die den rechtlichen und organisatorischen Strukturen, den Aufgaben und Verantwortlichkeiten sowie der Unabhängigkeit der jeweiligen Führungsebenen, sowie der Geschäftstätigkeit und der wesentlichen Risiken auf Gruppen- und Einzelinstitutebene angemessen Rechnung tragen. Dabei sind im Besonderen die Risiken zu berücksichtigen, welche sich aus dem Zusammenschluss mehrerer Unternehmen zu einer wirtschaftlichen Einheit ergeben.

Die interne Revision der Gruppe erstreckt sich mindestens auf alle konsolidierungspflichtigen Unternehmen. Sofern selbständige Revisionsabteilungen bei Gruppengesellschaften bestehen, sind diese der internen Revision der Gruppe funktional zu unterstellen.

X. Offenlegung

Die Grundsätze und Strukturen, anhand derer ein Institut gesteuert und kontrolliert wird sowie das Risikomanagement müssen für Einleger, Investoren, Marktteilnehmer und weitere Anspruchsgruppen transparent dargestellt werden.

Folgende Informationen sind öffentlich zu publizieren:

- Die Zusammensetzung sowie der berufliche Hintergrund und die Ausbildung der einzelnen Mitglieder des Oberleitungsorgans. Die unabhängigen Mitglieder gemäss Rz 21 ff. sind auszuweisen.
- Die Organisation des Oberleitungsorgans, insbesondere die Besetzung des Präsidiums sowie die allfällige Konstituierung und Zusammensetzung von Ausschüssen gemäss Rz 36 ff.

• Die Zusammensetzung sowie der berufliche Hintergrund und die Ausbildung der einzelnen Mitglieder der Geschäftsleitung.	132
• Die Grundsätze des Wahlverfahrens für Mitglieder des Oberleitungsorgans und des Rekrutierungsprozesses für Mitglieder der Geschäftsleitung.	133
• Die risikostrategische Ausrichtung und das Risikoprofil des Instituts sowie die Einschätzung der Risikolage durch die Geschäftsleitung.	134
Folgende Informationen der <i>Richtlinie der SIX Exchange betreffend Informationen zur Corporate Governance</i> sind von Instituten der Aufsichtskategorien 1 - 3 öffentlich zu publizieren:	135
• Die Konzernstruktur (gemeint Finanzgruppe) sowie bedeutende Aktionäre und allfällige Kreuzbeteiligungen. (Ziff 1. der SIX-Richtlinie)	136
• Die weiteren Tätigkeiten und Interessenbindungen der Mitglieder des Oberleitungsorgans. (Ziff. 3.2)	137
• Die interne Organisation und die Arbeitsweise des Oberleitungsorgans sowie die Informations- und Kontrollinstrumente gegenüber der Geschäftsleitung. (Ziff. 3.5 – 3.7)	138
• Die weiteren Tätigkeiten und Interessenbindungen der Mitglieder der Geschäftsleitung. (Ziff. 4.2)	139
• Die Grundlagen und die Elemente der Entschädigungen und der Beteiligungsprogramme für die Mitglieder des Oberleitungsorgans und der Geschäftsleitung sowie die Zuständigkeit und das Verfahren zu deren Festsetzung. (Ziff. 5.1.).	140
• Bezüglich der Revisionsstelle und der aufsichtsrechtlichen Prüfgesellschaft die Dauer des Revisions- bzw. des Prüfmandats, die Amtsdauer des leitenden Revisors und des leitenden Prüfers, das Revisions- und das Prüfhonorar für das vergangene Berichtsjahr, die zusätzlichen Honorare sowie die Informationsinstrumente des Revisionsunternehmens gegenüber dem Oberleitungsorgan. (Ziff. 8.1 – 8.4)	141
• Die vom Institut angewandte Informationspolitik. (Ziff. 9)	142
Die Offenlegung erfolgt einfach zugänglich auf der Internetseite des Instituts und in einem separaten Kapitel im Geschäftsbericht. Materielle Veränderungen werden innerhalb eines Monats auf der Internetseite nachgeführt. Falls einzelne Informationen bereits im ordentlichen Geschäftsbericht oder aufgrund der Anforderungen des FINMA-RS 16/1 „Offenlegung Banken“ publiziert werden, kann auf eine separate Offenlegung verzichtet werden.	143

XI. Inkrafttreten und Übergangsbestimmungen

Dieses Rundschreiben tritt am [...] in Kraft.	144
Die Umsetzung folgender Anforderungen hat bis spätestens ein Jahr nach Inkrafttreten zu erfolgen:	145
Die Umsetzung der Drittelsregel zur Unabhängigkeit des Oberleitungsorgans gemäss Rz 21.	
Die Einführung eines Prüfausschusses und eines davon separaten Risikoausschusses für Institute der Aufsichtskategorien 1 – 3 gemäss Rz 36ff respektive Rz 46ff.	
Die Erstellung und Genehmigung eines Rahmenkonzepts für das institutsweite Risikomanagement gemäss Rz 66.	
Das Führen einer separaten CRO-Position, u.a. als Teil der Geschäftsleitung für systemrelevante Banken gemäss Rz 87-88.	
Die FINMA kann in begründeten Einzelfällen die Übergangsfrist verlängern.	

Anhörung