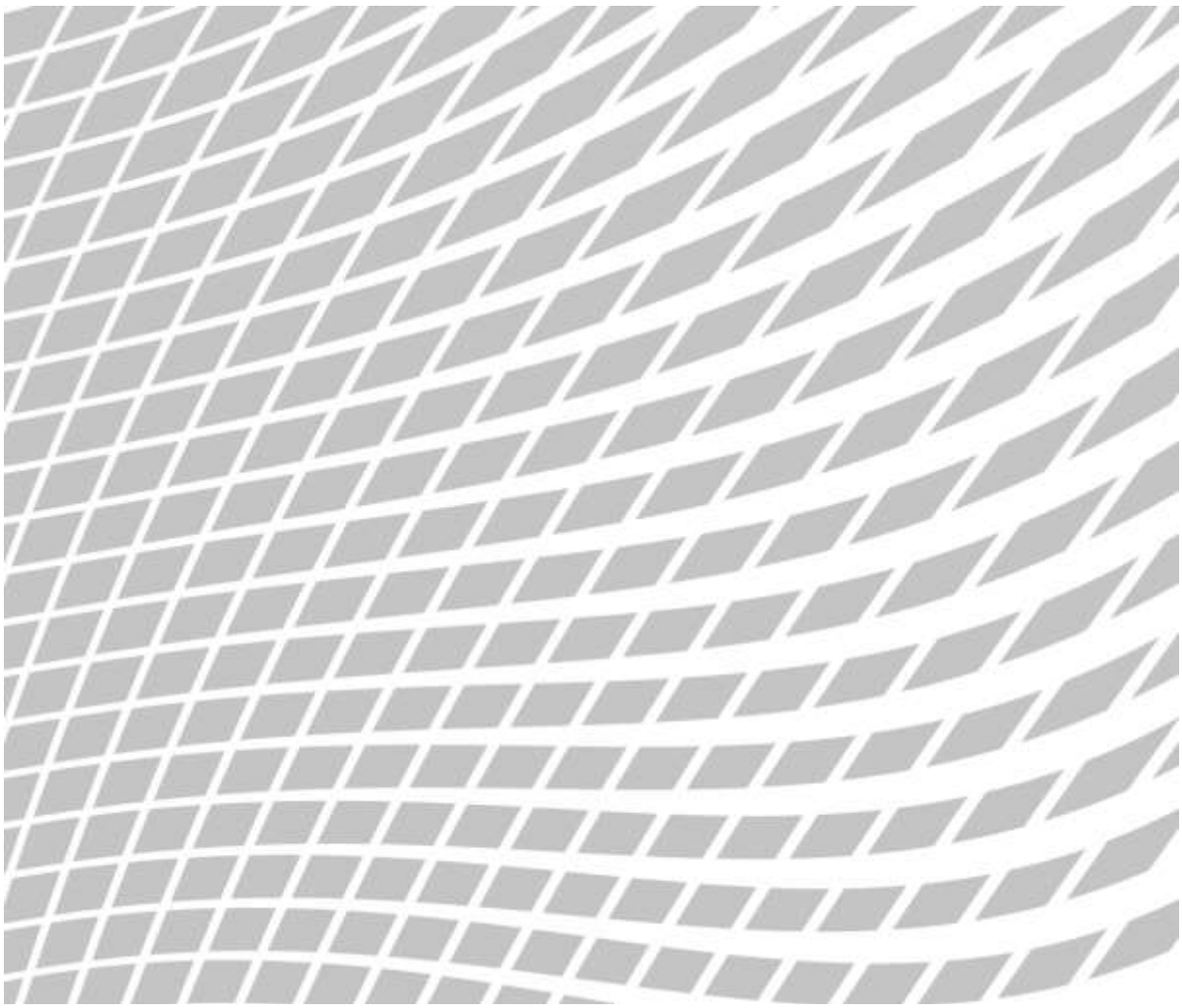
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

1. März 2016

Rundschreiben 2016/x „Corporate Governance – Banken“

Erläuterungsbericht (Totalrevision FINMA-RS 08/24 „Überwachung und interne Kontrollen Banken“; Teilrevision FINMA-RS 08/21 „Operationelle Risiken Banken“; Teilrevision FINMA-RS 10/1 „Vergütungssysteme“)



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

Inhaltsverzeichnis

Kernpunkte

Die FINMA unterwirft das FINMA-RS 08/24 „Überwachung und interne Kontrollen Banken“ einer Totalrevision. Das Rundschreiben wurde 2006 von der EBK erlassen und seither nur geringfügig angepasst. Nicht widerspiegelt werden im Rundschreiben grundsätzliche Entwicklungen im Bereich der Corporate Governance und wichtige Erkenntnisse für das Risikomanagement aus der Finanzmarktkrise. Internationale Standardsetter, unter anderem der Basler Ausschuss für Bankenaufsicht, haben in der Zwischenzeit ihre Richtlinien für eine zeitgemässe Corporate Governance und ein effektives Risikomanagement angepasst. Die FINMA nimmt die überarbeiteten internationalen Standards zum Anlass, das FINMA-RS 08/24 umfassend zu revidieren. Damit wird auch entsprechenden Empfehlungen des Internationalen Währungsfonds Rechnung getragen, die im Rahmen des Financial Sector Assessment Programm 2014 abgegeben wurden.

Konkret sind folgende wesentliche Neuerungen und Anpassungen vorgesehen:

1. Neben den Kontrollaspekten werden für das Oberleitungsorgan und die Geschäftsleitung auch Grundsätze und Strukturen zur Steuerung der Bank eingeführt („checks and balances“). In Bezug auf das Oberleitungsorgan erfolgt eine weitgehende Integration der heutigen FAQ ins Rundschreiben.

2. Banken der Aufsichtskategorien 1 – 3 werden neu je einen separaten Prüf- und Risikoausschuss einzurichten haben.

3. Sämtliche Institute haben über ein durch die Geschäftsleitung ausgearbeitetes und durch das Oberleitungsorgan verabschiedetes Rahmenkonzept für das Risikomanagement zu verfügen.

4. Alle Banken der Aufsichtskategorien 1 bis 3 haben eine Risikokontrolle zu unterhalten, die durch den CRO geführt wird. Bei Banken der Aufsichtskategorien 1 und 2 muss der CRO in der Geschäftsleitung vertreten sein.

5. Für alle Banken werden minimale Vorgaben zur Offenlegung im Bereich Corporate Governance festgehalten. Banken der Aufsichtskategorien 1 bis 3 unterstehen einer erweiterten Publikationspflicht entlang den Corporate Governance Offenlegungsrichtlinien der SIX.

Im Kontext der Totalrevision des FINMA-RS 08/24 werden die FINMA-RS 08/21 „Operationelle Risiken Banken“ und das FINMA-RS 10/1 „Vergütungssysteme“ teilrevidiert.

Das FINMA-RS 08/21 wird im Kapitel der qualitativen Anforderungen zum Risikomanagement um jene Teile entschlackt, die neu als „übergeordnete“ Anforderungen ins FINMA-RS „Corporate Governance – Banken“ integriert werden. Zusätzlich wird der Risikomanagementgrundsatz zur Technologinfrastruktur um die Aspekte IT- und Cyber-Risiken ergänzt und ein neuer Grundsatz zu Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft eingeführt. Zudem wird der Grundsatz zur Kontinuität

bei Geschäftsunterbrechung um Vorgaben zur Erhaltung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken ergänzt.

Die zwingende Anwendung des FINMA-RS 10/1 soll auf Banken mit Mindesteigenmittel grösser CHF 10 Mia. beschränkt werden. Das Rundschreiben erfährt zudem kleinere Änderungen bei den Anforderungen zur Ausgestaltung der Vergütungssysteme.

1 Ausgangslage

Auf den 1. Januar 2007 setzte die Eidgenössische Bankenkommission das heutige FINMA-RS 08/24 *Überwachung und interne Kontrolle Banken* in Kraft. Das Rundschreiben definiert die Anforderungen zum internen Kontrollsystem und zur Corporate Governance bei Banken, insbesondere bezüglich des Oberleitungs- und Geschäftsführungsorgans, der internen Revision, der Compliance-Funktion und der Risikokontrolle.

Zum Zeitpunkt des Erlasses reflektierte das FINMA-RS 08/24 das aktuelle Wissen und die zeitgemässe Praxis bezüglich Überwachung und internen Kontrollen bei Banken. Das Rundschreiben wurde seither nur punktuell angepasst. Erkenntnisse aus der Finanzmarktkrise und jüngere Entwicklungen im Bereich der Corporate Governance werden im Rundschreiben nicht reflektiert.

Schwächen im Risikomanagement und in der Corporate Governance von Banken haben in der Finanzmarktkrise wesentlich zur Verschärfung der Krisensituation beigetragen. Defizite wurden auf verschiedenen Ebenen des Risikomanagements erkannt, so bei der Risikoerfassung, der Risikomessung und der Risikokommunikation. In den Führungsgremien von Banken sind sodann mangelnde Fachkenntnisse im Zusammenhang mit dem Umgang und mit der Beherrschung von Risiken offenkundig geworden. Zudem wurden Fehlentwicklungen durch Vergütungssysteme, die falsche Anreize setzen, zusätzlich beschleunigt.

Weltweit verstärkten in den vergangenen Jahren verschiedene Standardsetter ihre Erwartungen an die Corporate Governance von Unternehmen. Für die Finanzbranche massgebend sind insbesondere die *G20/OECD Principles of Corporate Governance* (November 2015) und die *Corporate Governance Principles for Banks* des Basler Ausschusses für Bankenaufsicht (Juli 2015).

Im Weiteren aktualisierte der Basler Ausschuss für einzelne Risikokategorien im Rahmen der Basel III Reformagenda die richtungsgebenden Prinzipien für eine adäquate Steuerung, Bewirtschaftung und Kontrolle der Risiken. In diesem Zusammenhang übernahm die FINMA 2013 die Basler Prinzipien betreffend das Management der operationellen Risiken und übertrug sie in das Rundschreiben FINMA-RS 08/21 *Operationelle Risiken Banken*. Im Einzelfall gibt es Überschneidungen mit den allgemeinen Regelungen zur Risikokontrolle im FINMA-RS 08/24.

Im Jahr 2014 wurde die Schweiz im Rahmen des *Financial Sector Assessment Program* durch den Internationalen Währungsfonds (IWF) geprüft. Der IWF kam im Regelungsbereich der Corporate Governance und des Risikomanagements u.a. zu folgenden Empfehlungen:

- Empfehlung zu expliziten und verdichteten Vorgaben bezüglich qualitativer Elemente des Risikomanagements und der Risikokontrolle aus der Optik des Gesamtunternehmens, bezüglich institutsweiter Risikoberichterstattung, integraler Analyse aggregierter Risikodaten und verbesserter Abstimmung zwischen Risikoappetit und Risikostrategie;
- Empfehlung zu klareren Vorgaben bezüglich des risikospezifischen Fachwissens der Verwaltungsratsmitglieder;

- Empfehlung zur Stärkung des Anteils an Mitgliedern des Verwaltungsrats mit hinreichender Unabhängigkeit gegenüber dem Eigentümer, namentlich mit Blick auf staatsnahe Banken;
- Empfehlung zur Verbesserung von Stellung und Profil der CRO-Funktion innerhalb des Unternehmens;
- Empfehlung zur Einführung von Regeln für separate Risikoausschüsse mit spezifischem Risikowissen;
- Empfehlung zur Einführung von Vorgaben für eine bankinterne Beurteilung von neuen Geschäftsfeldern, Produkten und veränderten Unternehmensstrukturen.

Die genannten Empfehlungen, welche die FINMA im Grundsatz unterstützt, sollen mit der Totalrevision des FINMA-RS 08/24 umgesetzt werden.

Im Zuge der technologischen Entwicklung mit einer vermehrten Digitalisierung des Finanzgeschäfts sowie einer erhöhten Auslagerung von Prozessen und Dienstleistungen an Drittparteien haben sich die IT- und insbesondere die Cyber-Risiken in den letzten Jahren merklich erhöht. Der Austausch mit den Experten verdeutlicht das hohe Gefahrenpotential und die enormen Herausforderungen vor dem der Schweizer Finanzplatz steht. Die FINMA hat sich bereits eingehend mit dieser Thematik beschäftigt und verschiedene Massnahmen ergriffen, um den Umgang von Beaufsichtigten mit diesen Risiken beurteilen zu können[1]. Aufgrund dessen und in Abstimmung mit den internationalen Bestrebungen erachtet die FINMA die Erweiterung des FINMA-RS 08/21 mit Grundsätzen für IT- und Cyber-Risiken als notwendig, um institutsübergreifend die Einhaltung von grundlegenden Prinzipien im Umgang mit diesen Risiken zu gewährleisten.

Die Sicherstellung einer Fortführung von kritischen Funktionen und Dienstleistungen im Insolvenzfall stellt eine kritische Anforderung insbesondere an systemrelevante Banken dar. Das Financial Stability Board (FSB) hat eine Konsultation dahingehender Anforderungen per Anfang 2016 abgeschlossen. Die FINMA erachtet die Erweiterung des FINMA-RS 08/21 um einen Grundsatz hinsichtlich der Sicherstellung der Kontinuität im Insolvenzfall als notwendig.

Das Geschäftsmodell vieler Vermögensverwaltungsbanken ist traditionell stark auf grenzüberschreitende Dienstleistungen für im Ausland wohnhafte Privatkunden ausgerichtet. Die Rechts- und Reputationsrisiken aus diesem Geschäft haben in den letzten Jahren spürbar zugenommen. Die FINMA erläuterte ihre Position zu diesem Themenbereich im Oktober 2010 in einem Positionspapier. Neu wird ein Grundsatz in das FINMA-RS 08/21 integriert, der diesen Aspekt aufgreift.

[1] Bspw. Durchführung von Zusatzprüfungen gemäss FINMA-RS 2013/03 „Prüfwesen“ bzw. einer Selbstbeurteilung betreffend den Umgang mit Cyberrisiken.

2 Regulierungsbedarf und Zielvorstellung

Die FINMA erachtet es als notwendig, dass Vorgaben zur Implementierung einer soliden Corporate Governance und eines effektiven Risikomanagements bei Banken und Effektenhändlern den wichtigsten aktuellen Richtlinien der internationalen Standardsetter angeglichen werden. Qualitative Anforderungen zum Risikomanagement, insbesondere zur Risk Governance, sollen aus den risikospezifischen Rundschreiben herausgelöst und im FINMA-RS „Corporate Governance – Banken“ zusammengeführt werden. Die in den FAQ enthaltenen Aspekte zum Oberleitungsorgan sollen in das FINMA-RS „Corporate Governance – Banken“ integriert werden. Dadurch soll die in der Bankenaufsicht in den letzten Jahren gelebte Praxis gefestigt sowie die Rechtssicherheit gestärkt werden.

In einigen Bereichen entspricht das FINMA-RS 08/24 nicht der Zielvorstellung einer prinzipienorientierten Regulierung. Diese Textstellen sollen zusammengefasst oder ersatzlos gestrichen werden.

Im Rahmen der Totalrevision des FINMA-RS 08/24 sollen u.a. die Aufsichtsbestimmungen zum institutsweiten Risikomanagement sowie die Aufgaben und Verantwortlichkeiten der Geschäftsleitung neu geregelt werden. Eine gesamtheitliche Darstellung dieser Anforderungen im neuen FINMA-RS „Corporate Governance – Banken“ ermöglicht es, im Rahmen einer Teilrevision eine Entschlackung der qualitativen Risikomanagementanforderungen im FINMA-RS 08/21 vorzunehmen.

Die Revision des FINMA-RS 08/21 bietet zudem die Möglichkeit, für die operationellen Risiken zentrale Themen wie IT- und Cyberrisiken, die Fortführung von kritischen Dienstleistungen im Insolvenzfall und die Beachtung von Risiken im grenzüberschreitenden Dienstleistungsgeschäft (Crossborder) zu integrieren. Weiter soll durch die Teilrevision des FINMA-RS 08/21 eine Vereinheitlichung bei der Anwendung des Proportionalitätsprinzips umgesetzt werden.

Im Rahmen der Teilrevision sollen zudem die FAQ zum FINMA-RS 08/21 sowie die FAQ zu den Rechts- und Reputationsrisiken im grenzüberschreitenden Finanzdienstleistungsgeschäft, soweit dies als sinnvoll erachtet wird, in das FINMA-RS 08/21 integriert werden.

Hinsichtlich der Einführung von Grundsätzen für die IT- und Cyberrisiken soll diese als Erweiterung des bereits bestehenden Grundsatzes über die Technologieinfrastruktur erfolgen und in Abstimmung mit den internationalen Bestrebungen vorgenommen werden. Diese Grundsätze sollen eine institutsweite Einhaltung von grundlegenden Prinzipien im Umgang mit diesen Risiken gewährleisten.

Die Integration der Fortführung von kritischen Dienstleistungen im Insolvenzfall soll im Rahmen einer Erweiterung des derzeitigen Grundsatzes über die Kontinuität bei Geschäftsunterbrechung, welche die Aufrechterhaltung und Fortführung von kritischen Dienstleistungen im Insolvenzfall sicherstellt, vorgenommen werden. Sie steht im Einklang mit internationalen Regulierungsentwicklungen in diesem Bereich.

Das FINMA-Positionspapier zu den Risiken im grenzüberschreitenden Finanzdienstleistungsgeschäft soll in einem separaten Grundsatz unter den qualitativen Anforderungen für den Umgang mit operationellen Risiken zusammengefasst werden. Dabei soll der bis anhin verfolgte risikobasierte Ansatz

weiterhin Anwendung finden. Anknüpfungspunkt sind hierbei die rechtlichen Risiken, die jedoch analog bei anderen Risikokategorien mit schwerwiegenden Reputationsrisiken verknüpft sein können.

Schliesslich soll im Zusammenhang mit den Entwicklungen im Bereich Corporate Governance auch das FINMA-RS 10/1 „Vergütungssysteme“ aktualisiert werden. Nebst kleineren Anpassungen soll die zwingende Umsetzung auf global tätige systemrelevante Banken und einzelne, durch die FINMA bestimmte, Institute begrenzt werden. So wird sichergestellt, dass nur Institute in den engeren Scope des Rundschreibens gelangen, bei welchen die Vergütungssysteme komplex und die Vergütungshöhen materiell relevant sind.

3 Erläuterungen zum FINMA-RS 16/x „Corporate Governance – Banken“

Das neue Rundschreiben soll eigenständig gelesen und verstanden werden können. In einzelnen Randziffern werden zur besseren Verständlichkeit deshalb Bestimmungen aus übergeordneten Regulierungstexten wiedergegeben.

Im vorliegenden Entwurf des Rundschreibens wurde der Text farblich hinterlegt. Die Farben weisen auf die Herkunft des Inhalts hin. Gelb markiert sind alle Passagen, die mit geringen textlichen Anpassungen aus dem FINMA-RS 08/24 übernommen wurden. In roter Farbe sind jene Teile gekennzeichnet die aus den FINMA-RS 08/21 und 08/32 entnommen wurden. Blau markiert sind Texte von internationalen Standardsettern. Und grün sind schliesslich jene Randziffern, die inhaltlich aus dem FAQ „Oberleitungsorgan“ stammen.

3.1 Gegenstand, Begriffe und Geltungsbereich

Der heutige Fokus des FINMA-RS 08/24 richtet sich auf die Überwachung der Geschäftstätigkeit sowie die internen Kontrollen und deren Überwachung. Mit der Totalrevision wird der Blickwinkel des Rundschreibens insofern geöffnet, als dass neben den Erfordernissen zum internen Kontrollsystem (IKS) grundsätzliche Erfordernisse an die interne Governance und das Risikomanagement bei Banken und Effektenhändlern eingeführt werden.

Der thematisch erweiterte Anwendungsbereich verlangt nach einer Definition und Abgrenzung der verwendeten Begriffe. Die im Rundschreiben definierten Begriffe dienen dem Verständnis für eine fachgerechte Umsetzung der einzelnen Anforderungen. Es besteht kein Anspruch auf eine über das Rundschreiben hinausgehende Anwendung der vorliegenden Begriffsdefinitionen.

Die Anforderungen im Rundschreiben sind grundsätzlich prinzipienorientiert. Deren Umsetzung soll im Einzelfall von der Grösse, Komplexität, Struktur und dem Risikoprofil abhängig gemacht werden. Corporate Governance und Risikomanagement sind Aufsichtsthemen, welche sich nicht mit einem „one size fits all“- Ansatz prüfen und überwachen lassen. Die Eigenheiten und Risiken der einzelnen Institute sollen in der Aufsichtspraxis, wie bis anhin, berücksichtigt werden. Damit die neuen, teilweise weitergehenden Anwendungsprinzipien nicht zu einer Überregulierung führen, werden Banken und Effek-

tenhändler der Aufsichtskategorien 4 und 5 zudem von der Umsetzung einzelner Erfordernisse explizit befreit.

Die konsequente Anwendung des Proportionalitätsprinzips löst den bis anhin in einigen Stellen des Rundschreibens verwendeten „comply or explain“ Ansatz ab. Das im Markt bewährte Prinzip, dass ein Nichteinhalten von selbstregulierenden Vorgaben im Geschäftsbericht erläutert werden muss, wird im regulatorischen Bereich selten angewendet und erschwert in der Aufsichtspraxis die zeitnahe Überwachung der Institute. Falls in spezifisch begründeten Einzelfällen die Anforderungen nicht umgesetzt werden können, soll zukünftig mit Hilfe von Ausnahmebewilligungen operiert werden. Dies entspricht teilweise bereits der gelebten Praxis, da die Organisation des Oberleitungsorgans und der institutsweiten Steuerungs- und Kontrollfunktionen meistens in bewilligungspflichtigen Reglementen abgebildet ist, so zum Beispiel die Drittelsregel zur Unabhängigkeit des Oberleitungsorgans oder die Einrichtung eines Prüfausschusses des Oberleitungsorgans.

3.2 Oberleitungsorgan

3.2.1 Aufgabenkatalog

Das Profil des obersten Leitungsorgans soll gezielt geschärft werden. Dabei wird nur soweit aufsichtsrechtlich geboten in den Organisationsspielraum des Instituts eingegriffen. Klargestellt wird namentlich die Rolle des Oberleitungsorgans als oberster Risikohüter des Instituts. Zudem wird der Aufgabenkatalog über die Kontrollperspektive hinaus auf sämtliche Kernkompetenzen nach Aktienrecht (vgl. Art. 716a Abs. 1 OR) ausgedehnt. Die Auffangrelation zum Aktienrecht entspricht der geltenden Aufsichtspraxis, die sich inhaltlich im Grundsatz am aktienrechtlichen Aufgabenkatalog orientiert.

3.2.2 Zusammensetzung

Nebst der absoluten Anzahl Mitglieder – für Banken gilt eine Mindestzahl von drei (Art. 11 Abs. 1 BankV) – ist vor allem eine ausgewogene Zusammensetzung des Oberleitungsorgans von besonderer Tragweite. Das Oberleitungsorgan soll genügend breit aufgestellt sein, so dass neben den Hauptgeschäftsaktivitäten sämtliche weiteren zentralen Bereiche wie Finanz- und Rechnungswesen, Risikomanagement, Compliance, Controlling und IT kompetent vertreten sind. Dies bedeutet nicht, dass jedes Mitglied eine mehrjährige Bankerfahrung vorweisen können muss. Jedes Mitglied verfügt aber über mindestens eine vertiefte Kernkompetenz, welche zu einer ausgewogenen Durchmischung des Gesamtorgans beiträgt.

Wird diesem Grundsatz der Diversität glaubwürdig nachgelebt, müssen gute Kenntnisse im Finanz- und Rechnungswesen und Erfahrung mit der Prüftätigkeit im Gesamtorgan angemessen vertreten sein. Die heutige Regel,[2] wonach bei Fehlen eines Prüfausschusses ein oder zwei qualifizierte Verwaltungsräte mit spezifischer Expertise mit den Aufgaben eines solchen Ausschusses betraut werden sollen, findet künftig somit keine Anwendung mehr.

[2] FINMA-RS 08/24, Rz. 30.

Der Anspruch auf eine ausgewogene Zusammensetzung bedeutet auch, dass das Gesamtorgan insgesamt mit dem Aktionsradius und den Zielmärkten des Instituts bzw. der Gruppe hinreichend vertraut ist. So sollte bei einem regional oder national ausgerichteten Institut eine massgebliche Zahl der Mitglieder aufgrund ihres Lebensmittelpunkts, ihrer beruflichen Laufbahn oder ihrer Ausbildung einen engen Bezug zur Schweiz haben, während bei global tätigen Konzernen zusätzlich auch auf einen globalen Rekrutierungsperimeter abgestellt werden kann.

3.2.3 Unabhängigkeit

Das Prinzip der Gewaltentrennung zwischen Oberleitungsorgan und Geschäftsleitung bleibt für den Bankenbereich weiterhin wegweisend. Zudem soll mindestens ein Drittel des Oberleitungssorgans kein besonderes Näheverhältnis zum Institut aufweisen. In Abkehr vom heutigen „comply or explain"-Ansatz (vgl. vorne 3.1) soll die Drittelregel inskünftig erhöhte Verbindlichkeit haben. Die FINMA kann jedoch in begründeten Einzelfällen Erleichterungen gewähren, wie z.B. bei kleinen Unternehmen während der Start-up-Phase.

Unabhängigkeit bedeutet auch Distanz gegenüber dem Eigentümer, insbesondere gegenüber Grossaktionären. Es muss sichergestellt sein, dass ein massgeblicher Teil der Mitglieder nicht am Institut qualifiziert beteiligt ist oder einen qualifiziert Beteiligten vertritt. Das erforderliche Mass an Unabhängigkeit ist hier bewusst offen formuliert. In gewissen Konstellationen braucht es eine mehrheitliche Unabhängigkeit, während z.B. bei rein schweizerischen Konzernstrukturen eine mehrheitliche Konzernvertretung in der Tochterbank durchaus denkbar ist. Der Vielfalt in der Praxis ist mit Augenmass und massgeschneiderten Lösungen im Einzelfall zu begegnen.

3.2.4 Mandatsführung

Die wichtigsten Grundsätze der Mandatsführung werden von den FAQ „Oberleitung von Banken und Effektenhändlern" in das vorliegende Rundschreiben überführt. Auf die Einführung einer starren Obergrenze zur Beschränkung von Mehrfachmandaten wird bewusst verzichtet. Von jedem Mitglied wird jedoch ein aktives und zeitlich angemessenes Engagement erwartet. Die einzelnen Mitglieder des Oberleitungsorgans haben sicherzustellen, dass sie ihrem Mandat genügend Zeit einräumen, um es sorgfältig auszuüben. Interessenkonflikte im Verhältnis zum Institut sind möglichst zu vermeiden. Auch müssen sich die Mitglieder des Oberleitungsorgans für Krisen- und Notsituationen dauernd zur Verfügung halten. Ihre Präsenzbereitschaft erschöpft sich nicht im ordentlichen Sitzungsrhythmus. Ebenfalls aus den FAQ übernommen werden die Erwartungen gegenüber dem Präsidenten des Oberleitungsorgans, dessen besonders prominente Stellung aufsichtsrechtlich ebenfalls mit geprägt ist.

3.2.5 Ausschüsse

Neu vorgesehen sind die verbindliche Einrichtung eines Prüfausschusses für grössere Banken (Aufsichtskategorien 1 – 3) und die Einführung eines separaten Risikoausschusses für Banken dieser Kategorien. Mit dieser regulatorischen Gleichschaltung von Prüf- und Risikoausschuss bewegt sich der Vorschlag auf der Linie des Basler Ausschusses, welcher solche Ausschüsse für grössere Banken dringend empfiehlt und für systemrelevante Banken zwingend vorsieht. Auch trägt die Einführung ei-

nes separaten Risikoausschusses der FSAP-Kritik Rechnung, welche gerade bei mittelgrossen Banken Defizite beim risikospezifischen Fachwissen auf Stufe Oberleitung ortete. Aufgrund der unterschiedlichen Perspektive und Stossrichtung der beiden Ausschüsse müssen sich diese zudem personell hinreichend unterscheiden.

Bis auf eine Ausnahme verfügen heute bereits sämtliche Banken der Kat. 1 -3 über einen Prüfausschuss. Risikoausschüsse dagegen gehören in der Schweizer Bankenlandschaft noch nicht zum festen Bestand. Von den Kat.-3-Banken verfügt nur knapp die Hälfte über einen separaten Risikoausschuss und rund ein Drittel über eine kombinierte Version (gemeinsamer Prüf- und Risikoausschuss).

Zur ordnungsgemässen Zusammensetzung eines Prüf- und Risikoausschusses gehört, dass seine Mitglieder mehrheitlich unabhängig und mit den nötigen Fachkenntnissen und Erfahrung im Spezialgebiet ausgestattet sind. Ebenso sollen die Präsidenten des Prüf- und des Risikoausschusses unabhängig sein und weder als Präsident des Oberleitungsorgans noch als Präsident eines andern Ausschusses fungieren. Der Präsident des Oberleitungsorgans sollte zudem nicht Mitglied des Prüfausschusses sein.

Systemrelevante Banken müssen zudem in Anlehnung an die Basler Standards einen separaten Vergütungs- und Nominationsausschuss einrichten.

3.3 Geschäftsleitung

Die geltende Fassung des FINMA-RS 08/24 beschränkt sich bei den Bestimmungen zur Geschäftsführung auf Ausführungen zur Umsetzung der Vorgaben des Oberleitungsorgans bezüglich Einrichtung, Aufrechterhaltung und regelmässiger Überprüfung der internen Kontrolle, zum Management Informationssystem (MIS) sowie zur Ausgestaltung der entsprechenden Organisationsstruktur.

Das neue Rundschreiben wurde diesbezüglich erweitert und enthält nun die wichtigsten der Geschäftsleitung zugeordneten Aufgaben und Verantwortlichkeiten: die Führung des Tagesgeschäfts und die Vertretung des Instituts gegenüber Dritten im operativen Bereich, die Antragstellung betreffend Geschäfte, die in die Zuständigkeit oder unter den Genehmigungsvorbehalt des Oberleitungsorgans fallen, die Ausgestaltung einer institutsweiten Führungs- und Organisationsstruktur inkl. Unterhalt eines Managementinformations- und internen Kontrollsystems sowie die operative Ertrags- und Risikosteuerung.

Die Übernahme dieser Aufgaben und Verantwortlichkeiten durch die Geschäftsleitung hat die FINMA bis anhin bereits im Rahmen der Genehmigung der Statuten und internen Reglemente verlangt. Damit wird die langjährige und unbestrittene Bewilligungspraxis in ein Rundschreiben überführt.

Der vorliegende Entwurf enthält neu ebenfalls Bestimmungen zu den Anforderungen an die Mitglieder der Geschäftsleitung. Sie müssen gemäss Art. 3 Abs. 2 lit. c BankG einen guten Ruf geniessen und Gewähr für eine einwandfreie Geschäftstätigkeit bieten. Das bedeutet, dass die Mitglieder der Geschäftsleitung als Gesamtorgan über hinreichend Erfahrung im Bank- und Finanzbereich, Integrität und Führungskompetenz sowie jedes einzelne Mitglied als Funktionsverantwortlicher über die nötigen Fachkenntnisse verfügen. Ausserdem hat die Geschäftsleitung ihre Vorbildfunktion wahrzunehmen

und mit ihrem persönlichen Verhalten die Unternehmens- und Risikokultur mitzutragen (sog. „tone at the top“).

Der Abschnitt *Funktionentrennung und Kontrollaktivitäten* wurde dagegen – im Sinne einer prinzipienorientierten Regulierung – ersatzlos gestrichen.

3.4 Rahmenkonzept für das institutsweite Risikomanagement

Im FINMA-RS „Corporate Governance – Banken“ werden die qualitativen Anforderungen an das Risikomanagement, heute definiert für das Management operationeller Risiken im FINMA-RS 08/21, für alle Risikoarten übernommen.

Das Rahmenkonzept besteht in der Regel aus einem Hauptdokument sowie weiteren internen Vorgaben und umfasst insbesondere die Risikopolitik, den Risikoappetit sowie Vorgaben hinsichtlich der Limiten (und Schwellenwerten) zur Einhaltung des Risikoappetits.

Es entspricht vielfach bereits heute der gelebten Praxis, dass Vorgaben und Richtlinien zu den einzelnen Aspekten des Rahmenkonzepts existieren und diese (teilweise) durch das Oberleitungsorgan genehmigt wurden. Jedoch bedarf es aufgrund des neuen Rundschreibens bei einigen Instituten einer Konsolidierung und Genehmigung dieser Aspekte bzw. des Rahmenkonzepts durch das Oberleitungsorgan.

Die Risikopolitik definiert sich über die Risikostrategie, die die Rahmenbedingungen für die Risikoidentifikation, Risikomessung, Risikobewirtschaftung, Risikoüberwachung sowie Risikoberichterstattung festlegt und damit die Einhaltung der Risikolimiten gewährleistet. Dabei werden bspw. nebst einer Aufbau- und Ablauforganisation für das institutsweite Risikomanagement auch die Instrumente zur Umsetzung der Risikostrategie festgehalten.

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 umfasst dabei sowohl die Risikosicht auf aggregierter Stufe als auch diejenige auf Stufe der wesentlichen Risikokategorien, d.h. Risiken nach Arten[3], Typen[4] und Ebenen[5], denen das Institut ausgesetzt ist.

Die Bestimmung der Risikolimiten orientiert sich am Risikoappetit, d.h. sowohl in Abstimmung auf die aggregierte Risikosicht als auch in Bezug auf die jeweiligen Risikokategorien. Die Limiten nehmen dabei eine Steuerungsfunktion wahr. Es sind typischerweise auch vorgelagerte Schwellenwerte vorzusehen, die eine (mögliche) Verletzung der festgelegten Risikolimiten frühzeitig erkennen lassen. Bei einer Überschreitung der Limiten muss das Oberleitungsorgan unverzüglich in Kenntnis gesetzt werden, um Risikominderungsstrategien und -instrumente einzusetzen, die die Einhaltung der Risikolimi-

[3] Bspw. Kredit-, Markt-, Liquiditäts-, operationelle Risiken, etc.

[4] Bspw. Erwarteter Verlust, Value-at-Risk, interne Liquiditätsmessgrössen, etc.

[5] Bspw. Produkte, Unternehmensbereiche, Länderengagements, etc.

ten zeitnah wieder gewährleisten, oder um eine temporäre Überschreitung dieser Limiten durch das Oberleitungsorgan zu genehmigen.

Das Rahmenkonzept beinhaltet Grundsätze für die Ausgestaltung einer Dokumentation, die es ermöglicht, die Festlegung des Risikoappetits sowie der Risikolimiten einer angemessenen, unabhängigen Überprüfung und Beurteilung sowohl durch das Oberleitungsorgan wie auch durch andere Kontrollinstanzen unterziehen zu können. Diese Grundsätze beinhalten namentlich Vorgaben, die eine Nachvollziehbarkeit der Risikobeurteilungen und der dabei verwendeten Grundlagen für die Bestimmung des Risikoappetits und der Risikolimiten erlauben. Diese Dokumentation kann bspw. auf einer jährlich, institutsweit durchgeführten Risikoanalyse beruhen oder sich auf die eingesetzten Risikomessmethoden und/oder -modelle beziehen.

Die Risikoberichterstattungs- und Managementinformationssysteme (MIS) entsprechen einer Berichterstattung zu Überwachungs- und Informationszwecken sowohl für interne wie externe Anspruchsgruppen.

Trotz des strategischen Charakters des Rahmenkonzepts ist dieses bei wesentlichen Änderungen, bspw. in der Geschäftstätigkeit des Instituts, im Marktumfeld oder bei aufsichtsrechtlichen und gesetzlichen Veränderungen den aktuellen Gegebenheiten, möglichst zeitnah anzupassen. Das Rahmenkonzept wird grundsätzlich durch das Oberleitungsorgan periodisch überprüft. Zusätzlich gilt es das Rahmenkonzept zeitnah und fortwährend einer Überprüfung und Anpassung durch eine eindeutig bezeichnete Organisationseinheit zu unterziehen, die genügend qualifiziertes Personal zur Verfügung hat. Typischerweise handelt es sich bei dieser Organisationseinheit um die Risikokontrolle resp. die Compliance-Funktion, die in ihren Rollen als unabhängige Kontrollinstanzen sowie im Hinblick auf ihre Teilnahme am Entwicklungsprozess (New Business Process) bzw. an der Sorgfaltsprüfung (Due Diligence) das Oberleitungsorgan bei seiner periodischen Überprüfung des Rahmenkonzepts unterstützen. Weiter erfolgt durch die interne Revision eine regelmässige, unabhängige und gesamtheitliche Überprüfung des Rahmenkonzepts im Hinblick auf die Ausgestaltung und Einhaltung sowie die Umsetzung als Teil des internen Kontrollsystems.

Die Vorgaben im Rahmenkonzept müssen institutsweit Anwendung finden. Das heisst nebst der Anwendung der Grundsätze auf die bestehenden Strukturen ist insbesondere zu gewährleisten, dass die Vorgaben im Rahmen eines Entwicklungsprozesses (New Business Process) bzw. einer Sorgfaltsprüfung (Due Diligence) beispielsweise bei organisatorischen Änderungen wie Auslagerungen, Fusionen oder Akquisitionen oder der Prüfung von neuen Geschäftsbereichen und Produkten berücksichtigt werden.

Für systemrelevante Banken gilt es, zusätzliche Bestimmungen zur Risikodatenaggregation und Risikoberichterstattung festzuhalten. Diese Bestimmungen sind als Bestandteil des Rahmenkonzepts für das institutsweite Risikomanagement vorzusehen und sollen dementsprechend durch die Geschäftsleitung entwickelt und umgesetzt sowie vom Oberleitungsorgan genehmigt werden. Die Bestimmungen zur Risikodatenaggregation und Risikoberichterstattung umfassen dabei Anforderungen an die Daten-Architektur und die IT-Infrastruktur, die insbesondere die Identifikation von Konzentrationsrisi-

ken[6] erlauben. Dabei ist zentral, dass eine möglichst flexible Daten-Architektur und IT-Infrastruktur angestrebt wird, die eine zeitnahe Berücksichtigung bzw. Integration von neuen Szenarioanalysen und Stressszenarien ermöglicht.

3.5 Internes Kontrollsystem

Die Überarbeitung des FINMA-RS 08/24 zielt auf die Einführung eines ganzheitlichen internen Kontrollsystems (IKS) ab. Hierbei sollen eine effektive Umsetzung des Rahmenkonzepts für das institutsweite Risikomanagement und insbesondere die Einhaltung des vom Oberleitungsorgan verabschiedeten Risikoappetits und der entsprechenden Risikolimiten sichergestellt werden.

Die Ganzheitlichkeit des IKS besteht darin, dass dieses mindestens aus drei voneinander unabhängigen Kontrollinstanzen, namentlich den ertragsorientierten Geschäftseinheiten, den von den ertragsorientierten Geschäftseinheiten unabhängigen Kontrollinstanzen sowie der internen Revision besteht.

Die Risikokontrolle und die Compliance-Funktion stellen die zentralen unabhängigen Kontrollinstanzen dar. Je nach Grösse, Geschäfts- und Organisationskomplexität und Risikoprofil eines Instituts können weitere unabhängige Kontrollinstanzen definiert werden. Verfügt ein Institut bspw. über eine separate Organisationseinheit, die sich mit institutsübergreifenden Sicherheitsthemen wie Informations-, Personen- und Objektschutz beschäftigt, oder verfügt das Institut über eine organisatorisch unabhängige Finanzkontrolle, können diese nebst der Risikokontrolle und der Compliance-Funktion als separate unabhängige Kontrollinstanz fungieren. Jedoch müssen die unterschiedlichen Verantwortlichkeiten der Kontrollinstanzen in jedem Fall eindeutig definiert und kommuniziert werden, d.h. es muss insbesondere festgehalten werden, wer Risiken eingeht und bewirtschaftet und wer unabhängig von einer Ertragskomponente die Überwachung dieser Risiken verantwortet. Weiter gilt es die Aufgaben der unabhängigen Kontrollinstanzen sowohl auf Gruppen- wie Einzelinstitutsebene wahrzunehmen.

Der Fokus der revidierten Bestimmungen zu einem ganzheitlichen IKS liegt hauptsächlich auf der Risikokontrolle, die eine von den ertragsorientierten Geschäftseinheiten unabhängige Überwachung des Risikoappetits und der Risikolimiten (gemäss Rahmenkonzept für das institutsweite Risikomanagement) sicherstellt. Die überarbeiteten Anforderungen bei der Einrichtung und Unterstellung der Risikokontrolle sehen die Anwendung des Proportionalitätsprinzips vor, d.h. die Einrichtung und Unterstellung soll je nach Aufsichtskategorie unterschiedlich erfolgen. Konkret bedeutet dies, dass Institute der Aufsichtskategorien 1 bis 3 über einen eigenständigen Chief Risk Officer (CRO) verfügen müssen, der mindestens für die Risikokontrolle verantwortlich zeichnet. Bei systemrelevanten Banken (Aufsichtskategorien 1 und 2) besteht zusätzlich die erhöhte Anforderung, dass der CRO zwingend in der Geschäftsleitung vertreten sein muss. Bei Instituten der Aufsichtskategorie 3 ist dies nicht zwingend. Bei Instituten der Aufsichtskategorien 4 und 5 kann die Risikokontrolle zudem mit anderen Funktionen der Bank (bspw. mit der Compliance-Funktion) zusammengelegt oder in Personalunion geführt werden, solange dies aus Sicht der Gewährleistung der Unabhängigkeit und Vermeidung von Interessenkonflikten angemessen erscheint[7]. Die Compliance-Funktion kann in jedem Fall unabhängig

[6] Bspw. auf Ebene Länder, Gegenparteien, etc.

[7] Bspw. keine Zusammenlegung oder Personalunion mit ertragsorientierten Geschäftseinheiten.

von der Aufsichtskategorie des jeweiligen Instituts zusammen mit dem Rechtsdienst eine Abteilung bilden. Weiter kann bei Instituten der Aufsichtskategorie 4 und 5 die Compliance-Funktion auch in einem Outsourcing-Verhältnis betrieben werden.

Die Risikokontrolle unterrichtet das Oberleitungsorgan unverzüglich, d.h. ohne schuldhaftes Zögern, über Verletzungen von Risikolimiten, die vom Oberleitungsorgan im Rahmenkonzept für das institutsweite Risikomanagement genehmigt wurden.

3.6 Interne Revision

Die Bestimmungen zur internen Revision werden im vorliegenden Rundschreibenentwurf neu positioniert und befinden sich nicht mehr im Anschluss an jene zum Oberleitungsorgan (Verwaltungsrat) sondern entsprechend dem gängigen IKS-Modell der drei Verteidigungslinien (three lines of defence) nach den Regelungen zum internen Kontrollsystem.

Die bisherigen Ausführungen zur internen Revision werden gemäss ihrer Bedeutung neu angeordnet und leicht angepasst. So wird die Unabhängigkeit der internen Revision als zentrale Bedingung hervorgehoben und das bestehende Anforderungsprofil geschärft. Ausserdem werden die Voraussetzungen zur Übertragung der Aufgaben der internen Revision an einen unabhängigen Dritten mit der Berichtsvorlage zur aufsichtsrechtlichen Prüfung abgestimmt.

3.7 Gruppenstrukturen

Das geltende Rundschreiben enthält – mit Ausnahme der Regelungen bezüglich des Wirkungskreises der internen Revision bei Finanzgruppen – keinerlei Bestimmungen zu Gruppenstrukturen. Da nach geltender Praxis jedoch bereits das aktuelle Rundschreiben auch auf Gruppenstrukturen analog Anwendung findet und internationale Richtlinien ebenfalls entsprechende Bestimmungen vorsehen, werden neu prinzipienbasierte Vorgaben in das neue Rundschreiben aufgenommen.

Der Entwurf sieht damit keine Änderung in der Aufsichtspraxis vor und regelt lediglich ausdrücklich, dass sämtliche Grundsätze und Bestimmungen des Rundschreibens für Finanzgruppen und -konglomerate sinngemäss gelten sollen, namentlich für die Einheiten mit Gesamtverantwortung für die Gruppenführung, unabhängig ob es sich um eine Holding-, Stammhaus- oder atypische Gruppenstruktur handelt.

3.8 Offenlegung

Die Transparenz von Unternehmen gegenüber ihren Stakeholdern wird heute als wichtiger Bestandteil einer guten Corporate Governance anerkannt (OECD, Basler Ausschuss für Bankenaufsicht, economissuisse). Die international und national postulierten Standards werden von grossen oder international tätigen Unternehmen heute selbstverständlich umgesetzt. Bei Unternehmen mit einem international anerkannten Rechnungslegungsstandard besteht zudem die Verpflichtung spezifische Informatio-

nen zur rechtlichen Unternehmensstruktur und zum Risikomanagement im Geschäftsbericht transparent darzustellen[8].

In der Schweiz sind die an der SIX Exchange kotierten Unternehmen gemäss der Richtlinie Corporate Governance[9] dazu verpflichtet, bestimmte Informationen zur Corporate Governance im Geschäftsbericht zu veröffentlichen. Die economiesuisse verweist im „Swiss Code of Best Practice for Corporate Governance“ unter dem Kapitel Offenlegung auf die Anwendbarkeit der SIX-Richtlinie.

Grundsätzlich gelten für alle Banken in der Schweiz die aktienrechtlichen Offenlegungsbestimmungen, welche mittels die Bankengesetzgebung konkretisiert werden. Bezüglich der Veröffentlichung von Informationen zum Thema Corporate Governance müssen lediglich die Minimalbestimmungen gemäss Obligationenrecht eingehalten werden (Art. 959c und Art. 961ff OR).

Zur Stärkung einer effektiven Corporate Governance erachtet es die FINMA als notwendig, dass über die aktienrechtlichen Bestimmungen hinaus den Stakeholdern grundsätzliche Informationen zum Oberleitungsorgan, zur Geschäftsleitung, zum Wahlverfahren dieser beiden Gremien und zur Risikopolitik zugänglich gemacht werden.

Bezüglich des Wahl- und Rekrutierungsverfahrens für Mitglieder des Oberleitungsorgans und der Geschäftsleitung sind beispielsweise die Eckpunkte der Anforderungsprofile sowie der Rekrutierungs- bzw. die Nominationspolitik darzustellen. Mit der Publikation der risikostrategischen Ausrichtung, des Risikoprofils und der Einschätzung der Risikolage durch die Geschäftsleitung soll eine rasche Einschätzung der geschäftsspezifischen Risikosituation ermöglich werden. Es werden keine spezifischen Formate (bspw. Tabellen) für diesen Offenlegungspunkt vorgegeben. Die Risikoinformationen sollen die Offenlegung gemäss FINMA-RS 16/1 ergänzen und das Gesamtbild zur Risk Governance des Instituts vervollständigen.

Die meisten Institute erfüllen die neuen Offenlegungserfordernisse bereits, sei es auf freiwilliger Basis oder aufgrund anderer regulatorischer Vorgaben.

Bei Banken der Aufsichtskategorien 1 bis 3 sind die minimalen Offenlegungsanforderungen zu ergänzen mit Informationen, die gemäss der SIX-Richtlinie nicht nur von reinem Aktionärsinteresse sind. Hierzu gehören insbesondere Angaben zur Struktur der Finanzgruppe (sofern existent), zu weiteren Tätigkeiten und Interessensbindungen der Mitglieder des Oberleitungsorgans und der Geschäftsleitung, zur Organisation des Oberleitungsorgans, zum Entschädigungssystem des Oberleitungsorgans und der Geschäftsleitung, zur Revisionsstelle und Prüfgesellschaft sowie zur Informationspolitik des Unternehmens.

Ungefähr die Hälfte aller Banken der Aufsichtskategorien 1 bis 3 sind kotiert und erfüllen hiermit diese Offenlegungsanforderungen bereits. Die nichtkotierten Institute publizieren häufig auf freiwilliger Basis

[8] U.a. IAS 1, IFRS 7 und IFRS Practice Statement ‘Management Commentary’

[9] Richtlinie betr. Informationen zur Corporate Governance (Corporate Governance Richtlinie, RLCG) vom 1. September 2014.

bereits etliche der verlangten Informationen. Es ist jedoch nicht auszuschliessen, dass bei einigen Instituten der Offenlegungsprozess angepasst werden muss, was punktuell zu Mehrkosten führen kann.

Um den Aufwand von zusätzlichen Offenlegungserfordernissen in Grenzen zu halten, soll auf eine separate Publikation verzichtet werden können, falls die Informationen bereits im ordentlichen Geschäftsbericht oder aufgrund des FINMA-RS 16/1 „Offenlegung – Banken“ publiziert werden.

3.9 Übergangsbestimmungen

Ein Grossteil der revidierten Bestimmungen beinhaltet keine materiellen Neuerungen, sondern verdeutlicht und präzisiert die bereits geltende Aufsichtspraxis. Einige wenige Bestimmungen bringen jedoch Neuerungen mit sich und können bei verschiedenen Instituten einen Anpassungsbedarf auslösen. Es sind dies namentlich die verdichteten Regeln zur Unabhängigkeit und zum Ausschusswesen auf Stufe Oberleitung, die Einführung eines institutsweiten Rahmenkonzepts sowie die Einrichtung und sachgerechte Positionierung der CRO-Funktion innerhalb des Instituts. Zur Verwirklichung dieser Vorgaben wird den betroffenen Instituten eine angemessene Übergangsfrist von einem Jahr ab Inkrafttreten der vorliegenden Änderungen gewährt. Die FINMA kann diese Frist auf begründeten Antrag im Einzelfall verlängern.

4 Erläuterungen zur Teilrevision FINMA-RS 08/21 „Operationelle Risiken Banken“

Die Teilrevision des FINMA-RS 08/21 sieht einerseits eine Entschlackung von Grundsätzen vor, die neu für alle Risikokategorien im revidierten FINMA-RS „Corporate Governance – Banken“ Anwendung finden sollen, und andererseits werden neue Grundsätze hinsichtlich IT- und Cyberrisiken sowie zur Fortführung von kritischen Dienstleistungen im Insolvenzfall und Risiken im grenzüberschreitenden Finanzdienstleistungsgeschäft aufgenommen. Diese Anpassungen betreffen hauptsächlich das Kapitel IV. Qualitative Anforderungen an den Umgang mit operationellen Risiken.

Alle geänderten Textstellen im FINMA-RS 08/21 wurde für die Anhörung gelb unterlegt.

4.1 Proportionalitätsprinzip in Kapitel IV. Qualitative Anforderungen an den Umgang mit operationellen Risiken

Das für das Kapitel IV. angewendete Proportionalitätsprinzip wurde dahingehend angepasst, dass sich kleine Banken grundsätzlich durch die FINMA-Aufsichtskategorien 4 und 5 definieren. Die FINMA kann im Einzelfall Erleichterungen oder Verschärfungen anordnen. Die Beurteilung darüber, ob eine Bank als kleine oder grosse Bank im Sinne der Umsetzung der qualitativen Anforderungen in Kapitel IV. gilt, wird nicht mehr durch die Bank selbst resp. die jeweilige Prüfgesellschaft sondern im Einzelfall durch die FINMA vorgenommen.

4.2 Entschlackung des Kapitel IV. Qualitative Anforderungen an den Umgang mit operationellen Risiken

Die Entschlackung des FINMA-RS 08/21 betrifft einerseits Grundsatz 1 über die Verantwortlichkeiten des Oberleitungsorgans und der Geschäftsleitung sowie andererseits Grundsatz 2 über das Rahmenkonzept und Kontrollsystem. Diese Grundsätze wurden ins FINMA-RS „Corporate Governance – Banken" integriert und sind neu für alle Risikokategorien anzuwenden. Im Hinblick auf den Grundsatz 1 über die Verantwortlichkeiten gilt es den Risikoappetit der operationellen Risiken weiterhin anhand einer separaten Beurteilung der Risikobereitschaft und Risikotoleranz festzulegen (sog. Klassifizierung der operationellen Risiken). Dies gilt es auch bei der Erstellung des Rahmenkonzepts und in Bezug auf den Grundsatz 2 zu beachten. Die Klassifizierung erfolgt typischerweise anhand einer Risikomatrix, die für jede Kategorie[10] von operationellen Risiken eine Beurteilung der Eintrittswahrscheinlichkeit und des Schadensausmasses beinhaltet, sowohl auf Stufe der Risikobereitschaft als auch auf Stufe der Risikotoleranz. Die Klassifizierung der einzelnen Kategorien von operationellen Risiken basiert dabei insbesondere auf den Risiko- und Kontrollbeurteilungen sowie den Revisionsergebnissen. Es können weitere Instrumente und Methoden wie die Erhebung und Analyse von Verlustdaten oder die Durchführung von Szenarioanalysen für die Klassifizierung der Kategorien von operationellen Risiken hinzugezogen werden.

4.3 Integration von Grundsätzen für IT- und Cyberrisiken

Die Aufnahme von Grundsätzen für IT- und Cyberrisiken erfolgt durch eine Erweiterung des bestehenden Grundsatzes 5 über die Technologieinfrastruktur. Dabei sind sowohl im Hinblick auf die IT- wie Cyberrisiken Bestimmungen zur Einführung eines Konzepts vorgesehen, das minimale Aspekte zu beinhalten hat.

Die Mindestanforderungen an das Konzept über die IT-Risiken umfassen u.a. eine möglichst aktuelle und vollständige Übersicht über die IT-Netzwerkumgebung. Es ist jedoch insbesondere bei Grossbanken angebracht, die Erstellung und das Führen einer solchen Übersicht unter Berücksichtigung einer gewissen Wesentlichkeit für den Geschäftsbetrieb sicherzustellen. Die Übersicht über die IT-Netzwerkumgebung soll u.a. als Grundlage für den Umgang mit Cyberrisiken dienen, um potenzielle Angriffspunkte für Cyberattacken und mögliche Schwachstellen identifizieren zu können.

Das Konzept über die Cyberrisiken umfasst Mindestanforderungen, die einen möglichst ganzheitlichen Ansatz im Umgang mit Cyberrisiken gewährleisten sollen, d.h. von der Berücksichtigung von Cyberrisiken bei der Festlegung des Risikoappetits für die operationellen Risiken bis zu einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach einer erfolgten Cyberattacke.

Zentral sind insbesondere die Identifikation und der Schutz von besonders schützenswerten Daten und Systemen vor Cyberattacken. Bei besonders schützenswerten Daten sind v.a. die Integrität und Vertraulichkeit von Kundenidentifikationsdaten sicherzustellen. Bei Systemen gilt es insbesondere diejenigen vor Cyberattacken zu schützen, die sowohl für eine laufende Verfügbarkeit der für das je-

[10] Bspw. IT-/Cyberrisiken, Recht/Compliance, Interner Betrug, etc.

weilige Institut kritischen Geschäftsprozesse unerlässlich sind wie auch diejenigen, die im Zusammenhang mit den kritischen Funktionen und Dienstleistungen[11] gemäss FINMA-RS 08/21 Grundsatz 5 stehen.

Weiter gilt es durch die Geschäftsleitung zu gewährleisten, dass eine regelmässige Verwundbarkeitsanalyse bzw. ein Penetration Testing durchgeführt wird, um insbesondere in Bezug auf die besonders schützenswerten Daten und Systeme Schwachstellen möglichst zeitnah zu identifizieren und beheben zu können. Die Analyse kann bei Vorhandensein von qualifizierten Ressourcen durch interne Stellen durchgeführt werden. Sind jedoch kein geeignetes Personal und Ressourcen intern vorhanden, muss die Durchführung der Verwundbarkeitsanalyse bzw. eines Penetration Testing an einen externen Dienstleister delegiert werden. Bei der Auswahl eines externen Dienstleisters soll dessen Qualifizierung durch die Durchführung einer Sorgfaltsprüfung (Due Diligence) sichergestellt werden.

4.4 Fortführung von kritischen Dienstleistungen im Insolvenzfall

Das Ziel dieser Anforderungen ist es zu vermeiden, dass der plötzliche Ausfall oder Unterbruch von institutsspezifischen Funktionen Auswirkungen auf die Finanzstabilität sowie die Restrukturierung oder die Abwicklung einer systemrelevanten Bank hat. Zur Aufrechterhaltung dieser Funktionen (sogenannte „kritische Funktionen“) ist es notwendig, dass systemrelevante Banken sicherstellen, dass auch die für die kritischen Funktionen notwendigen Dienstleistungen (sog. „kritische Dienstleistungen“) im (drohenden) Insolvenzfall fortgeführt werden können. Werden die kritischen Dienstleistungen von der regulierten Bank selbst erbracht (sog. „Inhouse“-Dienstleistungen), sind die für die Fortführung im Insolvenzfall nötigen Anforderungen im FINMA-RS 08/21 geregelt. Die Anforderungen für den Bezug von kritischen Dienstleistungen von einem Drittanbieter oder einer gruppeninternen Dienstleistungsgesellschaft werden im Rahmen der Teilrevision des FINMA-RS 08/7 „Outsourcing Banken“ aufgenommen.

Die neuen Vorschriften wurden in Anlehnung an internationale Rechtsentwicklungen in diesem Bereich ausgestaltet, insbesondere unter Berücksichtigung des FSB Konsultationspapiers „Guidance on Arrangements to Support Operational Continuity in Resolution“[12], welches Prinzipien für die Verbesserung der Fortführung von kritischen Dienstleistungen im Insolvenzfall enthält. Neben den nur für systemrelevante Banken verbindlichen Regeln sind einzelne Vorschriften, wo sinnvoll, auch auf nicht-systemrelevante Banken anwendbar. So haben auch nicht-systemrelevante Banken ein Inventar über die aus ihrer Sicht wichtigsten Dienstleistungen zu erstellen. Dies soll eine Abwicklung oder Restrukturierung im Insolvenzfall wesentlich vereinfachen.

4.5 Risiken im grenzüberschreitenden Finanzdienstleistungsgeschäft

Die Verletzung ausländischen Rechts kann gegen bestimmte offen formulierte schweizerische Aufsichtsnormen verstossen, so insbesondere gegen das Erfordernis der Gewähr für einwandfreie Ge-

[11] Vgl. Kapitel 4.4 Fortführung von kritischen Dienstleistungen im Insolvenzfall

[12] http://www.fsb.org/wp-content/uploads/Guidance-on-Arrangements-to-Support-Operational-Continuity-in-Resolution.pdf

schäftstätigkeit. Zudem gelten die Erfordernisse für das Risikomanagement auch für die Risiken aus dem grenzüberschreitenden Geschäft.

Im Oktober 2010 beschrieb die FINMA in einem Positionspapier ihre Erwartungen an das Management der Rechts- und Reputationsrisiken im grenzüberschreitenden Finanzdienstleistungsgeschäft. Am 19. Juni 2012 publizierte sie Antworten zu den häufigsten Fragen (FAQ) in diesem Kontext.

Die Behandlung dieser speziellen Risiken in einem gesonderten Positionspapier war angesichts der damals bestehenden Auslegungsfragen angezeigt. Inzwischen hat sich das rechtliche und sonstige Umfeld weiterentwickelt, und die Risiken aus dem grenzüberschreitenden Finanzdienstleistungsgeschäft sind den Marktteilnehmern bekannt und bewusst.

Mit einem neuen Grundsatz zu Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft werden die bekannten Erwartungen der FINMA im Interesse einer Konsolidierung und Verstetigung in das FINMA-RS 08/21 überführt. Der neue Grundsatz auf Stufe Rundschreiben ist prinzipienbasiert formuliert, nimmt aber die im Positionspapier beschriebene Verwaltungspraxis vollständig und ohne inhaltliche Änderung auf. Der bisherigen gesonderten Behandlung in einem eigenständigen Positionspapier und FAQ bedarf es daher nicht mehr.

Die FINMA wird das angemessene Management der Risiken aus dem grenzüberschreitenden Finanzdienstleistungsgeschäft auch weiterhin im Rahmen der normalen Aufsicht thematisieren.

4.6 Anhang 3: Umgang mit elektronischen Kundendaten

Durch die Integration des FAQ ins FINMA-RS 08/21 erfährt ebenfalls der Anhang 3 zum Umgang mit elektronischen Kundendaten geringfügige Anpassungen. Präzisiert werden einzelne Randziffern in den Grundsätzen 3 (Datenspeicherort und –zugriff), 5 (Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben) und 7 (Risikominderung in Bezug auf die CID-Vertraulichkeit).

5 Erläuterungen zur Teilrevision FINMA-RS 10/1 „Vergütungssysteme“

Der zwingende Geltungsbereich des Rundschreibens umfasst zurzeit die beiden grössten Versicherungsgruppen (Zurich und Swiss Re) und die Banken der Aufsichtskategorien 1 und 2.

Neu wird in Rz 3 explizit darauf hingewiesen, dass das Rundschreiben ergänzend zur Verordnung gegen übermässige Vergütungen bei börsenkotierten Aktiengesellschaften (VegüV) Anwendung findet. Für die meisten Institute besitzt das Rundschreiben nach wie vor einen Richtliniencharakter. Zwingend sind die einzelnen Anforderungen nur noch für Institute, die erforderliche Eigenmittel (Mindestanforderungen gemäss Art. 7 ff. bzw. Art. 42 der ERV) von mindestens CHF 10 Milliarden halten müssen. Hiermit werden Institute der Aufsichtskategorie 2 von einer nicht zielführenden Regulierung entlastet. Die FINMA behält sich allerdings weiterhin vor, Banken mit Mindesteigenmitteln unter dem

Schwellenwert in begründeten Fällen zu verpflichten, einzelne oder sämtliche Bestimmungen des Rundschreibens umzusetzen (Rz 9).

Eine weitere Änderung betrifft die Verantwortlichkeit des Verwaltungsrats, welcher künftig jährlich die Vergütungen der Geschäftsleitung, der Leiter der Kontrollfunktionen sowie den Gesamtpool für das Finanzinstitut genehmigen soll. Der Verwaltungsrat soll zudem unabhängig von der Grösse und Struktur des Finanzinstituts oder Komplexität von dessen Vergütungssystem einen Entschädigungsausschuss einsetzen. Dieser soll eine unabhängige und fachkundige Unterstützung des Verwaltungsrats sicherstellen.

In materieller Hinsicht müssen die Vergütungssysteme künftig zwei zusätzliche Bedingungen einhalten. Erstens sollen keine Transaktionen getätigt werden dürfen, welche der Wirksamkeit der Elemente des Vergütungssystems zuwiderlaufen (z.B. Absicherungsgeschäfte). Zweitens sind die Vergütungsverträge so auszugestalten, dass eine Rückforderung von bereits ausbezahlten variablen Vergütungen grundsätzlich möglich ist („Claw-back"). Die beiden zusätzlichen Erfordernisse dienen der besseren Wirksamkeit von Vergütungssystemen und sollten ohne grossen Aufwand umsetzbar sein.

6 Auswirkungen

Die Notwendigkeit und der Nutzen einer adäquaten Corporate Governance und eines effektiven Risikomanagements für Finanzinstitute sind unbestritten und durch die in der Finanzmarktkrise gemachten Erfahrungen nochmals unterstrichen worden. Mit der Bündelung zeitgemässer Vorgaben zur Corporate Governance und zum Risikomanagement bei Banken im neuen Rundschreiben wird die Sicherheit und Stabilität der einzelnen Institute verbessert. Die umfassende Sichtweise bezüglich der Themen Corporate Governance, internes Kontrollsystem und Risikomanagement entspricht der heutigen Praxis in der Finanzbranche. Das neue Rundschreiben postuliert weiterhin prinzipienorientierte Erfordernisse an die Finanzinstitute. Der Spielraum für die institutsbezogene Umsetzung bleibt erhalten. Insbesondere bezüglich der Anwendung des „three-lines-of-defences"-Modells existieren je nach Grösse und Risikoprofil sehr unterschiedliche Lösungen, die weiterhin ihre Berechtigung haben sollen, sofern die grundlegenden Ziele bezüglich ausgewogener „checks and balances" und eines effektiven Risikomanagements damit erreicht werden. Ein Grossteil der Neuerungen gibt lediglich die geltende Bewilligungspraxis wieder, schafft dadurch aber mehr Klarheit und Rechtssicherheit. Für die Mehrheit der beaufsichtigten Banken und Effektenhändler sind mit der vorliegenden Revision keine Änderungen angedacht. Für einzelne Institute ist allerdings nicht auszuschliessen, dass in Bezug auf die Unabhängigkeitserfordernisse beim Oberleitungsorgan, die Pflicht zum Unterhalt eines separaten Risikoausschusses für Banken der Aufsichtskategorien 1 – 3, die Installation einer separaten CRO-Funktion, die Konsolidierung des Rahmenkonzepts für das institutsweite Risikomanagement und die Umsetzung der Offenlegungsvorschriften in der Jahresberichtserstattung gezielte Anstrengungen nötig sein werden, um den geänderten Anforderungen zukünftig gerecht zu werden.

Mit der Einführung des Proportionalitätsprinzips im neuen Rundschreiben wird eine bewährte Methode weitergeführt[13], um Institute der Aufsichtskategorien 4 und 5 grundsätzlich von einzelnen Anforderungen zu entlasten. Das bisher angewendete Proportionalitätsprinzip im FINMA-RS 08/21 wird demjenigen im FINMA-RS „Corporate Governance – Banken“ angeglichen. Damit gelten rund 30 Institute gemäss FINMA-RS 08/21 neu als kleine Banken und werden von der Erfüllung weitergehender Anforderungen unter diesem Rundschreiben befreit.

Im FINMA-RS 10/1 werden einzelne Institute entlastet, da der Schwellenwert der Mindesteigenmittel für die zwingende Umsetzung von CHF 2 auf CHF 10 Mia. angehoben wird.

7 Weiteres Vorgehen

Die Resultate der Anhörung werden in einem Anhörungsbericht publiziert. Nach Vornahme allfälliger Anpassungen sollen das FINMA-RS „Corporate Governance - Banken“ sowie die überarbeiteten FINMA-RS 08/21 „Operationelle Risiken – Banken“ und 10/1 „Vergütungssysteme“ per 1. August 2016 in Kraft treten.

[13] Vgl. bspw. FINMA-RS 16/1 „Offenlegung Banken“