Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi (peter.ruetschi@finma.ch)
Laupenstrasse 27
CH-3003 Bern

Zürich, 11. April 2016

GEBÜNDELTE ANFORDFERUNGEN AN DIE CORPORATE GOVERNANCE - ANHÖRUNG

Sehr geehrter Herr Rütschi

Gemäss Medienmitteilung vom 1 März 2016 senden wir in diesem Schreiben das gemeinsame Feedback der Aduno Gruppe und der Governance Concept GmbH. Aus fachtechnischen Gründen wird sich unser Feedback auf das Thema ‚IT- und Cyber-Risiken' konzentrieren (FINMA-RS 2008/21 und FINMA-RS 2016/xx) - und innerhalb dieses Themas konzentrieren wir uns auf die nachfolgenden zehn Punkte. Als summarisches Feedback kann an dieser Stelle festgehalten werden, dass die beabsichtigte Regulation eine hervorragende Grundlage für die Verbesserung des Cyber-Schutzes in der Schweizer Finanzindustrie darstellt.

Feedback

1. Die Themenabgrenzung trägt aktuell den Titel ‚**IT- und Cyber-Risiken**'. Damit wird ein Grossteil der gewollten Risiken abgedeckt. Ein weiterer Teil relevanter Risiken fällt jedoch nicht in diesen Scope. Es handelt sich dabei um die Informationssicherheitsrisiken. Und zwar insbesondere diejenigen, welche mit konventionellen Informationsträgern (z.B. Papier) sowie mit dem gesprochenen Wort zu tun haben. Im Bereich des Social-Engineerings, eines beliebten Teilvektors von Angriffen, kommt der gesprochenen Information einen hohen Stellen werde zu. Aus diesem Grund empfehlen wir, zum Vornherein die Themenabgrenzung folgendermassen zu wählen: ‚**Informationssicherheits-, IT- und Cyber-Risiken**'.

2. Das Verlangen nach einer aktuell gehaltenen **Netzwerkübersicht** ist sinnvoll.[1] Es ist jedoch nicht üblich, dass auf einer solchen der Zusammenhang zwischen Applikationen und Servern ersichtlich ist: die Netzwerkübersicht konzentriert sich auf die Darstellung der Netzwerke, inkl. der darin vorkommenden Systeme und Kommunikationsverbindungen. Der Zusammenhang ‚Applikation zu Server' (welchen zu verlangen unbedingt notwendig ist) geht i.d.R. aus einer sogenannten **CMDB** (Configuration-Management-Database) hervor. Eine CMDB zu führen, kann jedoch nicht in jedem Fall erzwungen

[1] Siehe z.B. FINMA-RS 2008/21, Rz. 135.1.

werden - leider ist das aktuell noch nicht in allen Instituten gängige Praxis. Es gälte also eine Zusatzinformation zur Netzwerkübersicht zu verlangen, welche jedem Institut - unabhängig von der Grösse - zugemutet werden kann: hier bietet sich eine Art von **IT-Asset-Inventar** an. Wir empfehlen folgendes zu verlangen: *‚…eine Netzwerkübersicht und ein Inventar aller Applikationen und Servern; letzteres muss auch aufzeigen, auf welchem Server welche Applikationen betrieben werden… …sollte der Speicherort der Daten ein anderer sein als derjenige der Applikationen, so sind die entsprechenden Datenspeicherorte ebenfalls im genannten Inventar zu führen‘*. Durch die Ergänzung der bereits verlangten Netzwerkübersicht durch das IT-Inventar wird dann der gesamte relevante Meta-Informationsbereich abgedeckt. Zudem wird die Konsistenz zur Forderung in Rz. 16 Anh. 3 FINMA-RS 2008/21 hergestellt, welche explizit vom Applikationsinventar, inkl. Verbindung zur Infrastruktur spricht.

3. FINMA-RS 2008/21, Rz. 121 und insbesondere Fussnote (Fn.) 8. Im Paragraph wird über die **Risikokategorisierung** geschrieben. Die **Risikoklassifizierung** folgt erst im nächsten Paragraphen. Die Fussnote 8 bezieht sich jedoch zunächst auf die Risikoklassifizierung. Fn. 8 sollte u.E. folgendermassen lauten: ‚*Besteht keine einheitliche **Kategorisierung** der operationellen Risiken, kann dies die Wahrscheinlichkeit erhöhen, dass Risiken nicht identifiziert und **klassifiziert** werden oder keine Verantwortlichen für die Beurteilung, Überwachung, Kontrolle und Minderung der Risiken zugeordnet wird.*‘ [Die Reihenfolge der Begriffsverwendung ‚Kategorisierung‘ und ‚Klassifizierung‘ ist in unserem Vorschlag in Fn. 8 vertauscht - wir erachten das auch inhaltlich als sinnvoller/aussagekräftiger.]

4. FINMA-RS 2008/21, Rz. 135.1, Bst. d. Zusätzlich zu den Daten- und Prozessverantwortlichen sollten auch die **Applikationsverantwortlichen** erwähnt werden. Erst durch das Zusammenspiel aller drei Rollen entsteht das Gesamtbild. In kleineren Organisationen können Daten- und Applikationsverantwortliche oder auch Daten- und Prozessverantwortliche in Personalunion festgelegt werden (es handelt sich um Rollen, nicht um Personen).

5. FINMA-RS 2008/21, Fn. 16. Als Ergänzung zum bereits genannten COBIT-Standard von ISACA (vgl. Fn. 15) könnte hier das **Cybersecurity-Framework** von NIST erwähnt werden. Es handelt sich dabei um den weltweiten Standard in der Governance der Cybersicherheit (siehe http://www.nist.gov/cyberframework/).

6. FINMA-RS 2008/21, Rz. 135.3. Ergänzend zu den (1) Verwundbarkeitsanalysen und den (2) Penetration-Tests sollte die (3) ‚*umfassende Erhebung der Effektivität der Kontrollen im Zusammenhang mit relevanten Informationssicherheits-, IT- und Cyber-Risiken*‘ erwähnt werden. Ansonsten fehlt das dritte der drei wichtigsten Selbstanalyseaktivitäten, nämlich das Control-Self-Assessment.

7. Die Verwendung des Begriffs ‚besonders Schützenswerte Daten'[2] könnte zu Verwechslungen mit der ähnlichen Begriffsverwendung im Bereiche des Personendatenschutzes führen: vgl. Art. 3c DSG (SR 235.1). Hier könnte sich zur Verwendung im FINMA-Kontext folgender alternative Begriff anbieten: ‚**sensitive oder kritische Daten**' und entsprechend ‚sensitive oder kritische Systeme'. [Anmerkung: In der Sicherheitspraxis wird ‚sensitiv' als Indikator für ‚Vertraulichkeit' und kritisch als Indikator gleichsam für ‚Integrität' (im Sinne von ‚Richtigkeit') und ‚Verfügbarkeit' verwendet.]

8. Beim Grundsatz 6 (FINMA-RS 2008/21) zu Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft wird - was sicherlich richtig ist - ein Schwerpunkt auf geschäftliche Aspekte gelegt. Das Thema des grenzüberschreitenden Datenverkehrs wird jedoch nicht angesprochen. Die Klammer in der dritten Zeile Rz. 136.4 könnte folgendermassen ergänzt werden: ‚*(Steuer-, Straf-, Geldwäschereirecht,* ***Datenschutzbestimmungen****, usw.)*'

9. FINMA-RS 2008/21, Rz. 18 Anh. 3. Die Verwendung des Begriffs der ‚Endbenutzeranwendungen' entspricht u.E. nicht der gängigen Praxis. Nicht die Applikationen welche auf CID Zugriff gewährleisten werden ‚Endbenutzeranwendungen' genannt. Unter ‚Endbenutzeranwendungen' werden u.a. von Benutzern erstellte MS-EXCEL-Dateien, MS-ACCESS-Anwendungen, etc.[3] zusammengefasst. Natürlich können solche Endbenutzeranwendungen CID enthalten, hiervon ist jedoch abzuraten. Wenn ein zusammenfassender Begriff für Anwendungen/Applikationen gesucht wird, welche für Endbenutzer den Zugriff auf CID ermöglichen, dann sollte der Begriff ‚**Anwendungen mit Endbenutzerschnittstelle**' o.ä. gewählt werden.

10. FINMA-RS 2008/21, Rz. 33 Anh. 3. Dieser korrekte Paragraph sollte noch ergänzt werden durch die explizite Erwähnung von Systemadministratoren, diese haben nämlich keinen ‚funktionalen Zugriff auf Massen-CID', wohl aber einen Zugriff auf Betriebssystemebene. Der Schluss des Paragraphen könnte folgendermassen ergänzt werden: ‚*…z.B. chiffrierte Konten) anzuwenden. Zudem sind auch Systemadministratoren mit CID-Zugriff auf Systemebene zu den Schlüsselmitarbeitenden zu zählen.*' Anmerkung: In der Praxis wird der erweiterte Zugriff auf Anwendungsebene als ‚privilegierter Zugriff' (Privileged Access) und der erweiterte Zugriff auf Systemebene als ‚hoch-privilegierter Zugriff' (Highly-Privileged Access) bezeichnet - diese Begriffsverwendung ist jedoch nicht standardisiert, weshalb der Paragraph in der jetzigen Form zuzüglich der oben erwähnten Ergänzung genügend verständlich ist.

---

[2] Siehe FINMA-RS 2008/21, Rz. 135.2, Bst. a und Rz. 135.3.

[3] Endbenutzeranwendungen betreffen in jedem Fall die sogen. Individuelle Datenverarbeitung (IDV). Meist werden dazu Werkzeuge der sogen. Büroautomation verwendet (i.d.R. die MS-OFFICE-Software-Produkte).

Soweit das Feedback zur Anhörung aufgrund der auf der FINMA-Website zugänglichen Informationen. Wir sind uns bewusst, dass einzelne Feedbackpunkte Inhalte betreffen, welche bereits in der bestehenden gültigen Version des Rundschreibens 2008/21 vorhanden sind.[4] Es erschien uns jedoch angebracht, auch solche Punkte zu erwähnen. Für Fragen oder bei Bedarf nach zusätzlichen Informationen stehen wir jederzeit gerne zur Verfügung.

Freundliche Grüsse

Für die **Aduno Gruppe**:

Thomas Müller, Group Security Officer

<ELEKTRONISCHES EXEMPLAR OHNE UNTERSCHRIFT>

Kontakt: thomas.mueller@aduno-gruppe.ch

Für die **Governance Concept GmbH**[5]:

Rainer Kessler, Auditor & Consultant

<ELEKTRONISCHES EXEMPLAR OHNE UNTERSCHRIFT>

Kontakt: rainer.kessler@mensa.ch

Kopie geht an: Yves Obrist, Risk Management, Banks Division, FINMA.

[4] Z.B. Feedback zu ‚Endbenutzeranwendungen'.
[5] Unterstützung der Aduno Gruppe in Fragen der Technologie-Compliance.

Association de
Banques Privées Suisses
Vereinigung
Schweizerischer Privatbanken
Association of Swiss Private Banks

Par e-mail

(peter.ruetschi@finma.ch)

Autorité fédérale de surveillance des
marchés financiers FINMA
M. Peter Rütschi
Laupenstrasse 27
CH-3003 Berne

Genève, le 13 avril 2016

Projet de Circulaire FINMA 2016/xx « Gouvernance d'entreprise – banques »

Monsieur,

Dans le cadre de l'audition ouverte le 1er mars 2016, l'Association de Banques Privées Suisses (ABPS) souhaite prendre position à propos de l'objet cité sous rubrique.

Nous vous prions de bien vouloir trouver ci-après nos commentaires.

Le projet de circulaire n'opère pas assez de distinctions entre les différents types de banques, dont la diversité fait la richesse de la place financière suisse. En outre, le degré de détails du projet est tel qu'il relève plus du droit matériel que du droit prudentiel. Le contenu de la circulaire doit ainsi être revu de manière tellement approfondie que l'ABPS préconise qu'une consultation soit ouverte sur une deuxième version de celle-ci, qui tiendrait compte des commentaires suivants :

A) Commentaires généraux

- **Champ d'application / principe de proportionnalité: le projet de circulaire ne tient pas compte de la structure de détention de la banque ni du rôle et des fonctions occupées par son ou ses propriétaires majoritaires ou uniques. Les allégements prévus pour les banquiers privés ont été supprimés, alors qu'ils devraient être maintenus.**
- **Comparaison au niveau international : les « *Corporate governance principles for banks* », édictés en juillet 2015 par le Comité de Bâle, fixent un cadre structuré, clair et suffisamment détaillé. Le projet devrait davantage s'en inspirer.**
- **Répartition des compétences : le projet introduit des dispositions qui créent une confusion entre la surveillance et le contrôle, ce qui porte préjudice à l'équilibre souhaitable entre l'organe responsable de la direction supérieure et la direction.**

- **Composition des organes : les qualificatifs utilisés pour définir les critères que doivent remplir les membres des organes ne sont pas suffisamment précis.**
- **Publication : les dispositions relatives à la publication ne tiennent pas compte de la nature de la banque, de son statut ou de son mode de financement. Elles vont ainsi bien au-delà des principes définis par le Comité de Bâle.**
- **L'entrée en vigueur est prévue pour le 1er juillet 2016, ce qui laisse un délai d'adaptation beaucoup trop court. La date de l'entrée en vigueur devrait être repoussée au moins au 1er janvier 2017.**

B) <u>Commentaires spécifiques relatifs à la forme juridique de société en commandite par actions (SCA)</u>

- **La circulaire n'est pas adaptée aux besoins spécifiques des groupes bancaires contrôlés par une SCA. Il n'y a en effet pas d'organe dans la SCA qui cumule la haute direction, la surveillance et le contrôle. Ces fonctions sont partagées entre l'administration (haute direction et surveillance) et l'organe de contrôle (contrôle). Les holdings de groupes bancaires structurées sous forme de SCA devraient donc obtenir une exonération expresse pour la plupart des clauses de gouvernance d'entreprise.**

A) <u>Commentaires généraux</u>

<u>Nécessaire refonte de la circulaire</u>

Le projet de circulaire ressemble à un modèle de règlement d'organisation d'une banque, alors que l'art. 3 al. 2 let. a de la loi sur les banques consacre le principe fondamental de l'auto-organisation. Celui-ci permet de tenir compte de la réalité du terrain. La FINMA devrait s'en tenir à la mise en œuvre des standards internationaux, définis en l'occurrence par le Comité de Bâle. Le contenu de la circulaire doit être revu de manière approfondie pour éviter que sa mise en œuvre soit source de difficultés.

Compte tenu du grand nombre de modifications nécessaires, l'ABPS suggère que la FINMA élabore un nouveau projet qui tienne compte des remarques ci-après, et surtout de la forme spécifique des groupes bancaires contrôlés par une SCA, et qu'une nouvelle consultation soit organisée.

<u>Champ d'application</u>

L'actuelle circulaire FINMA 2008/24 tient expressément compte du statut particulier des banquiers privés. Le projet n'en fait toutefois aucune mention, prévoyant un système de gouvernance peu compatible avec cette forme juridique expressément autorisée.

De même, le projet ne tient nullement compte de la structure organique des établissements bancaires en général, respectivement des groupes bancaires, ni du mode de détention de ces derniers, alors même que ces deux éléments sont

consubstantiels à la gouvernance. Il en va ainsi des groupes détenus par un actionnariat privé (en mains familiales ou d'associés), en particulier des anciens banquiers privés qui se sont récemment restructurés, au niveau de la banque sous forme de société anonyme et au niveau du groupe sous forme de société en commandite par actions. Pour ces établissements, il est nécessaire de préciser les cm qui ne leur sont pas applicables respectivement de préciser la façon dont les cm doivent être appliqués au niveau du groupe.

Principe de proportionnalité

Le projet de circulaire ne considère pas le mode de détention ni ne tient compte de la nature des actionnaires (privés ou publics) ou de leur rôle dans la direction des banques et groupes bancaires. Ainsi la circulaire ne tient pas compte du rôle particulier des Associés des banques privées, qui non seulement sont responsables de la constitution des fonds propres mais sont également chargés d'exprimer la propension et la tolérance aux risques. Ce regroupement de responsabilités a pour conséquence une convergence des intérêts qui a pour effet de diminuer les risques de la place financière, des créanciers des banques concernées et de l'ensemble des parties prenantes, contrairement à ce que laisse entendre le cm 26.

Comme la FINMA le reconnaît elle-même en page 32 de son dernier rapport annuel, « *des modèles d'affaires et structures de risque différents des prestataires de services financiers doivent par exemple être pris en compte lors de la réglementation. Autrement dit, une réglementation proportionnée qui ne place pas tout le monde à la « même enseigne » est exigée* ».

Comparaison au niveau international

Les « *Corporate governance principles for banks* », édictés par le Comité de Bâle en juillet 2015, fixent un cadre structuré, clair et suffisamment détaillé, qui tient compte expressément du rôle des actionnaires dans l'application du principe de proportionnalité (§ 20). Dès lors qu'il apparaît que la FINMA est pressée de modifier la circulaire, elle aurait pu limiter son effort à reprendre de manière littérale ces « *principles* », en y ajoutant les particularités qu'elle juge nécessaire à la sauvegarde des intérêts de la place financière suisse.

Les utilisateurs de la circulaire gagneraient à disposer d'une terminologie basée sur un référentiel et des standards internationaux, ainsi que de définitions précises des termes, notamment en matière de gestion des risques et de gouvernance.

Nous comprenons que cette circulaire représente un socle pour l'ensemble des dispositions en matière de gouvernance et gestion des risques. Il est donc d'autant plus important qu'elle puisse constituer une référence sur les principes, le champ d'application et la terminologie. Nous suggérons dès lors la mise sur pied d'un comité de rédaction.

Répartition des compétences

En comparaison de la circulaire FINMA 2008/24, le projet introduit des dispositions qui créent de nombreuses confusions ou modifications dans la répartition des

compétences, ce qui porte préjudice à l'équilibre (« checks and balances ») souhaitable entre l'organe responsable de la direction (ORDS) et la direction.

En effet, l'ORDS se voit attribuer plusieurs tâches exécutives (cm 13 : édiction des directives nécessaires à l'exploitation commerciale ; cm 15 : décision d'engagement de cadres en sus des membres de la direction) ou voit sa responsabilité augmentée au-delà de ses capacités d'intervention (cm 16 : garantie de la compliance au sein de l'établissement).

De plus, au niveau des comités spécialisés de l'ORDS, nous relevons

- une confusion entre des tâches de contrôle (cm 49 : vérification de l'entretien par l'établissement d'une gestion des risques appropriée) qui sont normalement de la responsabilité de la direction avec des tâches de surveillance qui ressortent de la responsabilité de l'ORDS ;
- une confusion entre les tâches du comité d'audit et du comité des risques (cm 43, alors que le comité d'audit ne devrait pas être en charge du contrôle des risques).

Toutes ces règles représentent une véritable intrusion dans les affaires internes des banques, alors que la FINMA n'a pas pour mission d'expliciter le Code des Obligations.

Composition des organes

Les qualificatifs utilisés pour définir les critères que doivent remplir les membres des organes ne sont pas suffisamment précis et laissent place à un pouvoir d'appréciation arbitraire (cm 18 et 19) : les compétences et connaissances arrêtées pour les membres de l'ORDS ont pour conséquence de ne rendre éligibles à la fonction que des experts techniques ou des spécialistes, sans prendre en compte qu'au niveau de cet organe, il convient d'abord de disposer de personnes avec une vue stratégique ou des capacités créatives à même d'assurer la diversité des opinions et des points de vue. Par ailleurs, au cm 34, le caractère « exceptionnel » de l'intégrité requise n'est pas défini.

Nous suggérons de préciser que, dans les cas où un comité d'audit et un comité des risques séparés sont exigés, il est néanmoins permis que chaque comité soit composé des mêmes membres. Toute autre interprétation aurait pour effet une augmentation démesurée du nombre de membres de l'ORDS, dès lors que la FINMA maintiendrait le ratio minimum d'un tiers de membres indépendants exigé jusqu'à aujourd'hui. A ce titre, il convient de préciser quelle est la partie déterminante des membres de l'ORDS qui ne doit pas disposer d'une participation qualifiée, au risque de laisser un pouvoir de décision arbitraire à la FINMA.

Il convient aussi de préciser en quoi le comité d'audit doit se démarquer des autres comités.

Enfin, nous considérons que les exigences liées à l'évaluation de l'adéquation des profils (cm 30 à 33) a pour effet de faire primer les aspects formels sur les aspects matériels, alors même que les membres de l'ORDS et de la direction doivent dans tous les cas bénéficier de la garantie de l'activité irréprochable et engagent leur responsabilité de manière personnelle. La surabondance de détails vide de leur substance les principes qu'ils sont censés concrétiser.

Publication

Les dispositions envisagées sous le chapitre « X Publication » ne tiennent pas compte de la nature de la banque (établissement coté / non coté), de son statut (p. ex. banque cantonale) ou de son mode de financement (p. ex. appel à l'épargne). Ces éléments devraient être néanmoins considérés, conformément au principe de proportionnalité prévu sous cm 9 et s'aligner sur les standards internationaux (« *principle* » 12 du Comité de Bâle).

Dans tous les cas, il nous apparaît inapproprié d'imposer aux banques détenues en mains privées les mêmes exigences qu'aux sociétés cotées en bourse. Ainsi les dispositions prévues aux cm 135 à 143 devraient rester obligatoires pour les seules sociétés cotées en bourse.

Divers

Dans le cadre de notre prise de position, nous précisons n'avoir tenu compte que du projet de circulaire. En effet, l'ensemble des documents produits au moment de la mise en consultation présentent des redondances imparfaites et, du moins en apparence, des contradictions, ne facilitant pas la compréhension de l'ensemble.

Nous relevons également la nécessité de revoir la terminologie utilisée dans le projet afin de l'adapter aux termes en usage dans les standards internationaux (p. ex. « pilotage des risques », « pilotage opérationnel des revenus », « aménagement efficace de la comptabilité », « entretien du système de contrôle interne ») ou de l'aligner sur les termes déjà utilisés dans d'autres circulaires (p. ex. « appétence »).

Entrée en vigueur

L'entrée en vigueur est prévue pour le 1er juillet 2016, ce qui laisse un délai d'adaptation beaucoup trop court. La date de l'entrée en vigueur devrait être repoussée au moins au 1er janvier 2017.

B) Commentaires spécifiques relatifs à la forme juridique de société en commandite par actions (SCA)

Comparaison entre société en commandite par actions (SCA) et société anonyme (SA)

Suite à la restructuration de certains banquiers privés suisses, qui gèrent tout de même environ 10% des fonds déposés en Suisse, ces établissements, en matière de détermination et de suivi de la stratégie du groupe et de surveillance consolidée, ont une structure qui fait intervenir des organes distincts : l'administration et l'organe de contrôle. Il n'y a toutefois pas d'organe dans la SCA qui cumule la haute direction, la surveillance et le contrôle. Ces fonctions sont en effet partagées entre l'administration (haute direction et surveillance) et l'organe de contrôle (contrôle).

Afin d'adapter la circulaire aux besoins spécifiques des groupes bancaires contrôlés par une SCA, il est essentiel de se rappeler les différences juridiques entre une société anonyme (SA) et une société en commandite par actions (SCA) :

Cadre du débat

La SCA se caractérise par une administration composée des Associés indéfiniment responsables et chargée précisément d'administrer et de représenter la société (art. 765 CO), et d'un organe de contrôle qui est tenu d'exercer une surveillance permanente sur la gestion (art. 768 CO).

En comparant la structure de la SCA à celle d'une société holding traditionnelle constituée sous forme d'une SA, il est permis d'affirmer que la dualité formée par le conseil d'administration et la direction d'une SA ne peut être assimilée que de manière fort limitée à la dualité entre l'organe de contrôle et l'administration de la SCA. Il en résulte que la mission de l'organe de contrôle d'une SCA chapeautant un groupe bancaire doit être redéfinie par rapport à celle du conseil d'administration d'une SA dans une situation identique.

Mission de la holding d'un groupe bancaire sous forme de SCA

La holding d'un groupe bancaire assure la surveillance consolidée de l'ensemble des sociétés du groupe. Son objet statutaire peut être défini de la manière suivante :

- Définir la stratégie et la politique générale du groupe
- Assurer le développement et la coordination des activités

Dans le cadre d'une structure de SCA, cette mission est du ressort exclusif de l'administration et elle englobe toutes les sociétés du groupe actives dans le domaine financier. Elle complète par ailleurs la surveillance individuelle des banques faisant partie du groupe.

Quant à la surveillance consolidée, elle comporte des éléments quantitatifs et qualificatifs et peut être définie comme suit :

- Éléments quantitatifs : présentation des comptes, fonds propres, répartition des risques, liquidités
- Éléments qualitatifs : organisation du groupe, surveillance et contrôle interne à l'échelle du groupe, garantie d'une activité irréprochable des organes du groupe

Domaines de compétence de l'organe de contrôle

Les domaines spécifiques de compétence de l'organe de contrôle trouvent leur source à deux niveaux :

- dans le droit des sociétés (Code des Obligations)
- dans la réglementation bancaire et la pratique de la FINMA

Compétences du droit des sociétés (768 CO)

C'est le seul art. 768 CO qui définit les compétences de l'organe de contrôle au niveau du droit des sociétés. Ces compétences peuvent se résumer de la manière suivante :

- Organe chargé de la surveillance permanente de l'activité de l'administration (« gestion »)
- Protection des actionnaires non membres de l'administration (actionnaires minoritaires)
- Surveillance juridique, comptable et commerciale

Cette description doit être opposée aux attributions du conseil d'administration d'une SA qui sont définies à l'art. 716a CO :

- Exercer la haute direction
- Fixer l'organisation
- Fixer les principes de la comptabilité
- Nommer et révoquer les personnes chargées de la gestion
- Exercer la haute surveillance sur les personnes chargées de la gestion

Seul le dernier élément ressortant aux attributions du conseil d'administration d'une SA se recoupe avec les compétences de l'organe de contrôle d'une SCA. Toutes les autres attributions qui constituent les prérogatives de « haute direction » du conseil d'administration, sont dévolues à l'administration dans le cadre d'une SCA.

Compétences prudentielles

Les compétences prudentielles de l'organe de contrôle se basent essentiellement sur les exigences légales et les prescriptions réglementaires de la FINMA. Tant la circulaire 2008/24 en vigueur que le projet mis en consultation se réfèrent cependant expressément au conseil d'administration d'une SA (par l'intermédiaire de la notion de « Haute direction ») et ne peuvent par conséquent s'appliquer que « mutatis mutandis » à l'organe de contrôle d'une SCA.

On peut cependant admettre que, mis à part ces références à la « haute direction » exercée par le conseil d'administration d'une SA, la grande majorité des définitions fournies par la circulaire FINMA 2008/24 trouvent application au niveau de l'organe de contrôle de la SCA. Cette approche est d'ailleurs expressément confirmée dans le cadre des autorisations octroyées par la FINMA aux groupes bancaires disposant d'une holding sous forme de SCA. La FINMA stipule d'ailleurs expressément qu'outre sa mission de surveillance permanente de la gestion d'un groupe bancaire, l'organe de contrôle doit assumer les fonctions de comité d'audit et de comité des Risques pour le groupe.

Ces fonctions du comité d'audit et du comité des risques peuvent être définies de la manière suivante :

- Comités d'audit : surveillance et évaluation de l'intégrité des bouclements financiers du groupe, du contrôle interne dans le domaine de l'établissement des

rapports financiers et de l'efficacité de la société d'audit et de sa coopération avec la révision interne
- Comité des risques : surveiller le profil des risques du groupe

Définition de la mission de l'organe de contrôle dans les documents sociaux

La mission concrète de l'organe de contrôle est décrite de manière plus détaillée dans les documents sociaux d'une SCA.

L'organe de contrôle vérifie les éléments suivants :

- Résultats financiers et affectation du bénéfice
- Existence d'un système de contrôle interne adéquat
- Conformité aux dispositions légales et statutaires
- Existence d'une structure, organisation et gouvernance adéquate
- Mise en place et respect des politiques de gestion des risques
- Mise en place d'une politique de rémunération
- Bon fonctionnement de l'audit interne et externe

Les Statuts limitent cependant aussi expressément le rôle de l'organe de contrôle, ceci notamment par rapport au rôle qui est endossé par un conseil d'administration :

« L'organe de contrôle ne peut pas intervenir dans les fonctions et attributions de l'administration et de la gestion ou prendre des décisions qui dépassent son droit de contrôle et de surveillance. »

On constate dès lors que le rôle de l'organe de contrôle est nettement délimité par rapport à celui d'un conseil d'administration d'une SA qui lui « peut prendre des décisions sur toutes les affaires qui ne sont pas attribuées à l'assemblée générale par la loi ou les statuts » (art. 700 al. 1 CO).

<u>Adaptation de la circulaire aux spécificités des SCA</u>

Les explications qui précèdent mènent à la conclusion que de nombreuses dispositions du projet de circulaire ne sont pas adaptées aux SCA. La question qui se pose est de savoir si ces adaptations doivent être prévues directement dans la circulaire, ce que nous préférions, ou via des décisions particulières.

Le libellé du cm 9 laisse une certaine flexibilité au niveau du champ d'application (« Les exigences doivent être concrétisées au cas par cas … en fonction de la structure de l'établissement. », « La FINMA peut ordonner des allègements … au cas par cas.»). Dans tous les cas, les holdings de groupes bancaires structurées sous forme de SCA doivent bénéficier des dérogations détaillées ci-après.

Cm 10 : Il n'y a pas d'organe dans la SCA qui cumule « la haute direction, la surveillance et le contrôle ». Ces fonctions sont partagées entre l'administration (haute direction et surveillance) et l'organe de contrôle (contrôle).

- La stratégie commerciale et la politique de risque (a) sont du ressort de l'administration. L'approbation du concept-cadre pour la gestion des risques, de

même que la surveillance d'une gestion des risques efficace revient à l'organe de contrôle.

- L'organisation (b) est du ressort de l'administration.
- Pour les Finances (c), la responsabilité principale revient à l'administration, mais l'approbation de la planification des fonds propres et des liquidités, de même que l'adoption du rapport de gestion est du ressort de l'organe de contrôle.
- Les tâches relatives aux Ressources humaines (d) sont du ressort de l'administration.
- Les tâches de surveillance et de contrôle (e) sont essentiellement du ressort de l'organe de contrôle, mis à part la garantie de la compliance et la mise en place d'un système de contrôle interne efficace.
- Les changements structurels et investissements (f) sont du ressort de l'administration.

Il ne faut cependant pas perdre de vue que l'administration de la SCA d'une holding bancaire est l'organe faîtier d'un groupe de sociétés, et non pas l'organe d'une banque. Il en résulte que l'adaptation de la circulaire FINMA à la SCA s'en trouvera simplifiée, puisque l'administration sera en charge de la plupart des fonctions, mis à part les comités audit et risques et la surveillance permanente de la gestion.

Cm 20 : Les membres de l'organe responsable de la direction supérieure (administration) doivent pouvoir exercer certaines activités opérationnelles pour des Filiales du groupe, dans la mesure où il n'en résulte pas de conflits d'intérêt. Dans la mesure où l'activité opérationnelle se déroule au sein de la SCA et non pas de la banque filiale, le conflit d'intérêt devrait pouvoir être évité.

Cm 21 : L'organe responsable de la direction supérieure (administration) est composé exclusivement des Associés qui n'ont aucune indépendance par rapport au groupe. Si « la FINMA peut autoriser des exceptions s'il existe de justes motifs », il vaut mieux le préciser expressément pour tenir compte de la structure d'une SCA.

Cm 26 : Les Associés, en leur qualité de membres de l'administration, détiennent une participation qualifiée dans l'établissement. Cette disposition est par conséquent inapplicable.

Cm 35 : Le Président de l'administration ne peut entretenir un dialogue régulier avec le Président de la direction, étant donné qu'il cumule les 2 fonctions.

Cm 36 : Les éventuels comités, surtout le comité des risques et le comité d'audit, sont des émanations de l'organe de contrôle et non pas de l'administration. Il appartient par conséquent à l'organe de contrôle d'instaurer de tels comités.

Cm 40 et ss : les tâches du comité d'audit reviennent à l'organe de contrôle.

Cm 41 et 43 : L'organe de contrôle d'une SCA ne fait pas du tout partie de l'«ORDS» (contrairement au cas de l'«audit committee» et du «risk committee» composés de membres du conseil d'administration d'une société faîtière en forme de société anonyme). Or, ils sont totalement extérieurs à la fonction de direction suprême du groupe bancaire, et les fonctions attribuées au comité d'audit concernant le contrôle interne, le contrôle des risques et de la compliance, peuvent dépasser les possibilités

pratiques d'un organe complètement séparé des fonctions respectives. Les «effectiveness tests», s'ils doivent mener à des résultats dignes de confiance, sont extrêmement exigeants et présupposent, en pratique, l'emploi de techniques et de spécialistes d'audit opérationnel. Or, l'organe de contrôle, en sa qualité de «audit committee », ne procède pas lui-même à des opérations d'audit. L'organe de contrôle doit, par contre, se servir des services de la révision interne, qui lui est subordonnée. Ceci devrait être clarifié.

Cm 46 et ss : les tâches du comité des risques reviennent à l'organe de contrôle

Cm 47 : Les recommandations principales pour le concept cadre de la gestion des risques dans « l'Institut » doivent en principe émaner de la fonction de l'exécutif, pour être étudiés et examinés d'une manière critique par l'organe de contrôle. L'organe de contrôle n'organise pas la gestion des risques, conception clé émanant d'abord de « l'administration ». La politique et le choix du système de la gestion des risques doivent fondamentalement être une tâche de l'administration dans une SCA faîtière. Même le contrôle de l'efficacité des processus est tout d'abord une tâche clé de l'administration, parce qu'elle seule est complètement familiarisée avec les opérations, les risques et les êtres humains. A l'organe de contrôle d'examiner s'il y a harmonie entre la « stratégie des risques » et le « système » de gestion des risques et le «risk appetite» choisis par l'administration. Mais l'« organe de contrôle » n'est pas et ne peut être rapproché des fonctions opérationnelles de la gestion des risques, noyau dur de la responsabilité de l'« administration ». Le chapitre VI du projet souligne à juste titre la responsabilité primordiale de l'exécutif («Geschäftsführung») dans le domaine de la gestion des risques. Il faudrait donc adapter le texte au cas des SCA.

Cm 53 et ss : L'organe responsable de la direction supérieure (administration) cumule les tâches de la direction, sous réserve des Responsables des Business Lines et des Corporate Functions qui exercent leurs responsabilités tant au niveau de la banque principale du groupe que de la SCA holding du groupe bancaire qui contrôle cette banque (en principe sous forme d'un Service level agreement).

Cm 82 : Le projet introduit, avec une emphase et des répétitions inouïes, le nouveau concept des «instances indépendants de contrôle » qui sont (Chapitre VII alinéa 1) :

- La gestion des risques, et
- La fonction de compliance.

Du point de vue d'une SCA faîtière, il faut étudier de près ce chapitre VII, sous deux perspectives. Premièrement, le terme «indépendant » est ici compris d'une nouvelle manière, alors qu'il est déjà employé avec un sens très différent pour les réviseurs (Art. 728 CO) et les membres du conseil d'administration (Code Suisse de Bonne Pratique). Dans le contexte des « Instances indépendants de contrôle » on appelle indépendants des personnes appartenant justement à la fonction générale de la gestion («Personen … innerhalb der Geschäftsführung», VII/B/a, alinéa 3), à qui on attribue une certaine position indépendante, alors qu'ils restent assujettis à l'autorité, évidemment, de «l'administration ». La gestion des risques est une partie centrale et inséparable de la fonction de la gestion d'une banque et non pas une « fonction de contrôle indépendante». Elle ne peut être, sans brouiller les cartes, définie comme une « instance indépendante de contrôle ».

Cm 104 : La révision interne est, selon le projet, subordonnée directement à l'«ORDS» et « son comité d'audit ». Or, dans la SCA, l'organe de contrôle n'est pas une émanation de ORDS, mais justement un organe complètement séparé, ceci dû à son élection par des actionnaires qui ne sont pas membres de « l'administration », et sa position complètement en dehors du corps de « l'administration ». La position de la révision interne doit être clarifiée. Elle est assujettie à l'organe de contrôle, mais elle a nécessairement une ligne d'information – pointillée – aboutissant au président de « l'administration ». Il est logique que, dès lors, le chef de la révision interne ne soit pas nommé par l'«ORDS» (VIII/B, alinéa 3), mais par l'organe de contrôle, évidemment après consultation avec le président de « l'administration ».

Cm 110 : La Révision interne n'est pas subordonnée à l'organe responsable de la direction supérieure, mais à l'organe de contrôle.

Cm 125 : C'est cette disposition qui soumet la SCA sous forme de holding d'un groupe bancaire à la nouvelle circulaire FINMA (application « par analogie »). La phrase « Il faut s'assurer qu'il existe des prescriptions qui tiennent suffisamment compte des structures juridiques et organisationnelles … » permettrait également d'introduire la flexibilité requise pour tenir compte de la structure SCA.

Cm 128 et ss : les Publications requises ne sont en général pas fournies pour une banque privée constituée sous forme de SCA (holding d'un groupe bancaire) : procédure d'élection (cm 133), structure du groupe (cm 136), éléments de rémunération et programmes de participation (cm 140).

* * *

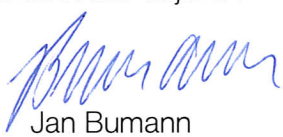
En vous remerciant par avance de l'attention que vous porterez à la présente, nous vous prions d'agréer, Monsieur, nos salutations distinguées.

ASSOCIATION DE
BANQUES PRIVEES SUISSES

Le Directeur :

Jan Langlo

Le Directeur adjoint :



Jan Bumann

Lugano, 13 aprile 2016

Indagine conoscitiva concernente la nuova circolare 2016/X "*Corporate governance- banche*"

Egregi signori,

le sottoscritte, in qualità di direttrice del CAS in Compliance management (CAS CM) del Centro studi Bancari e di collaboratrice scientifica nonché responsabile e docente in due moduli nello stesso CAS CM[1] , inoltrano con la presente alcune riflessioni all'attenzione della FINMA, nell'ambito della summenzionata indagine conoscitiva. A titolo di premessa, le seguenti succinte riflessioni di carattere generale fanno riferimento alla Circolare "*Corporate governance*", senza tuttavia estendersi alle due circolari aggiuntive sui "Rischi operativi" e sui "Sistemi di remunerazione". In particolare, e in considerazione delle esperienze maturate nell'ambito delle nostre professioni e della formazione CAS CM, le riflessioni vertono sui compiti e sulle aspettative inerenti la funzione compliance (quindi non sulle altre funzioni) , e sul sistema di controllo (ma non sulla tematica rischi operativi).

Nel comunicato stampa della FINMA del 1 marzo u.s. si fa stato dell'obiettivo della stessa Autorità di snellire e aggiornare i requisiti di *corporate governance* posti alle banche, ispirandosi tra gli altri, agli standard internazionali espressi nelle sue linee guida dal Comitato di Basilea per la vigilanza bancaria. Si accoglie con favore l'accorpamento in un'unica circolare delle disposizioni della Circolare 08/24, delle relative FAQ e dei requisiti sanciti da altre circolari. A titolo generale, si comprende l'idea di riformulare la circolare con un approccio orientato ai principi, rinunciando a descrizioni dettagliate di utilizzo. Tuttavia, l'attuazione da parte delle banche nella pratica, risulta spesso condizionata non tanto dalle dimensioni e dalle caratteristiche dell'attività svolta, quanto piuttosto da una interpretazione differenziata e, a volte, incoerente delle disposizioni relative alla *corporate governance*. Per tale motivo, si ritiene che l'aggiornamento della circolare in questione, possa rappresentare l'occasione per fare chiarezza su taluni principi fondamentali. Da qui, le presenti riflessioni che, come detto, non hanno la pretesa di essere esaustive.

I. Considerazioni generali

1. Il concetto di *corporate governance* e scopo della circolare

L'evoluzione dell'analisi economica e giuridica in ambito di Corporate Governance, fortemente condizionata dal realizzarsi di importanti scandali nel mondo economico e finanziario, ha favorito la presa di coscienza, da un lato, della parziale adeguatezza degli strumenti di *Corporate governance fino al allora* messi in atto; dall'altro, della centralità dei sistemi di controllo e di gestione dei rischi, quali strumenti di *sana corporate governance*. Questi sistemi , che le aziende finanziarie sono chiamate a predisporre affinché sia garantito il rispetto del principio di organizzazione adeguata[2], operano trasversalmente all'interno dell'istituto e toccano, in maniera diversa, tutti i collaboratori delle banche, conducendo a una maggiore protezione dell'insieme

[1] Si veda il programma tematico del CAS CM svolto in collaborazione con l 'università di Ginevra al seguente link: http://compliance-management.ch/

[2] Cui si fa riferimento alla nm. 13 della Circolare e che contraddistingue l'impresa bancaria da quella attiva in altro settore e regolamentata dal Codice delle obbligazioni

degli stakeholder. Infatti, come esplicitato dal Comitato di Basilea[3] e dalla normativa bancaria elvetica, la protezione in particolare dei depositanti[4], risulta essere un elemento centrale, cui le banche devono ispirarsi negli aspetti organizzativi, strutturali, di gestione oltre che di controllo impliciti nello svolgimento irreprensibile delle proprie attività

Certo, il concetto di *corporate governance, non si limita ai sistemi di controllo interno e di gestione dei rischi, sebbene, appunto, questi sistemi hanno oramai assunto il rango di strumenti centrali di sano governo di impresa,* ma implica l'attuazione di ulteriori elementi centrali pure parzialmente menzionati nella circolare (quali gli aspetti strategici e di politica aziendale in materia di rischi, la necessità di dotarsi di normativa e di procedure interne, i requisiti posti alla configurazione e al funzionamento del sistema informatico, la necessità di prevedere e concretizzare la separazione delle funzioni o la necessità di redigere organigrammi e mansionari, ecc). Si presume che tali aspetti sono stati volutamente trattati in maniera differenziata nella Circolare, che si prefigge dunque lo scopo di approfondire la centralità solo di alcuni specifici aspetti della Corporate Governance.

In considerazione della valenza della Circolare sulla *corporate governance* nella gerarchia della normativa bancaria, le sottoscritte propongono dunque che la Circolare espliciti in entrata lo scopo della medesima, riprendendo i concetti chiave di sistema di controllo interno e gestione dei rischi menzionati nel sottotitolo, sottolineandone la centralità per una sana Corporate governance, che concretizzi l'organizzazione adeguata e il principio di svolgimento irreprensibile dell'attività, assicurando la protezione degli stakeholder in generale e dei depositanti in particolare. Lo scopo così evidenziato andrebbe a integrare o sostituire l'oggetto di cui alle nm. 1 e 2 della Circolare e delimiterebbe il perimetro degli aspetti di *Corporate governance* evidenziati nella loro centralità.

2. Funzioni centrali in ambito di *Corporate governance* : definizioni

Come per gli strumenti di *Corporate governance*, anche in relazione alle funzioni, la Circolare menziona unicamente i compiti degli organi e delle funzioni centrali in ambito di *Corporate governance*, ed in particolare in relazione alla gestione dei rischi e al sistema di controllo interno (CdA, DGEN, comitati, audit, funzione compliance e controllo dei rischi). Per il corretto funzionamento del sistema di controllo interno/gestione dei rischi, ci sono numerose altre funzioni fondamentali (si pensi al back office, credit officer, middle office, controllo formalità, legal), che interagiscono per assicurare l'organizzazione adeguata e lo svolgimento irreprensibile delle attività. Quasi tutte le banche hanno queste funzioni al proprio interno o ricorrono alle possibilità di esternalizzazione date dalla FINMA a seconda della dimensione e delle attività svolte. Fermo restando che anche se si fosse in presenza di funzioni date in outsourcing, l'istituto nell'attuazione della propria *sana corporate governance* , deve comunque garantire un flusso regolare, tempestivo, affidabile di informazioni da queste istanze esterne verso l'interno.

[3] "La gouvernance d'entreprise doit avant tout viser à préserver de façon pérenne les intérêt des parties prenantes dans le respect de l'intérêt général. Parmi les parties prenants, en particulier dans le cas des banques de détail, l'intérêt des déposants l'emporte sur celui des actionnaires », Comitato di Basilea, Principes de gouvernance…, 2015 cifra 2

[4] Art. 1 LBCR

A mente di chi scrive, si ritiene che in considerazione della centralità di queste unità[5], la Circolare dovrebbe precisare il loro ruolo con particolare attenzione alle singole misure di controllo, che gli istituti cui è destinata la Circolare, saranno chiamati a implementare. Inoltre, sempre pensando ai principi fondanti della *Corporate governance*, la Circolare potrà precisare le linee di reporting che concretizzano il concetto di sorveglianza, anche laddove si fosse concretamente in presenza di un rapporto di esternalizzazione di funzioni topiche per il buon funzionamento del sistema di controllo e di gestione dei rischi.

3. Relazione tra Sistema di controllo interno e sistema di gestione dei rischi

Secondo la più recente comprensione delle autorità internazionali di vigilanza,[6] cui peraltro si ispira anche la FINMA nella presente Circolare, il sistema di controllo interno (SCI) sarebbe parte integrante del sistema più ampio di gestione dei rischi (ERM). La Circolare alla nm. 79, indica che il Sistema di Controllo Interno "doit notamment inclure l'identification, la mesure, l'administration et la surveillance des risques…", dando ad intendere che l'ERM sia parte integrante del SCI. La corretta definizione del SCI non è solo una prerogativa accademica, ma ha un impatto concreto sulle funzioni di controllo. Infatti, se l'ERM è parte integrante del SCI, allora, le funzioni di controllo si devono far carico anche del processo di gestione del rischio. A questo proposito, infatti, si constata che alcune banche attribuiscono alla funzione del compliance officer "la gestione dei rischi compliance". L'attribuzione dell'intero processo di gestione dei rischi alla funzione compliance non sembra però corrispondere alle aspettative della FINMA, che attribuisce alla funzione compiti di valutazione del rischio (cf. infra) e di controllo (componenti del sistema di controllo).

A mente di chi scrive, si impone il chiarimento del principio che regola la relazione esistente tra sistema di controllo interno e di gestione del rischio, per assicurare l'adeguatezza dell'organizzazione e la corretta attribuzione dei compiti e delle responsabilità alle funzioni centrali per l'attuazione di una sana *corporate governance*.

4. Attività di "valutazione" del Compliance officer

Ci pare inoltre fondamentale chiarire anche il concetto di "valutazione" dei rischi (Einschätzung, évaluation) attribuito quale compito alla funzione compliance, di cui alle nm. 100-102. Di norma il concetto di "valutazione" è strettamente legato al concetto di "quantificazione, misurazione" e solo in maniera estensiva al concetto di analisi. Il concetto di "valutazione" è a nostro avviso più adeguato se riferito al processo di gestione dei rischi "classici" (finanziari), che maggiormente si prestano ad essere "quantificati". Differentemente, i rischi compliance non si prestano ad una misurazione assimilabile a quella svolta per i rischi finanziari. Infatti, la valutazione dei rischi

[5] Unità che non sono "unités generatrices de revenu" ma forse neppure "instances de contrôle independantes des unités génératrices de revenu" come indicato alla nm. 80

[6] Così il COSO dal 2014, cui si ispira anche il Comitato di Basilea. A questo proposito il Comitato di Basilea (2015) indica che « Le système de contrôles internes est notamment conçu pour vérifier qu'à chaque risque majeur est associé une politique, un processus ou un autre outil, ainsi qu'un dispositif destiné à contrôler la mise en œuvre et le bon fonctionnement de ces outils. Il permet ainsi d'assurer l'intégrité, la conformité et l'efficacité des processus. De plus, il donne l'assurance raisonnable que les données financières et de gestion sont fiable, à jour et exhaustives, et que la banque est en conformité avec ses différentes politiques ainsi qu'avec les lois et règlements applicables. », cifra 115

finanziari serve a quantificare le potenziali perdite e quindi le necessità di accantonamenti (utili ai fini del calcolo del capitale proprio).
In quale modo questo principio è valido per i rischi compliance? Il compliance officer , dovrebbe a nostro avviso orientare la propria "valutazione", innanzitutto per stabilire - nella misura del possibile - se una data attività sia lecita (conforme) e a quali condizioni. Tale "valutazione" corrisponde in larga misura a un'analisi giuridica della situazione, che a nostro avviso costituisce un'attività di controllo più che di valutazione, intesa come misurazione del rischio con conseguente quantificazione. [7] In definitiva si tratta dunque piuttosto di un *processo di sussunzione e non di valutazione del rischio.* La terminologia utilizzata nel contesto della lotta al riciclaggio di denaro – attività peraltro storicamente attribuita alla competenza del compliance officer – confermerebbe questa interpretazione, giacché si parla esplicitamente di *attività di analisi e non di valutazione*. Inoltre, sovente nella pratica, ci si pone la domanda a sapere se , la "valutazione" debba essere fatta sul singolo dossier/transazione o/e in relazione ad una situazione generale , il cui scopo sia, per esempio, la scelta strategica da parte della direzione, o la redazione di direttive, ecc.

Infine, in relazione al l concetto di "valutazione", occorre definire l'estensione del principio. Nella prassi si constata che sovente il compliance officer preavvisa e/o accetta relazioni (o transazioni): questa attività (non menzionata esplicitamente dalla circolare FINMA, ma sovente svolta dai compliance officer) rientra nelle aspettative della FINMA o, al contrario, costituisce in pratica un'assunzione di rischio che non può essere svolta dal compliance officer?

Alla luce di tali riflessioni, le sottoscritte propongono che la Circolare specifichi il concetto di "valutazione" nel suo significato e nella sua portata o utilizzi il termine, a nostro avviso più confacente, di "analisi". In particolare, la circolare dovrebbe chiarire se la pratica in atto in numerosi istituti di preavviso/ accettazione da parte del compliance officer di relazioni (e/o transazioni) sia conforme alla definizione della funzione compliance quale funzione di controllo.

---

[7] Si veda anche il Comitato di Basilea, 2015. In particolare il CB attribuisce i seguenti compiti alla funzione compliance :
"**Principe 9** – Conformité.
Il incombe au conseil d'administration de surveiller la gestion du risque de non-conformité. Le conseil d'administration doit instaurer une fonction conformité et approuver les politiques et procédures de détection, d'évaluation et de suivi du risque, ainsi que celles régissant l'établissement de rapports et la fourniture de conseils à ce sujet.
132. Une fonction conformité indépendante est un élément clé de la deuxième ligne de défense de la banque. Elle est notamment chargée de veiller à ce que la banque mène ses activités avec intégrité et observe les lois, réglementations et politiques internes applicables.
133. Il revient à la direction de la banque d'établir une politique de conformité qui présente les principes fondamentaux que le conseil d'administration doit approuver et qui explique les principales procédures de détection et de gestion des risques de non-conformité à chacun des niveaux de la banque.
134. Si le conseil d'administration et la direction sont responsables de la conformité des activités de la banque, la fonction conformité a un rôle important à jouer dans la promotion du système de valeurs de la banque, des politiques et procédures qui contribuent à la conduite responsable de la banque et au respect de toutes les obligations applicables.
135. La fonction conformité doit exercer un rôle de conseiller auprès du conseil d'administration et de la direction sur les questions de respect des lois, règles et normes applicables et les tenir au courant des évolutions en la matière. Elle doit également participer à la formation du personnel sur les questions de conformité, répondre à toute demande des employés sur le sujet et leur fournir des orientations sur la bonne mise en œuvre des lois, règles et normes applicables, sous la forme de politiques, procédures et autres documents tels que manuel de conformité, code de conduite et recommandations pratiques. (…)

5. Attività di controllo del Compliance officer

Tra i compiti esplicitati in relazione alla funzione compliance (nm 99-103) neanche uno indica in maniera esplicita i controlli: ci sono dei controlli che devono essere svolti/garantiti/ supervisionati dal compliance officer?

A nostro giudizio, tale attività di controllo costituisce il fulcro dei compiti attribuiti al Compliance officer e dovrebbe essere esplicitato nella sua definizione e nella sua portata nella Circolare, al capitolo destinato a questa unità che è parte integrante per il buon funzionamento del SCI e di gestione dei rischi.

6. Corporate governance e Compliance Management parte integrante della cultura aziendale

La Circolare non si esprime esplicitamente sul concetto di una cultura aziendale che includa responsabilità di controllo da parte di tutti i collaboratori. Infatti, come auspicato dal Comitato di Basilea, tale principio risulta di fondamentale importanza anche per "les unités d'affaires generatrices de revenus" (nm 80). Il concetto di cultura aziendale è a nostro avviso un elemento centrale del sistema di controllo interno e del sistema di gestione dei rischi. Ad oggi, con riferimento agli aspetti di *corporate governance*, solo la normativa antiriciclaggio prevede un obbligo di formazione/sensibilizzazione su specifiche tematiche.

A nostro avviso la formazione obbligatoria non rappresenta solo uno strumento idoneo per sensibilizzare i collaboratori e le collaboratrici alle tematiche proposte, ma permette di implementare i principi di *sana corporate governance* in generale, e quelli di controllo e gestione dei rischi in particolare. La formazione – emanazione di una sana cultura aziendale - andrebbe dunque estesa a tutto il personale (sul modello della lotta al riciclaggio) .

II. Alcuni aspetti di dettaglio

1. Appetito di rischio (Circ. nm.5 e 71)

A nostro avviso questo principio dovrebbe essere maggiormente chiarito a beneficio dell'interpretazione che ogni banca dà nell'ambito della sua implementazione, in particolare con riferimento ai rischi compliance in generale, ed ai rischi di riciclaggio in particolare.

2. Finalità del SCI
Stando alla nm. 7, il sistema di controllo interno serve tra gli altri anche a "ridurre" i rischi?

A nostro avviso tale aspetto va ulteriormente specificato, nel senso che l' SCI ha anche la finalità di controllare il rispetto dei limiti di rischio (che per il rischio compliance comporta anche il controllo riguardo al rispetto della legge)

3. Informazione e comunicazione

La voce "informazioni e comunicazione" è un elemento centrale del sistema di controllo interno. **Nella Circolare tale aspetto è a nostro avviso un po' sottovalutato (in particolare in relazione al fatto che il compliance officer nella prassi non fa tutti i controlli di conformità, ma si basa su controlli effettuati da altre unità, anche esterne.)**

Cordiali saluti

Dr. Iur., lic. oec. Flavia Giorgetti Nasciuti **Avv. Tamara Erez**

Allegato 1

Cubo COSO SCI e ERM

CENTRO DI STUDI BANCARI VILLA NEGRONI

Con la pubblicazione del documento ERM nel 2004 ci si è iniziati a chiedere il rapporto tra i due sistemi (SCI e ERM): per alcuni autori il SCI era stato sostituito dal sistema ERM. Nel 2013 il COSO, con la pubblicazione del suo nuovo documento conferma che si tratta di due sistemi diversi: il sistema di gestione dei rischi include però il SCI (cfr. grafico), che però mantiene la sua ragione di esistere. Rimangono delle zone di ombra nei rapporti tra i due (tematica più organizzativa che giuridica, ma che ha delle conseguenze sulla ripartizione dei compiti all'interno della banche)

COSO 2013

CENTRO DI STUDI BANCARI VILLA NEGRONI

79

Cubo COSO 2013

CENTRO
DI STUDI BANCARI
VILLA NEGRONI
ASSOCIAZIONE BANCARIA TICINESE

CREDIT SUISSE

FINMA Consultation on

1. **Revising the corporate governance requirements for banks.**

2. **Updating circular 2008/21 "Operational risks – banks".**

(Issued for comment on 1 March 2016)

Official Comments of Credit Suisse AG

May 2016

Comments:

Circular 2016/xx Paragraph 88

Paragraph 87 of the consultation document states that "Institutions of supervisory categories 1 to 3 shall have stand-alone risk control and compliance functions acting as independent control bodies. They shall appoint a CRO who is responsible for risk control".

Paragraph 88 states that "Systemically important banks shall have a CRO who is a member of the executive board with sole responsibility for risk control".

It is possible to interpret paragraph 88 to mean the CRO's only responsibility is risk control. This is contrary to the practice in some of our peers where the CRO has responsibility for operational risk and compliance for example.

Please delete 'with sole responsibility for risk controls' from paragraph 88 .

As a result paragraph 88 should read:

Systemically important banks shall have a CRO who is a member of the executive board ~~with sole responsibility for risk control~~.

Circular 2008/21 section g) Principle 6: Risks from the Cross Border Business

Paragraph 136.4 deals with risks from cross border business and specifically mentions 'the risks resulting from the application of foreign legal guidelines (tax law, criminal law, money laundering law, etc.)'. In many large banks Regulatory Compliance is managed by the compliance function and not the operational risk function.

In addition the regulatory compliance function, rather than the operational risk function, would be best placed to undertake the role of informing 'FINMA if key risks materialize and/or they are contacted in this respect by foreign authorities'. However, paragraph 136.5 in Circular 2008/21 appears to place that responsibility on the operational risk function.

Please delete section g) Principle 6: Risks from the Cross Border Business. (Paragraphs 136.4, 136.5 and 136.6)

Circular 2016/xx Paragraph 98

Paragraph 98 states that 'risk control shall inform the supreme governing body immediately about any violations of risk limits that the latter has approved'. CS has a regular formal reporting process for risk limit violations and the proposal should be amended to require notifications of violations of risk limits to be incorporated into the regular formal reporting process rather than immediately they are identified.

In addition, the term immediately would be interpreted as meaning as soon as the violation is detected, irrespective of the materiality of the breach and the possible reason for such an event. Like CS, most banks report violations as part of the regular reporting cycle. Only if the nature or size of the breach warranted such action would a risk limit violation be escalated immediately.

Please amend paragraph 98 to read:

Risk control shall report to the supreme governing body at least once a year on the development of the risk profile of the institution and its activity as per margin no 89 et seq. Furthermore, risk control shall incorporate in the regular formal reporting process to ~~inform~~ the supreme governing body ~~immediately~~ information about any violations of risk limits that the latter has approved. A copy of these reports must be made available to internal audit and the statutory auditors.

Circular 2008/21 Paragraph 2

The current exclusion of strategic and reputational risk from the definition of operational risk mirrors the definition adopted by the BCBS, while the proposal to include strategic and reputational risk aligns to the definition in the EU's Capital Requirement Regulation.

Banks should be free to organise their operational, strategic and reputational risk functions as separate functions or as part of operational risk. Within CS we consider strategic and reputational risk to be separate from operational risk and the implications of such a change for existing day to day operational risk management practices have not been made clear. The change could impact the identification, measurement, management and reporting of operational, strategic and reputational risk. We do not feel the definition should be changed without banks being made fully aware of the consequences.

Please retain in paragraph 2 the current definition of operational risk as "the risk of loss, resulting from the inadequacy or failure of internal processes, people or systems or from external events. This definition shall comprise legal risk, including regulatory fines and settlements, but excludes strategic and reputational risk."

Circular 2008/21 Paragraph 122

Paragraph 122 proposes that the classification of operational risks "should comprise an assessment of both risk appetite, as measured through inherent risks, and risk tolerance, as measured through residual risks. The assessment typically pursues the dimensions of 'probability of occurrence' and 'extent of damage' ".

The references to risk appetite and risk tolerance are confusing and should be removed.

Industry tends to refer to 'probability of occurrence' as likelihood and 'extent of damage' as severity. These terms are more familiar to operational risk functions and their stakeholders and they should be used in this paragraph. For many banks damage is a component of severity and use of the term "extent of damage" could result in an underestimation of the potential severity.

In paragraph 122 please:

- Remove the references to risk appetite and risk tolerance;
- Replace the terms 'probability of occurrence' with likelihood and 'extent of damage' with severity.

As a result paragraph 122 should read:

The uniform classification of operational risks shall be based on the categorization of operational risks as per margin no. 121, and should comprise an assessment of both ~~risk appetite, as measured through~~ inherent risks[9], and ~~risk tolerance, as measured through~~ residual risks[10]. The assessment typically pursues the dimensions of ~~"probability of occurrence"~~ "likelihood" and ~~"extent of damage"~~ "severity".

The classification should also in particular serve to determine risks with far-reaching consequences as per margin no. 137.

economiesuisse

Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
CH-3003 Bern

Per E-Mail an: peter.ruetschi@finma.ch

20. April 2016

FINMA-Rundschreiben 2016/x „Corporate Governance – Banken“
FINMA-Rundschreiben 2008/21 „Operationelle Risiken Banken“
FINMA-Rundschreiben 2010/01 „Vergütungssysteme“

Sehr geehrte Damen und Herren

Am 1. März 2016 haben Sie die Konsultation zu den obgenannten FINMA-Rundschreiben eröffnet. economiesuisse nimmt aus einer gesamtwirtschaftlichen Sicht zum Rundschreiben 2016/x „Corporate Governance – Banken“ wie folgt Stellung:

Zusammenfassung

economiesuisse lehnt den Entwurf zum FINMA-Rundschreiben 2016/x „Corporate Governance – Banken“ aus prinzipiellen Überlegungen zur Corporate Governance ab. Inhaltlich stösst die FINMA zwar vereinzelt Themen an, welche aus Sicht einer modernen Corporate Governance Unterstützung verdienten. Ihre Vorgaben führt die FINMA aber als grösstenteils zwingende Normen unter hoher Detaillierungsdichte ein. Verschärft wird dies dadurch, dass Rundschreiben der FINMA bei den Adressaten faktisch Gesetzescharakter haben. Auf Grund des hohen Detailierungsgrades und der mangelnden Flexibilität bei der Umsetzung engt das Rundschreiben die Adressaten stark ein.

Die Corporate Governance in der Schweiz ist geprägt von einem erfolgreichen und etablierten System der Selbstregulierung, präzise eingebettet in die gesetzlichen Vorgaben. Die Empfehlungen des Swiss Code of Best Practice for Corporate Governance („Swiss Code“) werden in allen Branchen als Benchmark in Bezug auf Coporate Governance Richtlinien anerkannt, dies auf einer grundsätzlich freiwilligen Basis auf der Grundlage von „Comply or Explain“.

Branchenspezifische Detailregelungen, wie sie die FINMA nun für die von ihr regulierten Institute vorschreiben will, beeinträchtigen das funktionierende Zusammenspiel zwischen Selbstregulierung und „hard law“. Ein mögliches Überschwappen der vorgeschlagenen Bestimmungen der FINMA auf weitere Branchen würde diesen negativen Einfluss noch verschärfen.

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

1 Generelle Ausführungen zu den Rundschreiben der FINMA

Die FINMA macht den von ihr regulierten Unternehmen durch Rundschreiben wiederholt stark detaillierte Vorgaben. Diese Vorgaben macht die FINMA gestützt auf ihre aus den Aufsichtsgesetzen hervorgehenden Kompetenzen. Sie haben den demokratischen Prozess der Rechtssetzung nicht durchlaufen, haben aber für die angesprochenen Unternehmen faktischen Gesetzescharakter. Generell fordert economiesuisse von der FINMA Zurückhaltung in Bezug auf Regulierungen auf Stufe Rundschreiben. Die Normenhierarachie (Gesetz, Verordnung) ist zwingend zu respektieren.

Bei der Formulierung von Regularien ist auch stets der Grenznutzen im Auge behalten: Mehrkosten stehen selten im Verhältnis zu Sicherheitsgewinn. Im Zweifel hat sich die FINMA gegen eine Detailregulierung auszusprechen. Ebenfalls ist auch stets zu prüfen, in welchem Ausmass die FINMA auf Grund ihres Auftrages überhaupt legitimiert ist, die entsprechenden Regelungen zu erlassen.

2 Zum konkreten Rundschreiben

Die Empfehlungen des Rundschreibens gehen sehr weit. Das Rundschreiben enthält Detailregelungen zur Corporate Governance, welche als Best Practice Empfehlungen Sinn machen können, nicht aber als faktisches Hard Law. Dies ist aus den folgenden Gründen besonders kritisch und führt aus einer gesamtwirtschaftlichen Sicht zur klar ablehnenden Position von economiesuisse:

- Die FINMA spricht mit ihren detaillierten Vorgaben nicht nur die grossen, kotierten Banken, sondern generell alle Banken an: sie differenziert hierbei nicht ausreichend. Viel zu detailliert sind – dies lediglich exemplarisch - die folgenden Punkte:
  - Note 18 macht zu weitgehende Detailvorschriften zur Zusammensetzung des Verwaltungsrates (einschliesslich etwa Controlling, Compliance und IT Kompetenz). Innert der kurzen Übergangsfrist von einem Jahr dürfte es zudem nahezu unmöglich sein, einen kompetenten IT-Vertreter zu finden.
  - Note 32 sieht eine detaillierte Regelung der Selbstevaluation des Verwaltungsrates (einschliesslich schriftlicher Festhaltung der Ergebnisse vor. Damit geht das Rundschreiben bedeutend weiter als die entsprechende Empfehlung im Swiss Code und verlangt durch die Dokumentationspflicht ein juristisch zumindest fragwürdiges Verhalten.
  - Noten 36-38 sehen zwingende Vorschriften zu einem separaten Prüf- und Risikoausschuss des Verwaltungsrates und der entsprechenden Zusammensetzung vor. Dies macht keinen Sinn. Wieso will man die Banken zwingen, je einen separaten Prüf- und Risikoausschuss mit personell hinreichender Unterscheidung zu haben, nur um dann andererseits geeignete Informationsflüsse zwischen diesen Ausschüssen zu postulieren. Gerade die Trennung von Ertragssicht (Erfolgsrechnung, Audit) und Risikosicht (Risk) kann Gefahren bergen.
  - Schliesslich sehen Noten 85-88 sehr weitgehende Detailregeln zur Organisation der Geschäftsleitung in Bezug auf die Kontrollinstanzen vor.
- Die FINMA vermengt Empfehlungen zu Best Practice mit Hard Law und stellt damit ohne Not das international anerkannte Prinzip „Comply or Explain“ in Frage. Damit riskiert sie auch, das in der Schweiz etablierte System der Selbstregulierungen im Bereich Corporate Governance zu beschädigen.

— Haben sich die zwingenden Empfehlungen der FINMA im Rahmen des Adressatenkreises etabliert, ist nicht auszuschliessen auszugehen, dass es zu einem schädlichen Überschwappen der faktisch zwingenden Standards auch in andere Branchen kommt.

3 Der Swiss Code 2014

Der „Swiss Code of Best Practice for Corporate Governance“ ist seit 2002 eine von economiesuisse herausgegebene, etablierte, breit angewandte und vielfach zitierte Handlungsempfehlung für börsenkotierte und volkswirtschaftlich bedeutende Unternehmen. Unter anderem die Finanzkrise und die Annahme der Minder-Initiative (Artikel 95 Absatz 3 BV) sowie gesellschaftspolitische Veränderungen hatten im Jahr 2014 eine Überarbeitung des Regelwerks erforderlich gemacht. Nach einer intensiven und breiten Vernehmlassung konnte economiesuisse im Oktober 2014 die neue Version des überarbeiteten „Swiss Code“ präsentieren.

Auch der neue Swiss Code ist breit abgestützt. Er nahm bei den Neuerungen auf internationale Entwicklungen sowie auf wissenschaftliche Erkenntnisse Rücksicht. Im Bestreben, den adressierten Unternehmen in einem heterogenen Umfeld klare Empfehlungen zu machen, jedoch gleichzeitig ein Maximum an Handlungsspielraum für die ganz verschieden funktionierenden Unternehmen offen zu lassen, ist der Swiss Code konsequent prinzipienbasiert.

Neu sollen Unternehmen die Gründe für Abweichungen von den Empfehlungen des Swiss Code erläutern. Der Grundsatz dabei ist: „comply or explain“. Damit richtet sich der Swiss Code noch mehr an den bereits seit längerem international geltenden Massstäben aus.

4 Zu starre Vorgaben durch die FINMA

Während der Swiss Code prinzipienbasiert ist und damit den Adressaten bei der Umsetzung der Empfehlung ein Maximum an Gestaltungsspielraum offen lässt, weist der Entwurf der FINMA eine hohe Regelungsdichte auf. Für die Unternehmensführung und damit auch für die Regelung der Details zur Corporate Governance sind aber die Unternehmen selbst und nicht deren Aufsichtsbehörde verantwortlich. Mit einer exzessiven Detailregulierung würde die Aufsichtsbehörde faktisch zum Organ der von ihr regulierten Institute.

Die Aufsicht durch den Regulator sollte auf das Ergebnis bezogen und nicht "methodenorientiert" erfolgen. Die Entwürfe der FINMA verlassen den Grundsatz „comply or explain“ und stipulieren ein Bewilligungssystem auf einer fallbezogenen Basis. Damit wird ohne Not von einem international anerkannten Instrument bei der Durchsetzung von Corporate-Gonvernance-Bestimmungen abgewichen. Die Einführung von zwingenden Bestimmungen und die Aufgabe von „comply or explain“ führen für die von den Bestimmungen angesprochenen Unternehmen zu Rechtsunsicherheit und zu einem Mehr an Bürokratie.

Das Argument der FINMA, dass das Prinzip „comply or explain“ wenig zur Anwendung gelange und schwierig in der Anwendung sei, geht fehl. Bei dem nun vorgeschlagenen Ansatz es wird für die FINMA bei der von ihr gewählten Regelungsdichte, verbunden mit einer hohen Verbindlichkeit der Normen, mit grossen Schwierigkeiten verbunden sein, in Zukunft notwendige Anpassungen an ihren Vorgaben in der für die Adressaten zwingend erforderlichen Geschwindigkeit nachzuvollziehen.

Die FINMA hat in der Vergangenheit selber festgehalten, dass Regelungen der Corporate Governance unmöglich im Sinne eines „One size fits all“-Ansatzes durch den Bankenregulator vorgegeben werden

können. Eine derart weitgehende Standardisierung, wie sie die FINMA nun vorschlägt, würde negativen Einfluss auf den sehr heterogen und dadurch auch effizient aufgestellten Schweizer Finanzplatz haben.

Gerade auch angesichts dieser Aussagen ist economiesuisse auch der Ansicht, dass die FINMA nicht über ausreichende Kompetenzen als Bankenregulator verfügt, nun derart weitgehende, detaillierte Regelungen im Bereich der Corporate Governance zu Lasten der von ihr regulierten Unternehmen vorzusehen.

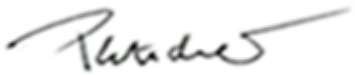
5 Fazit

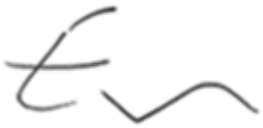
economiesuisse lehnt die Vorlage aus prinzipiellen Überlegungen zur Corporate Governance ab und verlangt die Überarbeitung der Rundeschreiben im Sinne einer grösstmöglichen Flexibilität der Adressaten. Auf keinen Fall dürfen international anerkannte Grundprinzipen der Corporate Governance wie „Comply or Explain“ sowie der etablierte prinzipienbasierte Ansatz ohne erkennbaren Nutzen einfach preisgegeben werden.

Was detaillierte Ausführungen zu einzelnen Bestimmungen angeht, so verweisen wir auf die Eingabe der Schweizerischen Bankiervereinigung (SBVg), welche wir umfassend unterstützen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse





Thomas Pletscher
Mitglied der Geschäftsleitung

Erich Herzog
Stv. Leiter Wettbewerb & Regulatorisches

De: dlb@ethics-compliance.ch
Envoyé: Mittwoch, 13. April 2016 11:55
À: Rütschi Peter
Cc: Obrist Yves; paolo.bernasconi@pblaw.ch; Brentini Simona
Objet: Rundschreiben zur Corporate Governance bei Banken / Stellungnahme

Importance: Haute

Sehr geehrte Damen und Herren

Ethics and Compliance Switzerland („ECS“) ist ein unabhängiger gemeinnütziger Verein mit Sitz in Bern zur Förderung ethisch verantwortlicher Führung und Integrität in allen Organisationen (s. www.ethics-compliance.ch). Wir befassen uns in unseren Arbeitsgruppen unter anderem mit den Grundsätzen guter Führung, mit Compliance Management Systemen und mit Whistleblowing.

Der Vorstand von ECS hat beschlossen, dass der Verein an der Anhörung zum FINMA Rundschreiben zur Corporate Governance bei Banken (hiernach „Rundschreiben“) teilnimmt. Gerne unterbreiten wir Ihnen fristgerecht unsere Stellungnahme:

Insgesamt geht der Entwurf des FINMA-RS 16/xx „Corporate Governance – Banken“ („RS“) in die richtige Richtung. Der Entwurf widerspiegelt aber den aktuellen Stand der internationalen Diskussion zur Integrität in Organisationen zu wenig und sollte deshalb in folgenden Punkten verbessert werden:

1. Das RS ist stark auf Elemente der betrieblichen Organisation und gewisser Reporting-Prozesse ausgerichtet. Es fehlt einleitend die Aussage, dass die Gewähr für ein einwandfreie Geschäftstätigkeit in erster Linie von der Führung und der Kultur des Instituts abhängt. Zudem wird unter Ziffer I eine Unsicherheit geschaffen, indem die Elemente eines integralen Kontrollsystems falsch dargestellt werden.

   Unsere Stellungnahme: Ziffer I, erster Absatz sei wie folgt neu zu fassen:

   Das vorliegende Rundschreiben erläutert die Anforderungen an die Corporate Governance und die interne Kontrolle bestehend aus Risikomanagement System, Compliance Management System, internem Kontrollsystem und der internen Revision bei Banken, Effektenhändlern, Finanzgruppen (Art. 3*c* Abs. 1 BankG) und bank- oder effektenhandelsdominierten Finanzkonglomeraten (Art. 3*c* Abs. 2 BankG). Diese werden nachfolgend als Institute
   bezeichnet.
   Gute Führung (Leadership), Werte und Unternehmenskultur sind die Basis wirksamer Corporate Governance und interner Kontrolle. Gute Führung äussert sich in einem sichtbaren Bekenntnis und einem aktiven Engagement der Mitglieder der Führung für die Werte und Kultur des Instituts.

2. Seit einigen Jahren bestehen internationale Standards, welche best practices und die Regeln der Kunst im Risiko- und im Compliance Management wiederspiegeln. ECS engagiert sich bspw. bei der Förderung der Verbreitung des internationalen Standards ISO 19600 – Compliance Management Systems, des ersten weltweiten Standards zum Compliance Management. Diese Standards sollen den zwar Instituten nicht auferlegt werden, die Institute sollen aber angehalten werden, festzulegen und öffentlich bekannt zu machen, welchen Standards oder anerkannten materiellen Regelwerken sie bezüglich der Corporate Governance, im Risiko-, im Compliance Management um bei der internen Revision folgen.

   Unsere Stellungnahme: Ziffer IV sollte wie folgt ergänzt werden:

   IV. Oberleitungsorgan

   A. Aufgaben und Verantwortlichkeiten

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

Seine Aufgaben umfassen insbesondere:

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 legt die Regelwerke fest und genehmigt die Rahmenkonzepte für das institutsweite Risikomanagement, Compliance Management und interne Revision und trägt die Verantwortung für den Aufbau, die Entwicklung, die Verwirklichung, Bewertung, das Aufrechterhalten und die fortlaufende Verbesserung der Kontrollsysteme. [...]

3. Das RS ordnet dem Compliance Management und der Compliance Funktion eine subalterne Rolle zu. Dies steht im Widerspruch zu den Erfahrungen aus der Finanzkrise, die aufgezeigt hat, dass die Rechtsrisiken zu den grössten Risiken aller Organisationen gehören. Das Compliance Management System ist ein eigenständiges und vollwertiges Element des Kontrollsystems eines Unternehmens, das in Zusammenwirken mit dem Risikomanagement System, dem (auf die operativen Prozesse ausgerichteten) IKS und überwacht durch die interne Revision das Gesamtsystem der internen Kontrolle bildet. Entsprechend ist bei der Schaffung von besonderen Kontrollausschüssen und bei der Bezeichnung von Geschäftsleitungsmitgliedern mit Kontrollfunktion stets auch die Compliance Funktion zu integrieren. Sodann kann keinesfalls eine operative Einheit Teil des Kontrollsystems sein (s. Rz 80).

   Unsere Stellungnahme: Ziffer VII ist neu zu fassen:

   VII. Internes Kontrollsystem

   Das Institut verfügt über ein adäquates, dokumentiertes internes Kontrollsystem, das auf Vorgaben, Prozessen und Systemen aufbaut. Das interne Kontrollsystem besteht aus Risiko Management System, Compliance Management System und operativem internem Kontrollsystem („Finanzkontrolle“). Die interne Revision überwacht die Wirksamkeit des gesamten internen Kontrollsystems.

   Der Begriff Risikoausschuss ist durch Risiko- und Compliance Ausschuss zu ersetzen (s. Rz. 36 ff.). Die Aufgaben des Risikoausschusses sind durch die zentralen Elemente eines Risikomanagement Systems gemäss ISO 19600 zu ergänzen:

   i) Sicherstellung des Zugangs der Compliance Funktion zum Oberleitungsorgan, ihrer Unabhängigkeit (von der Linie) und der adäquaten internen Kompetenzen und Ressourcen (s. Ziffer 4.4 des Standards, good governance Grundsätze)
   ii) Überwachung des Aufrechterhaltens der Grundwerte der Organisation und Sicherstellung, dass das Bekenntnis zu Compliance aufrechterhalten wird;
   iii) Sicherstellung, dass die Compliance-Politik und die Compliance-Ziele festgelegt und mit den Werten, den Zielen und der strategischen Ausrichtung des Instituts vereinbar sind und
   iv) Sicherstellung, dass Weisungen und Prozesse entwickelt, geschult und umgesetzt werden, um die Compliance-Ziele zu erreichen (s. Ziffer 5.3.3 des Standards).

   Der Begriff und die Funktion des CRO sind durch einen Begriff und eine Funktion zu ersetzen, die auch die Compliance Funktion einbinden (nicht aber die Rechtsfunktion, die operativer Natur ist). In Deutschland besteht beispielsweise die Position des Compliance Vorstandes.

4. Ausgehend von ISO Standard 31000 stellen wir fest, dass die FINMA in ihren Rundschreiben für den gleichen Gegenstand unterschiedliche Begriffe des Risikomanagements verwendet und gewisse Begriffe nicht verwendet. So wurde in der Vergangenheit der ISO 31000 konforme Begriff Risikotoleranz verwendet. Der zentrale Begriff und damit die zentrale Bedeutung der Risikobewältigung fehlt hingegen vollständig. Im Rundschreiben wird der Begriff „Risikoappetit“ verwendet, der nicht definiert ist und eine (US amerikanische) Randerscheinung in der ISO 31000 Praxis darstellt und als Wort ein völlig falsches Signal sendet.

Ausgehend von ISO 19600 stellen wir fest, dass der definierte Begriff Compliance nicht verwendet bzw. im Text nicht berücksichtigt wird (Compliance ist die Einhaltung aller bindenden Verpflichtungen einer Organisation; s. Ziffer 3.17 des Standards).

Unsere Stellungnahme: Im RS sollte der Begriff Risikoappetit nicht verwendet werden. Der Begriff ist durch den von der FINMA bisher verwendeten ISO 31000 konformen Begriff Risikotoleranz oder – alternativ – durch den in ISO 31000 definierten Begriff Risikoeinstellung zu ersetzen. Im RS ist zudem im Zusammenhang mit Compliance von der Einhaltung der bindenden Verpflichtungen zu sprechen (so nicht abschliessend in Rz. 8 und 103).

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme. Bei Fragen stehen Ihnen unser Vorstand und unsere Mitglieder gerne zur Verfügung.

Wir bitten Sie, uns den Empfang der Stellungnahme per E-Mail zu bestätigen. Besten Dank.

Freundliche Grüsse

Ethics and Compliance Switzerland

Prof. Dr. h. c. Paolo Bernasconi, Chairman
Dr. Daniel Lucien Bühr, Vice-Chairman

EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Per E-Mail: Peter.Ruetschi@Finma.ch
Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
3003 Bern

Zürich, 13. April 2016

Betreff: Anhörung FINMA-RS:

- **2016/xx „Corporate Governance – Banken“**
- **2008/21 „Operationelle Risiken – Banken“**
- **2010/1 „Vergütungssysteme“**

Sehr geehrter Herr Rütschi

Für die Zustellung der Unterlagen und die Gelegenheit zur Stellungnahme danken wir Ihnen bestens. Die Kommission für Bankenprüfung von EXPERTsuisse hat sich mit dem Entwurf des Rundschreibens intensiv auseinander gesetzt.

Im neuen Rundschreiben „Corporate Governance“ ist der bisher praktizierte „Comply oder Explain-Ansatz“ nicht mehr vorgesehen. Wir gehen davon aus, dass dies insbesondere bei kleineren Instituten zu einem nicht zu unterschätzenden Anpassungsbedarf auf Stufe Verwaltungsrat führen wird. Wir regen daher an, die Beibehaltung des „Comply oder Explain-Ansatzes“ zu prüfen. Sollte dieser nicht anwendbar bleiben, müsste für die Umsetzung der E-Rz 21 eine deutlich längere Übergangsfrist zugestanden werden.

In der Beilage überlassen wir Ihnen gerne weitere Bemerkungen und Anregungen.

EXPERTsuisse – Schweizer Expertenverband für Wirtschaftsprüfung, Steuern und Treuhand
Limmatquai 120, Postfach 1477, CH-8021 Zürich, Tel. +41 58 206 05 05, Fax +41 58 206 05 09
info@expertsuisse.ch, www.expertsuisse.ch

Für Rückfragen steht Ihnen Herr Rolf Walker gerne zur Verfügung.

Freundliche Grüsse
EXPERTsuisse

Dr. Thorsten Kleibold
Mitglied der Geschäftsleitung

Rolf Walker
Präsident der Kommission für Bankenprüfung

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	FINMA-RS 2016/xx Corporate Governance Banken		
	II. Begriffe		
5	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.	Ergänzung: Der Risikoappetit umfasst dabei sowohl die Risikosicht auf aggregierter Stufe als auch diejenige auf Stufe der wesentlichen Risikokategorien, d.h. Risiken nach Arten (bspw. Kredit-, Markt-, Liquiditäts-, operationelle Risiken, etc), Typen (bspw. erwarteter Verlust, Value-at-Risk, interne Liquiditäts-messgrössen, etc.) und Ebenen (bspw. Produkte, Unternehmensbereiche, Länderengagements, etc.), denen das Institut ausgesetzt ist.	Im Erläuterungsbericht (Ziff. 3.4) wird der Begriff Risikoappetit weitergehend definiert, weshalb diese Definition auch im Rundschreiben selber aufgenommen werden sollte.
8	Die Compliance-Funktion kontrolliert die Einhaltung regulatorischer und interner Vorschriften sowie die Beachtung marktüblicher Standards und Standesregeln.	.. und unterstützt und beratet die Geschäftsleitung sowie die Mitarbeiter bei der Ausarbeitung, Durchsetzung und Überwachung der regulatorischen und internen Vorschriften und unterstützt die Geschäftsleitung bei der Ausbildung und Information der Mitarbeiter bezüglich Compliance.	Die Compliance-Funktion weist auch präventive und unterstützende Funktionen auf. Wir empfehlen diese in der Begriffsdefinition ebenfalls aufzuführen (vgl. auch Rz 103).
	III. Geltungsbereich (Proportionalitätsprinzip)		
9	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.	...Die Anforderungen sind im Einzelfall unter Berücksichtigung der Grösse, der Komplexität,....	Präzisierung. *Ergänzende Bemerkung:* Im FINMA-Rundschreiben 2008/24 war der Geltungsbereich in den Rz 3-8 umfassend ausgeführt. Im neuen Rundschreiben wird darauf verzichtet.

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
			Dies dürfte zu abweichenden Auffassungen bezüglich des Geltungsbereiches (z.B. Zweigniederlassungen ausländischer Banken) führen. Dasselbe gilt bezüglich einer Anforderung der Umsetzung im Sinne des zweiten Satzes der Rz.
	IV. Oberleitungsorgan		
	A. Aufgaben und Verantwortlichkeiten		
	b) Organisation		
13	Das Oberleitungsorgan ist verantwortlich für eine angemessene Unternehmensorganisation mit ausgewogenen „Checks and Balances“. Es erlässt die für den Geschäftsbetrieb und die für die Kompetenzverteilung und Überwachung notwendigen Reglementе, insbesondere das Organisations- und Geschäftsreglement, und Weisungen.	... ausgewählte Weisungen	Die Formulierung könnte darauf schliessen lassen, dass alle Wiesungen durch das Oberleitungsorgan zu erlassen sind. Dies entspricht jedoch nicht der Praxis (Weisungen werden zu einem massgeblichen Anteil durch die Geschäftsleitung erlassen). Wir gehen nicht davon aus, dass ein abweichendes Vorgehen mit der Formulierung angestrebt ist.
	c) Finanzen		
14	Das Oberleitungsorgan trägt die oberste Verantwortung für die finanzielle Lage und Entwickung 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.	... und Entwicklung... .. die zur Veröffentlichung bestimmten Zwischenabschlüsse..	Typo. Präzisierung.
	e) Überwachung und Kontrolle		
16	Das Oberleitungsorgan übt die Oberaufsicht über die Geschäftleitung 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	...Geschäftsleitung aus...	Typo.

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	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.		
	f) Strukturveränderungen und Investitionen		
17	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.	...<u>bedeutende</u> Funktionsauslagerungen...	Wir empfehlen, auch bei den Funktionsauslagerungen den Hinweis auf deren Bedeutung zu ergänzen.
	B. Mitglieder des Oberleitungsorgans		
	a) Allgemeine Voraussetzungen		
18	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 Bank- und Finanzbereich. Das Oberleitungsorgan ist genügend breit aufgestellt, so dass nebst 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.		Gehen wir richtig in der Annahme, dass die Anforderung im letzten Satz z.B. für kleine Strukturen im Sinne der Rz 9 nicht vollumfänglich erfüllt sein muss? Anderenfalls würde dies mutmasslich erhebliche Veränderungen in den Oberleitungsorganen von kleinen Banken bedingen und die Besetzung der Funktionen dürfte schwierig zu bewerkstelligen sein.
	b) Unabhängigkeit		
26	Zudem sollte ein massgeblicher Teil des Oberleitungsorgans nicht am Institut qualifiziert beteiligt sein oder einen qualifiziert Beteiligten vertreten. Die Gläubigerinteressen auf Ebene des Einzelinstituts haben gegenüber abweichenden Eigentümer- oder Gruppeninteressen Vorrang.		Der Begriff „massgeblicher Teil“ definiert u.E. nicht klar genug, wie gross der Anteil der Vertreter eines qualifiziert Beteiligten sein darf. Ausserdem signalisiert das Wort „sollte“ dass es sich bei dieser Vorgabe eher um eine Empfehlung, nicht aber um eine verbindliche Vorgabe handelt.

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
			Für die Beurteilung im Rahmen einer Aufsichtsprüfung halten wir diese Bestimmung als derart offen formuliert, dass der vorgefundene Sachverhalt nicht wirkungsvoll gegen ein aufsichtsrechtliches Kriterium gemessen werden kann.
	C. Grundsätze der Mandatsführung		
30	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.	... oder Notfälle zeitnah bereitzuhalten. Anzahl...	Eine dauernde Bereitschaft erscheint nicht realistisch. Mit „zeitnah“ soll die Erwartung an die Bereitschaft realistischer formuliert werden.
31	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.	Das Oberleitungsorgan legt das Anforderungsprofil seiner Mitglieder, seines Präsidenten und allfälliger Ausschuss-mitglieder sowie des Vorsitzenden der Geschäftsleitung schriftlich fest. Es.....	Der Klarheit und Nachvollziehbarkeit halber sollte das Anforderungsprofil den Grundsatz der Schriftlichkeit erfüllen. Überdies ermöglicht ausschliesslich ein schriftliches Anforderungsprofil dessen Prüfung.
33	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.	... Bestehende und frühere Interessenbindungen sind gegenüber dem gesamten Oberleitungsorgan offenzulegen...	Wir gehen davon aus, dass die bestehenden und früheren Interessenbindungen intern offenzulegen sind. Dies sollte präzisiert werden. Sollten die Interessenbindungen extern offengelegt werden, muss dies ausdrücklich erwähnt werden.
	D. Arbeitsteilung und Ausschüsse		
	b) Ausschüsse		
36	Zu seiner Unterstützung kann das Oberleitungsorgan aus seiner Mitte Ausschüsse einrichten oder Aufgaben einzelnen Mitgliedern übertragen. Institute der Aufsichtskategorien 1 - 3		Gehen wir richtig in der Annahme, dass die FINMA auf der Grundlage eines begründeten

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	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.	… , der Vorbereitung und Durchführung von ausgewählten Personalentscheiden sowie bei der Nachfolgeplanung von Schlüsselpersonen unterstützt …	Gesuchs auch Ausnahmen von der Pflicht zur Einrichtung eines separaten Prüf- und Risikoausschuss zu gewähren gedenkt? Dies erscheint in Einzelfällen angemessen. Typo und Präzisierung.
37	Der Prüfausschuss soll sich von andern Ausschüssen personell hinreichend unterscheiden.		Die Aussage "personell hinreichend unterscheiden" ist sehr ungenau und lässt einen grossen Auslegungsspielraum zu. So stellt sich die Frage, ob beispielsweise eine personelle Unterscheidung des Vorsitzes in den Ausschüssen bereits als ausreichend interpretiert werden kann. Der Umfang der als notwendig erachteten personellen Unterscheidung dürfte im Speziellen auch für kleinere Banken relevant sein.
38	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.	..und Vergütungs- und Nominationsausschusses muss…	Analoge Formulierung wie in Rz 36. *Ergänzende Bemerkung* Wir empfehlen auch den Begriff der Finanzgruppe zu definieren (unklar, ob sich dieser auf die Muttergesellschaft des Instituts und/oder regulierte Tochtergesellschaften des Instituts bezieht).
Neue Rz		Die Präsidenten des Prüf- und des Risikoausschusses sollen	Diese Bestimmung ist im Erläuterungsbericht (Ziff. 3.2.5)

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
		grundsätzlich unabhängig sein und weder als Präsident des Oberleitungsorgans noch als Präsident eines anderen Ausschusses fungieren.	aufgeführt. Für deren Verbindlichkeit sollte die Bestimmung im Rundschreiben selber aufgeführt werden.
39	Aufgaben und Funktionsweise von ständigen Ausschüssen sind vom Oberleitungsorgan in einem Organisationsreglement zu regeln.	..im Organisationsreglement oder in einem separaten Reglement (...)	In der Praxis finden sich im Organisationsreglement (oft Organisations- und Geschäftsreglement) wiederholt nur Verweise auf bestehende Ausschüsse. Deren Aufgaben und Funktionsweise wird daher oft in separaten Reglementen verankert.
	V. Geschäftsleitung		
	A. Aufgaben und Verantwortlichkeiten		
54	Die Geschäftsleitung ist insbesondere verantwortlich für:		
59	• die Ausgestaltung sowie den Unterhalt eines internen Kontrollsystems (IKS) gemäss Rz 79;	...(IKS) gemäss Kapitel VII. dieses Rundschreibens;	Wir empfehlen einen generellen Bezug auf Kapitel VII des Rundschreibens zu erfassen (nicht isoliert auf Rz 79).
63	• 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.	die Sicherstellung, dass...	Anpassungsvorschlag soll passende Überleitung zu Rz 54 sicherstellen.
	VII. Internes Kontrollsystem		
79	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	Im Weiteren sind Kontrollen vorzusehen, um insbesondere mögliche Verletzungen der Risikolimiten (Schwellenwerte	Präzisierung.

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	das Finanzinstitut angemessene Risikominderungs- und/oder Risikotransferstrategien zu implementieren.	oder Grenzwerte) und Abweichungen von der festgelegten Risikopolitik frühzeitig zu erkennen und effektive Limitenüberschreitungen (feste Limiten) zu vermeiden.	
	B. Unabhängige Kontrollinstanzen		
82	Das Vergütungssystem für unabhängige Kontrolllinstanzen 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.	...unabhängige Kontrollinstanzen	Typo.
	a) Einrichtung und Unterstellung		
87	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.	Sie bestimmen einen CRO (Chief Risk Officer), der für die Risikokontrolle zuständig ist.	Präzisierung, da der Begriff CRO nicht anderweitig erläutert wird.
	b) Aufgaben und Verantwortlichkeiten der Risikokontrolle		
95	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.		
Neue Rz		Es sind typischerweise auch Schwellenwerte vorzusehen, die eine (mögliche) Verletzung der festgelegten Risikolimiten frühzeitig erkennen lassen.	Diese sinnvolle Bestimmung ist im Erläuterungsbericht (Ziff. 3.4) aufgeführt. Es wäre u.E. sinnvoll, diese Bestimmung im Rundschreiben ebenfalls aufzuführen.
98	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	... dem Oberleitungsorgan und dem Risikoausschuss mindestens... Im Weiteren unterrichtet die Risikokontrolle das Oberleitungs-	Ergänzung. In der Praxis kann sich auch ein Ausschuss des Oberleitungs-

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	Berichte ist der internen Revision und der Prüfgesellschaft zur Verfügung zu stellen.	organ oder einen seiner Ausschüsse unverzüglich (...)	organs primär mit Verletzungen der Risikolimiten beschäftigen. Daher sollte es auch in diesem Fall zulässig sein, an einen entsprechenden Ausschuss des Oberleitungsorgans zu gelangen.
	X. Offenlegung		
128	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.	.... Anspruchsgruppen transparent erläutert werden.	Präzisierung.
	XI. Inkrafttreten und Übergangsbestimmungen		
144	Dieses Rundschreiben tritt am [...] in Kraft.		Wir regen an, dass das Rundschreiben auf den Beginn des Geschäftsjahres der Mehrzahl der Institute, nämlich auf den 1. Januar 2017, inkraftgesetzt wird.
145	Die Umsetzung folgender Anforderungen hat bis spätestens ein Jahr nach Inkrafttreten zu erfolgen: 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.		Vgl. Begleitbrief zur Umsetzungsfrist von Rz 18/21.

Rz	Text gemäss Anhörungsentwurf	Anpassungsvorschläge	Begründung / Bemerkungen
	FINMA-RS Corporate Governance Banken		
1	La présente circulaire explique les exigences à l'égard de la gouvernance d'entreprise, au système de contrôle interne et à la gestion des risques chez les banques, les négociants en valeurs mobilières, les groupes financiers (art. 3c al. 1 LB) et les conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières (art. 3c al. 2 LB). Ceux-ci sont désignés ci-après par le terme d'« établissements ».	La présente circulaire explique les exigences en matière de gouvernance d'entreprise, de système de contrôle interne et de gestion des risques auprès des banques, des négociants en valeurs mobilières, des groupes financiers (art. 3c al. 1 LB) et des conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières (art. 3c al. 2 LB). Ceux-ci sont désignés ci-après par le terme d'« établissements »	Klarere Formulierung.
12	Sur proposition de la direction, l'organe responsable de la direction supérieure détermine la stratégie commerciale, fixe les principaux objectifs de l'entreprise ainsi que la charte de l'entreprise et édicte des principes directeurs concernant la culture d'entreprise et les valeurs de l'entreprise. Elle approuve le concept-cadre pour la gestion des risques à l'échelle de l'établissement et supporte la responsabilité de la réglementation, de la mise en place et de la surveillance d'une gestion des risques efficace ainsi que du pilotage des risques globaux. Elle appréhende les structures de l'entreprise et les risques de chaque champ d'activité de l'établissement.	Elle comprend les structures de l'entreprise et les risques de chaque champ d'activité de l'établissement.	Ersatz von « appréhende » durch « comprend ».
16	L'organe responsable de la direction supérieure exerce la haute surveillance sur la direction et garantit la compliance au sein de l'établissement. Il veille au caractère approprié de l'environnement de contrôle et de risque au sein de l'établissement. Il met en place un système de contrôle interne efficace, mandate et surveille la révision interne, désigne la société d'audit prudentielle et en évalue les rapports. L'organe responsable de la direction supérieure ou son comité responsable surveille et juge l'efficacité de la révisioninterne et s'assure régulièrement que celle-ci dispose de ressources et de compétences appropriées ainsi que de l'indépendance et de l'objectivité adéquates pour assumer ses tâches de contrôle au sein de l'établissement.	….ou son comité responsable surveille et évalue l'efficacité de la révision	Ersatz von « juge » durch « évalue ».

Rz	Text gemäss Anhörungsentwurf	Anpassungsvorschläge	Begründung / Bemerkungen
34	Le président est une personne présentant une faculté de jugement, des capacités de gestion et une intégrité exceptionnelles. Il marque de façon décisive la stratégie, la communication et la culture de l'entreprise.	....et une intégrité éprouvé.	Das Wort « exceptionnelles » scheint uns den deutschen Begriff « ausgewiesen » nicht richtig wiederzugeben.
35	Il est à la tête de l'organe collectif et est responsable de son bon fonctionnement conformément au règlement. Il représente l'organe responsable de la direction supérieure tant à l'intérieur de l'entreprise que vis-à-vis de l'extérieur. Il entretient un dialogue régulier avec le président de la direction et les autres membres de celle-ci, avec les personnes à la tête des fonctions de contrôle et est responsable de la préparation et de la diffusion du flux d'informations au sein de l'organe responsable de la direction supérieure.		Im ersten Satz besteht eine Abweichung zwischen der französischen und der deutschen Version. Der Satzteil „conformement au règlement" fehlt in der deutschen Version. Die beiden Versionen sind aufeinander abzustimmen.
93	Le contrôle des risques participe au processus de développement des produits, services, domaines d'activité ou secteurs de marché nouveaux ou étendus ou des transactions complexes et à l'examen de la diligence (due diligence).	Le contrôle des risques participe au processus de développement de nouveaux produits, services, domaines d'activité ou secteurs de marché ou à leur extension ou aux transactions complexes au niveau de leur développement, respectivement à l'examen de la diligence (due diligence).	Klarere Formulierung.
97	Le contrôle des risques remet au moins une fois par semestre un rapport à la direction relatif aux risques et aux positions-risque. En cas d'évolution particulière de la situation, il en informe immédiatement la direction et la révision interne et, en cas de faits de grande portée, l'organe responsable de la direction supérieure et le comité des risques.	.... la direction supérieure respectivement le comité des risques.	Anpassung an die deutsche Version (..Oberleitungsorgan bzw. den Risikoausschuss).
102	• la remise à l'organe responsable de la direction supérieure d'un rapport annuel sur l'évaluation du risque de compliance et l'activité de la fonction de compliance. Une copie du rapport doit être mise à disposition de la révision interne et aussi de la société d'audit.	.....de la révision interne et ~~aussi~~ de la société d'audit.	Das Wort « aussi » ist überflüssig.
	FINMA-RS OpRisk Banken		
	Annexe 3		
33	La banque doit disposer d'exigences claires en matière de sécurité pour les collaborateurs qui ont accès aux CID. Elle doit		

Rz	Text gemäss Anhörungsentwurf	Anpassungsvorschläge	Begründung / Bemerkungen
	vérifier périodiquement si les exigences relatives à un traitement adéquat des CID sont toujours remplies. Des exigences supérieures de sécurité doivent s'appliquer aux utilisateurs de l'informatique et usagers privilégiés disposant d'un accès fonctionnel 26 à une grande quantité de CID (« collaborateurs clés »). Ces exigences supérieures de sécurité doivent également s'appliquer aux usagers privilégiés ayant accès à des souscatégories de CID hautement confidentielles (par ex. comptes chiffrés).	.. s'appliquer au personnel de l'informatique et usagers privilégiés....	Präzisierung.
34			Die in Rz 33 vorgeschlagene Formulierung müsste in Rz 34 nachvollzogen werden.
35	Des dispositifs tels que la tenue de fichiers-journaux doivent être introduits afin de permettre l'identification des utilisateurs qui ont accès à une grande quantité de CID. Les transactions individuelles et les accès individuels doivent être attribués aux différents utilisateurs.	... ont eu accès	Es ist zu prüfen, ob mit dieser Änderung die deutsche Formulierung „zugreifen" nicht zutreffender wiedergegeben wird. (Der Zugriff [ont eu accèes] wird aufgezeichnet und nicht die blosse Möglichkeit des Zugriffs [ont accès].).

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	FINMA-RS 08/21 Operationelle Risiken Banken		
	Anpassungen		
	IV. Qualitative Anforderungen an den Umgang mit operationellen Risiken		
	B. Qualitative Grundanforderungen		
	e) Grundsatz 4: Technologieinfrastruktur		
135.1	Die Geschäftsführung stellt sicher, dass das IT-Konzept in Anlehnung an die internationalen Standards das Vorhandensein der folgenden minimalen Aspekte gewährleistet: a. Aktuelle und vollständige Übersicht über die wesentlichsten Bestandteile der IT-Netzwerkumgebung mit Schnittstellen zwischen Systemen und Applikationen, b. Vorgaben und Prozesse, die eine explizite Identifikation und Beurteilung von inhärenten IT-Risiken sowie die Überwachung der Risikominderung und einen angemessenen Umgang mit den IT-Residualrisiken sicherstellen, c. Systematischer Prozess im Hinblick auf die Identifikation und Beurteilung von IT-Risiken im Rahmen der Sorgfaltsprüfung (Due Diligence) insbesondere bei Akquisitionen resp. Auslagerungen im IT-Bereich, d. Eindeutige Festlegung von Rollen, Aufgaben und Verantwortlichkeiten in Bezug auf Daten- und Prozessverantwortliche, e. Überwachungsprozess, der die Einhaltung von regulatorischen und institutsinternen Vorgaben für IT-Systeme und -Prozesse sicherstellt, f. Prozesse zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Verantwortung zur Reduk-	a. Aktuelle und vollständige Übersicht über die wesentlichsten Bestandteile der IT-Architektur mit Schnittstellen zwischen Systemen, Applikationen und Dritten. d. Eindeutige Festlegung von Rollen, Aufgaben und Verantwortlichkeiten in Bezug auf Basisinfrastruktur, Applikationen, Daten und Prozesse. f. Prozesse zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf	a. Mit der IT-Architektur werden alle statischen und dynamischen Aspekte der IT in einer Organisation umschrieben. Hierzu zählen unter anderem die Infrastruktur-Bestandteile (Hardware, Standorte, Netzwerke, Software [Anwendungen], Daten).Darüber hinaus sollten funktionale Aspekte wie die notwendigen Schnittstellen, die eine reibungslose IT-Unterstützung der Prozesse in der Organisation und zu Dritten (Providern) ermöglichen, Teil einer Beschreibung sein. d. Präzisierung: Festlegung von Rollen, Aufgaben und Verantwortlichkeiten in Bezug auf die IT-Komponenten sowie Prozesse. f. Präzisierung: Mit der Informationssicherheit werden die Schutzziele Vertraulichkeit, Ver-

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	tion von IT-Risiken sowie Einhaltung der IT-Sicherheit und –Verfügbarkeit,	ihre Verantwortung zur Reduktion von IT-Risiken sowie der Einhaltung und Stärkung der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit).	fügbarkeit und Integrität sichergestellt.
	g. Technologie- und Investitionsplanung zur Sicherstellung einer angemessenen IT-Kapazität sowohl unter normalen Geschäftsbedingungen wie auch in Stressperioden sowie zur Reduktion der Komplexität und Fragmentierung der IT-Infrastruktur.	g. ~~sowie zur Reduktion der Komplexität und Fragmentierung der IT-Infrastruktur~~.	g. Die aktuelle Formulierung erscheint missverständlich. Die Ausführung kann so verstanden werden, dass die Technologie- und Investitionsplanung zwingend zu einer Reduktion der Komplexität und Fragmentierung der IT-Infrastruktur beitragen muss. Die ist nicht zwingend der Fall. Wir empfehlen daher eine Umformulierung oder Streichung des letzten Teils des Satzes.
135.2	Die Geschäftsführung hat zudem ein Konzept für den Umgang mit Cyberrisiken zu implementieren. Dieses Konzept hat mindestens die folgenden Aspekte abzudecken und eine effektive Umsetzung durch geeignete Prozesse sowie eine eindeutige Festlegung von Aufgaben, Rollen und Verantwortlichkeiten zu gewährleisten:	.... ein Konzept in Anlehnung an einen anerkannten Standard (z.B. NIST Standard) für den Umgang... *Fussnote: Definition „Cyber Risiken“:* (Beispiel) Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.	Die definierten Aspekte [a)-e)] basieren auf dem NIST Standard, welcher auch beim Self Assessment der FINMA als Grundlage angewendet wurde. Dieser verlangt implizit einen weitaus spezifischeren Anforderungskatalog als die im Rundschreiben pauschal formulierten Anforderungen. Wir empfehlen daher das Konzept zur Behandlung von Cyberrisiken an den NIST Standard oder einen anderen Standard anzulehnen, um das gemeinsame Verständnis zu fördern. Zudem wäre eine Definition des Begriffs Cyberrisken wünschenswert, da es unterschiedliche Definitionen gibt.
	a. Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyberattacken, insbesondere in Bezug auf besonders schützenswerte Daten und Systeme,	a)... im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und IT Systeme *Fussnote: Definition „Cyberattacke“* (Beispiel): An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously con-	a. Präzisierung/Ergänzung. Eine Definition des Begriffs „Cyberattacke“ würde ein einheitliches Vorgehen bei der Identifikation der institutsspezifischen Bedrohungspotenziale unterstützen.

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
		trolling a computing environment/ infrastructure; or destroying the integrity of the data or stealing controlled information. (SOURCE: Committee on National Security Systems Instruction No. 4009) Cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (SOURCE: Committee on National Security Systems Instruction No. 4009)	
	b. Schutz der Technologieinfrastruktur vor Cyberattacken, insbesondere im Hinblick auf die Verfügbarkeit der Systeme und die Integrität resp. Vertraulichkeit von Daten,	b. Schutz der Geschäftsprozesse und Technologieinfrastruktur vor Cyberattacken, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und IT Systeme.	b. Präzisierung. Cyberrisiken bedrohen nicht nur die Technologie, vielmehr auch die Geschäftsprozesse. Vertraulichkeit, Integrität und Verfügbarkeit (CIA) - Fachlich korrekte Reihenfolge
	c. Erfassung von Cyberattacken auf Basis einer systematischen Überwachung der Technologieinfrastruktur,	c. Zeitnahe Erkennung und Aufzeichnung von Cyberattacken auf Basis eines Prozesses zur systematischen Überwachung der Technologieinfrastruktur,	c. Präzisierung. Terminologie dem NIST Standard folgend. Cyberattacken können anhand von Anomalien in der IT Infrastruktur erkannt werden. Dazu müssen neben den technischen auch organisatorische Massnahmen getroffen werden.
	d. Reaktion auf Cyberattacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyberattacken in Abstimmung mit dem	d. Reaktion auf Cyberattacken durch zeitnahe und gezielte präventive Massnahmen, wie bedrohungsspezifische Desaster Recovery Pläne, sowie bei we-	d. Präzisierung. Technische Massnahmen des BCM's wie aktives spiegeln (hot site) der Datencenter kann unter Umständen bei einem Malwarebefall auch die Backupinfrastruktur

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
	BCM, und	sentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyberattacken in Abstimmung mit dem BCM, und	beinträchtigen.
	e. Sicherstellung einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyberattacken durch geeignete Massnahmen.	e. .... durch <u>proaktive, detektive und reaktive</u> Massnahmen.	e) Präzisierung und Komplementierung zu den vorangegangenen Anforderungen: die Aspekte [a)-d)] erfordern unterschiedliche Arten von Massnahmen bzw. Kontrollen.
	g) Grundsatz 6: Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft		
136.4	Wenn Banken oder ihre Gruppengesellschaften grenzüberschreitend Finanzdienstleistungen erbringen oder Finanzprodukte vertreiben, sind auch die aus einer Anwendung ausländischer Rechtsvorschriften (Steuer-, Straf-, Geldwäschereirecht usw.) resultierenden Risiken angemessen zu erfassen, begrenzen und kontrollieren. Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Banken ausländisches Aufsichtsrecht einhalten. Die Banken unterziehen ihr grenzüberschreitendes Finanzdienstleistungsgeschäft sowie den grenzüberschreitenden Vertrieb von Finanzprodukten einer vertieften Analyse der rechtlichen Rahmenbedingungen und der damit verbundnenen Risiken. Gestützt auf diese Analyse treffen die Banken die erforderlichen strategischen und organisatorischen Massnahmen zur Risikoeliminierung und -minimierung und passen diese laufend geänderten Bedingungen an. Insbesondere verfügen sie über das notwendige länderspezifische Fachwissen, definieren sie spezifische Dienstleistungsmodelle für die bedienten Länder, schulen die Mitarbeiter und stellen durch entsprechende organisatorische Massnahmen, Weisungen, Vergütungs- und Sanktionsmodelle die Einhaltung der Vorgaben sicher. Auch externe Vermögensverwalter, Vermittler und andere Dienstleister sind entsprechend sorgfältig auszuwählen und in ihrer Rolle als Beauftragte zu schulen.	...damit <u>verbundenen</u> Risiken.	Typo.

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
136.5	Die Institute informieren die FINMA, wenn sich wesentliche Risiken materialisieren und/oder sie in diesem Zusammenhang von ausländischen Behörden kontaktiert werden.		Es wäre wünschenswert, wenn diese Informationspflicht auch im FINMA-RS 08/1 aufgeführt würde.
	Anhang 3		
2	Kleine Banken sind von der Erfüllung folgender Randziffern ausgenommen: • Rz 15-19 sowie 22 des Grundsatze 3; • Alle Randziffern der Grundsätze 4-6; • Rz 41 des Grundsatzes 7.		Obwohl Rz 2 nicht Gegenstand von Anpassungen resp. der Vernehmlassung ist, möchten wir auf folgenden Sachverhalt hinweisen: Rz 2, Anhang 3 FINMA-RS 2008/21 nimmt kleine Banken von der Erfüllung bestimmter Randziffern aus. Im Gegensatz dazu werden bei den Randziffer 135 und 136 ff Anforderungen gestellt, die einen Konflikt mit dem Anhang 3 darstellen: Wir sehen folgende Konflikte: Op.Risk — Anhang 3 135.1.a Inventar IT Netzwerkumgebung und Schnittstellen — Rz 16 Inventar Applikationen und Infrastruktur 135.1.b. Überwachung der Risikominderung; angemessener Umgang mit IT-Residualrisiken — Rz 23 Sicherheitsstandards für Infrastruktur und Technologie; Rz 36 Identifikation und Bewertung inhärente und Residualrisiken betreffend Vertraulichkeit von CID 135.1.c Identifikation und Beurteilung von IT-Risiken — Rz 36 Identifikation und Bewertung inhärente und Residualrisiken betreffend Vertraulichkeit von CID

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
			135.1 f Bewusstsein der Mitarbeiter zur Reduktion der IT-Risiken sowie Einhaltung IT-Sicherheit Rz 32 Schulung auf Kundendaten-sicherheit Wir empfehlen diesen Konflikt zu bereinigen (z.B. in dem die genannten Grundsätze auch auf die kleinen Banken anwendbar erklärt werden. Anforderungen sind dabei abhängig von der Grösse, Komplexität und des Risikoprofils des Instituts umzusetzen).
41.1	Wendet ein als kleine Bank eingestuftes Institut bei der Entwicklung, Veränderung und Migration von Systemen (bspw. bei der Generierung von Testdaten oder bei der Zwischenspeicherung von Daten während der Datenmigration) keine Methoden zur Anonymisierung, Pseudonymisierung oder Verschlüsselung an (Arbeiten „in Klartext"), so wendet es bei diesen Tätigkeiten die Vorgaben gemäss Rz 40 an.		Der Paragraph impliziert, dass grosse Banken nicht mit Daten im Klartext während der Entwicklung, Migration etc. arbeiten. Obwohl die Anonymisierung, Pseudonymisierung oder Verschlüsselung als Good Practice für die meisten Stufen eines Entwicklungs- oder Transformationsprojekts angesehen werden kann, besteht hierfür keine direkte Anforderung. Wir regen an, Ziffer 41.1 auf alle Banken anwendbar zu erklären.
	FINMA-RS 10/1 „Vergütungssysteme"		
4	Adressaten des Rundschreibens sind alle der schweizerischen Finanzmarktaufsicht unterstellten Banken, Effektenhändler, Finanzgruppen und Finanzkonglomerate, Versicherungsunternehmen, Versicherungsgruppen und Versicherungskonglomerate sowie Bewilligungsträger nach Art. 13 Abs. 2 und 4 des Kollektivanlagengesetzes (KAG; SR 951.31). Diese werden nachfolgend als Finanzinstitute bezeichnet.	... Bewilligungsträger nach Art. 13 Abs. 2 ~~und 4~~ des Kollektivanlagengesetzes (KAG; SR 951.31). ...	Abs. 4 des Art. 13 KAG wurde mit Wirkung auf den 1. März 2013 aufgehoben.
8	Finanzinstitute, welche unterhalb der Schwellenwerte von Rz 6 und 7 sind, müssen das vorliegende Rundschreiben nicht zwingend umsetzen. Ihnen wird jedoch empfohlen, die nachstehenden Grundsätze als Leitlinien für ihre Vergütungssysteme heranzuziehen.	Finanzinstitute, welche unterhalb der Schwellenwerte von Rz 6 und 7 sind sowie Bewilligungsträger nach Art. 13 Abs. 2, müssen das vorliegende Rundschreiben nicht zwingend umsetzen.	Auf dem Deckblatt und unter Rz 4 des Rundschreibens(RS) werden KAG Bewilligungsträger ebenfalls diesem RS unterstellt. Allerdings fehlt für KAG Bewilligungsträger eine entsprechende Ausnahme in der Rz 8, welche für diese

Rz	Entwurf RS	Anpassungsvorschläge	Begründungen / Bemerkungen
		Ihnen wird jedoch empfohlen, die nachstehenden Grundsätze als Leitlinien für ihre Vergütungssysteme heranzuziehen.	analog zu kleineren Banken und Versicherungen dieses RS lediglich als Empfehlung gilt. Somit wäre das RS auch für kleine KAG Bewilligungsträger vollständig anwendbar, was u.E. nicht sachgerecht ist. Für KAG Bewilligungsträger sollten gleichen Regeln gelten, wie für kleinere Banken und Versicherungen.

De :	Bühr Daniel Lucien
A :	Rütschi Peter
Cc :	Troller Alexander; Baizeau Domitille; Meienberger Rita
Objet :	Anhörung Rundschreiben zur Corporate Governance bei Banken - Stellungnahme LALIVE SA
Date :	Dienstag, 12. April 2016 16:00:35
Pièces jointes :	E_RS_16_xx_CorpGovBanken_Anh20160301_de_Stellungnahme LALIVE SA.pdf
Importance :	Elevée

Sehr geehrte Damen und Herren

Wir beraten Schweizer Banken zu Fragen der Corporate Governance, des Risikomanagements und des Compliance Managements. Gerne nehmen wir an der Anhörung zum FINMA Rundschreiben zur Corporate Governance bei Banken (hiernach „Rundschreiben“) teil.

Das Rundschreiben wiederspiegelt wichtige internationale „GRC“ (Governance, Risk and Compliance Management) Entwicklungen der letzten Jahre. In seiner Gesamtheit betrachten wir den Entwurf des Rundschreibens als gute Basis, die in einigen Punkten jedoch fachlich verbessert werden sollte. Aus dem guten Entwurf kann ein international Massstäbe setzendes Rundscheiben werden, das die Schweizer Banken anleitet, internationale Best Practice umzusetzen, was den guten Ruf des Finanzplatzes festigen wird.

In der Beilage senden wir Ihnen unsere detaillierte Stellungnahme zu (PDF Datei), die gemeinsam mit der folgenden Zusammenfassung der Stellungnahme und Erläuterung zu lesen ist:

i) Die Finanzkrise hat aufgezeigt, dass einwandfreie Geschäftstätigkeit in allererster Linie das Resultat von guter Führung, einer massvollen Risikokultur und einer Kultur der Werte und Integrität ist. Diese zentralen Elemente werden im Rundschreiben zu wenig betont, vielmehr ist der Fokus auf (grundsätzlich richtige) Anforderungen an die Organisation und auf Prozesse ausgerichtet. Organisation und Prozesse für sich alleine sind aber leere Instrumente, wenn sie nicht auf einer werteorientierten Führung aufbauen.

   Stellungnahme: Die zentrale Bedeutung von guter Führung (Leadership) sowie einer Werte- und Risikokultur sind im Rundschreiben stärker hervorzuheben.

ii) Das Rundschreiben befasst sich richtigerweise nicht mit der zentralen Frage, was denn inhaltlich wirksames Risikomanagement und Compliance Management ist. Diese Frage beantworten Standards wie beispielsweise ISO 31000 oder das COSO Enterprise Risk Management Framework oder ISO 19600 im Bereich des Compliance Managements. Was das Rundschreiben aber unterlässt, ist zu verlangen, dass das Oberleitungsorgan die anwendbaren Regelwerke festlegt. Ohne Regelwerk wird eine Organisation nach eigenen Regeln arbeiten, die nach der allgemeinen Lebenserfahrung kein gleichwertiger Ersatz für Regelwerke sein können, die, wie die genannten Regelwerke, von dutzenden führender Experten in strukturierten, transparenten Verfahren erarbeitet wurden. Die Regeln der Kunst werden nur dann zuverlässig befolgt werden, wenn eine Organisation sich an einen materiellen Standard hält (ein materieller Standard regelt den Gegenstand inhaltlich umfassend; Konzepte, bspw. das Three Lines of Defense Risk Governance Konzept, sind keine Standards). Damit wird für die FINMA das Risiko- und Compliance Management der

Banken transparent und vergleichbar und für die Banken werden Komplexität und Kosten reduziert.

Stellungnahme: Das Oberleitungsorgan muss das für das Risikomanagement und das für das Compliance Management anwendbare Regelwerk festlegen. Das Regelwerk muss den Gegenstand materiell regeln und anerkannt sein, bspw. durch Erlass durch eine Standardisierungsbehörde.

iii) Das Rundschreiben soll wiederspiegeln, dass die FINMA in den Bereichen Risiko- und Compliance Management sich von einem bestimmten Konzept und einer einheitlichen Terminologie leiten lässt. Die einzigen weltweiten Standards, welche Begriffe des Risikomanagements und des Compliance Managements definieren sind ISO 31000 und ISO 19600. Vorab ist der Begriff „Risikoappetit" durch den ISO 3100 Begriff risk attitude / Risikoeinstellung zu ersetzen. Der Begriff Risikoappetit (der aus den USA stammt und keine klare Grundlage hat) suggeriert Risikohunger und ist fehl am Platz. Richtig sind die ISO 31000 Begriffe Risikoeinstellung oder Risikotoleranz (diesen Begriff verwendet die FINMA bspw. im Rundschreiben 2015/2 Liquiditätsrisiken Banken). Auch im Bereich Compliance Management existieren standardisierte Begriffe (bspw. Compliance / bindende Verpflichtungen etc.).

Stellungnahme: Das Rundschreiben soll international standardisierte Begriffe des Risikomanagements und des Compliance Managements verwenden. Der Begriff „Risikoappetit" ist durch Risikoeinstellung oder Risikotoleranz zu ersetzen. Die FINMA soll die Begriffe konsistent einheitlich verwenden.

iv) Die Bedeutung des Compliance Management Systems als Teil eines integralen Kontrollsystems (IKS, Risikomanagement System, Compliance Management System, Interne Revision; s. Kalia/Müller, Risk Management at Board Level, Haupt Verlag, 2015, S. 68) kommt im Rundschreiben nicht zur Geltung. Compliance-Risiken zählen zu den grössten Risiken aller Unternehmen und das Compliance Management muss gleichwertig neben dem Risikomanagement stehen. Im Rundschreiben wird aber der Fokus primär auf das Risikomanagement gelegt und dem Compliance Management wird eine subalterne Rolle zugeordnet. Das Compliance Management ist eine eigene Management-Disziplin, die Aufgaben sind andere als die Aufgaben des Risikomanagements (obwohl beide Bereiche komplementär und interdependent sind). ISO Standard 19600 bildet die vielfältige, multidisziplinäre und komplexe Aufgabenstellung wirksamen Compliance Managements gut ab und bezeichnet die Rahmenbedingungen wirksamer Compliance: Berücksichtigung der good compliance governance Prinzipien (Zugang zum Oberleitungsorgan, Unabhängigkeit von der Linie, adäquate Kompetenzen und Stellung sowie ausreichende Ressourcen; s. Ziffer 4.4 des Standards), Festlegung einer Compliance Strategie und Ziele durch das oberste Organ, Umsetzung der Compliance durch alle Mitarbeiter auf allen Stufen und in allen Bereichen der Organisation etc.

Stellungnahme: Die Systematik des Rundschreibens ist anzupassen: VI IKS (primär eine operative Prozesskontrolle), VII Risikomanagement, VIII Compliance Management, IX Interne Revision. Das Oberleitungsorgan soll (bei Banken der Aufsichtskategorien 1 bis 3) einen Risiko- und Compliance Ausschuss bilden und bei

allen Banken soll ein Mitglied der Geschäftsleitung für Risiko- und Compliance Management verantwortlich sein (Vollzeitanstellung; Ausnahme: Aufsichtskategorien 4 und 5 / Teilzeitfunktion). Die Funktion soll so bezeichnet werden, dass die Verantwortung für das Management in beiden Bereichen klar ist. Die Person soll Fachkenntnis und Erfahrung in beiden Bereichen besitzen. Sie berichtet regelmässig unabhängig schriftlich und mündlich an das Oberleitungsorgan.

Bei Fragen stehen wir Ihnen gerne zur Verfügung.

Dürfen wir Sie bitten, uns den Empfang der Stellungnahme kurz per E-Mail zu bestätigen? Danke vielmals.

Freundliche Grüsse

LALIVE SA

Daniel Bühr

Daniel Lucien Bühr
Partner
LALIVE SA

Stampfenbachplatz 4
P.O. Box 212
8042 Zurich
Switzerland
www.lalive.ch
Tel +41 58 105 2100
Fax +41 58 105 2160
dbuhr@lalive.ch

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

Stellungnahme LALIVE SA - 12. April 2016

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, 3*b*–3*g*, 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	Vertriebsträger	Vertreter ausl. KKA	Andere Intermediäre	SRO	DUFI	SRO-Beaufsichtigte	Prüfgesellschaften	Ratingagenturen		
x	x						x																

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

Inhaltsverzeichnis

Inhaltsverzeichnis

Farbliche Unterlegung zur Textherkunft:

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

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

Internationale Richtlinien (insbesondere BCBS Corporate Governance Principles)

FAQ Oberleitungsorgan

I. Gegenstand

Risiko- und Compliance-Management

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

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

Schaffung einer Risikokultur und der

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

Analyse, Bewertung, Bewältigung, Überwachung und Bewältigung von Risiken dienen. [Terminologie ISO 31000]

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

Risikoappetit ist ein US amerikanisch inspirierter Begriff; steht im Widerspruch zur Terminologie von ISO 31000: Risikoeinstellung / risk attitude ist richtig.
Der Begriff Risikoappetit schafft schon in sich einen psychologischen Fehlanreiz.
Es wird hiernach darauf verzichtet jedes mal den Begriff Risikoappetit durch Risikoeinstellung zu ersetzen. Dieser Hinweis gilt für jede Wiederholung des Wortes Risikoappetit.

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.~~ unterstützt und überwacht die Einhaltung aller bindenden Verpflichtungen. [siehe ISO 19600, der den Begriff Compliance definiert] 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

bezeichnet die Werte,

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

Einhaltung der Werte und die ...
[ISO 19600 - die wichtigsten Voraussetzungen für Compliance sind Führung/Leadership und Werte/values]

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

und legt die Risikoeinstellung und Compliance Strategie fest.

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 Entwickung 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 Geschäftleitung 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 Risikomanagement und das Compliance-Management

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 nebst 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

zur Hälfte [sonst ist die Unabhängigkeit illusorisch]

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

überwiegender Teil; s. Kommentar oben

Zudem sollte ein ~~massgeblicher~~ Teil des Oberleitungsorgans nicht am Institut qualifiziert beteiligt sein oder einen qualifiziert 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 angehö- 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 Urteilskraft. 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 Kotrollfunktionen 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 Personalentescheiden 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

Risiko- und Compliance Ausschuss

[ohne Risikomanagement keine wirksame Compliance, ohne Compliance Management kein wirksames Risikomanagement

Der Prüfausschuss soll sich von andern Ausschüssen personell hinreichend unterscheiden.

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; 41
- 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; 42
- Überwachung und Beurteilung der Wirksamkeit der internen Kontrolle, ~~namentlich auch der Risikokontrolle und der Compliance-Funktion, und der internen Revision;~~ 43

Reihenfolge unlogisch: besser: Unabhängigkeit und Wirksamkeit

- Überwachung und Beurteilung der Wirksamkeit und Unabhängigkeit der Prüfgesellschaft sowie deren Zusammenwirken mit der internen Revision, einschliesslich Besprechung der Prüfberichte mit dem leitenden Prüfer; 44
- Würdigung des Prüfplans, des Prüfrhythmus und der Prüfergebnisse der internen Re- 45

, bestehend aus internem Kontrollsystem, Risikomanagement System und Compliance Management System, überwacht durch die interne Revision; s. dazu bspw. Kalia/Müller, Risk Management at Board Level, Haupt-Verlag 2015, S. 68.

vision und der Prüfgesellschaft.

d) Aufgaben des Risikoausschusses - und Compliance-Ausschusses

Die Aufgaben umfassen insbesondere die: 46

- Prüfung ~~Erörterung~~ des Rahmenkonzepts für das institutsweite Risikomanagement System 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 , der Wirksamkeit und der Anwendung der Regeln der Kunst für das institutsweite Risikomanagement und Veranlassung der notwendigen Anpassungen; 48
- Kontrolle, ob das Institut ein geeignetes Risikomanagement und Compliance Management mit wirksamen Prozessen unterhält, die der jeweiligen Risikolage und Compliance Management des Instituts gerecht werden; 49
- Überwachung der Umsetzung der Risikostrategien und den Compliance Zielen, insbesondere im Hinblick auf deren Übereinstimmung mit dem vorgegebenen Risikoappetit und den Risikolimiten gemäss Rahmenkonzept für das institutsweite Risikomanagement. 50

Prüfung des Rahmenkonzepts für das institutsweite Compliance Management System ...

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~~ Risiko- und Compliance Management (gemäss Rz 66ff.) und dessen Einhaltung. , dem Chief Compliance Officer 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

und den bindenden Verpflichtungen

V. Geschäftsleitung

A. Aufgaben und Verantwortlichkeiten

den Werten,

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~~ bindenden Verpflichtungen im Rahmen der operationellen Geschäftstätigkeit verantwortlich. 53

dem Rahmenkonzept für das institutsweite Compliance Management

Die Geschäftsleitung ist insbesondere verantwortlich für: 54

- die Führung des Tagesgeschäfts und die Vertretung des Instituts gegenüber Dritten im operativen Bereich; 55

des Rahmenkonzepts für das institutsweite Compliance Management

- 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

bindenden Verpflichtungen, inklusive aufsichtsrechtliche Vorschriften,

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 Werte, die

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

Die Systematik ist anzupassen: VI IKS, VII Risikomanagement, VIII Compliance Management, IX Interne Revision

Festlegung der Ziele des Risikomanagements und der Risikoeinstellung

VI. Rahmenkonzept für das institutsweite Risikomanagement

Das Rahmenkonzept für das institutsweite Risikomanagement wird von der Geschäftsleitung ausgearbeitet und durch das Oberleitungsorgan verabschiedet. 66

und das anwendbare Risikomanagement-Regelwerk (ISO 31000, COSO ERM o.ä.) [zentral, das sonst das RM beliebig ist]

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

nach ISO 31000 ist Risiko = Auswirkung von Unsicherheit auf Ziele; die Bildung von Risikoarten etc. ist künstlich und willkürlich; Vorschlag Verzicht auf Kategorien

Folgende Aspekte sind im Rahmenkonzept abzudecken: 68

- Einheitliche Kategorisierung der wesentlichen Risiken zur Gewährleistung von Konsistenz bei den Zielsetzungen im Risikomanagement, bei der Risikoidentifikation, Risikomessung, Risikobewirtschaftung, Risikoüberwachung und Risikoberichterstattung; 69

Gemein ist wohl, das Risikoprofil zu Beschreiben, und die Risiken bestimmter Aktivitäten zu nennen

- 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

Bewältigung [genau so wichtig, wie die Risikobeurteilung]

- Festlegung des Risikoappetits und Risikolimiten in Bezug auf sämtliche Risikokategorien und Definition von Risikominderungsstrategien und -instrumenten; 71

- Definition von Massnahmen, um Verletzungen der Risikolimiten rechtzeitig zu erkennen und zu beheben; 72

- Einrichtung organisatorischer Strukturen für die Bewirtschaftung sämtlicher Risikokategorien, einschliesslich Kompetenzen, Rechenschaftspflichten und Berichtslinien; 73

- Ausgestaltung einer Dokumentation, welche einen angemessenen unabhängigen Nachvollzug bzw. eine Überprüfung und Beurteilung der Festlegung des Risikoappetits sowie der Risikolimiten ermöglicht; 74

- Unterhalt eines Risikoberichterstattungs- und Managementinformationssystems (MIS) für sämtliche Risikokategorien; 75

- 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

Risikoprofils

- Vorgaben zur institutsweiten konsistenten Anwendung des Rahmenkonzepts, insbesondere alle neuen und wesentlichen bestehenden Produkte, Aktivitäten, Prozesse und Systeme betreffend; 77

- Bestimmungen zur Risikodatenaggregation und Risikoberichterstattung bei systemrelevanten Banken. 78

Anmerkung: Das Risikomanagement sollte nicht nur auf Ereignisse, sondern vorallem auch auf Entwicklungen ausgerichtet sein (in historischer Betrachtung bspw: Steuertransparenz und strafrechtliche Ahnung der Beihilfe zur Steuerhinterziehung im Ausland)

VII. Internes Kontrollsystem

Hiernach wird nicht das IKS sondern eigentlich das umfassende interne "GRC" System beschrieben

richtig!

79 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 ange[illegible] Risikotransferstrategien zu implementieren.

Das IKS dient der Kontrolle der sorgfältigen Geschäftsführung mit Bezug auf interne Prozesse, Risiken und die Einhaltung der bindenden Verpflichtungen.

80 Die Kontrollinstanzen umfassen mindestens drei verschiedene Bereiche des Instituts: die ertragsorientierten Geschäftseinheiten, die von den ertragsorientierten Geschäftseinheiten unabhängigen Kontrollinstanzen sowie die interne Revision.

Die Kontrollinstanzen sind interne Revision, Risikomanagement und Compliance Management. Die Linie kann nie eine Kontrollinstanz sein (da nicht unabhängig und müsste sich selbst überwachen).

A. Ertragsorientierte Geschäftseinheiten

81 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.

sind verantwortlich für die Einhaltung der Risikopolitik und der bindenden Verpflichtungen in ihrem Zuständigkeitsbereich.

B. Unabhängige Kontrollinstanzen

82 Das Vergütungssystem für unabhängige Kontrolllinstanzen 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 Ges

Das Oberleitungsorgan bestimmt die Regelwerke, nach denen die Kontrollsysteme aufgebaut, entwickelt, verwirklicht, bewertet, aufrechterhalten und fortlaufend verbessert werden. [Ohne verbindliches Regelwerk macht jedes Institut etwas anderes nach dem Prinzip "invented here" - das ist teuer und nur ungenügend wirksam]

a)

83 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.

richtig: besser: adäquaten, s. ISO 19600, 4.4

84 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.

wirksame

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

organisatorisch ... ; alle Organisationen sollten nach den ISO Standards Risikokontrolle und Compliance Funktion haben, ev. als Teilzeit-Pensum in Kombination mit anderen Aufgaben, sofern die Unabhängigkeit gewährleistet ist; eine Verbindung mit operativen Einheiten, wie bspw. dem Rechtsdienst ist nicht zulässig

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

und einen CCO, der für das Compliance Management

Systemrelevante Banken bestimmen einen ~~CRO, der Mitglied der Geschäftsleitung und ausschliesslich für die Risikokontrolle zuständig ist~~. 88

es sollte ein Risiko- und Compliance Officer bezeichnet werden, wie richtig in Rz 85; CRO ist zu eng; s. Diskussion in Deutschland zur Bezeichnung eines Vorstands- mitglieds, das operativ die Kontrollfunktionen leitet

b) Aufgaben und Verantwortlichkeiten der Risikokon

Unklar, ob zwischen Risikomanagement und Risikokontrolle ein Unterschied besteht. Nach ISO 31000 richtig: Nur von Risikomanagement zu sprechen, da Kontrolle und Überwachung der Risiken Bestandteil des Risikomanagements sind.

Risikokontrolle stellt die umfassende und systematische Überwachung und ichterstattung von einzelnen wie auch aggregierten Risikopositionen sicher. Dies nhaltet als Teil der quantitativen und qualitativen Analysen die Durchführung von esstests und Szenarioanalysen unter ungünstigen Geschäftsbedingungen. 89

Risikokontrolle überwacht insbesondere in Abstimmung mit dem im Rahmenkonzept das institutsweite Risikomanagement festgelegten Risikoappetit und den Risikolimiten Risikoprofil des Instituts. 90

Risikokontrolle stellt die für die Risikoüberwachung notwendigen Informationen bereit. 91

lie 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

adäquate

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

schriftlich und mündlich

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

Der ganze Abschnitt sollte konzeptionell und bez. Terminologie an ISO 19600 angepasst werden; ISO 19600 ist der einzige weltweite Standard für Compliance Management (Systeme)

c) Aufgaben und Verantwortlichkeiten der Compliance-Funktion

Die Aufgaben und Verantwortlichkeiten der Compliance-Funktion Kontrollinstanz umfassen ~~in der Regel~~ folgende Tätigkeiten:

- 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

der Wirksamkeit des Compliance Managements und ...

- 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

- 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

die Umsetzung des Regelwerks, die Wirksamkeit des Compliance Managements, die Einschätzung ...

Nebst den Aufgaben und Verantwortlichkeiten der Compliance-Funktion in ihrer Rolle als unabhängige Kontrollinstanz unterstützt und beratet die Compliance-Funktion die Geschäftsleitung sowie die Mitarbeiter bei der Ausarbeitung, Durchsetzung und 103

ohne Verpflichtung zu einem Regelwerk, ist der Inhalt der Aufgaben und Verantwortlichkeiten völlig unbestimmt; ISO 19600 nennt die (allgemeinen) Aufgaben und Verantwortlichkeiten präzise; s. 5.3.4

bindenden Verpflichtungen

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

Werte und

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

- 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
- einer zweiten Prüfgesellschaft, welche von der Prüfgesellschaft des Instituts unabhängig ist, oder 108
- einem unabhängigen Dritten, vorausgesetzt die Prüfgesellschaft bestätigt dessen professionelle Kompetenzen und angemessene technische und personelle Ressourcen. 109

B. Unterstellung und Organisation

Die interne Revision ist dem Oberleitungsorgan oder dessen Prüfausschuss unterstellt und nimmt die ihr übertragenen Prüf- und Überwachungsaufgaben in unabhängiger Art und Weise wahr. 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

und finanziell adäquat

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 Prüfrecht 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

und seinen Compliance Zielen

und Beurteilung der Wirksamkeit des Compliance Managements

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

mündlich und schriftlich

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. 124

IX. Gruppenstrukturen

Die Grundsätze und Bestimmungen dieses Rundschreibens gelten für Finanzgruppen und -konglomerate („Gruppen“) sinngemäss. 125

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 Einzelinstitutsebene angemessen Rechnung tragen. Dabei sind im Besonderen die Risiken zu berücksichtigen, welche sich aus dem Zusammenschluss mehrerer Unternehmen zu einer wirtschaftlichen Einheit ergeben. 126

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. 127

Gruppen müssen für das Risiko- und das Compliancemanagement je ein einheitliches Regelwerk für die ganze Gruppe bezeichnen. [nur so kann systematisches, wirksames, transparentes und kosteneffizientes Risiko- und Compliance-Manangement erfolgen]

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. 128

und Compliance-Management [Transparenz: Richtig; s. vorhergehender Kommentar]

Folgende Informationen sind öffentlich zu publizieren: 129

- Die Zusammensetzung sowie der berufliche Hintergrund und die Ausbildung der einzelnen Mitglieder des Oberleitungsorgans. Die unabhängigen Mitglieder gemäss Rz 21 ff. sind auszuweisen. 130

- Die Organisation des Oberleitungsorgans, insbesondere die Besetzung des Präsidiums sowie die allfällige Konstituierung und Zusammensetzung von Ausschüssen gemäss Rz 36 ff. 131

sowie das Fachwissen der Mitglieder der Ausschüsse

- 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 Risikoeinstellung

- ~~Die risikostrategische Ausrichtung~~ und das Risikoprofil des Instituts sowie die Ein- 134

die Compliance Politik und die Compliance Ziele sowie die Grundzüge des Compliance Management Systems

Folgende Informationen der *Richtlinie der SIX Exchange betreffend Informationen zur Corporate Governance* 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.

LENZ & STAEHELIN

Lenz & Staehelin
Bleicherweg 58
CH-8027 Zürich
Tel: +41 58 450 80 00
Fax: +41 58 450 80 01

Route de Chêne 30
CH-1211 Genf 17
Tel: +41 58 450 70 00
Fax: +41 58 450 70 01

Avenue du Tribunal-Fédéral 34
CH-1005 Lausanne
Tel: +41 58 450 70 00
Fax: +41 58 450 70 01

www.lenzstaehelin.com

Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
3003 Bern

Zürich, 13. April 2016
M2.5092545_1

Anhörung zum Entwurf des Rundschreibens 2016/xx Corporate Governance – Banken
Kurzstellungnahme betreffend Auslagerung der Compliance-Funktion

Sehr geehrte Damen und Herren

Bezugnehmend auf unser Telefongespräch mit Herrn Michael Brügger vom 7. April 2016 sowie die von der FINMA publizierten Anhörungsunterlagen zum Entwurf des FINMA-Rundschreibens 2016/xx Corporate Governance – Banken ("**RS 2016/xx**"), reichen wir hiermit fristgerecht unsere Kurzstellungnahme ein, welche sich absprachegemäss auf Aspekte der Zulässigkeit einer Auslagerung der Compliance-Funktion beschränkt.

1. Ausgangslage und Fragestellung

Das RS 2016/xx enthält detaillierte Ausführungen über das Interne Kontrollsystem und dessen unabhängige Kontrollinstanzen (Rz. 79 ff.), insbesondere über deren Einrichtung und Unterstellung (Rz. 82 ff.) sowie über die Aufgaben und Verantwortlichkeiten der Risikokontrolle (Rz. 89 ff.) und die Aufgaben und Verantwortlichkeiten der Compliance-Funktion (Rz. 99 ff.).

Das RS 2016/xx nimmt dabei keine Stellung zur Frage der Zulässigkeit einer Auslagerung der unabhängigen Kontrollinstanzen im Allgemeinen, bzw. der Zulässigkeit einer Auslagerung der Compliance-Funktion im Besonderen. Dies gilt sowohl hinsichtlich einer Auslagerung an Dritte als auch bezüglich einer Auslagerung an eine Bank innerhalb derselben Finanzgruppe.

Hingegen enthält der Erläuterungsbericht zum RS 2016/xx vom 1. März 2016 ("**Erläuterungsbericht**") diesbezüglich gewisse Ausführungen, insbesondere mit Blick auf Rz. 87 des RS 2016/xx.

Rz. 87 des RS 2016/xx besagt: *"Die Institute der Aufsichtskategorien 1 bis 3 verfügen über eine eigenständige Risikokontrolle und Compliance-Funktion als unabhängige Kontrollinstanzen."*

Die Autoren des Erläuterungsberichts scheinen diese Rz. 87 des RS 2016/xx spezifisch interpretiert zu haben. Je nach Lesart enthalten denn auch gewisse Passagen des Erläuterungsberichts Interpretationsspielraum rund um die für die Banken bedeutsame Frage, ob das RS 2016/xx eine wesentliche Praxisänderung dahingehend einführen möchte, dass neuerdings den Banken der Kategorien 1 bis 3 im Sinne einer organisatorischen Vorschrift eine Auslagerung der Compliance-Funktion verboten werden soll.

Die obenstehende Frage ergibt sich aus einem möglichen Umkehrschluss zu folgender Passage im Erläuterungsbericht (Kapitel 3.5 am Ende): *"Weiter kann bei Instituten der Aufsichtskategorie 4 und 5 die Compliance-Funktion auch in einem Outsourcing-Verhältnis betrieben werden."*

Aus dieser Passage im Erläuterungsbericht könnte – wohl fälschlicherweise – geschlossen werden, dass das Erfordernis einer *"eigenständigen Risikokontrolle und Compliance-Funktion als unabhängige Kontrollinstanzen"*, welches den Banken der Kategorien 1 bis 3 die Errichtung der genannten Kontrollinstanzen und entsprechende qualitative Anforderungen u.a. an ihre Unabhängigkeit auferlegt, plötzlich dahingehend verstanden werden soll, dass das Wort *"eigenständig"* als organisatorische Anforderung eine Trennung zwischen den Instituten verlangen und neu eine Auslagerung der Compliance-Funktion an Dritte und selbst an eine Bank innerhalb derselben Finanzgruppe verbieten würde.

2. Wesentliche Änderung von Recht und Praxis?

Eine solche Lesart der erwähnten Passage im Erläuterungsbericht (Kapitel 3.5 am Ende) bedeutete eine wesentliche Änderung der langjährigen Praxis, welche im Einklang mit den internationalen Vorgaben des BCBS und den einschlägigen Rundschreiben der FINMA eine Auslagerung der Compliance-Funktion ausdrücklich erlaubt.

Das Rundschreiben 2008/7 Outsourcing Banken ("**RS 2008/7**") sieht die Auslagerung der Compliance-Funktion sowohl auf Dritte als auch gruppenintern ausdrücklich vor (siehe Auflistung im Anhang). Und das Rundschreiben 2008/24 Überwachung und interne Kontrolle Banken ("**RS 2008/24**") bezeichnet eine Auslagerung der Compliance-Funktion ebenfalls als grundsätzlich zulässig (RS 2008/24 Rz. 105).

3. Weitere Zulässigkeit einer Auslagerung der Compliance-Funktion

Die Möglichkeit einer Auslagerung der Compliance-Funktion auch für Institute der Kategorien 1 bis 3 bei gegebenen Voraussetzungen wie u.a. hinsichtlich Unabhängigkeit steht im Einklang mit internationalen und schweizerischen Vorgaben und ist aus Risikoperspektive konsistent und sinnvoll.

Der Erläuterungsbericht zum RS 2016/xx verweist eingangs darauf, dass die überarbeiteten internationalen Standards und insbesondere die *"BCBS Corporate governance principles for banks"* für die FINMA Anlass zur Totalrevision des Rundschreibens waren. Diese Richtlinien des BCBS äussern sich unter Principle 9 zur Compliance-Funktion und betonen dabei in Rz. 132 insbesondere deren qualitative Anforderung betreffend Unabhängigkeit: *"An independent compliance function is a key component of the bank's second line of defence."* Dies bedeutet aber keine organisatorische Anforderung. Vielmehr verweist das BCBS auf die spezifische Richtlinie *"Compliance and the compliance function in banks."* Diese enthält in Principle 10 die ausdrückliche Zulässigkeit einer Auslagerung der Compliance-Funktion und sieht diesbezüglich als weitere qualitative Anforderung eine angemessene Überwachung durch den Compliance-Verantwortlichen vor: *"Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance."* Sodann wird wie üblich festgehalten, dass dabei die Verantwortung nicht ausgelagert werden kann: *"Regardless of the extent to which specific tasks of the compliance function are outsourced, the board of directors and senior management remain responsible for compliance by the bank with all applicable laws, rules and standards."* Aus Sicht einschlägiger internationaler Standards besteht demnach kein Erfordernis, die grundsätzliche Möglichkeit der Auslagerung der Compliance-Funktion einzuschränken.

Auch ist das Verhältnis der Compliance-Funktion zu den anderen unabhängigen Kontrollinstanzen, namentlich der Risikokontrolle und der internen Revision, zu berücksichtigen. Während eine Auslagerung der Risikokontrolle durch den Erläuterungsbericht nicht ausdrücklich angesprochen wird, ist für die interne Revision eine Auslagerung ausdrücklich vorgesehen (RS 2016/xx Rz. 106 ff.). Würde dasselbe Rundschreiben die Auslagerung der Compliance-Funktion für Banken der Kategorien 1 bis 3 grundsätzlich untersagen wollen, so wäre dies gegenüber der Risikokontrolle wie auch gegenüber der internen Revision eine wohl nicht nachvollziehbare Unterscheidung bzw. Ungleichbehandlung. Insbesondere gegenüber der Risikokontrolle, die im *Three Lines of Defence*-Modell ebenfalls auf der zweiten Stufe angesiedelt ist, erschiene eine solche Unterscheidung fragwürdig, zumal keine offenkundigen Unterschiede gegenüber der Compliance-Funktion bestehen, die eine solche Ungleichbehandlung rechtfertigen würden.

4. Zu Gruppenverhältnissen im Besonderen

Besonders akzentuiert erscheint die Problematik eines möglichen Verbots der Auslagerung der Compliance-Funktion für Institute der Kategorien 1 bis 3 in Gruppenverhältnissen.

In Gruppenverhältnissen wird verlangt, dass die unabhängigen Kontrollinstanzen im Rahmen des IKS ihre Tätigkeiten in einer Art und Weise erfüllen, welche eine Aggregation der Kontrollergebnisse ermöglicht. In diesem Zusammenhang sieht auch das RS 2016/xx u.a. vor, dass *"im Besonderen die Risiken zu berücksichtigen [sind], welche sich aus dem Zusammenschluss mehrerer Unternehmen zu einer wirtschaftlichen Einheit ergeben."* (RS 2016/xx Rz. 125). Institutsübergreifende unabhängige Kontrollinstanzen sind der effektivste Weg, um gruppenweite Risiken wirksam zu messen, zu kontrollieren und zu bewirtschaften. Die Zentralisierung der unabhängigen Kontrollinstanzen stellt auch eine wirksame und angemessene Massnahme dar, um die regulatorischen Vorgaben mit den betriebswirtschaftlichen Realitäten in Übereinstimmung zu bringen.

Die Einführung eines Verbots der Auslagerung der Compliance-Funktion innerhalb derselben Finanzgruppe würde für die betroffenen Institute der Kategorien 1 bis 3 die Compliance-Funktion im jeweiligen Einzelinstitut automatisch sowohl personell als auch organisatorisch separieren und der Wirksamkeit des von der FINMA verlangten gruppenweiten Risikomanagements mit entsprechender Vereinheitlichung von Systemen und Prozessen sowie gruppenweiter Datenaggregation entgegenstehen.

Nachdem das RS 2016/xx in Rz. 127 (wie schon das geltende RS 2008/24) verlangt, dass sich die interne Revision einer Finanzgruppe mindestens auf alle konsolidierungspflichtigen Gesellschaften zu erstrecken hat, erschiene es denn auch widersprüchlich, wenn für Teile der unabhängigen Kontrollinstanzen (hier, der *Second Line of Defence*) der Wirkungsbereich durch dasselbe Rundschreiben wieder auf das einzelne Institut beschränkt würde. Vielmehr erscheint es auch mit Blick auf die Wirksamkeit der Kontrollen sinnvoll, für beide unabhängigen Kontrollinstanzen der *Second Line of Defence* eine Zusammenführung innerhalb einer Finanzgruppe zu ermöglichen.

Dementsprechend verlangen denn auch die berechtigten Interessen der Institute der Kategorien 1 bis 3 und ihrer Anspruchsgruppen geradezu die grundsätzliche Möglichkeit einer Auslagerung der Compliance-Funktion. Durch eine gruppeninterne Zusammenführung und entsprechende Vereinheitlichung der Compliance-Prozesse können auch aus Risikoperspektive erwünschte Vorteile hinsichtlich Qualität und Kosteneffizienz erreicht werden.

5. Fazit

In Übereinstimmung mit internationalen Standards und mit Blick auf die angestrebten Regulierungszwecke und deren bestmögliche Erfüllung ergibt sich, dass das RS 16/xx keine grundsätzliche Ein-

schränkung der Möglichkeit zur Auslagerung der Compliance-Funktion für Banken der Kategorien 1 bis 3 enthalten sollte. Dies ist aus unserer Sicht im aktuellen Entwurf des RS 16/xx so auch nicht vorgesehen, sondern durch den Erläuterungsbericht entsprechend interpretiert worden. Die Anforderung einer *"eigenständigen"* Compliance-Funktion für Banken der Kategorien 1 bis 3 ist eine qualitative Anforderung, welche sich an internationalen Vorgaben orientiert, und enthält keine Notwendigkeit einer personellen und organisatorischen Separierung – und insbesondere nicht einer erzwungenen Trennung zwischen den Instituten derselben Finanzgruppe, welche auch der Vereinheitlichung von Kontrollprozessen und einer gruppenweiten Datenaggregation und damit auch der Wirksamkeit des Risikomanagements entgegenstehen würde.

Eine Klarstellung der Zulässigkeit einer Auslagerung der Compliance-Funktion auch für Banken der Kategorien 1 bis 3 wäre unseres Erachtens wünschenswert.

Wir danken Ihnen herzlich für die Entgegennahme und wohlwollende Prüfung der vorstehenden Ausführungen und stehen Ihnen für etwaige Rückfragen gerne zur Verfügung.

Mit vorzüglicher Hochachtung

Dr. Lukas Morscher

PostFinance

PostFinance AG
Compliance
Mingerstrasse 20
3030 Bern

Telefon +41 58 386 60 60
Fax +41 58 667 44 22
www.postfinance.ch

P.P. 502301236 CH-4808 Zofingen

A-PRIORITY

Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
CH-3003 Bern

Datum 13. April 2016
Ihre Nachricht
Unser Zeichen
Kontaktperson Arno Gartmann
E-Mail arno.gartmann@postfinance.ch
Direktwahl +41 79 475 92 17

Anhörung zu den Entwürfen der FINMA-Rundschreiben 2016/x «Corporate Governance – Banken», 2008/21 «Operationelle Risiken Banken» und 2010/1 «Vergütungssysteme»

Sehr geehrter Herr Rütschi

Wir nehmen in rubrizierter Angelegenheit Stellung zu den vorgelegten Entwürfen vom 1. März 2016 und bedanken uns für die Berücksichtigung der nachfolgend vorgetragenen Anmerkungen. Der Konzern Post wird zu Punkten, die ihn betreffen, selbst Stellung nehmen, womit in diesem Schreiben nur Anmerkungen der PostFinance AG (PF) enthalten sind.

1 Generelle Bemerkungen

Es ist nicht klar, wann das Rundschreiben (RS) 16/x in Kraft treten soll. Gemäss Randziffer (Rz) 144 ist dies noch offen. Auf dem Titelblatt des RS ist der 1. Juli 2016 angegeben. Im Erläuterungsbericht in Kapitel 7 hingegen ist der 1. August 2016 angegeben. Für uns ist aus diesem Grund nicht klar, wann die überarbeiteten RS in Kraft treten werden.

Generell wirkt das RS 16/x auf uns noch nicht ausgereift. Man erkennt, dass es aus verschiedenen Regulativen und Grundlagen zusammengesetzt wurde, was zu gewissen Unklarheiten in den Begrifflichkeiten führt (siehe nachfolgend die konkreten Inputs zu den einzelnen Rz). Es erfolgt eine Vermischung von Funktion und Tätigkeiten bzw. gewisse Tätigkeiten werden gar nicht mehr aufgeführt. So wurde im RS 08/24 bspw. die Tätigkeit Compliance explizit ausgewiesen, was nun nicht mehr der Fall ist. Hingegen wird Risikomanagement als Tätigkeit beschrieben, Risikokontrolle wiederum nur als Funktion. Dies macht eine Vergleichbarkeit der Verantwortlichkeiten sehr schwer und wird zu Unstimmigkeiten in der Umsetzung führen.

Was wir am RS sehr positiv werten, ist der grundsätzlich prinzipienbasierte Ansatz. Es erscheint sinnvoll, den Banken einen gewissen Spielraum einzuräumen, um den Eigenheiten der einzelnen Institute weiterhin gerecht zu werden. Dieser sollte dann in der konkreten Umsetzung auch gewährt werden.

2 Besprechung einzelner Vorschriften

Nachfolgend werden die für PF erwähnenswerten Punkte in numerischer Reihenfolge besprochen, wobei, sofern nicht anders erwähnt, stets auf die Formulierung der Rundschreibenentwürfe Bezug genommen wird.

2.1 FINMA-Rundschreiben 2016/x «Corporate Governance – Banken»

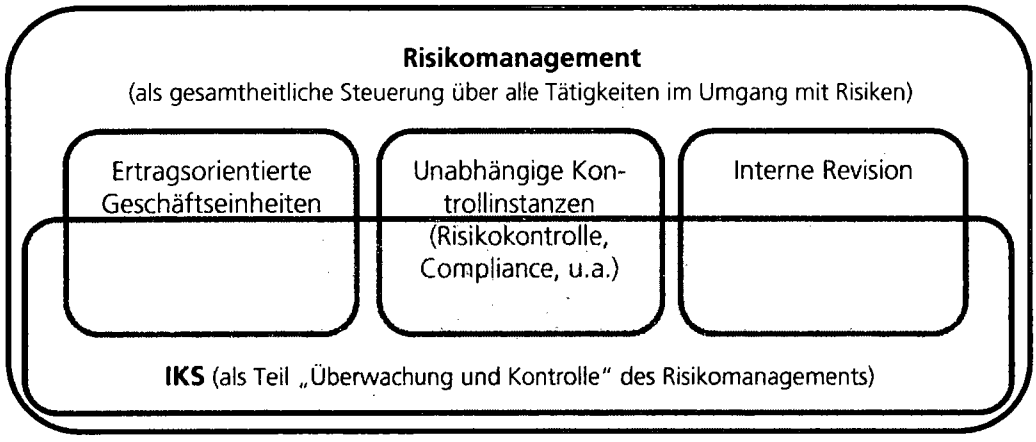
2.1.1 Randziffern 3 und 4

In Rz 3 wird von Risikomanagement als Tätigkeit (und nicht als Funktion) gesprochen. In Rz 4 spricht man von der Risikokontrolle als Funktion. Für die Abgrenzung der Tätigkeit stellt dies eine Schwierigkeit / Unklarheit dar. Im RS 08/24, Rz 126 wurde auf eine deutliche Abgrenzung zwischen Risikomanagement und Risikokontrolle Bezug genommen.

2.1.2 Randziffer 7

In der Darstellung des internen Kontrollsystems (IKS) bleibt offen, wie dieses in Bezug steht zu den im Kapitel II. definierten Begriffen wie Risikomanagement und Risikokontrolle sowie der Compliance-Funktion. U.E. besteht v.a. eine Unschärfe zwischen den Definitionen des Risikomanagements und des IKS. Für das bessere Verständnis der nachfolgenden Regelungen wäre eine systematisierende Darstellung der definierten Begriffe wünschenswert (angelehnt an die Ausführungen im Erläuterungsbericht).

Eine mögliche Interpretation / Definition kann wie folgt dargestellt werden:



Die nachfolgenden Bemerkungen nehmen auf diese Definition Bezug.

2.1.3 Randziffern 10 bis 17

Die Aufgaben des Oberleitungsorgans werden relativ ausführlich beschrieben. Dadurch besteht die Gefahr von Unstimmigkeiten zu den im OR stipulierten Verantwortlichkeiten des Verwaltungsrats (VR) einer Aktiengesellschaft.

2.1.4 Randziffer 13

Die in Rz 13 verwendeten Begrifflichkeiten «Reglemente» und «Weisungen» sind durch den generellen Begriff «Vorgaben» zu ersetzen. Somit ist gewährleistet, dass das Institut die Benennung der Vorgaben in der Erlasskompetenz des VR und / oder der Geschäftsleitung (GL) selbst wählen kann.

2.1.5 Randziffer 15

Die Oberleitung ist gemäss Rz 15 verantwortlich für die Wahl und Abberufung ihrer Ausschussmitglieder, der Mitglieder der GL, deren Vorsitzende sowie weiterer Personen in leitenden Kontroll- und Schlüsselfunktionen (z.B. Chief Risk Officer, Chief Compliance Officer, Head IT). Dies geht u.E. zu weit. Die Wahl und Abberufung weiterer Personen in leitenden Kontroll- und Schlüsselfunktionen in den Verantwortungsbereich des Oberleitungsorgans zu verschieben, erscheint unter gewissen organisatorischen Aspekten als nicht zielführend. Einerseits wird so die organisatorische Freiheit der GL eingeschränkt, andererseits besteht die Gefahr, gewisse Positionen gerade nicht als Kontroll- oder Schlüsselfunktion zu bezeichnen oder auf einem GL-Mitglied (GLM) zu vereinen, um so eine Aufblähung der Organisation zu vermeiden. Die Besetzung der Kontroll- und Schlüsselfunktionen sollte in der Kompetenz der GL liegen. Sinnvoll erscheint hingegen ein Veto- oder Mitspracherecht des Oberleitungsorgans im Bereich der Abberufung, um zu verhindern, dass leitende Personen eines Kontrollbereichs durch die GL wegen divergierender Interessen oder eines Spannungsverhältnisses aufgrund von Feststellungen der 2nd line abgesetzt werden.

2.1.6 Randziffer 16

Es wird von einem «Risiko- und Kontrollumfeld» gesprochen, wobei offen bleibt, was darunter zu verstehen ist. Insbesondere bleibt unklar, ob z.B. Einheiten mit Steuerungsfunktionen bzw. «ertragsorientierte Geschäftseinheiten» dem «Risikoumfeld» zugehörig sind und Einheiten der Risikokontrolle dem (unabhängigen) Kontrollumfeld. Eine präzisere Begriffsdefinition wäre wünschenswert.

Ausserdem wird die Verantwortlichkeit des Oberleitungsorgans in Bezug auf die interne Revision (IR) doppelt erwähnt.

2.1.7 Randziffer 17

Die Verantwortlichkeiten, die dem Oberleitungsorgan bezüglich Strukturveränderungen und Investitionen zugeschrieben werden, sind nach Ansicht von PF zu detailliert formuliert. Dem Oberleitungsorgan in all diesen Bereichen eine zwingende Entscheidungskompetenz zuzuschreiben, kann in der Praxis ein zu starkes Korsett sein, um in nützlicher Frist Entscheidungen treffen zu können. Es sollte den Unternehmen freigestellt werden, welche Themen dem Oberleitungsorgan als Entscheid vorgelegt werden und welche im Sinne einer Information.

Ausserdem ist der Begriff «bedeutend» schwer fassbar, und es bleibt damit unklar, welche Entscheidungen dem Oberleitungsorgan obliegen. Schliesslich sollten die Ausführungen bzgl. bedeutender Tochtergesellschaften vor dem Hintergrund der Bestimmungen zur konsolidierten Aufsicht präzisiert werden.

2.1.8 Randziffer 18

Es fällt auf, dass in der Aufzählung der Haupttätigkeitsfelder des Oberleitungsorgans zentrale Bereiche genannt sind, die Risikokontrolle und das IKS jedoch nicht erwähnt werden. Aufgrund der bereits zu Rz 7 gemachten Bemerkung bleibt unklar, ob dies beabsichtigt oder ein Versäumnis ist, oder ob diese Bereiche unter dem Begriff «Risikomanagement» subsumiert werden.

2.1.9 Randziffer 20

Die Auflage der personellen Trennung ergibt sich bereits aus Art. 3 Abs. 2 lit. a BankG i.V.m. Art. 8 Abs. 2 BankV und kann daher an dieser Stelle weggelassen werden.

2.1.10 Randziffer 31 und 35

In Rz 35 wird dargelegt, dass der Präsident des Oberleitungsorgans in regelmässigem Dialog u.a. auch mit «Personen in leitenden Kontrollfunktionen» steht. Es stellt sich die Frage, warum hier eine explizite Nennung der Kontrollfunktionen erfolgt. Aus unserer Sicht besteht der primäre Dialog des Oberleitungsorgans mit der GL. Weitere direkte Dialoge kann das Oberleitungsorgan mit jeder weiteren Funktion im Unternehmen verlangen. Dies sollte aber ein Recht der Oberleitung sein und nicht in bestimmten (und mit der gewählten Formulierung sehr eingeschränkten) Fällen innerhalb eines RS auferlegt werden.

2.1.11 Randziffer 36

Die Auflage, über einen Prüf-, einen Risiko- und einen Nominationsausschuss zu verfügen ist zwar für PF umsetzbar bzw. bereits umgesetzt. Der Vollständigkeit halber möchten wir aber darauf hinweisen, dass diese Auflage von Gesetzes wegen nicht verlangt ist.

2.1.12 Randziffer 38

Die Mehrheit der Mitglieder des Prüf-, Risiko- und Nominationsausschusses muss gemäss Rz 38 grundsätzlich unabhängig sein. Bei Instituten, deren VR zwar die Auflage von Rz 21 bezüglich Unabhängigkeit erfüllt, aber eine Minderheit an unabhängigen Mitgliedern hat, kann dies zu Schwierigkeiten führen bzgl. personeller Besetzung und zeitgleicher Erfüllung der Auflage nach Rz 37 bezüglich genügender personeller Unterscheidung. Zumindest beim Nominationsausschuss erscheint es aus unserer Sicht weniger wesentlich, die Unabhängigkeitsanforderungen zu erfüllen. Diese Annahme wird durch den Erläuterungsbericht gestützt, in welchem auch die FINMA keine Erwähnung bzgl. der Unabhängigkeit im Nominationsausschuss macht.

Kommt der Fall hinzu, dass der Vorsitzende des Oberleitungsorgans unabhängig ist (was im Grundsatz aus Unabhängigkeitsüberlegungen der Idealfall sein sollte), wird die Besetzung der Ausschüsse und die zeitgleiche Erfüllung der Auflagen zu seiner Positionierung in den Ausschüssen nach Rz 38 noch erschwert. Die sehr engen Auflagen bezüglich Unabhängigkeit und Besetzung der Ausschüsse führen zu Ämterkumulation bei den unabhängigen Mitgliedern des Oberleitungsorgans.

2.1.13 Randziffer 43

Es bleibt unklar, ob die in Rz 43 gemachte Nennung von Risikokontrolle, Compliance-Funktion und interner Revision abschliessend für die interne Kontrolle bzw. das IKS ist oder ob hier weitere Funktionen subsumiert werden müssen. Vgl. dazu auch die Bemerkung zu Rz 7. Insbesondere stellt sich die Frage, ob der Prüfausschuss auch die Wirksamkeit der Kontrollfunktionen in den «ertragsorientierten Geschäftseinheiten» zu überwachen und zu beurteilen hat. Sollte dem nicht so sein, wäre eine Präzisierung von Rz 43 mit Bezugnahme auf «unabhängige Kontrollinstanzen» zu prüfen. Siehe weiter auch die Bemerkungen zu Rz 86.

2.1.14 Randziffern 43 und 49

Ohne dass die Begriffe unter Kapitel II. nicht sauber abgegrenzt und definiert werden, ist hier nicht klar, welcher Ausschuss konkret welche Aufgaben inne hat bzgl. Risikomanagement und IKS. Der Prüfausschuss hat das IKS (inkl. Risikokontrolle, Compliance und IR) in seiner Kompetenz. Der Risikoausschuss hat die Kontrolle des Risikomanagements in seiner Obhut. Was ist mit der Kontrolle des Risikomanagements gemeint? Aus Sicht von PF beinhaltet die Kontrolle des Risikomanagements die Tätigkeiten innerhalb des IKS.

2.1.15 Randziffer 67 und 90

Im RS 08/24 war die Risikokontrolle nach Rz 122 dafür zuständig, die Grundlagen der Risikopolitik, des Risikoappetits und der Risikolimiten zu legen. Diese Bestimmung wurde im neuen RS 16/x nicht aufgenommen bzw. sie werden neu als Zuständigkeit der GL / des Oberleitungsorgans ausgewiesen (RS 16/x, Rz 66 und 67). Im Erläuterungsbericht (S. 14) werden die Risikokontrolle oder die Compliance-Funktion als typische Funktionen genannt, die für die zeitnahe und fortwährende Überprüfung und Anpassung des Rahmenkonzepts, welche obige Punkte enthält, zuständig sind. Diese Formulierung bzw. Nicht-Festlegung im RS lässt Spielraum offen, welcher Organisationseinheit die Verantwortlichkeit zugeteilt wird. Diesem Spielraum sollte Beachtung geschenkt werden bzw. den Instituten in der Praxis dieser dann auch zugestanden werden.

2.1.16 Randziffer 82

Als Einstieg in den Abschnitt unabhängige Kontrollinstanzen ist das Thema Vergütungen vorgesehen. Nachvollziehbarer wäre bspw. ein Einstieg mittels Definition, welche Einheiten als unabhängige Kontrollinstanzen gelten (können).

2.1.17 Randziffer 86

In Zusammenhang mit Rz 43 ist die Rz 86 unklar. In Rz 43 wird die Verantwortlichkeit für das IKS und damit für die unabhängigen Kontrollfunktonen inkl. IR dem Prüfausschuss zugeordnet. In der Rz 86 hingegen wird davon gesprochen, dass die unabhängigen Kontrollinstanzen einen direkten und regelmässigen Zugang zum Oberleitungsorgan als Ganzes oder zum Risikoausschuss haben sollen. Es stellt sich demnach die Frage, ob nun der Risikoausschuss oder der Prüfausschuss für die Kontrollfunktionen verantwortlich zeichnet.

2.1.18 Randziffer 87

Als unabhängige Kontrollinstanzen werden die Risikokontrolle und die Compliance-Funktion aufgeführt. Im Erläuterungsbericht wird auf S. 15 erwähnt, dass weitere Funktionen je nach Unternehmensorganisation ebenfalls als unabhängige Kontrollfunktionen gelten können. Aus Sicht von PF wäre eine entsprechende Formulierung im RS zu begrüssen. Es ist zudem nicht erkennbar, wieso ausschliesslich die Kontrollfunktion «Risikokontrolle» eine im RS erwähnte Führungsposition benennen muss.

2.1.19 Randziffer 87 und 88

In den Rz 87 und 88 wird festgehalten, dass systemrelevante Banken einen CRO haben müssen, welcher Mitglied der GL und ausschliesslich für die Risikokontrolle zuständig ist. Im Erläuterungsbericht auf S. 15 wird es offener formuliert. Demnach müssen Institute der Kategorie 1-3 einen CRO haben, der mindestens für die Risikokontrolle verantwortlich ist. Bei systemrelevanten Banken besteht zusätzlich die erhöhte Anforderung, dass dieser in der GL vertreten sein muss. Die offenere Formulierung aus dem Erläuterungsbericht wäre u.E. auch die richtige Formulierung für das RS.

Im Erläuterungsbericht nimmt die FINMA Bezug auf die Empfehlungen des IWF aus dem «Financial Sector Assessment Program» 2014, wonach u.a. eine Verbesserung der Stellung und des Profils der CRO-Funktion innerhalb des Unternehmens nahegelegt wird. Eine Lektüre des Reports des IWF zeigt auf, dass zwar der Einsitz des CRO als «full executive board member» empfohlen wird – eine zeitgleiche Empfehlung, dass das Aufgabenfeld dieses GLM nur auf die Risikokontrolle beschränkt sein sollte, kann jedoch nicht daraus abgeleitet werden. Eine solche Empfehlung kann auch in den Basler Standards nicht gefunden werden. Wir möchten an dieser Stelle darauf hinweisen, dass es aus unserer Sicht ungünstig ist, hier einen «Swiss-Finish» zu machen und strenger zu sein, als es internationale Standards empfehlen.

Aus Sicht von PF ist es nicht sinnvoll, den CRO als Mitglied der GL zu positionieren bzw. die Auflage zu machen, dass dieses GLM nur noch für die Risikokontrolle zuständig sein darf. Insbesondere folgende Überlegungen sprechen dagegen:

- Eventuell handelt es sich bei der Auflage um eine Inkonsistenz aufgrund der unterschiedlichen Bedeutung der Begrifflichkeiten im englischen und deutschen Sprachgebrauch. «Risk control» umfasst im englischen Sprachgebrauch nicht einzig die Kontrolle, sondern beinhaltet eben auch das Management bzw. die Steuerung der Risiken. Auch in der Praxis lässt sich beobachten, dass häufig die ganzheitliche Steuerung der Risiken von Bedeutung ist für das Management und auch eine entsprechende Positionierung in der GL vorgenommen wird. Diese Beobachtung stützt unsere Ansicht, dass ein GLM eine ganzheitliche Risikosicht wahrnehmen können sollte und somit sowohl eine Risikosteuerungseinheit als auch zeitgleich die Risikokontrolleinheit vertreten kann.
- Das Vertreten mehrerer Themen hindert das für die Kontrollfunktionen verantwortliche GLM nicht daran, die Positionierung der Risikokontrolle vornehmen zu können. Im Gegenteil ist eine Positionierung und Verankerung besser möglich, wenn ähnliche Themen mit ähnlichen Zielen (wie bspw. Compliance und Risikokontrolle) gemeinsam vorangetrieben und vernetzt angeschaut werden.
- PF kann nachvollziehen, dass Interessenkonflikte des GLM, welches die Risikokontrolle in der GL vertritt, verhindert werden sollen. Es ist für uns jedoch nicht nachvollziehbar, worin Interessenkonflikte bei der Kombination mit weiteren vom Business unabhängigen Tätigkeiten bestehen sollen.
- Die direkte (und ausschliessliche) Vertretung der Risikokontrolle in der GL, um das Einbringen einer unabhängigen Risikosicht sicherzustellen, kann auch mittels Einsitz bei relevanten Themen sichergestellt werden ohne Mitgliedschaft in der GL. Auf diese Weise ist die unabhängige Funktions- und Sichtweise der Risikokontrolle sogar besser sichergestellt. Falls der CRO direkt Mitglied ist und Entscheidungen der GL mit fällt, geht diese Unabhängigkeit ein Stück weit verloren. Sinnvoller erscheint uns ein direkter Rapportierungsweg des CRO in die zuständigen Gremien der GL und des VR.
- Es ist für PF auch nicht nachvollziehbar, weshalb diese Auflage nur für systemrelevante Banken gelten soll bzw. für alle systemrelevanten Banken unabhängig von deren Geschäftsmodell. Für Grosskonzerne, welche international tätig sind, kann dies eine sinnvolle Überlegung sein. Für national Tätige Institute, wie es PF ist, erscheint die Positionierung des CRO als GLM wenig zielführend.

2.1.20 Randziffer 92

Rz 92 stipuliert für die unabhängige Risikokontrolle die Verantwortung zur «Vorgabe und Anwendung von Grundlagen und Methoden für die Risikomessung». Derartige Methoden bzw. Grundlagen werden in den «ertragsorientierten Geschäftseinheiten» häufig spezifisch entwickelt und eingesetzt, um daraus Steuerungsmassnahmen abzuleiten bzw. analytisch zu begründen. Eine zu enge Vorgabe von Methoden und Grundlagen würde diese Einheiten u.U. unnötig einschränken. Wir gehen davon aus, dass den Banken der nötige Spielraum zugestanden wird bzw. diese Vorgabe breit ausgelegt werden kann und der vorzugebende Rahmen die Steuerung nicht unnötig einschränken darf. Ausserdem ist in der Formulierung der Randziffer u.E. eine Unschärfe enthalten: Im Satzteil «die Vorgabe und Anwendung von Grundlagen und Methoden für die Risikomessung (z.B. Bewertungs- und Aggregationsmethoden, Validierung von Modellen)» ist für uns nicht nachvollziehbar, weshalb die Validierung von Modellen aufgeführt wird. Die Validierung von Modellen ist eine Prüftätigkeit und keine Vorgabe oder Anwendung einer Methode für die Risikomessung.

2.2 FINMA-Rundschreiben 2008/21 «Operationelle Risiken Banken»

2.2.1 Anhang 3, Randziffer 16

Die Ausführungen zum Inventar der Applikationen sind u.E. zu ausführlich und unklar (z.B. «zeitnah» vs. «regelmässig»), was für Verwirrung sorgen kann. Wir schlagen deshalb vor, den zweiten Satz von Rz 16 zu streichen.

2.2.2 Anhang 3, Randziffer 33

Es stellt sich uns die Frage, ob mit «Es ist regelmässig zu überprüfen, ob die Anforderungen für einen angemessenen Umgang mit CID weiterhin erfüllt sind.» eine wiederkehrende Personenkontrolle, analog derjenigen vor einer Anstellung (Betreibungsregisterauszug, Strafregisterauszug) gemeint ist. Falls ja, erachten wir die Vorgabe mit Blick auf Aufwand und Ertrag als nicht zielführend.

2.2.3 Anhang 3, Randziffer 35

Aus unserer Sicht wiederholt der zweite Satz die Aussage des ersten in anderen Worten und kann so zu Verwirrung führen. Wir würden daher die Streichung des Satzes «Dabei sind einzelne Transaktionen bzw. Zugriffe den einzelnen Benutzern zuzuordnen.» begrüssen.

2.2.4 Anhang 3, Randziffern 40, 41 und 41.1

Rz 40 beschriebt den Umgang mit Daten im Produktionsumfeld und auferlegt hier deutliche Massnahmen im Umgang mit nicht anonymisierten, nicht verschlüsselten oder nicht pseudonymisierten Daten. Rz 41 behandelt den Umgang mit Testdaten bezüglich Schutz vor unberechtigten Zugriffen, sagt aber nichts zur Anonymisierung etc. aus.

Die neu erfasste Rz 41.1 macht eine Auflage, dass für kleine Institute im Falle fehlender Anonymisierung etc. von Testdaten die Auflagen von Rz 40 gelten. Diese Vorgabe verwirrt sowohl bezüglich Inhalt wie auch bezüglich Adressatenkreis.

- Inhaltlich fragt sich, ob damit implizit ausgesagt wird, dass Testdaten anonymisiert etc. werden sollten.
- Bezüglich Adressatenkreis fragt sich, ob die Zuweisung der Möglichkeit einer Anwendung von Rz 40 an kleine Institute den Umkehrschluss zulässt, dass grössere Banken diese nicht anwenden dürfen und somit eine Anonymisierung etc. der Testdaten vornehmen müssen.

2.3 FINMA-Rundschreiben 2010/1 «Vergütungssysteme»

2.3.1 Randziffer 20

Im Sinne unserer Bemerkung zu Rz 15 des RS 16/x erachten wir die Erweiterung der Verantwortlichkeit des VR um die Genehmigung der Vergütungen der Leiter der Kontrollfunktionen als zu weitgehend bzw. einen zu starken Eingriff in die operative Geschäftsführung. Auf diese Erweiterung ist daher zu verzichten.

Wir danken Ihnen an dieser Stelle für die Möglichkeit zur Stellungnahme im Rahmen der Anhörung und bitten um eine kritische Auseinandersetzung mit den vorgetragenen Argumenten. Für Rückfragen oder ergänzende Erläuterungen stehen wir jederzeit und gerne zur Verfügung.

Freundliche Grüsse

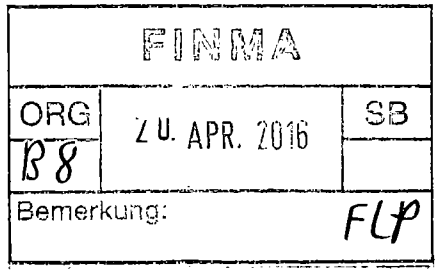
PostFinance AG

Patrick Graf
Leiter Corporate Center

PostFinance AG

Bianca Gebauer
Leiterin Risikokontrolle

RAIFFEISEN



Raiffeisen Schweiz

Raiffeisenplatz 4
Postfach
9001 St.Gallen
Telefon 071 225 49 98
www.raiffeisen.ch
finma-office@raiffeisen.ch

A-Post
Eidgenössische Finanzmarktaufsicht FINMA
Herrn Peter Rütschi
Laupenstrasse 27
3003 Bern
peter.ruetschi@finma.ch

Für Sie zuständig:
Gabriela Glaus, RA – 071 225 49 98

St.Gallen, 19. April 2016

Stellungnahme zu den Entwürfen zu

- **FINMA-Rundschreiben 2016/x „Corporate Governance – Banken"**
- **FINMA-Rundschreiben 2008/21 „Operationelle Risiken Banken"**
- **FINMA-Rundschreiben 2010/01 „Vergütungssysteme"**

Sehr geehrter Herr Rütschi

Wir beziehen uns auf die Eröffnung der Anhörung zu den eingangs erwähnten Entwürfen zu den diversen FINMA-Rundschreiben vom 1. März 2016. Wir bedanken uns für die Gelegenheit zur Stellungnahme.

Einleitende Bemerkungen zum Erläuterungsbericht zum FINMA-RS 2016/x

Die Überarbeitung der Rundschreiben (RS) 08/24 und RS 08/21 mit der angestrebten Entschlackung des RS 08/21 und Überführung der Corporate Governance Bestimmungen in das neue RS 2016/x ist zu begrüssen. Die Zusammenführung der Corporate Governance Themen in einem neuen RS 2016/x eröffnet die Chance, Doppelspurigkeiten und Inkonsistenzen abzubauen. Ebenso ist nicht von der Hand zu weisen, dass die Entwicklungen in der Corporate Governance generell sowie im Risikomanagement im Speziellen seit dem Erlass der beiden Rundschreiben in einem formellen Erlass abgebildet werden sollen. Fraglich ist jedoch, ob dabei – unbesehen von der heterogenen Schweizer Finanzwirtschaft – weitgehend identische Detailvorschriften für alle Banken sowie in erster Linie internationale Empfehlungen umgesetzt werden müssen. Banken und Effektenhändler weisen aufgrund ihrer verschiedenen internationalen, nationalen oder gar nur regionalen Geschäftsmodelle sehr unterschiedliche Risikoprofile auf. Das Überwachungskonzept der FINMA hat sich vermehrt nach den Risiken der Beaufsichtigten bzw. der Märkte für das Publikum und den Finanzplatz Schweiz zu richten. Die Rundschreiben, welche zur Vernehmlassung stehen, werden unseres Erachtens diesen unterschiedlichen Risikoprofilen nicht gerecht.

Sowohl das Regulierungs- als auch das Aufsichtskonzept der FINMA sind risikoorientiert. Ein Ausdruck davon ist das Prinzip des „comply or explain". Die Regulierung soll zudem prinzipienbasiert erfolgen. Entgegen der Feststellung der FINMA erachten wir die Inhalte der Rundschreiben jedoch nicht als prinzipienbasiert, sondern als übermässig detailliert. Dadurch besteht die Gefahr, dass der Fortschritt der Market Practice behindert wird und dass unreflektierte Regelkonformität an die Stelle von risikoadäquatem Verhalten tritt. Das "comply or explain"-Prinzip soll durch formelle Ausnahmebewilligungsprozesse ersetzt werden. Das Aufgeben des "comply or explain"-Prinzips, welches sich in den letzten Jahren bewährt hat, kann nicht nachvollzogen werden. Die Corporate Governance ist durch das Obligationenrecht gesteuert, insbesondere durch die Bestimmungen der dritten Abteilung betreffend die Handelsgesellschaften und Genossenschaften. Besondere aufsichtsrechtliche Regelungen sind nur gerechtfertigt, wo dies aus bankspezifischen Gründen erforderlich ist.

Wir sind weiter der Auffassung, dass Mitteilungen der FINMA, welche bisher in FAQ oder Positionspapieren Niederschrift gefunden haben, nicht unbesehen in ein Rundschreiben übernommen werden dürfen. Rundschreiben geben in allgemeiner Form die angewendete (kodifizierte) Aufsichtspraxis der FINMA wieder. Dies soll eine einheitliche, transparente Praxis für alle Betroffenen gewährleisten. Rundschreiben, die Vorgaben an die Ausgestaltung der Tätigkeit der

Finanzintermediäre enthalten, haben zudem Aussenwirkung. Mitteilungen in Form eines Positionspapiers oder FAQ als Instrument der Aufsichtspraxis dienen hingegen dazu, schnell und wenig formalistisch aktuelle Aufsichtsthemen oder drohende Gefahren anzusprechen. Eine unveränderte Übernahme solcher Mitteilungen in ein Rundschreiben ist deshalb nicht angezeigt. Weiter führt die Übernahme von Mitteilungen der FINMA in Rundschreiben zu einem Detaillierungsgrad, welcher für ein Rundschreiben nicht angemessen ist und dem Grundsatz der prinzipienbasierten Regelung nicht standhalten kann.

Eine zwingende Trennung in einen separaten Prüf- und Risikoausschuss ist – zumindest für national oder regional tätige Institute – nicht zweckmässig. Unbestrittenermassen sind sowohl Prüf- wie auch Risikothemen im Verwaltungsrat angemessen zu adressieren. Im Sinne der Organisationsfreiheit soll jedoch jede Bank im Rahmen ihrer Risiken und ihrer Zusammensetzung des Verwaltungsrates frei sein, die geeignete Organisationsstruktur im Verwaltungsrat einzurichten. Die Erfahrung zeigt, dass zahlreiche Fragestellungen gleichzeitig den Prüf- wie den Risikoausschuss betreffen und sich in der Praxis bei einer Trennung zahlreiche Abstimmungsprobleme zwischen den einzelnen Pflichtenheften ergeben, weil die Einheit der Materie verletzt wird. Weiter werden die Organisationsstrukturen sowie die Reporting- und Eskalationslinien unnötig komplex. Vielfach werden in beiden Ausschüssen gleiche Themen behandelt. Umfangreiche Wechselwirkungen machen ineffiziente Abstimmungen ("Joint Meetings") notwendig. Die von der FINMA verlangte Trennung in einen separaten Prüf- und Risikoausschuss entbehrt ausserdem einer ausreichenden Rechtsgrundlage. Hinzu kommen die Unabhängigkeitsvorschriften. Diesbezüglich schafft die FINMA Anforderungen an das Oberleitungsorgan, welche betreffend Grösse und Ausgestaltung sowohl des gesamten Organs wie auch der einzelnen Ausschüsse effiziente Lösungen massiv erschweren.

Schliesslich enthalten die Rundschreiben häufig unklare "Soll-Formulierungen" und unbestimmte Begriffe. Diese sind zu präzisieren, damit die beaufsichtigten Institute entsprechende Rechtssicherheit erhalten.

Zum Erläuterungsbericht zum FINMA-RS 2016/x im Einzelnen

Zu Ziffer 3.1

Die FINMA erklärt, dass die Anforderungen grundsätzlich prinzipienorientiert seien. Deren Umsetzung soll im Einzelfall von der Grösse, Komplexität, Struktur und dem Risikoprofil abhängig gemacht werden. Dabei hält die FINMA fest, dass Corporate Governance und Risikomanagement Aufsichtsthemen sind, welche sich nicht mit einem "one size fits all"-Ansatz prüfen und überwachen lassen. Die Eigenheiten und Risiken sollen in der Aufsichtspraxis, wie bis anhin, berücksichtigt werden. Dieser Wille der FINMA ist in den vorliegenden Rundscheiben nur schwer erkennbar. Durch die Aufnahme von FAQ, Positionspapieren und weiteren detaillierten Regelungen (wie z.B. zu Aufgaben, Besetzung der Ausschüsse des Oberleitungsorganes) äussern sich die Bestimmungen der Rundschreiben zum Teil sehr detailliert zu den Pflichten der beaufsichtigten Institute. Diese können nur über Ausnahmebewilligungen der FINMA individualisiert werden, was zu Rechts- und Planungsunsicherheit für die beaufsichtigten Institute führt. Dazu gehört auch die Einführung des Proportionalitätsprinzips zulasten des "comply or explain"-Prinzips. Dieser neue Ansatz ist schwer nachvollziehbar, weil das Proportionalitätsprinzip grundsätzlich nur greift, wenn die Institute der Aufsichtskategorien 4 und 5 von der Umsetzung einzelner Erfordernisse explizit befreit sind.

Zu Ziffer 3.2.2

Die Anforderung der FINMA, wonach das Oberleitungsorgan neben dem eigentlichen Bankgeschäft in zahlreichen Bereichen (Finanz- und Rechnungswesen, Risikomanagement, Compliance, Controlling, IT) kompetent vertreten sein und jedes Mitglied mindestens über eine vertiefte Kernkompetenz verfügen müsse, führt zu einer Aufblähung und einer unnötigen Spezialisierung der Verwaltungsräte. Der Verwaltungsrat muss in erster Linie über die Kompetenz verfügen, die Strategie der Bank zu definieren und die Geschäftsleitung zu kontrollieren. Nicht im Vordergrund steht das Spezialwissen in einzelnen Fachbereichen. Der Bank soll es selbst überlassen sein, welche Zusammensetzung der Verwaltungsrat bezüglich der Kompetenzen als angemessen erachtet. Von der Bank ist zu fordern, dass sie ein angemessenes Verfahren zur Auswahl der Verwaltungsräte (inklusive ihrer Kompetenzen) definiert und dieses konsequent anwendet. Wir schlagen vor, Ziff. 3.2.2 Absatz 1, 2. Satz des Erläuterungsberichts wie folgt zu ändern:

> „(...) Das Oberleitungsorgan soll **abgestimmt auf die Grösse und die Geschäftstätigkeit der Bank** genügend breit aufgestellt sein, so dass neben den Hauptgeschäftsaktivitäten sämtliche weiteren zentralen Berei-

che wie Finanz- und Rechnungswesen, Risikomanagement, Compliance, Controlling und IT kompetent vertreten sind, **soweit dies bei der konkreten Bank erforderlich ist**. (...)"

Zu Ziffer 3.2.3

Die FINMA weicht in Bezug auf die Unabhängigkeitsanforderungen der Verwaltungsräte unnötigerweise vom „comply or explain"-Prinzip ab und verweist die beaufsichtigten Institute auf einen Genehmigungsprozess, indem diese Ausnahmebewilligungen beantragen müssen.

Unklar ist zudem, wie diese Regelung bei Genossenschaftsbanken umzusetzen ist. Es muss ohne weiteres zulässig sein, als Mitglied des Verwaltungsrats einer Genossenschaftsbank Genossenschafter zu sein. Es gehört zum Wesen der Genossenschaft, dass der Verwaltungsrat sich aus Genossenschaftern zusammensetzt. Das ist angesichts des genossenschaftsrechtlichen Kopfstimmprinzips unter dem Gesichtspunkt der Unabhängigkeit nicht zu beanstanden. Wir schlagen vor, Ziff. 3.2.3 Absatz 2 des Erläuterungsberichts wie folgt zu ergänzen:

> „(...) Der Vielfalt in der Praxis ist mit Augenmass und massgeschneiderten Lösungen im Einzelfall zu begegnen. **Unwesentliche Beteiligungen oder Geschäftsbeziehungen zum Unternehmen tangieren die Unabhängigkeit nicht und sind zulässig."**

Zu Ziffer 3.2.5

Die FINMA bezieht sich bei ihrer Begründung für zwei separate Prüf- und Risikoausschüsse auf den Vorschlag des Basler Ausschusses. Der Basler Ausschuss hat keine Rechtsetzungsbefugnisse, weshalb die von der FINMA angeführte zwingende Vorgabe für systemrelevante Banken so nicht stimmt. Wohl ist sie im angelsächsischen Raum Good Practice – und dort teilweise auch vom Regulator gefordert. Jedoch gibt es für national oder regional tätige Institute keinen ersichtlichen Grund, diesen Ansatz zu übernehmen. Wir schlagen vor, Ziff. 3.2.5 Absatz 1 des Erläuterungsberichts wie folgt zu präzisieren:

> „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 eines ~~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 **bei international ausgerichteten** Instituten **als je separate Ausschüssen geführt sein, die sich** personell hinreichend unterscheiden."

Zu Ziffer 3.4

Das Rahmenkonzept Risikomanagement beschreibt Good Practice. Es stellt sich allerdings die Frage, ob die Formalisierung in einem Rundschreiben sachgerecht ist. Unseres Erachtens ist das Vorgehen, wie es etwa die österreichische Aufsichtsbehörde gewählt hat, Good Practice in einem separaten Leitfaden darzustellen, flexibler und daher besser geeignet. Dies gilt insbesondere in Verbindung mit einem "comply or explain"-Ansatz.

Den Einbezug der Liquidität in den Risikoappetit erachten wir als sinnvolle Regelung, welche Good Practice darstellt.

Die Forderung, dass systemrelevante Banken zusätzlich Bestimmungen zur Risikodatenaggregation und Risikoberichterstattung festhalten, schafft bei den Banken Rechtsunsicherheit in Bezug auf das Anspruchsniveau und den Nachweis der Einhaltung. Ein Bezug zu BCBS 239 ist sachlogisch vorhanden, formal im Rundschreiben aber nicht verankert. Hier besteht Präzisierungsbedarf.

Die organisatorischen Vorgaben zur Risikokontrolle systemrelevanter Banken entsprechen internationalem Standard. Angesichts der Heterogenität der systemrelevanten Institute in der Schweiz einerseits, der überschaubaren absoluten Anzahl andererseits, ist der Nutzen einer generellen Regelung der Organisation in einem Rundschreiben für die gesam-

te Gruppe der systemrelevanten Banken nicht erkennbar. Institutsspezifische Regelungen erscheinen hier angemessener.

Wie bereits oben ausgeführt ist die Trennung von Prüf- und Risikoausschuss – zumindest für inländische Banken – nicht angezeigt. In der Praxis ergeben sich – wie die Erfahrung zeigt – Abstimmungsprobleme zwischen den Pflichtenheften, weil die Einheit der Materie verletzt wird. Weiter werden die Organisationsstruktur, Eskalations- und Reportinglinien unnötig komplex.

Zu Ziffer 3.5

Wie oben ausgeführt ist der Nutzen der organisatorischen Vorgaben zur Risikokontrolle systemrelevanter Banken nicht erkennbar.

Detailregelungen, welche Funktion in eine Geschäftsleitung gehört, entsprechen nicht dem prinzipienbasierten Ansatz und sollten nicht auf Ebene von Rundschreiben abgehandelt werden. Insbesondere wird die von der FINMA geforderte Eigenständigkeit des CRO je nach Organisation des Instituts unterschiedlich sichergestellt. Der Zwang bei systemrelevanten Banken, den CRO in die GL zu entsenden, ist deshalb nicht nachvollziehbar und zu streichen.

Wir schlagen vor, Ziff. 3.5 Absatz 4 des Erläuterungsberichts wie folgt zu ändern:

> „(...) 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.~~ (...)

Als Alternative ist der CRO als Mitglied einer erweiterten Geschäftsleitung denkbar.

Zu Ziffer 3.8

Die Publikationsvorschriften gemäss SIX-RS sind auf börsennotierte Aktiengesellschaften ausgerichtet, weshalb Anpassungen für Unternehmen mit anderen Rechtsformen und nicht börsennotierte Institute notwendig sind. Die durch das Rundschreiben hinzukommenden Neuerungen zu den bereits bestehenden Pflichten müssen bei einzelnen Instituten zuerst analysiert und muss diesen genügend Zeit zur Umsetzung eingeräumt werden. Insbesondere die Offenlegung von Wahl- und Rekrutierungsverfahren gehen entschieden zu weit. Die Offenlegung im Geschäftsbericht muss selbstredend ausreichen. Zusätzliche Offenlegungserfordernisse sind nicht nachvollziehbar. Der Erläuterungsbericht ist entsprechend anzupassen.

Zu Ziffer 3.9

Die vorgesehene Übergangsfrist von einem Jahr ab Inkrafttreten sind für gewisse Vorgaben (1. August 2016 meint wohl 1. August 2017) zu kurz, insbesondere wenn neue Ausschüsse implementiert und/oder zusätzliche Verwaltungsräte rekrutiert werden müssen. Wir erachten eine Frist bis 31. Dezember 2018 für angemessen.

Zu Ziffer 4.1

Die FINMA bringt zum Ausdruck, dass sie für Banken der Aufsichtskategorie 4 und 5 für die qualitativen Anforderungen an den Umgang mit operationellen Risiken im Einzelfall Erleichterungen oder Verschärfungen anordnen kann. Diesbezüglich werden Fragen nach der Rechtssicherheit für die betroffenen Kategorien aufgeworfen. Das führt zu unnötigen Bewilligungsverfahren. Hier sind klare Kriterien festzulegen, von denen die FINMA grundsätzlich nicht abweicht.

Zu Ziffer 4.5

Wie bereits eingangs ausgeführt, ist die detaillierte Aufnahme von Mitteilungen der FINMA (Positionspapier / FAQ) in ein Rundschreiben abzulehnen. Es kann nicht mehr von einer prinzipienbasierten Regulierung gesprochen werden, insbesondere, wenn die im Positionspapier beschriebene Verwaltungspraxis in das Rundschreiben aufgenommen wird.

Zu Ziffer 5

Wir nehmen zur Kenntnis, dass die Limite, ab welcher das FINMA-RS 2010/1 anzuwenden ist, so hoch angesetzt wird, dass nur noch die beiden Grossbanken zwingend davon betroffen sind. Die Raiffeisen Gruppe fällt mit einem Eigenmittelerfordernis von deutlich weniger als CHF 10 Mia. nicht mehr darunter, wird aber die unter der bisherigen Fassung des FINMA-RS 2010/1 entwickelte Praxis weiterführen.

Dennoch halten wir fest, dass die generelle Einführung von „claw back"-Regelungen eindeutig zu weit geht. „Claw back"-Klauseln können ein sinnvolles Element eines Vergütungssystems sein, insbesondere wenn „risk takern" hohe Bonuszahlungen für Resultate gewährt werden, welche eine langfristige Komponente haben. Sie machen demgegenüber wenig Sinn, wenn der Anteil erfolgsabhängiger Zahlungen vergleichsweise gering ist oder bereits andersartige Kompensationsmechanismen bestehen, welche Risiken oder erwünschte Verhaltensarten angemessen berücksichtigen. Ob „claw back"-Regelungen überhaupt Sinn machen, ist demzufolge abhängig vom gesamten Kompensationssystem, weshalb eine zwingende Einführung sachfremd ist. Mithin bedarf es einer prinzipienbasierten Regelung.

Zum Entwurf FINMA-RS 2016/xx Gorporate Governance

Zu FINMA-RS 2016/xx, Rz 12

Bei wörtlicher Auslegung von Rz 12 kann das Oberleitungsorgan keine eigenen Ideen entwickeln und nur auf Antrag der Geschäftsleitung über die aufgeführten Punkte entscheiden. Das ist wohl kaum im Sinn der FINMA.

Der Verwaltungsrat soll zudem über die wesentlichen Unternehmensziele und das Unternehmensleitbild entscheiden und die Leitsätze zur Unternehmenskultur und den Unternehmenswerten erlassen. Hier werden Entscheidungen angesprochen, welche wesentlich durch die Unternehmenseigentümer mitzubestimmen sind, d.h. in die Kompetenz der Generalversammlung gehören.

Die Anforderungen an die Kompetenz der Mitglieder des Verwaltungsrats sind anderweitig umschrieben. Der letzte Satz ist unnötig und gehört in dieser Form nicht in ein FINMA-RS.

Wir schlagen folgende Änderung vor:

> „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 versteht die Unternehmensstrukturen und Risiken der einzelnen Geschäftsfelder des Instituts.~~**"

Zu FINMA-RS 2016/xx, Rz 13 - 17

Das BankG schreibt vor, dass die Leitung einer Bank auf zwei Stufen aufgeteilt sein muss, nämlich auf ein Organ für die Oberleitung und Kontrolle und auf ein Organ für die operative Führung (Geschäftsleitung) der Bank. Um eine klare Funktions- und Aufgabenteilung sicherzustellen, ist das Paritätsprinzip zu beachten, wonach kein Organ dem andern in seinen Kompetenzbereich eingreifen darf.

Unter dieser Voraussetzung regelt das Oberleitungsorgan die Tätigkeit des operativen Organs in Form von generell abstrakten Regelungen (in der Regel in Form von Reglementen) und überwacht deren Einhaltung. Es soll aber nicht in die Einzelentscheidungen eingreifen, soweit ihm durch die Kompetenzordnung der Entscheid nicht ausdrücklich vorbehalten ist. Entsprechend erlässt das operative Organ die generell abstrakten Regeln für die Steuerung der operativen Geschäftstätigkeit (in der Regel in Form von Weisungen).

Diverse Regeln des FINMA-RS 2016/xx sind diesbezüglich nicht klar und verwischen die Kompetenzzuteilung zwischen Oberleitungsorgan und operativem Organ. Diesbezüglich ist der gesamte Entwurf zu FINMA-RS 2016/xx zu überprüfen. Beispielhaft schlagen wir folgende Änderungen vor:

Rz 13
Weisungen sind das Gefäss, in dem das operative Organ seine Regelungen für das operative Geschäft erlässt.

> „Das Oberleitungsorgan ist verantwortlich für eine angemessene Unternehmensorganisation mit ausgewogenen „Checks and Balances". Es erlässt die für den Geschäftsbetrieb und die für die Kompetenzverteilung und Überwachung notwendigen Reglemente, insbesondere das Organisations- und Geschäftsreglement~~, und Weisungen~~."

Rz 14
Das Oberleitungsorgan beauftragt das operative Organ mit der Ausgestaltung des Rechnungswesens und überprüft dessen Wirksamkeit.

> „Das Oberleitungsorgan trägt die oberste Verantwortung für die finanzielle Lage und Entwicklung des Instituts. Es ~~sorgt~~ **ist verantwortlich** 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."

Rz 16
Das Oberleitungsorgan beauftragt das operative Organ mit der Ausgestaltung des internen Kontrollsystems und überprüft dessen Wirksamkeit, richtet dieses aber nicht selbst ein (= operative Aufgabe). Der dritte und vierte Satz der Bestimmung sind teilweise redundant. Wir schlagen deshalb folgende Änderung vor:

> „Das Oberleitungsorgan übt die Oberaufsicht über die Geschäftsleitung aus und stellt die Compliance des Instituts sicher. Es ~~sorgt~~ **ist verantwortlich** für ein geeignetes Risiko- und Kontrollumfeld innerhalb des Instituts **sowie**~~. Es richtet~~ ein wirksames internes Kontrollsystem.~~ ein,~~ **Es** bestellt ~~*und überwacht*~~ die interne Revision, bestimmt die aufsichtsrechtliche Prüfgesellschaft und würdigt deren Berichte. (...)"

Rz 17
Der Verwaltungsrat entscheidet über Beteiligungen an Konzerngesellschaften und nimmt auf dem Weg der Konzernführung Einfluss auf die Tochtergesellschaften. Uns ist nicht klar, was hier „wesentliche Veränderungen bei bedeutenden Tochtergesellschaften" bedeutet. Dieser Hinweis schafft nur Unklarheiten, jedoch keinen aufsichtsrechtlichen Mehrwert.

> „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."

Zu FINMA-RS 2016/xx, Rz 18

Die Anforderungen an die Fähigkeiten der Mitglieder des Oberleitungsorgans sind sehr umfassend und absolut formuliert. Diese werden mit dem Hinweis auf internationale Standards eingeführt. Die unbesehene Übertragung internationaler Standards auf Banken, die im Inland oder gar nur regional tätig sind, errichtet unnötig hohe Hürden für die sinnvolle Zusammensetzung eines Verwaltungsrats. Auf Ebene der einzelnen Raiffeisenbank schlagen wir vor, die lokale Verwurzelung als eine mögliche Kernkompetenz gelten zu lassen. Auf Ebene Verwaltungsrat der einzelnen Raiffeisenbank sind "die nötigen Fachkenntnisse und Erfahrungen im Bank und Finanzbereich" im Hinblick auf die Einbindung in die Gruppe auch ohne entsprechende Berufspraxis abdeckbar. Eine entsprechende Präzisierung begrüssen wir.

Auf Ebene Raiffeisenbank ist im Hinblick auf die Einbindung in die Gruppe zudem kein Verwaltungsratsmitglied mit IT-Kernkompetenz erforderlich, da die IT zentral durch Raiffeisen Schweiz sichergestellt wird. Auch hier würden wir eine Präzisierung für kleinere und in eine Gruppe eingebundene Institute begrüssen.

Wir schlagen eine flexiblere Formulierung vor wie folgt:

> „Die Mitglieder des Oberleitungsorgans geniessen einen guten Ruf und bieten Gewähr für eine einwandfreie Geschäftstätigkeit. Sie sind integer und verfügen als Gesamtorgan **abgestimmt auf die Grösse und die Geschäftstätigkeit der Bank** über hinreichende Führungskompetenz sowie die nötigen Fachkenntnisse und Erfahrung im Bank- und Finanzbereich. Das Oberleitungsorgan ist genügend breit aufgestellt, so dass nebst den Hauptgeschäftsfeldern ~~sämtliche weiteren~~ **auch die für die Bank relevanten** 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.**~~"

Zu FINMA-RS 2016/xx, Rz 21

Danach soll das Oberleitungsorgan zu mindestens einem Drittel aus unabhängigen Mitgliedern bestehen. Bei dieser Vorgabe schafft der Hinweis auf eine „genügende Anzahl" lediglich Unsicherheiten.

Bei Genossenschaftsbanken soll jedoch der Verwaltungsrat aus dem Kreis der Mitglieder gewählt werden, was angesichts des im Genossenschaftsrecht geltenden Kopfstimmprinzips unter dem Gesichtspunkt der Interessenkonflikte unproblematisch ist. Solche Fälle auf Ausnahmebewilligungen zu verweisen ist unnötig und verursacht vermeidbaren Aufwand. Wir schlagen folgende Präzisierung vor:

> „Das Oberleitungsorgan **besteht mindestens zu einem Drittel aus** ~~**verfügt über eine genügende Anzahl**~~ unabhängige**n** Mitglieder**n**~~**, die kein besonderes Näheverhältnis zum Institut aufweisen. Es besteht mindestens zu einem Drittel aus unabhängigen Mitgliedern**~~. ~~**Die FINMA kann in begründeten Fällen Ausnahmen bewilligen**~~. **Personen, die nur eine unwesentliche Geschäftsbeziehung zum Institut haben, weniger als 2% der Aktien der Bank besitzen oder Genossenschafter einer Genossenschaftsbank sind, gelten als unabhängig."**

Anstelle von Ausnahmebewilligungen ist das Prinzip „comply or explain" beizubehalten.

Zu FINMA-RS 2016/xx, Rz 26

Diese Randziffer ist auf Ebene FINMA-RS zu detailliert und kann mit der vorgeschlagenen Ergänzung von Rz 21 aufgefangen werden. Im Übrigen sind solche Abhängigkeitsverhältnisse entsprechend den allgemein im Gesellschaftsrecht gültigen Regeln im Einzelfall zu prüfen.

> **Die Bestimmung ist überflüssig und zu streichen.**

Zu FINMA-RS 2016/xx, Rz 30

Die Vorgabe, dass sich ein Mitglied des Oberleitungsorgans „dauernd" für das Mandat bereit zu halten hat, ist zu unpräzis und wörtlich ausgelegt lebensfremd. Wir schlagen folgende Formulierung vor:

> „Jedes Mitglied des Oberleitungsorgans widmet seinem Mandat genügend Zeit und wirkt aktiv an der strategischen Unternehmensführung mit. Es hat das Mandat persönlich auszuüben und **muss** ~~**sich**~~ über den ordentlichen Sitzungsrhythmus hinaus für Krisensituationen oder Notfälle ~~dauernd~~ ~~**bereitzuhalten**~~ **innert angemessener Frist verfügbar sein**. 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."

Zu FINMA-RS 2016/xx, Rz 33

Interessenkonflikte sind nicht grundsätzlich verboten und kommen regelmässig vor. Entscheidend ist der Umgang damit im Sinn der Transparenz und der notwendigen Massnahmen im Einzelfall. Es ist zu präzisieren, welche auf Dauer bestehenden Interessenkonflikte so wesentlich und untragbar sind, dass sie zur Niederlegung des Mandats verpflichten sollen. Frühere Interessenbindungen sind grundsätzlich nicht relevant, allenfalls auf einen angemessenen Zeitraum zu beschränken und bei der Beurteilung des Lebenslaufs eines Kandidaten zu bewerten. Im Übrigen gelten die Beschränkungen von Rz23 und 24.

> „(...) ~~**Bestehende und frühere**~~ Interessenbindungen sind offenzulegen und Interessenkonflikte ~~wirksam~~ **möglichst** zu beseitigen. **Das Mandat ist niederzulegen**, wenn sich ein Interessenkonflikt auf Dauer nicht vermeiden lässt**, der die Ausübung des Mandats in erheblichem Umfang einschränkt."**

Zu FINMA-RS 2016/xx, Rz 36

Wie bereits oben zu Ziff. 3.2.5 des Erläuterungsberichts zum FINMA-RS 2016/x, ausgeführt, gibt es für national oder regional tätige Institute keinen ersichtlichen Grund, den Ansatz des Basler Ausschusses zu übernehmen und je einen separaten Prüfungs- und Risikoausschuss zu verlangen. Die personelle Unterscheidung der geforderten zwei Ausschüsse schafft keinen Mehrwert und keine zusätzliche Sicherheit. Es ist eine Frage der Organisationsfreiheit jeder einzelnen Bank, wie sie den Prüf- und Risikoausschuss des Verwaltungsrats aufstellt. Verzichtet sie auf eine Separierung des Prüf- und Risikoausschusses, nutzt sie Synergien und vermeidet unnötig komplexe Organisationsstrukturen, Eskalations- und Reportinglinien. Die „georteten" Defizite beim risikospezifischen Fachwissen auf Stufe Oberleitung lassen sich nicht einfach mit mehr Personal beseitigen. Wichtig erscheint, dass die Mitglieder über das nötige Fach-Know-how und über die betreffenden Kompetenzen verfügen. In diesem Sinn sind in einem einzigen Prüf- und Risikoausschuss die richtigen Personen zusammen zu fassen.

Die BCBS Empfehlungen äussern sich zu diesem Punkt wie folgt (vgl. Rz 63 ff.):

> *"The number and nature of committees depend on many factors, including the size of the bank and its board, the nature of the business areas of the bank, and its risk profile."*

Unbestritten ist danach, dass es eines Prüf- und Risikoausschusses bedarf. Zur Frage, ob dieser zusammengelegt werden kann, wird keine Stellung bezogen.

Es soll nach Auffassung von Raiffeisen in der Verantwortung des betreffenden Instituts bleiben, wie der Prüf- und Risikoausschuss ausgestaltet wird.

Wir schlagen zu Rz 36 folgende Formulierungen vor:

> „Zu seiner Unterstützung kann das Oberleitungsorgan aus seiner Mitte Ausschüsse einrichten oder Aufgaben einzelnen Mitgliedern übertragen. **International ausgerichtete** Institute der Aufsichtskategorien 1 - 3 müssen je einen separaten Prüfausschuss und Risikoausschuss einrichten. Systemrelevante Banken ~~**müssen**~~ **können** über weitere Ausschüsse, **müssen** 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."

Zu FINMA-RS 2016/xx, Rz 37

Diese Bestimmung enthält eine für ein FINMA-RS wesentlich zu detaillierte Regelung.

> Die Bestimmung ist **zu streichen.**

Zu FINMA-RS 2016/xx, Rz 38

Zweckmässig erscheint, dass der Präsident des Oberleitungsorgans nicht Mitglied des Prüf- und Risikoausschusses sein kann, da dieser auch die unternehmerischen Entscheide des Verwaltungsrats kritisch hinterfragen soll. Hingegen ist nicht einzusehen, weshalb er nicht gleichzeitig Vorsitzender eines andern Ausschusses sein soll.

Die Anforderung, dass die Mehrheit der Mitglieder des Prüf- und Risikoausschusses unabhängig sein sollen, ist unbestritten und stellt kein Hindernis für die Auswahl geeigneter Kandidaten dar, wenn Prüf- und Risikoausschuss in einem Ausschuss zusammengefasst werden. Hingegen ist nicht einzusehen, weshalb die Mehrheit der Mitglieder des Nominationsausschusses unabhängig sein soll.

Wir schlagen folgende Formulierung vor:

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

Zu FINMA-RS 2016/xx, Rz 65 ff.

Zusätzliche Dokumente geben nicht zusätzliche Sicherheit. Das Rahmenkonzept für das Risikomanagement ist mit einer ausformulierten Risikopolitik, einem Limitensystem und dem Internen Kontrollsystem sowie deren Überwachung mittels Reportings abgedeckt. Wir gehen davon aus, dass hier nicht eine neue Anforderung geschaffen wird, welche die Ausgestaltung zusätzlicher Dokumente erfordert. Eine solche wird abgelehnt, da lediglich zusätzliche Redundanzen und Unübersichtlichkeit geschaffen würden.

Zu FINMA-RS 2016/xx, Rz 88

In Rz 87 wird die Pflicht festgehalten, die notwendigen unabhängigen Kontrollinstanzen zu schaffen und insbesondere einen CRO zu bestimmen. Es ist nicht zweckmässig, die Zusammensetzung der Geschäftsleitung in einem Detaillierungsgrad vorzusehen, wonach der CRO zwingend Mitglied der Geschäftsleitung sein muss.

> Rz 88 ist **zu streichen.**

Zu FINMA-RS 2016/xx, Rz 95

Die Ausführungen zur Risikokontrolle sind bereits anderweitig aufgeführt und redundant verteilt auf das Rundschreiben. Wir erwarten eine konsistente Abbildung der einzelnen Aufgaben, Kompetenzen und Verantwortlichkeiten, die innerhalb des Rundschreibens abgestimmt und systematisch aufgebaut ist.

> Rz 95 ist **zu streichen.**

Zu FINMA-RS 2016/xx, Rz 78 und 96

Die Bestimmungen über die Risikodatenaggregation und Risikoberichterstattung bei systemrelevanten Banken bedürfen Zeit für die Umsetzung. Entsprechende Übergangsfristen fehlen. Im Übrigen sind die Regelungen wesentlich zu detailliert. Angesichts der beschränkten Zahl von systemrelevanten Banken ist die Regelung auf Ebene FINMA-RS ohnehin fragwürdig. Hier müssten die Einzelverfügungen gegenüber den systemrelevanten Banken die notwendigen Regelungen beinhalten.

> Rz 96 ist **zu streichen.**

Zu FINMA-RS 2016/xx, Rz 99 – 103

Wir nehmen zustimmend davon Kenntnis, dass die Bestimmungen betreffend Aufgaben und Verantwortlichkeiten der Compliance-Funktion unverändert aus dem FINMA-RS 2008/24 übernommen wurden.

Zu FINMA-RS 2016/xx, Rz 128 und 133

Es besteht eine gewisse Unsicherheit, wie die Offenlegungsvorschriften im Rahmen einer Bankengruppe zu verstehen sind. Wenn sie ebenfalls für die Gruppenführung gelten und entsprechend das einzelne Institut (Rz 126) entlastet wird, wäre das zu begrüssen.

Uns ist nicht klar, was in Rz 128 mit „weiteren Anspruchsgruppen" gemeint ist. Jede Anspruchsgruppe kann den Geschäftsbericht einsehen. Zusätzliche speziell zu nennende Anspruchsgruppen erkennen wir nicht. Hier erwarten wir eine Präzisierung oder die Streichung dieser Worte.

Die Offenlegung des Wahlverfahrens für Mitglieder des Oberleitungsorgans und des Rekrutierungsprozesses für Mitglieder der Geschäftsleitung (Rz 133) bietet aber keinen ersichtlichen Mehrwert. Es sind die Kompetenzen der Personen, welche schlussendlich interessieren und nicht der Prozess der Wahl oder Rekrutierung. Auch gilt es zu bedenken, dass ein Rekrutierungsverfahren ein Wettbewerbsvorteil darstellen kann und somit ein Geschäftsgeheimnis darstellt.

> Rz 133 ist **zu streichen.**

Zu FINMA-RS 2016/xx, Rz 141

Es gibt keinen Grund, das Revisions- und das Prüfhonorar für das vergangene Berichtsjahr und weitere Honorare zu publizieren. Die Entschädigung ist eine Sache der Verhandlung mit der Prüfgesellschaft. Eine Offenlegung könnte die Kooperationsbereitschaft von Prüfgesellschaft und Bank beeinträchtigen. Sie könnte zudem den Wettbewerb unter den Prüfgesellschaften schwächen und kostentreibend wirken, was schliesslich die Dienstleistungspreise für die Bankkunden verteuern würde. Wir schlagen folgende Änderung der Formulierung vor:

> „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)"

Zu FINMA-RS 2016/xx, Rz 142

Uns ist unklar, was ist mit der „vom Institut angewandten Informationspolitik" gemeint ist bzw. was diese Bestimmung bewirken soll. Die Informationspolitik einer Unternehmung ist Teil ihres Marktauftrittes. Sie ist von den Marktteilnehmern „live" zu erleben und nicht als theoretische Beschreibung nachzulesen. Unklar sind die Folgen, wenn ein Unternehmen trotz „aktiver Informationspolitik" eine Information in gerechtfertigter Weise gerade nicht publizieren will.

> Rz 142 ist **zu streichen.**

Zu FINMA-RS 2016/xx, Rz 143

Grundsätzlich sind die Offenlegungspflichten der Banken im Rahmen des Geschäftsberichts wahrzunehmen, es sei denn, aufgrund von besonderen Vorfällen sei eine ad-hoc Publikation notwendig. Die Ausführungen von Rz 143 sind für ein FINMA-RS wesentlich zu detailliert und gehen zu weit. Im Übrigen sind die Offenlegungspflichten im FINMA-RS 2016/1 bereits niedergelegt. Wir schlagen deshalb folgendes vor:

> Rz 143 ist **zu streichen.**

Zum Revisionsentwurf FINMA-RS 2008/21 Operationelle Risiken Banken

Allgemeiner Hinweis

Der Detaillierungsgrad des Rundschreibens ist generell unnötig hoch. Besonders offensichtlich wird das in Rz 135 ff., Grundsatz 4 betreffend IT-Risiken. Hier werden Regeln in einer operativen Tiefe aufgestellt, welche nicht zu dem von der FINMA propagierten prinzipienorientierten Ansatz passen.

Zu FINMA-RS 2008/21, Rz 135.1- Grundsatz 4: Technologieinfrastruktur

Die Regelung von Rz 135.1 lit. a, welche die Banken verpflichtet, eine Übersicht über die bestehenden IT-Systeme zu erstellen, ist akzeptabel.

Zu weit gehen jedoch die Bestimmungen von Rz 135.1 lit. b – f. Sie verlangen Regelungen auf der Ebene von Prozessen in einem Detaillierungsgrad, der sich mit einer prinzipienbasierten Regelung nicht mehr verträgt. Die Risiken im IT-Bereich sind grundsätzlich nach den gleichen Kriterien zu handhaben wie die Risiken in anderen Risikofeldern. Unter anderem gelten die Grundsätze des FINMA-RS 2008/7 „Outsourcing Banken".

Die Formulierung in Rz 135.1 lit. g „Reduktion Komplexität und Fragmentierung" erscheint zu weitgreifend. Handlungsbedarf ist dann angezeigt, wenn sich aus Komplexität und Fragmentierung ein wesentliches Risiko ergibt. Wir schlagen folgende Formulierung von Rz 135.1 vor:

> „Die Geschäftsführung stellt sicher, dass das IT-Konzept in Anlehnung an ~~die~~ internationalen~~n~~ Standards das Vorhandensein der folgenden minimalen Aspekte gewährleistet:
> a. Aktuelle und vollständige Übersicht über die wesentlichsten Bestandteile der IT-Netzwerkumgebung mit Schnittstellen zwischen Systemen und Applikationen,
> ~~*b. – f.*~~ ***(streichen)***
> **g**~~**g**~~**b.** Technologie- und Investitionsplanung zur Sicherstellung einer angemessenen IT-Kapazität sowohl unter normalen Geschäftsbedingungen wie auch in Stressperioden ~~**sowie zur Reduktion der Komplexität und Fragmentierung der IT-Infrastruktur."**~~

Zu FINMA-RS 2008/21, Rz 135.2- Grundsatz 4: Technologieinfrastruktur

Rz 135.2 hat sich auf den Grundsatz zu beschränken. Das ist keine prinzipienbasierte Regelung mehr, der Detaillierungsgrad ist viel zu eng.

> Rz 135.2 lit. a – lit. e ist **zu streichen.**

Zu FINMA-RS 2008/21, Rz 135.3 - Grundsatz 4: Technologieinfrastruktur

Die Formulierung in Rz 135.3 „besonders schützenswert" ist ohne weiteren Zusatz gemäss Datenschutzgesetz Art. 3 lit. c eindeutig definiert (z.B. Gesundheitsdaten). Um Verwechslungen auszuschliessen, empfehlen wir die Formulierung gemäss Erläuterungsbericht zu präzisieren. Angemessen erscheint der Begriff „Daten und Systeme mit besonders hohem Schutzbedarf".

Die primäre Angriffsfläche für Cyberattacken sind exponierte Systeme. Zwingende Vorgaben für „penetration testing" sollten deshalb angemessen auf diese Angriffsfläche fokussieren. Eine zwingende Vorschrift alle IT-Systeme durch externe Dienstleister einem Penetrationstest zu unterziehen erscheint weder angemessen noch prinzipienorientiert. Eine fristgerechte Umsetzung bei Raiffeisen Schweiz ist volumenmässig und mit dem Qualtitätsanspruch von Raiffeisen Schweiz unmöglich umsetzbar. Die Kostenfolgen sind nicht angemessen im Vergleich zum bestehenden Risiko. Auch die Verfügbarkeit, Qualifikation und Prüfqualität externer Dienstleister unterscheidet sich erheblich.

Der Passus ist wie folgt zu präzisieren und zu ergänzen:

> „Die Geschäftsführung lässt insbesondere in Bezug auf die Sicherstellung eines angemessenen Schutzes der ~~**besonders schützenswerten**~~ **Daten und Systeme mit besonders hohem Schutzbedarf** vor Cyberatta-

cken regelmässig Verwundbarkeitsanalysen und Penetration Testings durchführen. Diese ~~müssen~~ **sollten** grundsätzlich **durch qualifiziertes Personal mit entsprechenden Ressourcen** ~~geeignete externe Dienstleister~~ durchgeführt werden~~., können bei Vorhandensein von qualifiziertem Personal und Ressourcen jedoch auch durch interne Stellen vollzogen werden~~."

Zu FINMA-RS 2008/21, Rz 136.2 - Grundsatz 4: Technologieinfrastruktur

Der Begriff „ebenfalls"in Rz 136.2 sollte durch „angemessen" ersetzt werden. Eine zwingende Umsetzung aller internationalen Standards wäre nicht angemessen.

Wir empfehlen die Formulierung wie folgt zu präzisieren:

"Die systemrelevanten Banken treffen die hierfür erforderlichen Massnahmen im Rahmen der Notfallplanung (Art. 9 Abs. 2 lit. d BankG i.V.m. Art. 60 ff. BankV). Bestehen zu diesem Themengebiet international anerkannte Standards, so sind diese ~~ebenfalls~~ **angemessen** zu berücksichtigen."

Zu Anhang 03, Rz 17 - Grundsatz 3: Datenspeicherort und -zugriff

Die Formulierung in Rz 17 des Entwurfs zum Rundschreiben „...die Granularität des Inventars der Bank erlaubt, entlang der CID-Kategorien und den daraus resultierenden Sicherheitsvorkehrungen, zu ermitteln:" stellt ein übermässig hoher und komplexer Detaillierungsgrad auf einer operativen Tiefe dar, die nicht mehr prinzipienorientiert wirkt. Konsequenz wäre ein nicht zielführendes und komplexes Re-Design des Inventars, obwohl das Inventar gemäss Rz 16 besteht und mit Rz18 angemessen abgedeckt ist.

Wir empfehlen die Formulierung in Rz 17-19 wie folgt anzupassen:

„Es wird vorausgesetzt, dass die Granularität des Inventars der Bank erlaubt, ~~entlang der CID-Kategorien und den daraus resultierenden Sicherheitsvorkehrungen,~~ zu ermitteln:

- wo CID gespeichert sind, durch welche Anwendungen und IT-Systeme CID verarbeitet werden und wo elektronisch auf CID zugegriffen werden kann (Endbenutzeranwendungen);
- von welchen nationalen und internationalen Standorten und Rechtseinheiten aus auf Daten zugegriffen werden kann (einschliesslich ausgelagerter Dienstleistungen und externer Firmen)."

Zu Anhang 03, Rz 33 - Grundsatz 5: Absatz c) Sicherheitsanforderungen

Die Formulierung „höchst vertraulich" im Entwurf des Rundschreibens existiert bei Raiffeisen Schweiz nicht als Klassifikation. Ein angemessener CID Schutz gilt für alle Kategorien von CID und ist in den ersten drei Sätzen umfassend und angemessen definiert. Privilegierte Anwender sind automatisch Schlüsselmitarbeitende.

Fussnote 26:
Die Formulierung im Entwurf des Rundschreibens „Insbesondere auch" soll gestrichen werden. Man könnte sonst annehmen, dass auch Mitarbeitende ohne erweiterte Zugriffsrechte als Schlüsselmitarbeiter gelten, obwohl in diesem Fall kein wesentliches Risiko besteht.

Die Formulierung in der Fussnote 26 zum Entwurf des Rundschreibens „Grosse Datenmengen" erscheint unspezifisch. Der Begriff sollte konsistent verwendet und durch: „Massen CID" ersetzt werden.

Wir empfehlen die Formulierungen wie folgt zu schärfen:

Anhang 3, Rz 33
„Die Bank muss über klare Sicherheitsanforderungen für Mitarbeitende, die auf CID zugreifen, verfügen. Es ist regelmässig zu überprüfen, ob die Anforderungen für einen angemessenen Umgang mit CID weiterhin erfüllt sind. Erhöhte Sicherheitsanforderungen müssen für privilegierte IT-Benutzer und Anwender mit funktionalem Zugriff auf Massen-CID („Schlüsselmitarbeitenden") gelten. ~~Diese erhöhten Sicherheitsanforderungen~~

~~sind auch auf privilegierte Anwender mit Zugriff auf höchst vertrauliche Unterkategorien von CID (z.B. chiffrierte Konten) anzuwenden.~~"

Anhang 3, Fussnote 26:
~~„Insbesondere auch~~ bei erweiterten Zugriffsrechten wie z.B. die Abfrage und Extraktion/Migration von **Massen CID** ~~grossen Datenmengen~~."

Zu FINMA-RS 2008/21 Rz 136.4 ff. Grundsatz 6: Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft

Die Formulierung im Entwurf des Rundschreibens berücksichtigt nicht die unterschiedlichen Geschäftsmodelle der Schweizer Banken. So betreiben gewisse Banken das Geschäft mit Kunden Domizil Ausland aktiv, hingegen andere Banken rein passiv. Die unterschiedlichen Geschäftsmodelle finden im Entwurf keinen Niederschlag und es bedarf differenzierter Ausführungen. Eine Bank muss die Risiken im grenzüberschreitenden Geschäft risikobasiert erfassen, begrenzen und kontrollieren können. Rz 136.4 ist wie folgt zu ergänzen:

„Wenn Banken oder ihre Gruppengesellschaften grenzüberschreitend Finanzdienstleistungen erbringen oder Finanzprodukte vertreiben, sind auch die aus einer Anwendung ausländischer Rechtsvorschriften (Steuer-, Straf-, Geldwäschereirecht usw.) resultierenden Risiken **unter Berücksichtigung des jeweiligen Geschäftsmodells** angemessen zu erfassen, begrenzen und kontrollieren. Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Banken ausländisches Aufsichtsrecht **unter Berücksichtigung des jeweiligen Geschäftsmodells** einhalten. (...) treffen die Banken die erforderlichen strategischen und organisatorischen Massnahmen zur Risikoeliminierung und -minimierung und passen diese laufend geänderten Bedingungen an. Insbesondere verfügen sie **risikobasiert** über das notwendige länderspezifische Fachwissen, definieren sie spezifische Dienstleistungsmodelle für die bedienten Länder (...)."

Zum Revisionsentwurf FINMA-RS 2010/1 Vergütungssysteme

In der News/Medienmitteilung vom 1. März.2016 erwähnt die FINMA, dass das Rundschreiben nur noch bei Instituten angewendet wird, welche komplexe Vergütungssysteme und materiell relevante Vergütungshöhen aufweisen. Daher hat die FINMA den entsprechenden Schwellenwert für die zwingende Umsetzung angepasst. Es wird erwähnt, dass es somit nur noch für die beiden Grossbanken und grössten Versicherungskonzerne verbindlich ist. In Rz 6 wurde demzufolge der Schwellenwert der erforderlichen Eigenmittel von CHF 2 Mia. auf CHF 10 Mia. erhöht.

Durch die Erhöhung des Schwellenwertes unterliegt die Raiffeisen Gruppe neu nicht mehr zwingend diesem Rundschreiben. Wir begrüssen dies, werden in der Konsequenz aber unser bewährtes Vergütungssystem, welches dem bisherigen Rundschreiben Rechnung getragen hat, nicht ändern.

Wir sind überzeugt, dass unser genossenschaftliches Geschäftsmodell per Definition auf eine langfristige unternehmerische Entwicklung ausgerichtet ist. Gewinne werden nicht ausgeschüttet, sondern stärken das Eigenkapital. Es bestehen deshalb keine falschen Anreize, übermässige Risiken einzugehen, um überdurchschnittliche Renditen zu erzielen, welche zu übermässigen Vergütungen führen könnten.

Unser eigenständiges Vergütungssystem zeichnet sich insbesondere dadurch aus, dass für alle Gruppen von Risikoträgern nach oben limitierte Maximalvergütungen („Caps") definiert sind, der Anteil der variablen Vergütungen eingeschränkt ist und die gesamte Vergütung als Barzahlung in nicht aufgeschobener Form ausgerichtet wird. Raiffeisen betrachtet die Festlegung von Maximalvergütungen für ihre spezifische Situation als zielführender, als Teile der variablen Vergütung aufzuschieben. Das tiefe Risikoprofil und die nachhaltig stabilen Erträge, die sich aus dem Raiffeisen Geschäftsmodell ergeben, sind zwei der entscheidenden Faktoren für diesen Entscheid. Betragsmässige Obergrenzen sind zudem klar, einfach in der Handhabung und transparent. Damit wird insbesondere einem wesentlichen Grundsatz des Rundschreibens Rechnung getragen.

Wir hoffen Ihnen mit unseren Ausführungen gedient zu haben und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Raiffeisen Schweiz

Dr. Patrik Gisel
Vorsitzender der Geschäftsleitung

Nadja Ceregato
Leiterin Legal & Compliance

Kopie an:
- PwC via E-Mail (raiffeisen.coordination@ch.pwc.com)

RBA holding

RBA-Holding AG, Mattenstrasse 8, CH-3073 Gümligen

Per Post und per E-Mail
Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
CH - 3003 Bern

E-Mail: peter.ruetschi@finma.ch

Kontakt: Fritz Jörg
T +41 31 660 44 20
fritz.joerg@entris-banking.ch
Gümligen, 19. April 2016

Stellungnahme im Rahmen der Anhörung zu
FINMA-Rundschreiben 2016x „Corporate Governance – Banken"
FINMA-Rundschreiben 2008/21 „Operationelle Risiken Banken"
FINMA-Rundschreiben 2010/01 „Vergütungssystem"

Sehr geehrter Herr Rütschi

Am 1. März 2016 haben Sie die Anhörung zu den obenerwähnten Rundschreiben eröffnet.

Unsere Anliegen konnten wir in den Gremien der Schweizerischen Bankiervereinigung einbringen; darauf basierend unterstützen wir ausdrücklich deren Stellungnahme.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und stehen Ihnen für allfällige Auskünfte gerne zur Verfügung.

Freundliche Grüsse
RBA-Holding AG

Jürg Gutzwiller
CEO

Hans Ulrich Bacher
CRO

Regiobank Solothurn AG
Westbahnhofstrasse 11
CH-4502 Solothurn
www.regiobank.ch

regiobank
Banking wie ich es will

Markus Boss
CEO
Telefon 032 624 16 06
markus.boss@regiobank.ch

A-Post
Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
3003 Bern

Solothurn, 18. März 2016

FINMA-Rundschreiben 2016/x "Corporate Governance - Banken"
Vernehmlassungsantwort

Sehr geehrter Herr Rütschi

Gemäss FINMA-News vom 1. März 2016 geben Sie den Banken die Gelegenheit, sich zum Entwurf des FINMA-Rundschreibens 2016/x "Corporate Governance - Banken" zu äussern.

Gerne nehmen wir zum vorgelegten Entwurf wie folgt Stellung:

1. Grundsätzliches

Wir begrüssen die Zusammenfassung der in verschiedenen Dokumenten aufgeführten Bestimmungen in ein neues Rundschreiben. Dies erhöht die Transparenz und Übersichtlichkeit.

Ebenso sinnvoll erscheint es uns, dass kleinere Institute vor der Anwendung bestimmter Bestimmungen ausgenommen werden.

2. Bemerkung zu RZ 38 (Ausschüsse)

In Randziffer 38 wird die Zusammensetzung des Prüf-, Risiko- und Nominationsausschusses festgelegt. Sie schlagen vor, dass der Präsident des Oberleitungsorgans (in unserem Falle der Verwaltungsrats-präsident) weder einem der erwähnten Ausschüsse angehören noch Vorsitzender eines anderen Ausschusses sein darf.

Antrag:
Die Bestimmung, dass der Verwaltungsratspräsident einem Ausschuss nicht angehören darf, soll ersatzlos gestrichen werden.

Begründung:
Die Geschäftstätigkeit einer Regionalbank unterscheidet sich wesentlich von derjenigen grosser und/oder international tätiger Banken. Bei Regionalbanken ist der Präsident des Verwaltungsrates im Nebenamt tätig. Unseres Erachtens ist es für einen Präsidenten wichtig, in den entsprechenden Ausschüssen (bei der Regiobank im Prüfungsausschuss "Audit Committee") anwesend sein zu können, damit er direkt und umfassend orientiert wird. Alternativ sollte mindestens die Anwesenheit als Beisitzer ohne Stimmrecht möglich sein.

regiobank
Banking wie ich es will

Wir bedanken uns, sehr geehrter Herr Rütschi, für den Miteinbezug unseres Antrages in Ihre weiteren Überlegungen und in den definitiven Wortlaut.

Mit freundlichen Grüssen

Regiobank Solothurn AG

Felix Leuenberger
Präsident des Verwaltungsrates

Markus Boss
CEO

Regiobank Solothurn AG | Westbahnhofstrasse 11 | 4502 Solothurn | www.regiobank.ch

SwissBanking

Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
3003 Bern

PER MAIL peter.ruetschi@finma.ch

Bâle, le 20.4.2016
J.4.6 MST / YSA

Prise de position sur les projets
Circulaire FINMA 2016/xx « Gouvernance d'entreprise – banques »
Circulaire FINMA 2008/21 « Risques opérationnels – banques »
Circulaire FINMA 2010/01 « Systèmes de rémunération »

Cher Monsieur,

Vous avez bien voulu consulter notre Association dans le cadre de la révision des trois projets susmentionnés, ce dont nous vous remercions vivement.

La révision a pour but d'une part, d'épurer la Circulaire 08/21 Risques opérationnels – banques (Circ - FINMA « Risques opérationnels »), tout en ancrant les attentes de la FINMA par rapport à la gestion des risques IT (y compris cyber-risques) et d'opérations transfrontalières. D'autre part, il s'agit de rassembler en une nouvelle Circulaire FINMA sur la gouvernance d'entreprise, gestion des risques et contrôles internes des banques (Circ – FINMA « Gouvernance d'entreprise ») les exigences imposées aux banques en matière de gouvernance d'entreprise. Il s'agit également de prendre en considération les principes posés par les instances internationales, notamment, le Comité de Bâle sur le contrôle bancaire et le Fonds Monétaire International.

Nous approuvons l'orientation générale des projets de révision. Toutefois, nous devons souligner que les nouvelles circulaires sont, par endroit, trop détaillées et trop formalistes ce que l'Association suisse des banquiers déplore.

Executive Summary

L'ensemble des projets a suscité de vives et nombreuses inquiétudes auprès des établissements que représente notre association et qui appréhendent de faire face à de nouvelles exigences non justifiées et inutilement formalistes. Les points les plus critiques sont résumés ci-dessous.

S'agissant de la Circ – FINMA « gouvernance d'entreprise », l'ASB relève d'abord que la suppression du principe « *Comply or explain* » ne répond à aucun

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org

impératif objectif. Il entrainera un surcroit de travail tant pour les banques (avec à terme une augmentation des coûts pour les clients) que pour la FINMA. Il est essentiel pour l'ASB que la FINMA revienne sur l'abandon du principe.

De même, l'obligation pour l'ensemble des banques de catégorie 1 à 3 et non pas uniquement les banques d'importance systémique de disposer de deux comités d'audit et de risques séparés ne se justifie pas non plus. La FINMA va au delà des recommandations du Comité de Bâle, avec pour conséquence, de nouvelles charges administratives lourdes pour les banques non systémiques.

La régulation proposée est trop détaillée en ce qui concerne les tâches des différents organes des sociétés et parfois, clairement en contradiction avec le droit des obligations. La gouvernance d'entreprise ressortit à ce dernier et la FINMA n'a pas la compétence d'imposer des règles divergentes en cette matière aux banques. Il en résulte une insécurité juridique et un risque de modification des règles de responsabilités pourtant déjà réglées, de manière exhaustive, dans le Code des obligations.

Aucun intérêt prépondérant ne justifie d'imposer des règles de publication aussi étendues que le prévoit le projet à l'heure actuelle.

Enfin, l'entrée en vigueur ne saurait intervenir avant le 1er janvier 2018 avec une période transitoire d'une année.

Les dispositions introduites par le projet Circ – FINMA « risques opérationnels » en relation avec les risques informatiques, de par leur niveau de détail, s'éloignent d'une réglementation basée sur les principes et les propositions de l'ASB visent à les élaguer.

Enfin, l'ASB s'oppose vigoureusement à l'instauration *de* « *claw-backs* » qui auront un impact non négligeable sur la compétitivité de la place financière suisse.

Remarques introductives

La révision des circulaires Circ – FINMA « Gouvernance d'entreprise » et Circ – FINMA « Risques opérationnels » est à saluer en tant qu'elle permet, notamment, de réunir en une seule circulaire l'ensemble des questions relatives à la gouvernance d'entreprise et de prendre en considération l'évolution de la pratique en matière de gestion des risques. Cependant, il est discutable de vouloir imposer à l'ensemble des instituts suisses, sans différenciation, des recommandations internationales qui s'adressent, avant tout, à des instituts systémiques ou d'importance. Les banques suisses présentent de nombreux profils différenciés tant sur le plan géographique (marchés internationaux, nationaux ou même régionaux) que sur le plan des modèles d'affaires (banque universelle, banque d'affaires, gestion de fortune, crédits hypothécaires ou crédits commerciaux) et qui n'emportent pas les mêmes risques. La surveillance et les prescriptions de la FINMA devraient ainsi se conformer aux réalités du marché. Une

telle surveillance, orientée risques, est basée sur des principes et non pas sur des prescriptions détaillées qui ne tiennent pas compte des différents risques présentés par les instituts soumis à surveillance.

Or, contrairement à ce qu'affirme le Rapport explicatif de la FINMA du 1 mars 2016 en son chiffre 3.1, nous sommes d'avis que le projet de Circ – FINMA « Gouvernance d'entreprise » est par trop détaillé. En lieu et place de laisser les instituts s'organiser en fonction des risques qui leurs sont propres, on impose une conformité de nature formelle. Cela est d'autant plus vrai avec l'abandon du principe « *Comply or explain* » remplacé par un processus d'autorisation. De même, la transposition, mots pour mots, de prises de position de la FINMA ou de FAQs n'obéit à aucun impératif. Il en résulte une approche formaliste et peu flexible.

La séparation entre comité d'audit et comité des risques pour l'ensemble des banques de catégorie 1 à 3 est inutilement complexe et ne tient pas compte des particularités du marché, même si le Comité de Bâle le prévoit dans ses recommandations. De nombreux instituts n'ont qu'une activité nationale ou régionale et on peine à comprendre pourquoi la FINMA pose une telle exigence pour ces instituts qui va au delà des principes édictés par le Comité de Bâle.

Enfin, les deux projets contiennent de nombreux concepts indéfinis et des formulations ambigües. Ceux-ci doivent être définis en vue de la sécurité juridique.

Principales Observations relatives au projet de Circ – FINMA « Gouvernance d'entreprise » et propositions de modifications

Pour plus de clarté nous suivons la numérotation des chiffres marginaux (« cm ») du projet de circulaire ; les propositions de modifications sont soulignées et les suppressions barrées.

<u>En général :</u>

I. Objet

Les principes de gouvernance d'entreprise ressortissent, en premier lieu, au droit des obligations et la FINMA ne saurait se substituer au législateur en édictant de nouvelles normes en la matière, faute de délégation de compétence. Elle doit se limiter à en préciser certains aspects spécifiques aux banques. L'ASB souligne qu'une circulaire vise à préciser certaines attentes et codifier une certaine pratique ; il ne s'agit ni d'une loi, ni d'une ordonnance d'application et, à ce titre, elle ne peut imposer de nouveaux devoirs aux établissements. La circulaire emporte de nombreuses atteintes à la liberté de commerce et d'industrie sans constituer pourtant une base légale valable.

La notion de « *checks and balances* » est utilisée en politique et est à la base de la séparation des pouvoirs. Elle n'a pas à être transposée à des d'entreprises lesquelles visent à obtenir le succès en affaires. La responsabilité des divers organes, leurs compétences et leur subordination hiérarchique sont réglées dans le droit des obligations lequel n'a pas vocation à organiser un système de contrôle ou de

supervision. La gouvernance d'entreprise vise à ce que la société considérée se comporte de manière conforme à la loi et ce rôle de surveillance appartient au conseil d'administration. Dès lors, il serait plus conséquent de spécifier certains principes à suivre par le conseil d'administration dans la conduite globale d'un institut, plutôt que d'imposer un catalogue de tâches et de critères à remplir. Il n'appartient pas ici à la FINMA de se substituer au législateur, mais de renforcer certains aspects de droit civil au niveau régulatoire.

II. Terminologie

Le projet introduit plusieurs concepts qui méritent d'être définis. La terminologie utilisée nécessite d'être revue de manière approfondie afin de l'aligner sur le cadre théorique qui prévaut en matière de gouvernance et de gestion des risques. A ce titre, le projet devrait veiller à s'inspirer davantage des *Corporate governance principles for banks* de juillet 2015 du Comité de Bâle.

III. Champ d'application

Cette section consacre l'abandon du principe « *Comply or explain* » au profit d'un régime d'autorisation dérogatoire à solliciter au cas par cas[1]. Or, cette renonciation à un principe consacré par les instances internationales (notamment par le Comité de Bâle sur le contrôle bancaire et par l'Union européenne [2]) et récemment encore invoqué par la FINMA elle-même [3] n'obéit à aucun impératif objectif. Au contraire, il entraînera pour les établissements concernés une insécurité juridique majeure et un surcroît de bureaucratie préjudiciable pour de nombreux acteurs de l'industrie.

L'argument de la FINMA selon lequel le principe « *Comply or explain* » est peu utilisé et peu pratique tombe à faux. En effet, il sera bien plus complexe pour la FINMA de devoir gérer et coordonner, en temps utile, de nombreuses demandes d'allègements ou de changements. La FINMA affirme elle-même, dans son rapport explicatif, que : « *La gouvernance d'entreprise et la gestion des risques sont des thèmes de surveillance impossibles à contrôler et à surveiller dans le cadre d'une approche de type « one size fits all. »* [4]. Sur ce point, l'ASB est d'avis que le projet ne repose sur aucune base légale.

Par ailleurs, le projet ne tient aucun compte de la structure de détention de la banque ni du rôle et des fonctions occupées par son ou ses propriétaires majoritaires ou

---

[1] Cf. Rapport explicatif, p. 10 : « *L'application systématique du principe de proportionnalité remplace l'approche « comply or explain » jusqu'à présent utilisée à certains endroits de la circulaire.* ».

[2] Cf. Directive 2006/46/CE du Parlement européen et du Conseil du 14 juin 2006 modifiant les directives du Conseil 78/660/CEE concernant les comptes annuels de certaines formes de sociétés, 83/349/CEE concernant les comptes consolidés, 86/635/CEE concernant les comptes annuels et les comptes consolidés des banques et autres établissements financiers, et 91/674/CEE concernant les comptes annuels et les comptes consolidés des entreprises d'assurance, *JO* L 224/1 du 16 août 2006, pp. 1-7.

[3] Voir notamment le Rapport de la FINMA sur les résultats de l'audition relative au projet de circulaire « Publication banques », du 28 octobre 2015, p. 8.

[4] Rapport explicatif, p. 8.

uniques. Les restrictions qui s'appliquent aux banquiers privés ont été supprimées, alors qu'elles devraient être maintenues (cm 9). L'interdiction, au chiffre marginal 26, pour une « *partie déterminante de l'organe responsable de la direction supérieure* »[5] de détenir une participation qualifiée au sein de la banque ne tient pas compte des groupes se trouvant en mains familiales. Cette disposition, appliquée au pied de la lettre, reviendrait à empêcher l'existence des banquiers privés et des groupes bancaires détenus majoritairement par des actionnaires familiaux, y compris par l'intermédiaire d'une holding (société anonyme ou société en commandite par actions). Les mêmes remarques s'appliquent, *mutatis mutandis*, aux banques cantonales et aux caisses d'épargne en mains publiques. La FINMA n'a pas à interférer de la sorte, sans base légale et sans aucune nécessité objectivement justifiable par des considérations de risque, dans la composition du cercle des acteurs de la place financière suisse, dont la diversité est l'une des forces.

Le champ d'application de la Circulaire (Cm 9) comprend l'ensemble des banques de catégorie 1 à 3, tandis que les banques en catégorie 4 à 5 peuvent bénéficier de certaines exceptions. Or, il n'est pas possible de pouvoir imposer les mêmes exigences à l'ensemble des banques de catégorie 3, sans différenciation aucune. La catégorie 3 englobe des établissements dont le niveau de risques et le type d'activité et de marché diffèrent grandement. L'ASB demande ainsi à la FINMA que la Circulaire prenne en compte la diversité des instituts en catégorie 3. A cet effet, la Circulaire pourrait, par exemple, exclure les banques de la catégorie 3 de certaines prescriptions à l'instar des catégories 4 e 5 et régler les exceptions ou bien traiter la catégorie 3 ensemble avec les catégories 1 et 2 tout en les excluant de certaines exigences.

IV. Organe responsable de la direction supérieure

La répartition des compétences entre l'organe responsable de la direction supérieure et la direction n'est pas conforme à un équilibre des pouvoirs adéquat ; en effet, il donne à l'organe responsable de la direction supérieure non seulement des tâches stratégiques, mais également des tâches de mise en œuvre, jusque-là de la compétence de la direction. Il crée dès lors une confusion entre la surveillance et le contrôle (cm 16). Les prescriptions doivent être limitées aux domaines de la gestion des risques, du système de contrôle interne et de la *compliance*. La compétence obligatoire de l'organe responsable de la direction supérieure en matière de changements structurels ou d'investissement est un empiétement inadmissible sur le droit des obligations et devrait être supprimé.

Les dispositions relatives à la composition et l'indépendance de l'organe responsable de la direction supérieure ne trouvent aucune base juridique, ni dans le droit des obligations, ni dans la Loi sur les banques. La protection des créanciers est déjà réglée tant en droit public, qu'en droit privé et, à nouveau, la FINMA n'a pas à faire œuvre de législateur. Consacrer la primauté de certains créanciers dans une circulaire ne se justifie pas et n'est pas nécessaire.

[5] La notion de « partie déterminante » dans ce contexte n'est pas déterminée, ni du reste determinable. Les termes allemands de « *ein massgeblicher Teil des Oberleitungsorgans* » ne sont pas plus clairs.

Enfin, l'ASB s'oppose vigoureusement à l'obligation faite aux banques de catégorie 2 et 3 d'avoir un comité d'audit et un comité des risques séparés. Cette exigence ne tient pas compte de la diversité des instituts en catégorie 2 et 3. Elle rend les lignes de responsabilité inutilement complexes, oblige les comités à traiter des mêmes sujets deux fois ce qui risque d'entraîner une perte de synergie et une séparation artificielle des thèmes à traiter ou des conflits de compétences.

V. Direction

Selon le droit des obligations, la direction est compétente pour tous les domaines que lui délègue le règlement d'organisation, sauf compétences inaliénables d'autres organes. Or, le projet de circulaire attribue obligatoirement certaines compétences à la direction. Il s'agit, à nouveau, d'un empiètement inadmissible sur la liberté de la société de s'organiser comme elle l'entend, dans le respect des prescriptions légales. La circulaire devrait être limitée ici aux aspects qui relèvent de la vie bancaire, soit, la gestion des risques, les systèmes de contrôle interne et la *compliance*.

VI. Gestion des risques, système de contrôle interne et audit interne (chiffre romain IV à VIII du projet)

A nouveau ici, la circulaire est par trop détaillée en ce qui concerne ces domaines. Certaines dispositions empiètent sur les attributions d'autres organes selon l'organisation voulue par le droit civil. Le principe d'une réglementation basée sur des principes et orientée risques n'est pas respecté.

VII. Publication (chiffre X du projet)

Les prescriptions en matière de publication vont trop loin et sont inutilement contraignantes pour les instituts non cotés, augmentant, par là, leurs charges. La protection des investisseurs doit être ancrée au niveau de la loi et non pas dans une circulaire.

VIII. Entrée en vigueur (chiffre XI du projet)

Au vu de l'ensemble des nouveautés des trois projets, une entrée en vigueur au 1er juillet 2016 et un délai transitoire d'une année dès l'entrée en vigueur sont beaucoup trop courts pour permettre aux instituts de s'organiser en conséquence. La date la plus raisonnable pour l'entrée en vigueur est le 1er janvier 2018 avec un délai transitoire d'une année. Aucune raison ne justifie une adoption précipitée des nouvelles règles.

<u>En particulier :</u>

Ad Cms 3ss :
Commentaire : l'indépendance des instances de contrôle interne doit être définie de manière précise. Une définition additionnelle au sein du paragraphe « Définitions » serait la bienvenue.
Proposition : « <u>Die unabhängigen Kontrollinstanzen überwachen die Risiken sowie die Einhaltung regulatorischer und interner Vorschriften. Institutsspezifisch können verschiedene unabhängige Kontrollinstanzen definiert werden.</u> »

Ad Cm 5 *:*
Commentaire : certaines catégories de risques ne doivent être définis que de manière qualitative. Une légère adaptation de la formulation est nécessaire.
Proposition : compléter les première et dernière phrases ainsi : « Der Risikoappetit beinhaltet grundsätzlich sowohl quantitative wie qualitative Überlegungen (...)…Institutsebene festgelegt, sofern relevant ».

Ad Cm 8 *:*
Commentaire : le libellé *« marktüblicher Standards und Standesregeln* », en français « normes et usages déontologiques en usage sur le marché » est trop vague et doit être supprimé ; la référence à des règles de déontologie ne se justifie pas. La traduction française de « *Regeln* » par « norme » n'est pas correcte, en tant que le terme « norme » se réfère à une règle posée par le législateur, ce qui n'est pas le cas ici. Le terme de « règle » serait plus approprié.
Proposition *«* kontrolliert die Einhaltung gesetzlicher, regulatorischer und interner Vorschriften ~~sowie die Beachtung marktüblicher Standards und Standesregeln~~*.* »

Ad Cm 9 :
Voir commentaire sous rubrique « En général », « III. Champ d'application »

Ad Cms 10 – 17 :
Commentaire : le chiffre marginal 10 souligne le rôle de haute surveillance du conseil d'administration. Or, la terminologie utilisée pour décrire ses tâches lui confère un rôle plus opérationnel. En effet, celui-ci est « responsable d'une organisation appropriée » (cm 13), « doit garantir » (cm 15), « garantit la *compliance* » (cm 16), toutes notions qui impliquent une implication concrète dans l'activité opérationnelle et qui pourraient entrainer des conflits de compétences et de responsabilité. L'ASB demande que les termes utilisés soient choisis de telle sorte qu'il n'existe pas de doute quant à la tâche de haute direction et surveillance du conseil d'administration. Pour plus de détails, voir immédiatement *infra*.

Ad Cm 12 :
Commentaire :Ie texte proposé est par trop restrictif, en tant qu'il ne permet au conseil d'administration de décider uniquement sur proposition de la direction. Le terme « Sur proposition » doit être biffé. De plus, la dernière phrase décrit un état de fait et n'est pas prescriptive. Elle doit donc être biffée dans son entier.
Proposition : « 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 Risikomanagement sowie die Steuerung der Gesamtrisiken. ~~Es versteht die Unternehmensstrukturen und Risiken der einzelnen Geschäftsfelder des Instituts~~. »

Ad Cm 13 :
Commentaire : ce chiffre marginal reprend sensiblement l'art. 716a CO et pourrait donc être biffé. Il contient, en outre, de nombreux termes juridiques vagues qui devront être

explicités si cette disposition devait être maintenue. Enfin, il n'est pas possible d'attribuer à l'organe responsable de la direction supérieure la compétence exclusive d'édicter les directives; les unités opérationnelles doivent pouvoir le faire. Le terme « Checks and balances » ne recouvre pas de réalité juridique.
Proposition : « Das Oberleitungsorgan ist verantwortlich für die ~~eine angemessene~~ Unternehmensorganisation ~~mit ausgewogenen „Checks and Balances“~~. Es erlässt die für den Geschäftsbetrieb und die für die Kompetenzverteilung und Überwachung notwendigen Reglemente, insbesondere das Organisations- und Geschäftsreglement~~, und Weisungen.~~ »

Ad Cm 14 :
Commentaire : selon le projet, il appartiendrait à l'organe responsable de la direction supérieure d'approuver, en plus du rapport de gestion et du rapport annuel, les comptes trimestriels. Il en résulte une complication de l'organisation des instituts et une dérogation non justifié au droit des obligations. En pratique, les comptes trimestriels sont, le plus souvent, et notamment dans le cas des sociétés cotées, approuvés par le Comité d'audit. La nouvelle réglementation impose un nouveau rythme de réunion au conseil d'administration qui n'est pas praticable et modifie les règles de responsabilité lesquelles sont déjà inclues dans le Code des obligations. Dès lors, nous proposons de biffer l'approbation des comptes trimestriels par l'organe responsable de la direction supérieure.
Proposition : « (…) Es verabschiedet den Geschäftsbericht, das Jahresbudget, ~~die Zwischenabschlüsse~~ sowie die finanziellen Jahresziele. »

Ad Cm 15 :
Commentaire : Le libellé « (…) et décide de la nomination et de la révocation (...) » implique la responsabilité définitive de l'organe responsable de la direction supérieure dans la nomination des postes clés et fonctions de contrôle, y compris pour les personnes ne siégeant pas dans la direction. Il s'agit ici d'un empiètement massif et injustifié sur le pouvoir de délégation du conseil d'administration. A titre d'exemple, le chef de l'audit est généralement nommé par le Comité d'audit et s'écarter de la pratique actuelle ne se justifie pas. De plus, les termes fonctions clés et fonctions de contrôle ne sont pas définis : jusqu'à quel niveau hiérarchique la fonction de contrôle est-elle comprise par la FINMA ?
Proposition : « 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.~~

Ad Cm 16 :
Commentaire : il n'appartient pas à l'organe responsable de la direction supérieure d'organiser en détail le contrôle des risques, mais bien de formuler des principes adéquats. Il y a ici une confusion entre la surveillance et le contrôle. Par ailleurs, le conseil d'administration – pas plus d'ailleurs que la direction - n'est pas en mesure de « garantir » la compliance (« *stellt die Compliance des Instituts sicher.* »), au sens d'une obligation absolue de résultat. Ni l'organe de direction supérieure, ni la direction

opérationnelle ne saurait assumer une responsabilité causale pour tout manquement possible aux règles au sein de l'établissement. En ce qui concerne la désignation de la société d'audit prudentielle par l'organe responsable de la direction supérieure, il faut préciser que d'autres prescriptions sont réservées, voir par exemple le droit cantonal s'agissant des banques cantonales. La formulation du Cm 16 doit être revue en conséquence.
Proposition : « Das Oberleitungsorgan übt die Oberaufsicht über die Geschäftsleitung ~~aus~~ und ~~stellt~~ die Compliance des Instituts ~~sicher~~ aus. Es ~~sorgt~~ ist verantwortlich für ein geeignetes Risiko- und Kontrollumfeld innerhalb des Instituts sowie.~~Es richtet~~ ein wirksames internes Kontrollsystem. ~~Ein~~. Es bestellt und überwacht die interne Revision, bestimmt die aufsichtsrechtliche Prüfgesellschaft und würdigt deren Berichte. »

Ad Cm 17 :
Commentaire : le chiffre marginal empiète sur de nombreux domaines qui sont déjà réglés au niveau du droit des obligations et de la Loi sur les fusions (changements structurels), ce qui pourrait entraîner des conflits contraires à la sécurité juridique. Le terme « projets d'importance stratégique » est trop vague et laisse la porte ouverte à de nombreuses interprétations. Il en va de même pour le terme « changements essentiels touchant des filiales significatives ».
Proposition : suppression de la note marginale en sa totalité.
Proposition alternative : préciser que l'organe responsable de la direction supérieure ne se prononce que sur les changements matériels visés par le chiffre marginal 17.

Ad Cm 18 :
Commentaire : la Loi sur les banques en son art. 3, al. 2 lit. c règle déjà la composition de l'organe responsable de la direction supérieure. Il n'existe aucune base légale pour poser de nouvelles exigences au delà d'une bonne réputation et de la garantie d'une activité irréprochable. Le contraire revient à une violation de la liberté de commerce et d'industrie, car la formation de l'organe responsable de la direction supérieure relève de l'autonomie privée de la société.
En outre, la circulaire emporterait une grande insécurité juridique, puisque les instituts seraient dans l'impossibilité de nommer leur conseil d'administration sans l'imprimatur de la FINMA, ce d'autant plus que la note marginale comprend de nombreux termes et concepts indéfinis. L'ASB rajoute que, fondamentalement, ces nouveaux critères seront difficilement mis en œuvre au sein des instituts de taille moyenne à petite. Ce qui importe, avant tout, c'est la mise en œuvre d'une procédure de nomination et de composition appropriée.
Proposition : suppression pure et simple de la note marginale.
Proposition alternative : « 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 Bank- und Finanzbereich.~~Das Oberleitungsorgan ist genügend breit aufgestellt, so dass nebst den Hauptgeschäftsfeldern auch die für die Bank relevanten ~~sämtliche weiteren~~ 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. »

Ad Cm 19 :
Commentaire : idem que ad 18 *supra*.
Proposition : suppression du chiffre marginal 19.

Ad Cm 20 :
Commentaire : il conviendra de préciser que ce chiffre marginal ne s'applique qu'à la société faîtière d'un groupe et non pas aux sociétés filles.

Ad Cm 21 :
Commentaire : le critère de l'indépendance du tiers des membres de l'organe responsable de la direction supérieure est difficilement praticable pour les instituts de catégorie 4 et 5, voire 3. L'abandon du principe « *comply or explain* » et son remplacement par une procédure en autorisation lourde et coûteuse ne se justifie pas pour les instituts de ces catégories. La nouvelle circulaire devra reprendre ce dernier principe (chiffre marginal 19 de l'ancienne circulaire).
Proposition : « Ausser für die Institute in Kategorie 3, 4 und 5, die eine Abweichung von der Regel im Jahresbericht begründen können, besteht das Oberleitungsorgan mindestens zu einem Drittel aus ~~verfügt über eine genügende Anzahl~~ unabhängigen Mitgliedern.~~, die kein besonderes Näheverhältnis zum Institut aufweisen. Es besteht mindestens zu einem Drittel aus unabhängigen Mitgliedern. Die FINMA kann in begründeten Fällen Ausnahmen bewilligen.~~ Personen, die nur eine unwesentliche Geschäftsbeziehung zum Institut haben, weniger als 2% der Aktien der Bank besitzen oder Genossenschafter einer Genossenschaftsbank sind, gelten, unter anderem, als unabhängig. »

Ad Cm 26 :
Commentaire : l'exigence posée par le chiffre marginal 26 n'est pas praticable pour les instituts de taille moyenne à petite. Au surplus, il est redondant avec le chiffre marginal 21. Il ne tient pas compte, s'agissant de la participation qualifiée, des instituts se trouvant en mains familiales. Enfin, la primauté des intérêts des créanciers contredit l'art. 717 CO selon lequel le conseil d'administration doit sa loyauté et sa diligence en premier lieu à la société elle-même.
Proposition : suppression du chiffre marginal 26.

Ad Cm 30 :
Commentaire : la façon dont les membres de l'organe de direction supérieur exercent leur mandat n'a pas à être réglée par une circulaire relevant du droit de la surveillance. Le Code des obligations est suffisant à ce titre. Les termes choisis sont souvent vagues et entraînent une grande insécurité juridique pour les membres qui pourront voir leurs décisions mesurées à l'aune de critères indéfinis tirés du droit de la surveillance. Enfin, l'organe responsable de la direction supérieure est inutilement chargé de tâches administratives, alors qu'il devrait se concentrer sur la conduite et la stratégie de l'entreprise.
Proposition : suppression du chiffre marginal
Proposition alternative : « Jedes Mitglied des Oberleitungsorgans widmet seinem Mandat genügend Zeit und wirkt ~~aktiv~~ an der strategischen Unternehmensführung mit. Es hat das Mandat persönlich auszuüben und muss ~~sich~~ über den ordentlichen Sitzungsrhythmus hinaus für Krisensituationen oder Notfälle ~~dauernd~~ innert angemessener Frist verfügbar sein ~~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. »

Ad Cm 31 :
Commentaire : idem que ad Cm 30.
Proposition : suppression du chiffre marginal 31.
Proposition alternative : « 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 und der Geschäftsleitung sowie weiterer Schlüsselpersonen~~. Es stellt die Nachfolgeplanung sicher. »

Ad Cm 32 :
Commentaire : à nouveau, ce chiffre marginal est formulé de manière vague et ouverte et n'apporte aucune valeur ajoutée à la circulaire.
Proposition : suppression du chiffre marginal 32.

Ad Cm 33 :
Commentaire : les conflits d'intérêts sont déjà réglés dans le droit de la surveillance et le chiffre marginal 33 apparaît ainsi redondant. Au delà, l'ASB estime que le traitement des conflits d'intérêts dans le projet de circulaire est trop contraignant. La récusation devrait rester une *ultima ratio* et l'organe responsable de la direction supérieure doit être laissé libre de mettre en œuvre d'autres solutions (par exemple, le double vote, une fois avec et une fois sans le membre concerné, un minimum de votes de membres indépendants). Enfin, si le chiffre marginal devrait être maintenu, il conviendrait de préciser quels sont les conflits d'intérêts qui obligent à la démission.
Proposition : suppression du chiffre marginal 33.
Proposition alternative : « Das Oberleitungsorgan regelt den Umgang mit Interessenkonflikten. ~~und legt Ausstandspflichten fest~~. ~~Bestehende und frühere~~ Interessenbindungen sind offenzulegen und Interessenkonflikte wirksam zu beseitigen. Das Mandat ist niederzulegen, wenn sich ein Interessenkonflikt auf Dauer nicht vermeiden lässt, der die Ausübung des Mandats in erheblichem Umfang einschränkt.»

Ad Cm 34 :
Commentaire : les compétences requises du président ne trouvent aucune base légale. De plus, elles ressortissent à un jugement de valeur (« *une faculté de jugement, des capacités de gestion et une intégrité exceptionnelles* ») qui n'ont aucune place dans un contexte normatif et qui ne sont pas objectivement vérifiables. L'ASB souligne également qu'on ne saurait parler d'intégrité « exceptionnelle » en tant qu'il serait dangereux d'élaborer des niveaux d'intégrité. Les autorités de régulation ne sauraient procéder à un examen des qualités du président (et des autres membres de l'organe responsable de la direction supérieure) allant au delà de la bonne réputation et de la garantie d'une activité irréprochable.
Commentaire : suppression du chiffre marginal.

Ad Cm 35 :
Commentaire : le chiffre marginal est redondant par rapport aux dispositions qui relèvent du Code des obligations. Le président ne devrait pas être le seul responsable du bon fonctionnement de l'organe responsable de la direction supérieure ; il s'agit de

la responsabilité de l'ensemble de ses membres.
Proposition : suppression du chiffre marginal 35.
Proposition alternative : « 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 Kotrollfunktionen und ist für die Aufbereitung und Steuerung des Informationsflusses innerhalb des Oberleitungsorgans verantwortlich. »

Ad Cm 36 :
Commentaire : l'obligation pour l'ensemble des banques de catégorie 1 à 3 et non pas uniquement les banques d'importance systémique de disposer de deux comités d'audit et de risques séparés ne se justifie en aucun cas. (Sur ce point, l'Association des banques étrangères en Suisse est d'un avis divergent et ne soutient pas la proposition de l'ASB. Selon elle, toutes les banques de la catégorie 3 devraient disposer d'un comité de risques complémentaire du comité d'audit.) C'est aller au delà des recommandations du Comité de Bâle. L'ASB peine à comprendre pourquoi la FINMA entend faire du *Swiss Finish* qui ne tient pas compte de la pratique actuelle. Pour les instituts d'importance, mais non systémiques, il en résulte une charge administrative lourde au niveau organisationnel. Le recrutement sera encore plus difficile. Les mêmes thèmes seront traités par deux instances séparées, mais de manière redondante sans synergie aucune et au risque de conflits de compétence. Il n'est pas discutable que les questions d'audit et de gestion de risque doivent être correctement traitées au sein de l'organe responsable de la direction supérieure. Cependant, il doit être laissé à la libre appréciation des instituts de s'organiser en fonction de leurs risques et activités. S'agissant des instituts systémiques, la FINMA exige obligatoirement des « comités supplémentaires » aux côtés du comité des rémunérations et des nominations, sans toutefois en nommer aucun, ni ne donner d'exemples ou de pistes à suivre. Il est difficilement envisageable d'exiger de tels comités de ces établissements sans expliquer quels seront ces comités. En tout état de cause et au niveau organisationnel, le comité des rémunérations et nominations doit se situer au niveau du groupe pour assurer un alignement de la politique de rémunération dans l'ensemble du groupe et non pas au niveau de l'institut de nature systémique comme le prévoit le projet en sa teneur actuelle. Ce point précis doit impérativement être pris en considération. Enfin, la première phrase du chiffre marginal est déjà réglée au niveau du droit privé et peut être supprimée.
Proposition : « ~~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 einen Prüf- und Risikoausschuss verfügen (...) ».

Ad Cm 37 :
Commentaire : le chiffre marginal 37 est inutile et peut être supprimé.
Proposition : suppression du chiffre marginal 37.

Ad Cm 38 :
Commentaire : l'exigence selon laquelle le président de l'organe de direction supérieure ne préside pas de comité ne trouve aucune justification au niveau

réglementaire et prend à contre-pied la pratique actuelle au sein de certains établissements. La FINMA ne dispose pas de base légale pour l'imposer. De même, il n'est pas nécessaire que le comité des rémunérations et des nominations soit composé en majorité de membres indépendants. De plus, il faut clairement indiquer qu'au niveau des groupes, la FINMA peut accorder des dérogations relatives à l'ensemble des aspects des comités (existence, indépendance de leurs membres) dès lors qu'il est difficile en pratique pour certains groupes de remplir toutes ces exigences. Enfin, le libellé « d'excellentes connaissances » est vague et inapproprié ; il confère à l'Autorité de surveillance un pouvoir d'appréciation trop étendu. Le terme « suffisantes » serait plus approprié.
Proposition : « Die Mehrheit der Mitglieder des Prüf~~-~~, und Risiko~~- und Nominations~~ausschusses muss grundsätzlich unabhängig (vgl. Rz 20ff) sein. Die FINMA kann bei Finanzgruppen Erleichterungen sowohl im Hinblick auf die erforderlichen Ausschüsse als auch die Unabhängigkeit der Mitglieder gewähren. Der Präsident des Oberleitungsorgans soll grundsätzlich ~~weder~~ nicht dem Prüfausschuss ~~grundsätzlich nicht~~ angehören ~~noch Vorsitzender eines andern Ausschusses sein~~. Die Mitglieder sämtlicher Ausschüsse müssen insgesamt über ~~ausgewiesene~~ hinreichende Kenntnisse und Erfahrung im Aufgabenbereich des entsprechenden Ausschusses verfügen.»

Ad Cm 43 :
Commentaire : la surveillance et l'évaluation de l'efficacité des contrôles internes doivent pouvoir aussi être le fait du Comité des risques.
Proposition : « Überwachung und Beurteilung der Wirksamkeit der internen Kontrolle, namentlich auch der Risikokontrolle und der Compliance – Funktion (sofern dies nicht durch den Risikoausschuss erfolgt), und der internen Revision ».

Ad Cm 47 :
Commentaire : il manque un chiffre marginal après le chiffre marginal 47. Le paragraphe 47 (premier bullet point) et le paragraphe suivant (deuxième bullet point) devraient être réunis en un.

Ad Cm 50bis (nouveau) :
Commentaire : en relation avec le chiffre marginal 43 selon la proposition de modification de l'ASB, le Comité des risques doit aussi être habilité à surveiller et évaluer l'efficacité des contrôles internes. Un nouveau chiffre marginal 50bis doit ainsi être introduit.
Proposition : « Überwachung und Beurteilung der Wirksamkeit der internen Kontrolle, namentlich auch der Risikokontrolle und der Compliance – Funktion (sofern dies nicht durch den Prüfausschuss erfolgt) ».

Ad Cm 53ss :
Commentaire : l'énumération des tâches confiées à la direction est par trop détaillée et représente de facto un empiètement sur la liberté des instituts de s'organiser selon leur modèle d'affaire et leurs risques.

Ad Cm 60 :
Proposition : compléter « (...) Bilanzstrukturmanagement und Liquiditätsmanagement ».

Ad Cm 62 :
Commentaire : nous suggérons de reformuler légèrement le chiffre marginal en tant qu'il n'est pas possible pour les instituts d'anticiper systématiquement et de manière suffisante les changements d'un paysage régulatoire en perpétuelle évolution.
Proposition : « deren Kapazitäten den ~~aktuellen und längerfristigen~~ Geschäftsbedürfnissen (…) ».

Ad Cms 64 et 65 :
Commentaire : on retrouve ici des exigences similaires à celles de l'organe responsable de la direction supérieure. Or, il n'est pas justifiable d'aller au delà de l'exigence d'une bonne réputation et de la garantie d'une activité irréprochable, sauf à mettre sous tutelle les instituts par des prescriptions obligatoires. De plus, les termes utilisés sont vagues et laissent une grande marge de manœuvre à la FINMA s'agissant des nominations.
Proposition : suppression des notes marginales 64 et 65.

Ad Cm 70 :
Commentaire : un complément est nécessaire.
Proposition : « Präzisierung der materiellen institutsspezifischen (…) ».

Ad Cms 71, 73 et 75 :
Commentaire: il convient de préciser qu'il s'agit de catégories de risques matérielles.
Proposition: « (…) auf sämtliche materielle Risikokategorien (...) ».

Ad Cm 72 :
Commentaire : pour chaque type de limites, différentes mesures sont envisageables. Il appartient à la direction de formuler ces mesures dans des directives; elles ne devraient pas faire partie d'un concept cadre qui doit rester un concept et non pas un manuel détaillé.
Proposition: « Definition von ~~Massnahmen~~ Prozessen, um (….) ».

Ad Cm 73 :
Commentaire : il conviendra de préciser que l'implémentation des principes mis en place par l'organe responsable de la direction supérieure est du ressort de la direction.

Ad Cm 78 et 96 :
Commentaire : les dispositions relatives à l'agrégation des risques et aux rapports de risques pour les banques d'importance systémique prendront un certain temps à être mises en place : le délai transitoire est, à ce titre, trop court. De plus, au vu du petit nombre d'instituts concernés, l'ASB suggère de procéder par voie de décision, plutôt que par l'insertion dans la circulaire de dispositions, par ailleurs, trop détaillées.
Proposition : suppression du chiffre marginal 78 et application par voie de décision si nécessaire.

Ad Cm 79 :
Commentaire : le rôle du contrôle des risques selon la note marginale 79 ne correspond pas à la description ressortant à la note marginale 7. La formulation des deux devrait être adaptée à des fins d'uniformisation.

Ad Cms 80ss :
Commentaire : la structure du chapitre 7 (systèmes de contrôle interne) n'est pas cohérente. Ainsi, le premier chiffre marginal cite la révision interne en tant que troisième ligne de défense, alors que le reste du chapitre ne traite que des deux premières et que la révision interne est traitée dans un chapitre différent.

Ad Cm 82 :
Commentaire : il serait bienvenu ici de désigner quelles instances indépendantes de contrôle sont visées.

Ad Cm 83 :
Commentaire : selon le rapport explicatif (p. 16), les fonctions *compliance* et contrôle des risques peuvent être réunies s'agissant des banques de catégorie 4 et 5. La circulaire n'en fait pas mention, ce qui devrait être le cas.
Proposition : mentionner que les fonctions *compliance* et contrôle peuvent être réunies s'agissant des banques de catégorie 4 et 5.

Ad Cm 87 et 88 :
Commentaire : les établissements en catégorie 1 à 3 devraient impérativement avoir une fonction *compliance* complètement séparée de la fonction risque. Or, il existe une véritable synergie et de réels gains en termes de capacités et de connaissances lorsque la fonction *compliance* est rattachée à la fonction risque et rapporte au *chief risk officer*. Les instituts d'importance systémique veulent continuer à pouvoir décider librement de réunir (ou pas) les deux fonctions sous la houlette du *chief risk officer*. Pour les banques de catégorie 4 et 5, la possibilité d'externalisation de la fonction *compliance* n'est plus mentionnée de manière explicite. Ce point devra être réintroduit. Enfin obliger les établissements d'importance systémique à faire siéger le CRO dans la direction va trop loin et n'est pas justifié par un impératif régulatoire. La note marginale devra être supprimée.
Proposition : suppression de l'ensemble du texte de la note marginale 87 et remplacement par « Die Institute der Aufsichtskategorien 4 und dürfen die *Compliance*-Funktion auslagern».

Ad Cm 88 :
Commentaire : voir immédiatement *supra*.
Proposition : suppression de la note marginale 88.

Ad Cm 91 :
Commentaire : la préparation du flux d'information relève du *reporting* et non de la fonction de contrôle.
Proposition : « Die Risikokontrolle ~~stellt~~ legt die für …notwendigen Informationen ~~bereit~~ fest »

Ad Cm 92 (1) :
Commentaire : il appartient aux unités IT et / ou changement de procéder aux adaptations nécessaires des systèmes de surveillance.
Proposition : «In die Verantwortung der Risikokontrolle fallen zudem die Ausarbeitung und ~~umsetzung~~ der Betrieb von (…) Risikoüberwachungssystemen (…) ».

Ad Cm 92 (2) :
Commentaire : selon la pratique actuelle dans certains des instituts, c'est le *chief financial officer* qui surveille le respect des limites : cette possibilité doit être laissée à ceux-ci. Nous proposons une reformulation du chiffre marginal 92.
Proposition : « (….) ~~sowie die~~ . Die Überwachung von Systemen für die Einhaltung von aufsichtsrechtlichen Vorschriften (insbesondere Eigenmittel-, Risikoverteilungs- und Liquiditätsvorschriften) liegt in der Verantwortung des CFO oder CRO ».

Ad Cm 93 :
Commentaire : selon le chiffre marginal 93, le contrôle des risques participe au processus de développement des nouveaux produits et à la *due diligence* y afférente. A rigueur de texte, tous les produits nouveaux, mais semblables à d'autres déjà émis, devraient faire partie du processus ce qui représentera une augmentation significative de la charge de travail (par exemple, tous les nouveaux produits structurés). Une clarification s'impose.
Proposition : « Die Risikokontrolle nimmt bei der Entwicklung von neuen oder erweiterten Produkten~~n~~kategorien, Dienstleistungen, Geschäfts- oder Marktbereichen sowie bei wesentlichen oder komplexen Transaktionen am Entwicklungsprozess bzw. an der Sorgfaltsprüfung (Due Diligence) teil. ».

Ad Cm 95 :
Commentaire : les stress de résistance ne sont pas toujours les meilleurs outils pour contrôler l'appétence aux risques. Nous suggérons une clarification.
Proposition : « (...) mit dem Risikoappetit stehen und gegebenenfalls mit den Ergebnissen aus den Stresstests abgestimmt (…) ».

Ad Cm 96 (et 78):
Commentaire : la mise en œuvre des dispositions relatives à l'agrégation des données de risque et au rapport sur les risques nécessitent un délai transitoire approprié (voir commentaire ad Cm 78). Dès lors que l'ASB propose de renoncer au chiffre marginal 78, en toute logique, le chiffre marginal 96 devrait aussi être supprimé.
Proposition : suppression du chiffre marginal 96.

Ad Cm 98 :
Commentaire : par souci d'efficacité et de rapidité de réaction, l'information devrait remonter en premier lieu à la direction, dont les membres exercent leurs activités à plein temps, et non pas à l'organe responsable de la direction supérieure. La direction est mieux à même de prendre des mesures rapides. L'organe responsable de la direction supérieure devra être informé s'agissant de violations durables ou matérielles. De plus, il faudra clarifier qu'aucune limite stricte n'est envisagée pour les risques stratégiques et opérationnels. Enfin, une information immédiate n'est, en pratique, pas envisageable. Le terme « régulièrement » sera plus approprié.
Proposition : « (...) informiert die Risikokontrolle ~~das Oberleitungsorgan~~ die Geschäftsleitung ~~unverzüglich~~ innerhalb einer angemessenen Frist über Verletzungen der Risikolimiten (...) ».

Ad Cm 100 :
Commentaire : le plan d'action est un outil prévu pour l'audit interne. Les tâches de la

Compliance sont déterminées de manière précise dans le cadre régulatoire et le plan d'action n'est pas approprié pour planifier les activités de la *Compliance*.
Proposition : « (..) des Instituts~~- und Ausarbeitung eines risikoorientierten Tätigkeitsplanes, der durch die Geschäftsleitung zu genehmigen ist. Der Tätigkeitsplan ist auch der internen Revision zur Verfügung zu stellen~~. »

Ad Cms 118, 119 et 120 :
Commentaire : le terme « évaluation des risques » (« *Risikobeurteilung* ») peut entraîner une certaine confusion par rapport au rôle de la révision interne. Nous suggérons de reformuler le chiffre marginal comme suit.
Proposition : remplacer « *Risikobeurteilung* » par « *Beurteilung* ».

Ad Cms 125 – 127 :
Commentaire : les dispositions relatives aux groupes et structures de groupe sont les bienvenues. En revanche, elles devraient être alignées sur le principe 5 des Guidelines/Corporate governance principles for banks du Comité de Bâle sur le contrôle bancaire. Ainsi, les principes de conduite de groupe (échange d'informations, échanges au sein du groupe, uniformisation des documents) devraient être repris dans la circulaire.
L'ASB suggère de reformuler légèrement les chiffres marginaux 125 et 126 en vue de rendre le pilotage des sociétés membres d'un groupe plus pratique.
Proposition : ~~Die Grundsätze und Bestimmungen d~~ Dieses Rundschreiben~~s~~ ~~gelten~~ gilt für Finanzgruppen und -konglomerate („Gruppen") sinngemäss.

Ad Cm 126 :
Commentaire : les deux premières phrases du chiffre marginal 126 sont peu claires et doivent être reformulées de sorte à ce que les banques puissent se conformer aux attentes du régulateur.
Proposition : ~~Die~~ Gruppen müssen die Aufgaben und Verantwortlichkeiten des Oberleitungsorgans und der Geschäftsleitung gemäss diesem Rundschreiben ~~auf Oberleitungs- und Geschäftsführungsebene der~~ für die Einheiten regeln, welche die Gesamtverantwortung für die Führung der Gruppe~~nführung~~ haben. Es ist sicherzustellen, dass Vorgaben bestehen, die eine angemessene Berücksichtigung des Interesses der Gruppe, deren effiziente und harmonisierte Steuerung und entsprechenden Informationsaustausch erlauben und den rechtlichen und organisatorischen Strukturen, den Aufgaben und Verantwortlichkeiten sowie der erforderlichen Unabhängigkeit der jeweiligen Führungsebenen, ~~sowie~~ der Geschäftstätigkeit und den wesentlichen Risiken auf Gruppen- und Einzelinstitutsebene angemessen Rechnung tragen. Dabei sind im Besonderen die Risiken zu berücksichtigen, welche sich aus dem Zusammenschluss mehrerer Unternehmen zu einer wirtschaftlichen Einheit ergeben.

Ad Cm 128 à 134 :
Commentaire : les dispositions relatives à la publication sont par trop détaillées, n'ont pas de valeur ajoutée par rapport aux autres normes traitants du même sujet et vont bien au-delà des principes définis par le Comité de Bâle. Le projet confond les intérêts des actionnaires des sociétés cotées en bourse avec les intérêts des autres parties prenantes (créanciers, mandants, employés, public) qui ont moins de prétentions à

faire valoir en matière de gouvernance d'entreprise. Il n'existe ni base légale, ni intérêt public pour un tel Swiss finish. On relève en outre que le cercle des « autres ayants-droit » n'est pas défini et qu'il n'est pas précisé si la publication doit intervenir au niveau du groupe (ce qui serait à saluer) ou au niveau de chaque institut. On peine à voir l'utilité de la divulgation du processus du recrutement ou d'élection des membres de la direction supérieure, quand c'est bien leur profil et leurs connaissances qui priment.
Proposition : suppression des chiffres marginaux 128 à 134.

Ad Cm 141 :
Commentaire : la publication des honoraires de révision et d'audit pour l'exercice écoulé ne répond à aucun impératif objectif. Au contraire, ceux-ci font l'objet de négotiations entre les cabinets et l'établissement concerné et une telle divulgation entraînerait sûrement un affaiblissement de la concurrence. A terme, les coûts de la révision augmenteront et, par effet ricochet, les coûts des services bancaires pour les clients. De plus, nous sommes d'avis que la relation de confiance entre la société d'audit et la banque s'en trouvera affectée rendant par la une bonne coopération plus difficile.
Proposition : « 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) »

Ad Cm 142 :
Commentaire : ni le concept de « politique d'information », ni le but poursuivi par la FINMA ici ne sont compréhensibles pour l'ASB.
Proposition : suppression du chiffre marginal 142.

Ad Cm 143 :
Commentaire : la publication visée par ce chiffre marginal est déjà contenue dans la Circulaire 2016/1 et, à nouveau, par trop détaillée.
Proposition : suppression du chiffre marginal 143.

Ad Cms 144 et 145 :
Commentaire : l'entrée en vigueur prévue pour le 1er juillet 2016 avec un délai transitoire d'un an est trop court. L'entrée en vigueur devrait être repoussée au 1er janvier 2018 avec un délai transitoire d'un an au minimum.

Principales Observations relatives au projet de Circ-FINMA « Risques opérationnels » et propositions de modifications

Pour plus de clarté nous suivons la numérotation des chiffres marginaux du projet de circulaire ; les propositions de modifications sont soulignées et les suppressions barrées.

En général :

Le projet est trop détaillé et notamment la partie couvrant les risques IT. On passe d'un système fondé sur des principes à un système rigide fondé sur une réglementation détaillée et, par endroit, tatillonne.

Le projet ne contient pas de date d'entrée en vigueur. Celle-ci devrait être similaire à celle de la Circulaire « Corporate Governance » et être alignée sur la période d'exercice usuelle des établissements (1er janvier au 31 décembre). Dès lors, la date d'entrée en vigueur devrait être le 1er janvier 2018 et le délai transitoire d'une année dès celle-ci.

En particulier :

Ad Cm 2 :
Commentaire : la nouvelle définition des risques selon la version révisée n'est plus en ligne avec la définition donnée par le Comité de Bâle. En particulier, la délimitation entre risques réputationnels et risques stratégiques n'a pas été reprise.
Proposition : reprendre l'ancienne définition du Comité de Bâle.

Ad Cm 121 :
Commentaire : la note explicative de bas de page N°8 est inutile puisqu'elle ne contient aucune recommandation. En lieu et place, une référence à la Circ-FINMA « Gouvernance d'entreprise » serait plus indiquée.
Proposition : « (…) Die operationellen Risiken sind zur Gewährleistung der Konsistenz im Rahmen der Risikoidentifikation, der Risikobeurteilung und der Zielsetzung im operativen Risikomanagement einheitlich zu kategorisieren. Diese einheitliche Kategorisierung kann in Anlehnung an Anhang 2 dieses Rundschreibens oder mittels einer internen Terminologie oder Taxonomie erfolgen. »

Ad Cm 129 :
Proposition : faire de chacune des *littera* un chiffre marginal à part entière.

Ad Cm 132 :
Commentaire : faire de chacune des *littera* un chiffre marginal à part entière.

Ad Cm 135 :
Commentaire : le concept informatique devrait être traité également dans la Circ-FINMA « Gouvernance d'entreprise » et non pas dans cadre des principes de gestion des risques. De plus, l'étendue et le contenu du concept informatique devront être spécifiés par la FINMA tant les exigences peuvent être variées. Il semble à l'ASB que la réglementation proposée dans le projet est beaucoup trop détaillée s'agissant des risques informatiques ce qui contredit l'idée d'une réglementation fondée sur des principes. Enfin, s'agissant des banques de plus petite taille, la possibilité doit être donnée d'élaborer le concept IT en partenariat avec les prestataires IT lorsque cette activité a été externalisée.

Ad Cm135.1 :
Commentaire : le concept doit, respectivement ne peut, qu'être établi en conformité avec les normes internationales pertinentes et non pas l'ensemble des normes internationales.
Proposition : « (…) dass das IT-Konzept in Anlehnung an ~~die~~ relevanten internationalen Standards das Vorhandensein der folgenden minimalen Aspekte gewährleistet: (...) ».

Ad Cm 135.1 lit. b à e:
Commentaire : les exigences du concept informatique sont beaucoup trop détaillées. Il appartient aux instituts d'identifier et d'élaborer le concept.
Proposition : suppression des littera b à e.

Ad Cm 135.1 lit. f :
Commentaire : remplacer « processus » par « mesures » en tant qu'il appartient effectivement à la direction d'établir les mesures visant à éduquer les employés.
Proposition : « ~~Prozesse~~Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Verantwortung zur Reduktion von IT-Risiken sowie Einhaltung der IT-Sicherheit und – Verfügbarkeit »

Ad Cm 135.1. lit. g :
Commentaire : la complexité et la fragmentation des systèmes informatiques ne représentent pas en soi nécessairement un risque pour peu que des mesures soient mises en place visant à gérer celles-ci.
Proposition : suppression de la phrase « sowie zur Reduktion der Komplexität und Fragmentierung der IT-Infrastruktur ».

Ad 135.2 lit. a à e :
Commentaire : la réglementation est par trop détaillée s'agissant d'un principe à mettre en œuvre. La circulaire devra contenir une définition de la notion « cyber ». Les « cyber » risques ne constituent pas une classe de risques distincte des autres risques IT. La logique voudrait qu'ils soient intégrés dans le chiffre marginal 135.1.
Proposition : suppression des lit. a à e., alternativement leur déplacement dans la note marginale 135.1.

Ad Cm 135.3 :
Commentaire : en premier lieu, la notion de « données sensibles » (en allemand « *besonders schützenwert* ») est déjà contenue dans la Loi sur la protection des données. Pour éviter une confusion, un autre qualificatif serait approprié. L'exigence des « *penetration tests* » doit se limiter aux systèmes informatiques exposés et non pas à tous les systèmes informatiques en usage. L'ASB doute qu'il existe assez de prestataires de service qualifiés pour tester l'ensemble des systèmes dans un délai approprié et estime que les tests peuvent être conduits systématiquement à l'interne.
Proposition : « Die Geschäftsführung lässt insbesondere in Bezug auf die Sicherstellung eines angemessenen Schutzes der ~~*besonders schützenswerten*~~ sensitiven Daten und exponierten Systeme vor Cyberattacken regelmässig Verwundbarkeitsanalysen und Penetration Testings durchführen. Diese ~~müssen~~ sollten grundsätzlich durch ~~geeignete **externe Dienstleister** durchgeführt werden, können bei Vorhandensein von~~ qualifiziertes Personal mit entsprechenden Ressourcen ~~jedoch auch durch interne Stellen vollzogen werden~~ durchgeführt werden».

Ad Cm 136ss :
Commentaire : la plupart des dispositions concernées par les chiffres marginaux 136ss ont pour objet d'assurer les prestations essentielles en cas de liquidation ou d'interruption grave de l'activité en ce qui concerne les banques de nature systémique. Or, ce principe est déjà réglé, de manière exhaustive, pour les banques systémiques dans la Loi sur les banques et son ordonnance (notamment les articles 60ss). Si de nouvelles mesures sont attendues de la part de celles-ci, il convient de modifier les textes législatifs pertinents et non pas simplement traiter le sujet par voie de circulaire. L'ASB relève en outre, que les chiffres marginaux 136ss traitent ensemble de risques opérationnels et des exigences de stabilité entrainant par la une confusion des thèmes.
Proposition : suppression des chiffres marginaux 136 à 136.3.

Ad Cm 136.1 :
Commentaire : la circulaire introduit les concepts de « fonctions critiques « et « prestations critiques », alors que la Loi sur les banques et l'ordonnance parlent de « fonctions qui ont une importance systémique ». Il appartient à la BNS de définir les banques d'importance systémique et leurs fonctions de nature systémique et il semblerait que la circulaire empiète sur la prérogative de la BNS sur ce point. De plus, il n'est pas explicité si et comment les « fonctions critiques », « prestations critiques » et « fonctions de nature systémique » se complètent ou se différencient l'une de l'autre.
Proposition : supprimer le chiffre marginal 136.1.

Ad Cm 136.2 :
Commentaire : une circulaire de la FINMA ne saurait renvoyer les instituts vers des normes de nature internationale sans les transposer en droit suisse.
Proposition : supprimer le chiffre marginal 136.2.
Proposition alternative: « Die systemrelevanten Banken treffen die hierfür erforderlichen Massnahmen im Rahmen der Notfallplanung (Art. 9 Abs. 2 lit. d BankG i.V.m. Art. 60 ff. BankV). ~~Bestehen zu diesem Themengebiet international anerkannte Standards, so sind diese ebenfalls zu berücksichtigen~~ ».

Ad Cm 136.3 :
Commentaire : l'ASB estime qu'il n'existe aucune justification pour exiger des banques non systémiques l'établissement et la mise à jour régulière d'un inventaire des prestations qu'elles jugent essentielles en cas de liquidation. Il s'agirait d'une trop grande charge de travail pour celles-ci pour un bénéfice / coût trop réduit. De plus, la FINMA ne dispose d'aucune base légale pour imposer de telles mesures.
Proposition : suppression du chiffre marginal 136.3.

Ad Cm 136.4 (début):
Commentaire : le projet ne tient pas compte, s'agissant des risques transfrontières, de la diversité des modèles d'affaires des banques. Le chiffre marginal 136.4 devra être adapté comme suit.
Proposition : « Wenn Banken oder ihre Gruppengesellschaften grenzüberschreitend Finanzdienstleistungen erbringen oder Finanzprodukte vertreiben, sind auch die aus einer Anwendung ausländischer Rechtsvorschriften (Steuer-, Straf-, Geldwäscherei-recht usw.) resultierenden Risiken unter Berücksichtigung des jeweiligen Geschäfts-

modells angemessen zu erfassen, begrenzen und kontrollieren. Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Banken ausländisches Aufsichtsrecht unter Berücksichtigung des jeweiligen Geschäftsmodells einhalten. (…) treffen die Banken die erforderlichen strategischen und organisatorischen Massnahmen zur Risikoeliminierung und -minimierung und passen diese laufend geänderten Bedingungen an. Insbesondere verfügen sie risikobasiert über das notwendige länderspezifische Fachwissen, definieren sie spezifische Dienstleistungsmodelle für die bedienten Länder (…). »

Ad 136.4 (dernière phrase) :
Commentaire : les gérants indépendants ne sont, en aucun cas, mandataires des banques et celles-ci n'ont donc pas à les « former à leur rôles de mandataire ». Il s'ensuivrait une confusion des genres et une grande insécurité juridique. Les gérants indépendants sont des clients « *execution only* ». De plus, l'ASB peine à voir qui sont les « intermédiaires » et « autres prestataires ». Par l'adjonction de formules vagues et indéfinies, on crée de nombreuses charges administratives pour les instituts qui doivent ainsi naviguer à vue et sans sécurité juridique.
Proposition : suppression de la dernière phrase « (…) ~~Les gérants de fortune indépendants, les intermédiaires et d'autres prestataires doivent également être sélectionnés avec soin et formés à leur rôle de mandataires~~ ».

Annexe 3 Traitement des données électroniques des clients

Ad Cm 9ss :
Commentaire : de plus en plus de banques font appel à des prestataires de services externes s'agissant de l'exécution de leurs tâches. Cela est d'autant plus vrai dans le domaine du stockage des données en Suisse ou à l'étranger. L'ASB est d'avis que la question de la protection des données clients mérite une réflexion approfondie et le remaniement de la Circulaire 2008/21 dans ce sens est positif.

Toutefois, la nouvelle version ne tient pas compte de certains éléments clefs en matière de protection des données, en particulier des « Client Identification Data – CID ». En effet, en cas d'outsourcing à l'étranger, la circulaire renvoie dans tous les cas à l'art. 6 de la Loi fédérale sur la protection des données. Or, dans son interprétation de la loi, le Préposé fédéral à la protection des données, va beaucoup plus loin que ce qui est requis par la Circulaire « 2008/7 Outsourcing – banques » et pose des exigences qui ne sont pas en phase avec la réalité. Ainsi, contrairement à ce que statue le projet de nouvelle circulaire, le renvoi vers l'art. 6 de la LPD ne devrait être d'actualité que lorsque les CID ne sont ni anonymisées, ni pseudonymisées. On rappellera que par le processus de pseudonymisation, des CIDs sont changées de sorte à ce que les éléments d'identification ne soient intelligibles qu'en vertu d'une clé d'identification. Des CID anonymisés ou pseudonymisés – pour autant que la clé d'identification demeure en Suisse – ne peuvent pas être considérées comme des données sujettes à l'application de la LPD.
Proposition : reformulation des chiffres marginaux 9ss en ligne avec ce qui précède.

Ad Cm 16 :
Commentaire : l'actualisation de l'inventaire « dans les meilleurs délais » peut, selon la

complexité du cas, apparaître trop rigide.
Proposition : « innerhalb einer angemessenen Frist » en lieu et place de « zeitnah ».

Ad Cm 17 :
Commentaire : le chiffre marginal 17 s'écarte d'une réglementation fondée sur des principes, est inutilement détaillé et s'immisce, sans justification aucune dans l'organisation des établissements.
Proposition : « Es wird vorausgesetzt, dass die Granularität des Inventars der Bank erlaubt, ~~entlang der CID-Kategorien und den daraus resultierenden Sicherheitsvorkehrungen,~~ zu ermitteln »

Ad Cm 33 et note de bas de page 26 :
Commentaire : cette disposition mérite quelques adaptations, car certains termes sont vagues et / ou indéfinis. De plus, il n'existe aucune justification pour établir des sous-catégories de CID : tous les CID sont confidentiels et de nombreuses banques ne disposent plus de comptes à numéro. Les trois premières phrases sont suffisantes.
Proposition (Cm 33): « Die Bank muss über klare Sicherheitsanforderungen für Mitarbeitende, die auf CID zugreifen, verfügen. Es ist regelmässig zu überprüfen, ob die Anforderungen für einen angemessenen Umgang mit CID weiterhin erfüllt sind. Erhöhte Sicherheitsanforderungen müssen gemäss dem *Need-to-Know Prinzip* für privilegierte IT-Benutzer und Anwender mit funktionalem Zugriff 26 auf Massen-CID („Schlüsselmitarbeitenden") gelten. ~~Diese erhöhten Sicherheitsanforderungen sind auch auf privilegierte Anwender mit Zugriff auf höchst vertrauliche Unterkategorien von CID (z.B. chiffrierte Konten) anzuwenden.~~ »
Proposition (ndb 26) : «~~ Insbesondere auch~~ bei erweiterten Zugriffsrechten wie z.B. die Abfrage und Extraktion/Migration von Massen CID ~~grossen Datenmengen~~. »

Ad Cm 35 :
Commentaire : il s'agit ici d'une nouvelle exigence posée par le régulateur en vue d'identifier les personnes ayant accès à un grand nombre de CID. Or, que ce soit par la tenue de fichiers-journaux ou d'autres dispositifs, la mise en œuvre d'une telle exigence sera synonyme de nouvelles charges et dépenses pour les instituts lesquelles ne sont pas justifiées par le but poursuivi.
Proposition : suppression du chiffre marginal 35.

Principales Observations relatives au projet de Circ – FINMA « Rémunération » et propositions de modifications

Pour plus de clarté nous suivons la numérotation des chiffres marginaux du projet de circulaire.

En général :

Le projet ne contient pas de date d'entrée en vigueur. Celle-ci devrait être similaire à celle de la Circulaire « Corporate Governance » et alignée sur la période d'exercice usuelle des établissements (1er janvier au 31 décembre). Dès lors, la date d'entrée en vigueur devrait être le 1er janvier 2018 et le délai transitoire d'une année dès celle-ci.

En particulier :

Ad Cm 20 :
Commentaire : il conviendrait d'énumérer les fonctions de contrôle visées ici.

Ad Cm 46 :
Commentaire : l'instauration de « *claw-back*s » se heurtera à de nombreux obstacles juridiques et pratiques. Le droit du travail est réticent à accepter ce genre de clause ; que faire lorsqu'un récipiendaire se trouvera à l'étranger et soustrait au droit suisse ? De plus, l'instauration de tels « *claw-backs* » heurtera la compétitivité des banques suisses par rapport à leurs concurrents étrangers qui ne connaissent pas de telles barrières. On peine à voir ce qu'en retirerait la place financière suisse ici.
Proposition : l'ASB recommande fortement à ce que la FINMA renonce à l'instauration d'un « claw-back » difficilement praticable. (Sur ce point, l'Association des banques étrangères en Suisse, vu la situation internationale, est d'un avis divergent et ne soutient pas la proposition de l'ASB.) Dans le cas contraire, la FINMA devra impérativement clarifier les concepts, expliquer s'ils se complètent, édicter des règles à suivre pour les contrats de travail futurs et soumettre ces dispositions à un délai transitoire étendu.

Ad Cms 68 et 69 :
Commentaire : en relation avec les nouveautés introduites dans la nouvelle version, le rapport de rémunération devra ainsi également contenir des informations sur les « malus » et « claw-back ». Cela impliquerait une charge énorme pour procéder aux calculs inclus dans le rapport.

* * *

Nous vous remercions vivement de l'attention que vous aurez bien voulu porter à ces lignes et restons bien sûr à votre entière disposition pour toute question que vous pourriez avoir.

Nous vous prions de croire, cher Monsieur, à nos sentiments les meilleurs.

Association suisse des banquiers

Rolf Brüggemann Markus Staub

STELLUNGNAHME DER EXPERTEN ZUM

ENTWURF DES RUNDSCHREIBENS „2016/XX CORPORATE GOVERNANCE“

Der Entwurf des Rundschreibens 2016/xx Corporate Governance – Banken nimmt wichtige Elemente der internationalen Corporate Governance, Risiko und Compliance Diskussion und wirksamer Best Practices auf. Allerdings besteht zentraler Verbesserungsbedarf mit Bezug auf die Berücksichtigung internationaler Standards im Allgemeinen und konkret der Regeln der Kunst im Risiko- und Compliance-Management.

Seit 2009 (Schaffung der ISO Norm 31000 – Risk Management) und 2014 (Schaffung der ISO Norm 19600 – Compliance Management Systems) bestehen internationale Standards, die die Regeln der Kunst im Risiko und Compliance-Management in allen Organisationen wiedergeben. Die SNV hat massgeblich zur Entstehung dieser Standards beigetragen und ist aktuell massgeblich an der Weiterentwicklung dieser Standards beteiligt.

Die ISO Standards 31000 und 19600 sind Management System Standards, die, wie ISO 9001 – Quality Management Systems, die Grundsätze systematischen und wirksamen Managements nach dem Plan-Do-Check-Act Prozess darlegen. Zu den beiden internationalen Standards ISO 31000 und ISO 19600 gibt es keine gleichartigen (also unabhängige, international abgestützte) Alternativen. So ist gemäss der OECD der ISO Standard 31000 de facto der Weltstandard im Risikomanagement (s. OECD Bericht Risk Management and Corporate Governance, 2014, S. 16) und zu ISO 19600 schreibt einer der führenden deutschen Experten, Prof. Peter Fissenewert, dass er davon überzeugt ist, dass ISO 19600 sich in absehbarer Zeit als meistgenutzter globaler Standard für Compliance-Management-Systeme durchsetzen wird (s. http://www.risknet.de/wissen/rezensionen/praxishandbuch-internationale-compliance-management-systeme/cab867763ebdaae3ff0399ef6898ad04/). Die Berücksichtigung beider Standards sollte bezüglich der Terminologie sowie der Grundelemente der Regeln der Kunst erfolgen. Die Standards selber sollen aber nicht explizit erwähnt werden, da jede Organisation frei ist, zu entscheiden, an welchem Regelwerk sie sich ausrichtet. Wichtig ist aber, dass einem anerkannten Regelwerk gefolgt wird (aus Gründen der Transparenz, Messbarkeit, Vergleichbarkeit, Kosteneffizienz und Wirksamkeit).

Wir nehmen im Einzelnen wie folgt Stellung:

1. Die Schweizer Banken, Finanzgruppen und Effektenhändler (die „Adressaten“) sollen angehalten werden, ein anerkanntes Regelwerk festzulegen, nach dem sie ihr Risikomanagement System bzw. ihr Compliance Management System betreiben.

2. Es sind die in ISO 31000 und ISO 19600 international definierten Begriffe zu verwenden. Vorab ist der Begriff „Risikoappetit“, der für die Finanzkrise steht, durch den Begriff Risikoeinstellung (risk attitude) oder Risikotoleranz (risk tolerance) zu ersetzen (s. ISO 31000, Ziffer 2.5, 5.4.4). Weil der Begriff Risikoappetit weltweit zwar genutzt wird, aber inhaltlich völlig unklar ist und alle möglichen Interpretationen zulässt, wurde er bei der aktuellen Revision der ISO 31000 gänzlich aus der Terminologie der Norm gestrichen.

3. Das Rundschreiben ist stark prozessorientiert. Zu kurz kommt die Bedeutung der Vorbildfunktion der Führung (Leadership), die Kultur (risk culture, compliance culture) und die Werteorientierung (values). Führung, Kultur und Werte sind die Kernbegriffe der Regeln der Kunst nach ISO Standards 31000 und 19600. Das Rundschreiben sollte die Bedeutung von Führung (auf allen Stufen), Kultur und Werten klar hervorheben.

4. Einige zentrale Elemente des Risikomanagements nach ISO 31000 sollten konzeptionell Berücksichtigung finden, beispielsweise der Fokus des Risikomanagements auf die breitere Erfassung von Ereignissen (Zwischenfällen) und Entwicklungen (strategische Veränderungen des Umfelds) und zudem auf die zentrale Bedeutung der Risikobewältigung.

5. Wir empfehlen, dass das Oberleitungsorgan einen Risiko- und Compliance Ausschuss bildet und dass bei allen Adressaten ein Mitglied der Geschäftsleitung für Risiko- und Compliance Management verantwortlich ist (Teilzeitanstellung oder bei Adressaten der Aufsichtskategorien 1 bis 3 Vollzeitanstellung). Nur so kann der Spezialität und gleichzeitigen Interdependenz von Risiko und Compliance-Management Rechnung getragen werden.

DIE POST

Die Schweizerische Post AG
Wankdorfallee 4
3030 Bern

Telefon +41 58 386 64 91
www.post.ch

C, Wankdorfallee 4, 3030 Bern

Einschreiben und per E-Mail
Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
3003 Bern

Datum 12. April 2016
Ihre Nachricht
Unser Zeichen 2016.04.0645
Kontaktperson Markus Schumacher
E-Mail markus.schumacher@post.ch
Direktwahl 058 386 64 91

Anhörung zum FINMA-Rundschreiben 2016/x: Corporate Governance – Banken

Sehr geehrter Herr Rütschi

Die Schweizerische Post bedankt sich bestens für die Möglichkeit, an der Anhörung zum FINMA-Rundschreiben 2016/x: Corporate Governance – Banken teilnehmen zu können. Nachfolgend erhalten Sie fristgerecht unsere Stellungnahme.

1 Generelle Bemerkungen

Die Schweizerische Post AG ist als Dachgesellschaft für die einheitliche Führung des Konzerns Post, die Umsetzung der strategischen Ziele des Bundesrates für die Schweizerische Post AG sowie für die Gewährleistung der Grundversorgung gemäss Postgesetzgebung verantwortlich. Damit sie ihre gesetzlichen Verpflichtungen wahrnehmen kann, muss die Schweizerische Post AG gemäss Art. 14 Abs. 2 Postorganisationsgesetz (POG) über die kapital- und stimmenmässige Mehrheit an der PostFinance AG verfügen. In der Verordnung zum POG (VPOG) wird zudem in Art. 2 Abs. 3 konkretisiert, dass die Schweizerische Post AG die Mehrheit der Vertreterinnen und Vertretern im Verwaltungsrat der PostFinance AG zu stellen hat.

Mit Bezug auf diese gesetzlichen Grundlagen finden Sie nachfolgend unsere Bemerkungen zu einzelnen Randziffern des FINMA-Rundschreiben 2016/x: Corporate Governance – Banken.

2 Bemerkungen zu einzelnen Randziffern

Rz 26	„Zudem sollte ein massgeblicher Teil des Oberleitungsorgans nicht am Institut qualifiziert beteiligt sein oder einen qualifiziert Beteiligten vertreten. Die Gläubigerinteressen auf Ebene des Einzelinstituts haben gegenüber abweichenden Eigentümer- oder Gruppeninteressen Vorrang."
Bemerkung	Die VPOG gibt vor, dass der Verwaltungsrat der Post für die Umsetzung der Ziele auch in den Postkonzerngesellschaften verantwortlich ist und die einheitliche Führung des ganzen Konzerns sicherzustellen hat. Konkret müssen im Verwaltungsrat derjenigen Postkonzerngesellschaften, denen die Erfüllung der Verpflichtung zur Grundversorgung übertragen wurde, die Vertreterinnen und Vertreter der Post über die Mehrheit verfügen (vgl. Art. 2 Abs. 3 VPOG). Diese Bestimmung ist auch für die PostFinance AG, welche den Grundversorgungsauftrag Zahlungsverkehr ausübt, anwendbar. Gemäss Erläuterungsbericht der FINMA ist das erforderliche Mass an Unabhängigkeit bewusst offen formuliert, damit der Vielfalt in der Praxis mit Au-

	genmass und massgeschneiderten Lösungen im Einzelfall begegnet werden kann. Wir beantragen, bereits im Rundschreiben eine Formulierung aufzunehmen, die eine Abweichung von einer externen Mehrheit im Verwaltungsrat zulässt, sofern bestehende übergeordnete oder gleichrangige gesetzliche Grundlagen dies erforderlich machen.

Rz 33	„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."
Bemerkung	Im Zusammenhang mit der bereits vorstehend zu Rz 26 eingebrachten Bemerkung ist darauf hinzuweisen, dass ein Mandat und/oder Anstellungsverhältnis im Postkonzern auch künftig nicht als dauernder Interessenkonflikt zu qualifizieren ist.

Rz 38	„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."
Bemerkung	Der Verwaltungsrat der PostFinance AG besteht aufgrund der Vorgabe aus Art. 2 Abs. 3 VPOG aus mehrheitlich abhängigen Mitgliedern (gemäss der von der FINMA zur Anwendung gebrachten Unabhängigkeits-Definition). Mit dieser Ausgangslage ist es nicht möglich, dass die Mehrheit der Mitglieder des Prüf-, Risiko- und Nominationsausschusses des Verwaltungsrates der PostFinance AG unabhängig besetzt werden kann. Gekoppelt mit der Anforderung aus Rz 37 (hinreichende personelle Unterscheidung des Prüfausschusses) hätte die Anwendung des Grundsatzes zur Folge, dass die Ausschüsse nicht mehr in erster Linie aufgrund der Kenntnisse und Erfahrungen im Aufgabenbereich besetzt werden könnten. Wiederum beantragen wir, bereits im Rundschreiben eine Formulierung aufzunehmen, die eine Abweichung in der Besetzung der Ausschüsse zulässt, sofern bestehende übergeordnete oder gleichrangige gesetzliche Grundlagen dies erforderlich machen (vgl. Bemerkung zu Rz 26).

Rz 126	„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 Einzelinstitutsebene angemessen Rechnung tragen. Dabei sind im Besonderen die Risiken zu berücksichtigen, welche sich aus dem Zusammenschluss mehrerer Unternehmen zu einer wirtschaftlichen Einheit ergeben."
Bemerkung	Gemäss dem erläuternden Bericht zum Rundschreiben sieht der Entwurf keine Änderung in der Aufsichtspraxis vor. Wir verstehen dies dahingehend, dass der Postkonzern auch künftig nicht insgesamt als Finanzgruppe zu betrachten ist und sich der Aufsichtsbereich der FINMA auch künftig lediglich auf die PostFinance AG und ihre Tochtergesellschaften beschränken wird.

Wir danken Ihnen für die Kenntnisnahme und Berücksichtigung unserer Anträge und stehen für Fragen selbstverständlich gerne zur Verfügung.

Freundliche Grüsse

Die Schweizerische Post AG

Markus Schumacher
Leiter Corporate Center

Katrin Nussbaumer
Leiterin Regulation

Kopie an:

- *Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK, Frau Karin Schmitter, Kochergasse 6, CH-3003 Bern*
- *Eidgenössische Finanzverwaltung EFV, Herr Frank Schley, Bundesgasse 3, 3003 Bern*

Wir tragen massgeblich dazu bei, dass das Interne Audit ein integraler Bestandteil der Good Corporate Governance ist.

FINMA Rundschreiben 2016/xx, Corporate Governance - Banken

(Corporate Governance, Risikomanagement und interne Kontrollen bei Banken)

	Thema
	II. Begriffe
3	Der **Begriff Kontrollinstanzen** (Randziffer 80) sollte im Teil II unter Begriffe aufgeführt werden, da er auch interne Revision umfasst. Interne Revision ist nicht im Teil VII (welcher Randziffer 80 beinhaltet) sondern im Teil VIII geregelt. Es fehlen **Definitionen** der verwendeten Begriffe. Eine Definition ist notwendig, um die aufsichtsrechtliche Unterschiede der verschiedenen Begriffe erkennen zu können. a) Ausarbeitung (z.B. Rz 41) b) Überwachung (z.B. Rz 42, 43, 44 sowie u.a. Rz 4 für Risikokontrolle) c) Würdigung (z.B. Rz 45, 47) d) Erörterung (z.B. Rz 47) e) Kontrolle (z.B. Rz 49 sowie u.a. Rz 8 für Compliance-Funktion, Rz 10 für Oberleitungsorgan) f) Beurteilung (z.B. Rz 31, 32) • In Anlehnung an FINMA-RS 13/3 Rz: Kritische Beurteilung; verschafft sich einen angemessenen Überblick über den Sachverhalt g) IKS Gemäss HWP Band 1, Teil II Ziff. 6.3.2 umfasst ein **IKS** gemeinhin folgende Bestandteile a.Kontrollumfeld b.Risikobeurteilungsprozesse des Unternehmens c.Rechnungslegungsrelevante Informationssysteme - einschliesslich der damit verbundenen Geschäftsprozesse - und Kommunikation d.Kontrollaktivitäten auf Unternehmens- und auf Prozessebene e.Überwachung der Kontrollen Die verwendete Terminologie zu IKS ist in sich nicht stimmig. So umfasst IKS in Rz 7 vier Teilaspekte (i. Zie-lerreichung, also operative Geschäftsprozesse; ii. Finanzielle Berichterstattung; iii. Risikomanagement; iV. Compliance). In Teil VII (Rz 79) wird unter IKS nur ein Teilaspekt (Risikomanagement) genannt.
4 + 8	Randziffer 4 (für Risikokontrolle) und 8 (für Compliance-Funktion) sind als Aufgaben im jeweiligen Teil II bereits aufgeführt und könnten so im Teil II weggelassen und das RS so entschlackt werden.
5	Die **Risikobegriffe** „Risikotoleranz“ und „Risikoappetit“ sind nicht konsistent zu anderen RS (2008/21, 2008/15, 2008/32). Der Begriff „Risikoappetit“ wird im RS aus unserer Sicht nicht richtig verwendet, sondern entspricht viel eher der „Risikotoleranz“. - Die Begriffe in den verschiedenen Rundschreiben müssen konsistent verwendet werden. - Wir sind der Auffassung, dass die „Risikotoleranz“ dem Risiko entspricht, welches ein Unternehmen bereit ist zu tragen oder tragen kann. Sie diktiert damit die Risikolimiten des Oberleitungsorgans. Der „Risikoappetit“ entspricht dem Risiko, dass ein Unternehmen im Rahmen seiner Möglichkeiten eingehen will. (Diese Auffassung entspricht 1:1 auch der Auffassung der FINMA im RS Corporate Governance Versicherungen 2008/32, Rz. 17) - FINMA-Rundschreiben Corporate Governance Versicherungen 2008/32: „Das Unternehmen legt seiner Grösse und Komplexität angemessene Risikostrategien fest, wobei der Risikoappetit und die Risikotoleranz zu berücksichtigen sind. Die Risikotoleranz begrenzt sich durch die ökonomische Wertverminderung, die ein Unternehmen zu tragen bereit ist oder aufgrund geeigneter Massnahmen tragen kann. Sie hängt ab von den vorhandenen Ressourcen (Kapital, HR, IT) und diktiert die Risikolimiten. Der Risikoappetit umfasst das Risiko, das ein Unternehmen im Rahmen seiner Möglichkeiten eingehen will.“
8	Die Kontrolle der Einhaltung von **Compliance** ist nicht alleinige Aufgabe der Compliance-Funktion (als 2. Ebene IKS) sondern muss zwingend ein Element der 1. Ebene IKS (mit den Elementen i. Steuerung und Kontrolle in den Prozessen und ii. Steuerung und Kontrolle durch die Führung) sein. Die Aufgaben der Compliance-Funktion sollten in Teil VII beschrieben werden.

	III. Geltungsbereich
9	Im Sinne einer besseren Lesbarkeit des Dokumentes wäre es hilfreich hier aufzuführen, welche Randziffern von den Kategorie 4 und 5 Banken nicht oder nur teilweise eingehalten werden müssen.
	IV. Oberleitungsorgan
	A. Aufgaben und Verantwortlichkeiten
10	Sachlogischer wäre für uns, wenn die Geschäftsleitung (siehe Randziffer 12) die **Geschäftsstrategie** (beinhaltet die strategischen Ziele) entwickelt und dem Oberleitungsorgan zur Genehmigung beantragt.
12	Bei wörtlicher Auslegung von Randziffer 12 kann das Oberleitungsorgan **keine eigenen Ideen** entwickeln und nur auf Antrag der Geschäftsleitung über die aufgeführten Punkte entscheiden. Das ist wohl kaum im Sinn der FINMA und sollte angepasst werden
13	Grundsätzlich sollte das Oberleitungsorgan die **Reglemente** erlassen. **Weisungen** sollten durch die Geschäftsleitung, resp. entsprechend Delegierte, erlassen werden, da sie operative Bereiche regeln, resp. detailliertere Ausführungen zu Reglementen darstellen sollten. Daher auch teilweise Überschneidung mit Randziffer 61.
15	Die Wahl resp. Abberufung von Personen in Schlüsselfunktionen durch die Oberaufsicht betrachten wir kritisch. Dies aus mehreren Gründen: - AKV Aufgaben/Kompetenzen/Verantwortlichkeiten: Da diese Personen oft Geschäftsleitungsmitgliedern unterstellt sind, kann dies zu Interessenskonflikten führen (Kontroll- und Schlüsselfunktionen als "Puffer/Manöveriermasse" zwischen GL und VR ist nicht zweckdienlich). - Die Bezeichnung "weiterer Personen" ist sehr offen. Dies kann dazu führen, dass ein grosser Personenkreis der zweiten Führungsebene durch den Verwaltungsrat gewählt, resp. abberufen wird. - Das Durchgriffsrecht des Verwaltungsrats in operative Belange halten wir für problematisch Zwingend aufzuführen ist der Leiter interne Revision (dafür Randziffer 112 streichen). Alternativ gehörten die personellen Entscheide zum CEO bzw. MGL in den Teil V.
16	Das Oberleitungsorgan muss gemäss RS die **externe Prüfgesellschaft** bestimmen. Das steht für uns im Widerspruch mit Art. 698 OR Abs2 sowie dem relevanten Gesetz über verschiedene Kantonalbanken. Wir sind der Meinung, dass das Obligationenrecht auch für FINMA-Rundschreiben zwingend ist. Das heisst, die externe Revisionsstelle ist durch die Eigentümer zu bestimmen. Das Oberleitungsorgan ist für das IKS zuständig (welches gemäss Randziffer 7 aus den Teilaspekten i. Zielerreichung, also operative Geschäftsprozesse, ii. Finanzielle Berichterstattung, iii. Risikomanagement und iV. Compliance besteht). Deshalb Erwähnung von Compliance und Risiko-/Kontrollumfeld doppelt.
17	Der VR sollte – analog zu den übrigen Aufzählungspunkten – nur über **wesentliche** (bzw. bedeutende) Änderungen der Unternehmensstruktur entscheiden. Auch im Falle von Funktionsauslagerungen sollten lediglich wesentliche Auslagerungen im Oberleitungsorgan entschieden werden: „Das Oberleitungsorgan entscheidet über, wesentliche Funktionsauslagerungen,…“
	B. Mitglieder des Oberleitungsorgans
18	Die **Voraussetzungen** für die Mitglieder des Oberleitungsorgans als Ganzes sind zwar wünschenswert, aber bei kleineren Kantonen ohne grossen Finanzplatz schwierig umsetzbar, insbesondere hinsichtlich der Bankerfahrung. Die Umsetzungsfrist von 1 Jahr ist nicht realistisch. Gemäss Rundschreiben muss der Bereich IT kompetent im Oberleitungsorgan vertreten sein. Wir sind der Meinung, dass an dieser Stelle keine einzelnen Themen genannt werden sollen (es gibt auch weitere ungenannte Themen, die wichtig sind). Vielmehr braucht es diversifizierte Kompetenzen im Bankrat, welche in Bezug auf die Geschäftsfelder und Risiken adäquat sind. Die Einhaltung der FINMA Rundschreiben ist jährlich zu prüfen. Während wir mit dem Inhalt dieser Paragraphen als Revisoren natürlich einig sind, stellt sich die Frage, wie guter Ruf, Integrität und Fachkennt-

	nisse praktisch geprüft werden sollen. Zweiter Satz analoge Formulierung wie Randziffer 64 (für GL): … die Oberleitung angemessen sicherzustellen. Es fehlt in der Aufzählung Corporate Governance. Es fehlt eine analoge Anforderung zum persönlichen Verhalten (analog Randziffer 64 für Geschäftsleitung).
	C. Grundsätze der Mandatsführung
31	Unseres Erachtens gehören das Anforderungsprofil CEO sowie Mitglieder der Geschäftsleitung thematisch in den Teil A. Die Genehmigung von Anforderungsprofilen weiterer Schlüsselpersonen (nicht näher definiert) gehören (mit Ausnahme Leiter interne Revision) in den Kompetenzbereich Geschäftsleitung (Randziffer 15).
	D. Arbeitseinteilung und Ausschüsse
36	Eine Abkehr vom „prinzipienorientierten Ansatz" stellt insbesondere diese Randziffer dar, die verlangt, dass Institute der Aufsichtskategorie 1-3 einen **separaten Prüfausschuss und Risikoausschuss** einrichten müssen. Wie im Erläuterungsbericht festgehalten, sieht auch der Basler Ausschuss diese Separierung nur für systemrelevante Banken zwingend vor, für die übrigen grösseren Banken handelt es sich nur um eine Empfehlung. Diese regulatorische Auflage erachten wir als zu strikt. In der Praxis bei grossen Instituten zeigt sich regelmässig für die interne Revision, dass schlussendlich mehrere Ausschüsse über den gleichen Revisionsbericht diskutieren und dass die entsprechenden Verantwortlichkeiten teilweise überlappend sind. Diese Gefahr deutet sich auch in diesem Rundschreiben an. Die Behandlung von Randziffer 43 und 44 im Prüfungsausschuss ist inhaltlich zu grossen Teilen redundant mit Randziffer 48, 49 und 50 im Risikoausschuss. Generell führt eine redundante Behandlung von Sachgeschäften in unterschiedlichen Ausschüssen zu einer Schwächung der Effizienz des IKS, da die jeweiligen Ausschüsse daraus möglicherweise unterschiedliche Steuerungssignale ableiten, was zu Unklarheit und somit Unsicherheit führt. Berichte der Internen Revision und der Prüfgesellschaft beinhalten grossmehrheitlich auch Aspekte des Risikomanagements (dies ist gemäss RZ 115 in diesem Rundschreiben auch verbindlich gemachten Standards des Institute of Internal Auditors auch so vorgeschrieben). Damit beide Ausschüsse ihre Verantwortung wahrnehmen können, müssen somit die Prüfberichte in beiden Ausschüssen besprochen werden. Der Prüfausschuss soll sich von anderen Ausschüssen personell hinreichend unterscheiden. In der Praxis würde es VR Mitglieder geben, die in beiden Ausschüssen sitzen. Da gewisse Themen übergreifend behandelt werden, würde es nicht nur für GL sondern auch für einzelne VR Mitglieder zu Doppelspurigkeiten führen. Zwischen Prüfungsauschuss und Risikoausschuss sind gemäss RS geeignete Informationsflüsse einzurichten, welche eine wirksame gegenseitige Abstimmung und eine angemessene Reaktion auf Veränderungen im Risikoprofil des Institutes ermöglichen. Dieser Informationsfluss ist unseres Erachtens in der Praxis am effizientesten und effektivsten gewährleistet durch Beibehaltung des Status quo ohne Trennung. Gemäss altem RS 2008/24 Interne Kontrolle war die Einrichtung eines Audit Committees (Prüfungsausschuss) verbindlich. Viele Institute haben in der Folge einen um die Risikoaspekte erweiterten Prüfungs- und Risikoausschuss eingerichtet. Hier sollten nicht die Detailbestimmungen der internationalen Standards übernommen werden (mangelnde Flexibilität in der Ausgestaltung der Ausschüsse, Erweiterung VR tendenziell notwendig). Diese Regulierung sollte prinzipienbasiert ausgestaltet werden. Wir empfehlen, dass getrennte Prüfungs- und Risikoausschüsse lediglich für systemrelevante Banken als verbindlich erklärt werden. Die übrigen Banken sollten im Rahmen ihrer Geschäftsmodelle und der personellen Ausstattung selber entscheiden.
41	Die **Richtlinien** zur internen Revision sollten durch die interne Revision erfolgen und durch den Prüfungsausschuss genehmigt werden. Im gleichen Sinne sollte der CFO die Richtlinie zur finanziellen Berichterstattung erstellen und durch die GL dem Prüfausschuss (Antragsbestätigung) und Oberleitungsorgan (Entscheid) beantragt werden (siehe Bemerkung zu Rz 42).
43	Die **Überwachung der Risikokontrolle** sollte institutsspezifisch durch den Prüfausschuss oder den Risikoausschuss (siehe Rz 52) erfolgen.

	In der Aufzählung **fehlende Aufgaben des Prüfausschusses**: - Prozess zur Auswahl bzw. Wiederwahl der Prüfgesellschaft (siehe Rz 16), inkl. Beurteilung der Angemessenheit der Mandatsdauer sowie Empfehlung an das Oberleitungsorgan. - Festlegung und Beurteilung der Honorierung der Prüfgesellschaft.
45	**Planung nächste Prüfperiode** (siehe Randziffer 119) sowie Tätigkeitsbericht interne Revision (Randziffer 123) sollten im Prüfausschuss genehmigt bzw. falls Genehmigung in der Kompetenz Oberleitungsorgan, Antragsbestätigung und Unterbreitung einer entsprechenden Empfehlung durch den Prüfausschuss an das Oberleitungsorgan.
48	Gemäss Randziffer 66 wird das **Rahmenkonzept** durch die Geschäftsleitung ausgearbeitet. Genehmigt wird es gemäss Randziffer 12 durch das Oberleitungsorgan. Entsprechend ist Aufgabe des Risikoausschusses die Beurteilung und Unterbreitung einer entsprechenden Empfehlung an das Oberleitungsorgan.
49	Die **Überwachung des IKS** wird sowohl dem Prüfausschuss (Rz 43) als auch dem Risikoausschuss (Rz 49) zugewiesen.
51	Anstelle von Funktionsträgern (u.a. CRO) ist von **Funktionen** (u.a. Risikokontrolle gemäss Randziffer 89 ff) zu sprechen.
	V. Geschäftsleitung
53	Unseres Erachtens ist die Geschäftsleitung verantwortlich, dass in der operativen Geschäftstätigkeit **alle Aspekte des IKS** (gemäss Rz 7) eingehalten werden (und nicht nur aufsichtsrechtliche Vorschriften).
57	Die Randziffern 57 bis 62 sind **Teilaspekte des IKS** und müssten somit nicht einzeln aufgeführt werden.
59	Siehe Bemerkung zu Randziffer 53.
61	Ergibt sich unseres Erachtens bereits explizit aus Rz 79 (dokumentiertes IKS).
62	Gemäss Randziffer 15 ist das Oberleitungsorgan für **Ressourcen** wie z.B. Infrastruktur und IT verantwortlich und gemäss Randziffer 62 die Geschäftsleitung für die Technologieinfrastruktur. Dies sind für uns widersprüchliche Formulierungen.
	VI. Rahmenkonzept für das institutsweite Risikomanagement
66	Das ganze Kapitel entspricht unseres Erachtens nicht dem Konzept der prinzipienorientierten Aufsicht. Wir würden es begrüssen, wenn hier die Ausarbeitung der Details den einzelnen Banken überlassen würde.
70	Wo findet sich die in dieser Randziffer erwähnte aufsichtsrechtliche Definition?
71	Überschneidung mit Randziffer 67 bezüglich Festlegung von Risikoappetit.
76	Der Risikoausschuss muss sich mindestens jährlich mit dem Rahmenkonzept auseinandersetzen. Die Überprüfung ist dadurch bereits durch Randziffer 48 abgedeckt.
	VII. Internes Kontrollsystem
	Dieses Kapitel umschreibt die Verantwortlichkeiten der ertragsorientierten Geschäftseinheiten (A - first line) und der unabhängigen Kontrollinstanzen (B - second line). Von der Logik her sollte in der **Struktur** auch die interne Revision (third line) hier in das Kapitel VII integriert werden (C).
79	In Sinne der Risikoorientierung sollten sich die Anforderungen bezüglich internem Kontrollsystem auf **wesentliche** (und nicht sämtliche) **Arbeitsprozesse** beziehen. In der **Definition** bestehen Überschneidungen mit den Randziffer 7 und 72. Hier könnte das Rundschreiben entschlackt werden. Die **Terminologie für das IKS** ist zudem generell gehalten. Die Formulierung im letzten Satz impliziert, dass zur Steuerung von (identifizierten und gemessenen) Risiken ausschliesslich die Varianten Minderung bzw. Transfer zur Verfügung stehen und die Varianten (bewusste) Akzeptanz und Vermeidung nicht zur

	Verfügung stehen. Anstelle von unabhängig sollte eher von eigenständigen Kontrollinstanzen gesprochen werden.
80	In unserer Wahrnehmung wird hier der Ansatz der ‚**3 lines of defense**' eingeführt, ohne dies explizit so zu nennen. Dies ist für uns nachvollziehbar. Es kann hier noch angefügt werden, dass nicht alle Bereiche der ‚first line' ertragsorientiert sind, z.B. die Informatik, HR, etc.
81	Die **Kontrollfunktion der ‚first line'** sind hier generisch gehalten. Aus Sicht der internen Revision ist dies klar die wichtigste Verteidigungslinie; sind hier die Kontrollen nicht defniert oder werden sie nicht angemessen durchgeführt, sind die weiteren Verteidungslinien meist zu spät für Interventionen. Aus diesen Gründen würden wir hier eine klarere Einordung oder Beschreibung der Beziehung/Aufgaben/Verantwortlichkeiten zwischen der ersten und zweiten Verteidigungslinie erwarten und was konkret gemeint ist mit 'systematischer Ueberwachung' (RZ89) oder ‚Rolle als unabhängige Kontrollinstanz' (RZ 103).
84	Hier schlagen wir vor, dass dieselbe Formulierung wie in der Randziffer 111 verwendet wird: Die unabhängigen Kontrollinstanzen (2. Ebene IKS) sind der Grösse, Komplexität und dem Risikoprofil des Instituts entsprechend **ausgestattet** sein. Wir begrüssen den Hinweis auf die regelmässige **Aus- und Weiterbildung**.
88	Die **Funktion des CRO** lediglich auf die Risikokontrolle zu beschränken, macht keinen Sinn. In der Praxis sind diese Funktionen der ‚second line' generell für das ganze Risk Management verantwortlich. Es kann aus Sicht der internen Revision durchaus Sinn machen, dass die Front Kreditanträge bis zu einer bestimmten Höhe bewilligen kann. Für grössere Engagements ist dann ein Credit Office (CRM) oder der CRO verantwortlich, während sehr grosse Limiten zum Beispiel vom Risk Ausschuss gesprochen werden. Wir empfehlen, das Wording auszuweiten auf: der CRO ist <u>auch</u> für die Risikokontrolle verantwortlich. Obwohl es die interne Revision nicht direkt betrifft, erachten wir die Vorschrift, dass der **CRO Teil der Geschäftsleitung** sein muss, als zu starken Eingriff in die Autonomie der Institute. Dies ist in der Praxis häufig so und kann Sinn machen, aber es muss nicht.
89	Hier werden verschiedene Aufgaben der **Risikokontrolle** zugewiesen, die abhängig von der gewählten Organisationsform auch anderen unabhängigen Kontrollinstanzen zugewiesen werden können. So hat z. B. die „Überwachung von Systemen für die Einhaltung von aufsichtsrechtlichen Vorschriften" (Rz 92) nicht zwingend durch die Risikokontrollfunktion zu erfolgen, sondern kann einer anderen unabhängigen Kontrollinstanz wie der Compliance zugewiesen werden. Anderseits fehlen Themenbereiche wie **OpRisk** Management. Die spezifischen **Aufgaben der Compliance** sind nicht definiert und die Aufgabenteilung zwischen Compliance und Risikokontrolle ist nicht spezifiziert. Das gegenwärtige Wording kann sogar dahingehend interpretiert werden, dass die Risikokontrolle auch für Compliance Risiken zuständig ist.
96	Diese **Ueberwachungsaufgabe** kann auch der internen Revision zugewiesen werden. Die Risikokontrolle kann allenfalls die Einhaltung überwachen.
	VIII. Interne Revision
104 - 124	Wie im Begleitschreiben erwähnt, hätten wir es begrüsst, wenn die neuen **Standards des Basler Ausschusses** über die interne Revision bei Banken ebenfalls in dieses neue Rundschreiben eingeflossen wären. Wünschenswert wären hier im Sinne der Corporate Governance eine Präzisierung der Kommunikation mit dem Prüfungsausschuss, z.B. direkter Zugang, Art und Weise der Kommunikation, Meetings ohne Geschäftsleitung etc.
119	Es ist korrekt, dass die interne Revision die Prüfziele und die **Prüfplanung** für die Prüfperiode durchführt. Nicht erwähnt im Rundschreiben und für ein umfassendes Rundschreiben über Corporate Governance unseres Erachtens notwendig, ist ein Vermerk, dass die interne Revision die spezifischen Prüfbedürfnisse des Oberleitungsorgans und des Prüfausschusses berücksichtigen und die Prüfbedürfnisse der Geschäfts-

	leitung zumindest in Erwägung ziehen soll.
121	Auf die Forderung einer **Mehrjahresplanung** sollte verzichtet werden, weil sie weder einem Standard noch einer best practice entspricht. In der Tat kann man argumentieren, dass ein solcher Mehrjahresplan der Forderung einer risikoorientierten Prüfung widerspricht, da limitierte Resourcen für Prüfungen mit tiefem Risiko und tiefer Materialität verwenden werden müssen. • Standards - BCBS: The internal audit function in banks (Juni 2012) Ziff. 31: "annual audit plan that can be part of a multi year plan. … plan should be updated at least annually (or more frequently) - IIA: PS 2010.A.1: Die Prüfplanug der internen Revision muss auf Basis einer dokumentierten Risikobeurteilung erfolgen, die mindestens einmal pro Jahr durchzuführen ist. Der Input der leitenden Führungskräfte, der Geschäftsleitung und des Ueberwachungsorgans müssen dabei berücksichtigt werden. • Best practice - SVIR: In der Enquete 2011 war ein mittelfristiger Prüfplan noch ein Kriterium für die Ausrichtung der jährlichen Prüfplanung. Die aktuelle Bedeutung war zwar noch gegeben, die künftige Bedeutung nahm aber ab. In der Enquete 2014 war eine mittelfristige Planung bereits kein Kriterium mehr. 2011 erfolgte bei 79 % die Prüfplanung mit einem Jahr oder weniger. 2014 war dieser Wert bereits 82 %. - PwC State of the IA profession study 2015: Kein Hinweis, dass Mehrjahresplanung einen Beitrag zur Wertschöpfung liefert. Im Bereich der Prüfstrategie der externen Revision für die FINMA besteht zumindest für die aufsichtlichsrechtlichen Prüfungen eine Mehrjahresstrategie, welche mit der internen Revision abgestimmt wird.
	IX. Gruppenstruckturen
127	Wir schätzen es, dass die Rolle der internen Revision in der Gruppe unverändert geblieben ist.
	X. Offenlegung
128	Die **Offenlegungspflichten** der Banken werden grundsätzlich durch die Geschäftsberichte wahrgenommen. Zudem besteht mit dem FINMA Rundschreiben ‚Offenlegung Banken' bereits ein regulatorisches Rahmenwerk. Aus Sicht der Prüfung sollten alle Offenlegunspflichten im bestehenden Rundschreiben Offenlegung zusammengefasst werden und hier ersatzlos gestrichen werden. Dies verhindert Doppelspurigkeiten und allfällige Unterschiede in der Prüfung.

Wir tragen massgeblich dazu bei, dass das Interne Audit ein integraler Bestandteil der Good Corporate Governance ist.

FINMA Rundschreiben 2008/21, Operationelle Risiken Banken

(Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken)

Rz	**Thema**
	Allgemeine Kommentare
	Das neue Rundschreiben ist in vielen Bereichen zu detailliert. Dies widerspricht der bisherigen prinzipienorientierten Aufsicht und erreicht nicht das Ziel, diese Rundschreiben zu straffen.
	Begriff
2	Wir können nicht nachvollziehen, warum hier nicht die bisherige und bewährte **Definition** des Basler Ausschusses verwendet wird. Die im Rundschreiben verwendete Definition ist limitiert auf ‚Verluste'. Nicht erfasst sind dadurch neben Bussen auch andere Formen von Sanktionen. Wir schlagen vor, die bisherige Definition zu verwenden.
	Grundsatz 1: Kategorisierung und Klassifizierung von operationellen Risiken
122	Die **Messung, Bewirtschaftung und Limitierung** von operationellen Risiken ist naturgegeben nicht nur quantitativ möglich. Trotzdem verlangt RZ 71, dass alle Risikokategorien limitiert werden müssen. Es verbleibt unklar, wie das konzeptionell geht, auch unter Zuhilfenahme des Konzeptes der Eintretens Wahrscheinlichkeit und des Ausmasses, und welche Basis anzuwenden ist.
	Grundsatz 4: Technologieinfrastruktur
135	Aufgrund der erhöhten Risiken im Bereich **Cyber-Risk** ist die Aufnahme des Themas im Rundschreiben verständlich. Der verwendete Detaillierungsgrad ist jedoch eine Abkehr vom prinzipienbasierten Ansatz. Wir bevorzugen auch in Zukunft einen prinzipienorientierten Ansatz, welcher die unterschiedlichen Umstände der Banken angemessen berücksichtigen lässt. Daher sind unseres Erachtens die detaillierten Ausführungen zu streichen um die neuen Rundschreiben - wie gewünscht - zu straffen.
135.1	Die detaillierten Anforderungen an das **IT Risikomanagement Konzept** unter dieser Randziffer sind gemäss Erläuterungsbericht an einschlägigen internationalen Standards angelehnt. Das Cobit Framework ist spezifisch erwähnt. Wir empfehlen, die entsprechende Fussnote zu löschen um zu verhindern, dass die Bank gegenüber der externen Revision nicht nur die Einhaltung des Rundschreibens sondern auch noch die Einhaltung des Cobit Frameworks bestätigen muss.
135.2	Die Fussnote 16 definiert, dass das **Konzept** zu den **Cyber Risiken** als Bestandteil des IT Konzepts geführt werden kann. Für uns ist Cyber Risk ein Teil der IT Risiken. Entsprechend kann der Grundsatz zu Cyber Risiken unter Randziffer 135.1 abgehandelt werden oder sich hier auf den Grundsatz beschränken. Rz 135.2 lit. a – lit. e ist zu streichen.
135.3	Die Formulierung ‚**besonders schützenswert**' ist in anderen Industrien (z.B im Datenschutzgesetz) bereits definiert. Damit es zu keinen Unklarheiten kommt, sollte eine andere Formulierung gewählt werden, zum Beispiel ‚sensible Daten'. Als Revisoren befürworten wir die regelmässige Verwendung von Instrumenten wie Verwundbarkeitsanalysen und **Penetration Tests**. Die hier gewählte Formulierung ist jedoch zu offen und kann dahingehend interpretiert werden, dass solche Tests für alle Systeme durchgeführt werden sollen. Dies wäre weder operativ möglich noch finanziell tragbar. Wir empfehlen, diese Tests nur für ‚exponierte' oder Kernapplikationen anzuwenden. Den Vermerk auf ‚**externe Dienstleister**' für Penetration Tests verstehen wir nicht. Die Gewähr für einwandfreie Geschäftsführung verpflichtet die Bank bereits heute ganz klar, die nötigen Schutzmassnahmen für Daten und Systeme zu treffen. Wie sie dies sicherstellt, sollte dem einzelnen Institut überlassen werden. Der Passus sollte wie folgt präzisiert werden: „Die Geschäftsführung lässt insbesondere in Bezug auf die Sicherstellung eines angemessenen Schutzes der ~~besonders schützenswerten~~ sensiblen Daten und exponierten Systeme vor Cyberattacken regelmässig Verwundbarkeitsanalysen und Penetration Testings durchführen. Diese ~~müssen~~ sollten grundsätzlich durch qualifiziertes Personal mit entsprechenden Ressourcen ~~geeignete externe Dienstleister~~ durchgeführt werden~~. können bei Vorhandensein von qualifiziertem Personal und Ressourcen jedoch auch durch interne Stellen vollzogen werden.~~"

	Grundsatz 5: Abwicklung und Sanierung von (systemrelevanten) Banken
136	Die Abwicklung und Sanierung **(too big to fail)** von systemrelevanten Banken ist ein wichtiges Thema für den Finanzplatz. Die individuellen Auflagen und von der FINMA bewilligten Pläne sind jedoch so Institut-spezifisch und bereits so im Detail geregelt (Bankengesetz Art. 8, Bankenverordnung Art. 60), dass wir den Sinn dieses noch einmal ausformulierten Themas in diesem Rundschreiben nicht verstehen. Es besteht die Gefahr, dass die jährliche Prüfung dieses Rundschreibens zu Missverständnissen und Rückfragen führen wird. Unseres Erachtens, können daher die Randziffern 136 bis 136.3 ersatzlos gestrichen werden.
136.1	Die Begriffe ‚**kritische Funktion**' und ‚**kritische Dienstleistung**' sind möglicherweise unterschiedlich bei den als systemrelevant eingestuften Instituten. Zudem sind sie nicht definiert, womit Raum für Interpretationen besteht.
136.2	Dass **internationale Standards ebenfalls verbindlich** erklärt werden, erachten wir als nicht angemessen. Es ist nicht klar, welche damit gemeint sind. In der Anwendung besteht das Risiko, dass der Prüfer zum eigenen Schutz die global striktesten Standards anwenden wird. Zudem hebelt diese Regelung die entsprechenden Standards der Schweizerischen Bankiervereinigung aus. Der Begriff ‚ebenfalls' sollte durch ‚angemessen' ersetzt werden
	Grundsatz 6: Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft
136.4	Wir können nachvollziehen, warum das **Cross-Border** Thema spezifisch in das Rundschreiben aufgenommen worden ist. In der Praxis zeigt sich jedoch, dass diese Dienstleistung in den verschiedensten Variationen wahrgenommen wird und durch die vorgeschlagene Formulierung den verschiedenen Geschäftsmodellen und Risiken (Risiken bezüglich der gewählten Märkte, der aktiv oder passiv angebotenen Produkte, der Abwicklung der Transaktionen, und der lokalen regulatorischen Auflagen) nicht gerecht - und aus unserer Sicht nicht geprüft - werden kann. Um keine Unklarheiten zu schaffen, sollte diese Randziffer gestrichen werden. Alternativ müssten die Definitionen massiv ergänzt werden oder durch Hinweise auf die jeweiligen Geschäftsmodelle relativiert werden.
	Anhang 03, Umgang mit elektronischen Kundendaten
	Grundsatz 5: Absatz d) Liste von Schlüsselmitarbeitenden
35	Dass ‚**einzelnen Transaktionen bzw. Zugriffe den einzelnen Benutzern zuzuordnen**' sind, wird sich in der Praxis nur mit grossem administrativen Aufwand umsetzen und prüfen lassen und in der Regel Anpassungen an den Systemen bedingen. Dieser letzte Satz sollte gestrichen werden.

Wir tragen massgeblich dazu bei, dass das Interne Audit ein integraler Bestandteil der Good Corporate Governance ist.

FINMA Rundschreiben 2010/1, Vergütungssysteme

(Mindeststandards für Vergütungssysteme bei Finanzinstituten)

RZ	**II. Geltungsbereich**
Rz6	Die Erhöhung des **Schwellenwertes** von Fr. 2 Mrd auf Fr. 10 Mrd für die zwingende Umsetzung des Rundschreibens begrüssen wir. Die definierten Grundsätze erachten wir nach wie vor als relevant für die Branche. Als Kontrollfunktion werden wir uns weiterhin dafür einsetzen, dass diesen Leitlinien weitgehend gefolgt wird.
	IV Grundsätze
Rz20	Obwohl in der Rz 58 eine Definition von ‚**Leiter von Kontrollfunktionen**' aufgeführt ist, bestehen hier unseres Erachtens Unklarheiten, welche unterschiedliche Interpretationen zulassen. Grosse Banken haben zum Teil IKS Teams in den einzelnen Divisionen oder sogar bei Geschäftseinheiten angesiedelt. Die Vergütung deren Leiter ist eine operative Aufgabe und sollte klar nicht vom Verwaltungsrat genehmigt werden. In Anbetracht der klar genug definierten Grundsätze für eine angemessene Kompensation kann die Ausweitung auf Leiter Kontrollfunktionen gestrichen werden. Alternativ müsste mit Einschränkungen wie ‚Leiter von Kontrollfunktionen auf Gesamtbankstufe' oder ähnliche gearbeitet werden um die nötige Klarheit zu vermitteln.
Rz46	Grundsatz 6 Die generelle Einführung eines **Malus/ Claw Back** geht uns zu weit und sollte entfernt werden. Diese Bestimmung mag in bestimmten Instituten - insbesondere für international tätige Banken - sinnvoll sein. In vielen kleinen und mittleren Banken sind die variablen Elemente der Kompensationssysteme nicht von einer Bedeutung, welche eine solche grundsätzliche Regelung notwendig machen. Wir fürchten auch den administrativen Aufwand dieser Regelung, welche nicht nur eine Anpassung des ganzen internen Frameworks bedingen würde sondern allenfalls auch die Arbeitsverträge aller Mitarbeitenden. Unseres Erachtens wird dies auch zu höheren Rechts- und Steuerrisiken führen. Diese zusätzliche Komponente scheint uns auch nicht mit dem Grundsatz 2 vereinbar, dass Vergütungssysteme einfach und transparent ausgestaltet sein sollen. Alternativ könnte man diese Klausel auf Risk Taker beschränken, welche den Geschäftsverlauf aktiv beeinflussen können und ein Interesse am langfristigen Erfolg der Bank haben sollten. Eine andere Option wäre das Festlegen von relativen oder absoluten Schwellenwerten der variablen Entschädigung als Teil der gesamten Kompensation als Startpunkt der Claw Back Regelung. Dies wäre jedoch eine Abkehr von der bewährten prinzipienorientierten Aufsicht und könnte wahrscheinlich rasch umgangen werden.

UBS

UBS AG
Postfach
8098 Zürich
Tel. +41-44-234 11 11

Markus U. Diethelm
Group General Counsel
Member of Group Executive Board
Tel. +41-44-234 2060
Fax +41-44-234 8715
markus.diethelm@ubs.com

www.ubs.com

FINMA
D 0271334

Eidgenössische Finanzmarktaufsicht
FINMA
Herr Peter Rütschi
Laupenstrasse 27
3003 Bern

FINMA
ORG 25. APR. 2016 SB
BB
Bemerkung:

Zürich, 20 April 2016

Stellungnahme zu den Entwürfen der revidierten Rundschreiben zu 'Corporate Governance – Banken' / 'Operationelle Risiken' und 'Vergütungssysteme'

Sehr geehrter Herr Rütschi

Herzlichen Dank für die Einladung zum Entwurf der revidierten Rundschreiben Stellung zu nehmen und für die Verlängerung der Eingabefrist bis 20. April 2016.

Die UBS unterstützt das Bestreben der FINMA, die internationalen Entwicklungen im Bereich der Corporate Governance in die revidierten Rundschreiben einfliessen zu lassen. Für den Finanzplatz Schweiz ist eine zeitgemässe, international anerkannte Regulierung wichtig. Wir erachten die Stossrichtung der Anpassungen in weiten Teilen angebracht, möchten aber zu einigen Punkten Anpassungsvorschläge unterbreiten. Zur besseren Übersicht haben wir unsere Eingabe in "Wichtigste Punkte" (Anhang 1) und "Weitere Kommentare" (Anhang 2) aufgeteilt.

Wir hoffen, dass unsere Kommentare dienlich sind und stehen für die Klärung allfälliger Fragen jederzeit gerne zur Verfügung.

Freundliche Grüsse

UBS AG

Dr. Markus Diethelm
Group General Counsel

Dr. Luzius Cameron
Group Company Secretary

cc:
Ernst & Young AG, Patrick Schwaller, Maagplatz 1, P.O. Box, 8010 Zurich
UBS AG, Mark Stennett, Bahnhofstrasse 45, P.O. Box, 8001 Zurich
UBS AG, Markus Ronner, Pelikanstrasse 6/8, P.O. Box, 8001 ZurichBeilagen erwähnt

UBS

Anhang I

Rundschreiben Corporate Governance / Operationelle Risiken / Vergütungssysteme

Einleitende Bemerkungen

- Wir erachten die Anpassung an internationale Standards als sinnvoll. Da die Bankenlandschaft und Organisationsformen sehr unterschiedlich sind, sollten die Vorschriften unseres Erachtens in Form von prinzipienbasierten Regelungen in die Rundschreiben aufgenommen werden. Unseres Erachtens enthalten die Rundschreiben teilweise jedoch zu detaillierte Vorgaben und entsprechen nicht dem prinzipienorientierten Ansatz, welchen die FINMA sonst verfolgt.
- In zahlreichen Rz., z.B. Rz. 18 und 19 des RS Corporate Governance, werden aktienrechtliche Regelungen (zusätzlich) ins Aufsichtsrecht überführt oder gar zum Aktienrecht teilweise widersprechende Regelungen stipuliert (Rz. 26). Das schafft Konflikte zwischen dem Aufsichts- und Privatrecht, was vermieden werden sollte. In den Fällen, in denen es zudem fraglich ist, ob eine entsprechende aufsichtsrechtliche Grundlage besteht, sollte auf eine Regelung im RS unseres Erachtens verzichtet, auf die gesetzliche Regelung verwiesen oder allenfalls nur der Grundsatz wiederholt werden.
- Der Entwurf weist viele Aufgaben dem Oberleitungsorgan zu, welche operativer Natur sind und daher von der operativen Führung wahrzunehmen sind. Insbesondere bei grossen Finanzkonzernen erscheinen unseres Erachtens eine Reihe von Regelungen nicht als stufengerecht oder aktienrechtlichen Regelungen (Art. 716a OR) bzw. der dort vorgesehenen Möglichkeit der Delegation (Art. 716b OR) zu widersprechen. Diese Regelungen können nicht mittels eines aufsichtsrechtlichen Rundschreibens abgeändert werden. Soweit aufgrund der aktienrechtlichen Ordnung im RS Präzisierung zur Aufgabenteilung möglich sind, bedarf es unseres Erachtens zwingend der Möglichkeit der Delegation dieser Aufgaben, um die in den Grosskonzernen heute tatsächlich gelebte Organisationsstruktur abbilden zu können. (Beispiel Rz. 13: Erlass von Weisungen durch das Oberleitungsorgan, was für grössere Institutionen nicht praktikabel ist).
- Der Geltungsbereich der Rundschreiben ist teilweise unklar. So z.B. die Frage, ob die Rundschreiben für die Finanzgruppe oder auch für die jeweiligen Tochtergesellschaften (mit Banklizenz und den erforderlichen Eigenmitteln von CHF 10 Milliarden) gelten. Soweit diese auf Tochtergesellschaften mit Bank- oder Effektenhändlerlizenz Anwendung finden, sollte unseres Erachtens entweder im Zirkular oder im Erläuterungsbericht ausdrücklich klargestellt werden, dass die RS nicht für ausländische Tochtergesellschaften gelten, da aufgrund der blossen Konsolidierung keine direkten Verpflichtungen hinsichtlich Organisation usw. abgeleitet werden können.
- Einzelne Begriffe überlassen unseres Erachtens einen zu grossen Ermessensspielraum (z.B. 'Massen-CID'/ 'höchst vertrauliche Unterkategorien von CID' und 'erweiterte Zugriffsrechte'), insbesondere bezüglich deren Anforderungen und entsprechend auch den Auswirkungen. Wir empfehlen, die Begriffe klarer zu umzuschreiben.
- Wenn auf internationale Standards verwiesen wird, sollte der Standard, so konkret wie möglich genannt werden (vgl. z.B. Rz. 136.2 RS Operationelle Risiken).

Rundschreiben Corporate Governance

- Rz. 5: Der Risikoappetit beinhaltet sowohl quantitative wie qualitative Überlegungen und wird sowohl pro jeweilige Risikokategorie als auch auf Institutsebene festgelegt. Da es Risiken gibt, bei denen eine quantitative Einschätzung nicht möglich ist (z.B. Reputationsrisiken), empfehlen wir, hierzu Ausnahmen vorzusehen.
- Rz 8: Die Funktion von Compliance lässt sich unseres Erachtens nicht auf die Kontrolle reduzieren, sondern beinhaltet zusätzlich auch die Unterstützung und Beratung der Geschäftsleitung bzw deren Mitarbeiter in der Einhaltung regulatorischer und interner Vorschriften sowie der Beachtung marktüblicher Standards und Standesregeln (wie auch in den Rz 99 ff korrekt beschrieben). Ein limitieren der Compliance Funktion auf Kontrollen könnte den falschen Rückschluss auf Verantwortlichkeit zur Einhaltung regulatorischer und interner Vorschriften zulassen.

- Rz. 15-17: Die Ausführungen zum Oberleitungsorgan enthalten weitgehende Kompetenzausweitungen zulasten dieses Organs. So werden ihm operative Verantwortlichkeiten übertragen (z.B. für die Infrastruktur und die IT) sowie das Erlassen von Weisungen. Es ist unbestritten, dass das Oberleitungsorgan verantwortlich ist für die Strategie und die entsprechenden Ressourcen, welche für die Umsetzung notwendig sind (soweit sich dies aus Art. 716a OR ergibt). Demgegenüber ist die Geschäftsleitung (und nicht das Oberleitungsorgan) für sämtliche operativen Entscheide zuständig. Dies darf nicht vermischt werden.
- Rz. 26: Die vorgeschlagene Regelung widerspricht der grundlegenden gesellschaftsrechtlichen Ordnung des OR und umso mehr noch jener bei Personengesellchaften. Im Bankengesetz fehlt u.E. eine Grundlage, welche eine solche Einschränkung der Privatautonomie erlauben würde. Der zweite Satz widerspricht der gesetzlichen Regelung der Sorgfalts- und Treuepflicht des Verwaltungsrates, welche im Interesse der Gesellschaft erfolgen muss (Art. 717 OR).
- Rz. 30-33: Die Frage, wie die Organpflichten auszuüben sind, sollte unseres Erachtens nicht Gegenstand detaillierter aufsichtsrechtlicher Regulierung sein.
- Rz. 34-35: Wir sind der Meinung, dass die Regelungen über das Ziel hinausschiessen und die gesetzliche Grundlage fraglich erscheint. Ausser einem guten Ruf und der Gewähr für eine einwandfreie Geschäftstätigkeit sollten keine weiteren Anforderungen an den Präsidenten des Oberleitungsorganes gestellt werden. Ausserdem sollte nicht dem Präsidenten allein die Verantwortung für das Funktionieren des Gremiums übertragen werden, letztlich ist jedes Mitglied dafür verantwortlich.
- Rz. 36 sollte für Finanzgruppen mit systemrelevanten Banken als Tochtergesellschaften nur auf Gruppenstufe, jedoch nicht auf Stufe Einzelinstitut gelten, da dies sonst die gruppenweite Anwendung der Vergütungspolitik erschweren würde. Ausserdem sollte die Regelung auf den Vergütungs- und Nominationsausschuss beschränkt werden.
- Rz. 38: Für den Nominationsausschuss sollte der Präsident des Oberleitungsorgans als Vorsitzender zugelassen sein. Er erscheint uns für diese Position geradezu als prädestiniert.
- Rz. 88 schreibt vor, dass der CRO ausschliesslich für die Risikokontrolle zuständig ist. Wir sehen im Zusammenführen der Compliance Funktion und der Risikokontrolle wertvolle Synergien (z.B. spezialisiertes Finanzwissen und rechtliche Expertise), um Risiken zu erkennen und entschärfen zu können. Die Risikokontrollfunktion sollte daher mit der Compliance-Funktion eine Geschäftseinheit unter der Leitung des CRO bilden können.
- Rz. 109: Es sollte zulässig sein, die interne Revision in einer der zur Finanzgruppe gehörenden Service Company zu führen.
- Rz. 128ff: Die Bestimmung führt zum heutigen Recht zusätzliche Publikationspflichten ein. Unseres Erachtens fehlt hierfür die gesetzlichen Grundlage. Davon abgesehen erscheinen uns die Offenlegungsvorschriften der Banken bereits genügend detailliert geregelt. Wir beantragen deshalb, diese Rz. zu streichen.

Rundschreiben Operationelle Risiken

- Rz. 136 ff: In diesen Bestimmungen werden die Frage und Regelung von operationellen Risiken und die Anforderungen an die Systemrelevanz vermischt. Die Sicherstellung der Fortführung von systemrelevanten Funktionen (SIFs) gehört nicht zu diesen operationellen Risiken und sollte entsprechend nicht in diesem Rundschreiben geregelt werden.
- Bei den operationellen Risiken geht es unter anderem um die Sicherstellung der 'Operational Continuity of Critical Shared Services', d.h. der operationellen Fortführung bei technischen oder anderen Auswirkungen nicht wirtschaftlicher oder finanzieller Art, bis zur Wiederherstellung des ordentlichen Zustands nach einem Schadensereignis. Wir beantragen daher die entsprechenden Rz. zu überarbeiten und auf die erwähnten 'Critical Shared Services' auszurichten.

Rundschreiben Vergütungssysteme

- Rz. 6: Der Geltungsbereich dieses Rundschreibens erscheint uns unklar. So bleibt offen, ob das Rundschreiben nur für die Finanzgruppe oder auch für die Tochtergesellschaften mit Bankenlizenz und erforderlichen Eigenmitteln von CHF 10 Milliarden gelten soll. Da die FINMA gemäss Ihrer Medienmitteilung vom 1. März 2016 von den "beiden Grossbanken" spricht, darf angenommen werden, dass das Rundschreiben nur auf die Finanzgruppe und nicht auf einzelne Tochtergesellschaften Anwendung finden soll.
- Rz. 46: Unseres Erachtens sollte diese Bestimmung auf das Senior Management mit vergleichsweise hohen Gesamtvergütungen beschränkt werden. Aus Gründen der Rechtssicherheit sollten zudem die folgenden Punkten präzisiert werden:
    - Der Tatbestand für eine Rückforderung sollte möglichst genau umschrieben werden.
    - Es sollte bestimmt werden, wer die Rückforderungen auslöst (FINMA oder Finanzinstitut).
    - Die Frist, innert welcher eine Rückforderung möglich ist, muss bestimmt sein. Wir schlagen eine Frist von drei Jahren vor.
    - Mit der Bezeichnung "bereits ausbezahlten variablen Vergütungen" wird zudem eine mit der Rechtsordnung kaum vereinbare Rückwirkung auf sämtliche in früheren Jahren geleisteten Vergütungen geschaffen, welche aufgrund fehlender vertraglicher Vereinbarungen nicht durchsetzbar wäre. Eine Übergangsregelung wäre zu begrüssen.

Konsultation FINMA Rundschreiben 2016/X Corporate Governance - Banken

Referenz	Originaltext	Kommentar UBS
II. Begriffe Rz. 5	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.	Der Risikoappetit beinhaltet sowohl quantitative wie qualitative Überlegungen und wird sowohl pro jeweilige Risikokategorie als auch auf Institutsebene festgelegt. Da es Risiken gibt, bei denen eine quantitative Einschätzung nicht möglich ist (z.B. Reputationsrisiken) empfehlen wir hierzu Ausnahmen vorzusehen. Änderungsantrag: Der Risikoappetit wird - Ausnahmen vorbehalten - sowohl pro jeweilige Risikokategorie als auch auf Institutsebene festgelegt.
II. Begriffe Rz 8	Die Compliance-Funktion kontrolliert die Einhaltung regulatorischer und interner Vorschriften sowie die Beachtung marktüblicher Standards und Standesregeln.	Wie unter Rz. 99ff erläutert, lässt sich die Funktion von Compliance nicht auf die Kontrolle reduzieren, sondern beinhaltet auch die Unterstützung und Beratung der Geschäftsleitung bzw. deren Mitarbeiter in der Einhaltung der regulatorischen und internen Vorschriften. Weiter wird unter Rz. 81 korrekt beschrieben, dass die Geschäftsleitung für die Kontrolle und Bewirtschaftung der Risiken verantwortlich ist. Mit Verweis auf die Bestimmungen dieser beiden Randziffern beantragen wir folgende Berichtigung der Rz. 8. Änderungsantrag: Die Compliance-Funktion unterstützt und berät die Geschäftsleitung sowie die Mitarbeiter bei der Umsetzung regulatorischer und interner Vorschriften sowie der Beachtung marktüblicher Standards und Standesregeln und kontrolliert deren Einhaltung.
IV. Oberleitungsorgan Rz 10	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.	Unserer Auffassung nach schlägt die Geschäftsleitung die strategischen Ziele vor, welche als dann vom Oberleitungsorgan genehmigt und kontrolliert werden. Dies würde auch mit der Rz. 12 übereinstimmen. Änderungsantrag: 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~~ genehmigt die von der Geschäftsleitung vorgeschlagenen strategischen Ziele und kontrolliert die Geschäftsleitung im Hin-

		blick auf die Verfolgung dieser Ziele.
IV. Oberleitungsorgan Rz 12	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.	Der letzte Satz „Es versteht die Unternehmensstrukturen und Risiken der einzelnen Geschäftsfelder des Instituts" beschreibt unseres Erachtens eine Selbstverständlichkeit und kann gestrichen werden. Änderungsantrag: ~~Es versteht die Unternehmensstrukturen und Risiken der einzelnen Geschäftsfelder des Instituts.~~
IV. Oberleitungsorgan Rz 13	Das Oberleitungsorgan ist verantwortlich für eine angemessene Unternehmensorganisation mit ausgewogenen „Checks and Balances". Es erlässt die für den Geschäftsbetrieb und die für die Kompetenzverteilung und Überwachung notwendigen Reglemente, insbesondere das Organisations- und Geschäftsreglement, und Weisungen.	Gemäss Rz. 13 sind Weisungen vom Oberleitungsorgan zu erlassen. Dies ist in der Regel nicht stufengerecht: Die Weisungen werden von der *operativen* Unternehmensführung abgenommen. Änderungsantrag: Das Oberleitungsorgan ist verantwortlich für ~~eine angemessene~~ die Unternehmensorganisation ~~mit ausgewogenen „Checks and Balances".~~ Es erlässt die für den Geschäftsbetrieb und die für die Kompetenzverteilung und Überwachung notwendigen Reglemente, insbesondere das Organisations- und Geschäftsreglement. ~~und Weisungen~~.
IV. Oberleitungsorgan Rz 15	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).	Die Bestimmungen unter Rz. 15 weiten die Kompetenzen des Oberleitungsorgans überdurchschnittlich aus und würden diesem operationelle Verantwortlichkeiten zuweisen, was zu Unklarheiten der Zuständigkeiten, bzw. zu Konflikten mit den Aufgaben der Geschäftsleitung führen würde. Änderungsantrag: Streichen oder eventualiter wie folgt anpassen. 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 der Ausschussmitglieder, der Mitglieder der Geschäftsleitung und deren Vorsitzende ~~sowie weiterer Personen in leitenden Kontroll- und Schlüsselfunktionen (z.B. Chief Risk Officer, Chief Compliance Officer, Head IT).~~
IV. Oberleitungsorgan Rz 16	Das Oberleitungsorgan übt die Oberaufsicht über die Geschäftsleitung aus und stellt die Compliance des Instituts sicher. Es sorgt für ein geeignetes Risiko- und Kontrollum-	Die Rz. 16 fordert dass das Oberleitungsorgan die Compliance Funktion sicherstellt. Wir verweisen hierzu auf Art. 716a Ziff. 5 OR, wo geregelt ist dass der Verwaltungsrat die Oberaufsicht über die Com-

	feld 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.	pliance Funktion zusteht, diese jedoch nicht sicherzustellen hat. Änderungsantrag: Das Oberleitungsorgan übt die Oberaufsicht über die Geschäftsleitung ~~aus~~ und über ~~stellt~~ die Compliance des Instituts aus ~~sicher~~.
IV. Oberleitungsorgan Rz 18	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 Bank- und Finanzbereich. Das Oberleitungsorgan ist genügend breit aufgestellt, so dass nebst den Hauptgeschäftsfeldern sämtliche weiteren 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.	Jenseits der Anforderung für einen guten Ruf und die Gewähr für eine einwandfreie Geschäftstätigkeit ist es zufolge Privatautonomie dem Unternehmen freigestellt, wen es für eine Position einstellen oder mit einer Aufgabe betrauen will. Aufsichtsrechtliche Anforderungen erscheinen einer genügenden gesetzlichen Grundlage zu entbehren und würden einen ungerechtfertigten Eingriff in die Wirtschaftsfreiheit bedeuten. Auch für die aufsichtsrechtliche Regelung der Zusammensetzung des Oberleitungsorganes selber besteht unseres Erachtens keine hinreichende gesetzliche Grundlage. So wären sowohl die Bank als auch die Kandidaten bei der Rekrutierung darauf angewiesen, dass die Aufsichtsbehörde die Besetzung des Gremiums genehmigt. Schliesslich erscheint es uns nicht angemessen, einzelne Funktionen aufzuzählen, welche abgedeckt werden sollten. Insbesondere braucht es etwa keine IT oder Compliance Spezialisten auf dieser Ebene. Änderungsantrag: 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 Bank- und Finanzbereich. ~~Das Oberleitungsorgan ist genügend breit aufgestellt, so dass nebst den Hauptgeschäftsfeldern sämtliche weiteren 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.~~

IV. Oberleitungsorgan Rz 26	Zudem sollte ein massgeblicher Teil des Oberleitungsorgans nicht am Institut qualifiziert beteiligt sein oder einen qualifiziert Beteiligten vertreten. Die Gläubigerinteressen auf Ebene des Einzelinstituts haben gegenüber abweichenden Eigentümer- oder Gruppeninteressen Vorrang.	Dies widerspricht der grundlegenden gesellschaftsrechtlichen Ordnung des OR. Im Bankengesetz fehlt unseres Erachtens eine Grundlage, welche eine derartige Einschränkung der Privatautonomie erlauben würde. Der zweite Satz widerspricht einer weiteren grundlegenden Regelung des Obligationenrechts, insbes. der Sorgfalts- und Treuepflicht des Verwaltungsrates, welche im Interesse der Gesellschaft erfolgen muss (Art 717 OR). Dies beinhaltet auch die Verpflichtung zur Gewinnstrebigkeit. Beides bedeutet auch die Pflicht zur Wahrung der Interessen der Aktionäre. Die Verletzung der Sorgfaltspflicht führt deshalb zu indirektem Schaden der Aktionäre. Die Rz. 26 sollte daher mangels gesetzlicher Grundlage ersatzlos gestrichen werden. Etwas anderes lässt sich u.E. auch nicht aus Art. 1 BankG ableiten. Änderungsantrag: Streichen.
IV. Oberleitungsorgan Rz 30	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.	Die Rz. erschient uns viel zu detailliert formuliert und greift sehr stark in die Organisation der Gesellschaft ein. Zudem enthält die Rz. viele unbestimmte Rechtbegriffe, was für die Betroffenen Rechtsunsicherheit bringen würde. Änderungsantrag: Streichen oder eventualiter wie folgt anpassen. 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, so dass dieses mit der gebotenen Sorgfalt bewältigt werden kann.
IV. Oberleitungsorgan Rz 31	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.	Unserer Meinung nach ist dieser Grundsatz bereits im OR genügend geregelt. Der Vorschlag in Rz. 32 geht aber unseres Erachtens teilweise in unzulässiger Weise über diese Anforderung hinaus ("weitere Schlüsselpersonen"). Diese Ernennungen erfolgen durch die Geschäftsleitung oder delegierte tiefere Stufen. Änderungsantrag: Streichen oder eventualiter wie folgt anpassen. 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 Ge-

		schäftsleitung ~~sowie weiterer Schlüsselpersonen~~. Es stellt die Nachfolgeplanung sicher.
IV. Oberleitungsorgan Rz 32	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.	Die Bestimmung unter Rz. 32 hält grundsätzlich eine Selbstverständlichkeit fest und könnte prinzipienhafter formuliert werden, soweit dies die Leistungsbeurteilung betrifft. Eine allgemeine Weiterbildungspflicht für Verwaltungsräte zu stipulieren, ist abzulehnen. Hierfür sehen wir keine genügende Grundlage. Dass neue Mitglieder genügend eingeführt werden, stellt eine Selbstverständlichkeit dar, die nicht aufgeführt werden muss. Änderungsantrag: 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~~.
IV. Oberleitungsorgan Rz 34	Der Präsident ist eine Persönlichkeit mit ausgewiesener Integrität, Führungsstärke und Urteilskraft. Er prägt die Strategie, Kommunikation und Kultur des Unternehmens entscheidend mit.	Ausser einem guten Ruf und der Gewähr für eine einwandfreie Geschäftstätigkeit sollten unseres Erachtens keine weiteren Anforderungen an den Präsidenten des Oberleitungsorganes gestellt werden. Die in Rz. 34 vorgeschlagenen Kriterien sind kaum objektiv beurteilbar oder justiziabel und gehen unserer Meinung nach zu weit. Änderungsantrag: Streichen.
IV. Oberleitungsorgan Rz 35	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 Kotrollfunktionen und ist für die Aufbereitung und Steuerung des Informationsflusses innerhalb des Oberleitungsorgans verantwortlich.	Unseres Erachtens obliegt die Verantwortung für das Funktionieren des Gremiums nicht allein dem Präsidenten, letztlich ist jedes Mitglied dafür verantwortlich. Änderungsantrag: Er übt den Vorsitz über das Gesamtgremium aus ~~und trägt die Verantwortung für dessen ordnungsgemässes Funktionieren~~.
IV. Oberleitungsorgan Rz 36	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	Für eine Grossbank ist es unklar, ob die Ausschüsse konzernweit oder auf Institutionseben geschaffen werden müssen. Die Anforderungen sollten sich auf die Gruppenstufe beziehen. Änderungsantrag: "[...] Systemrelevante Banken müssen auf Stufe Finanzgruppe ~~über~~

	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.	~~weitere Ausschüsse, jedoch zwingend~~ über einen Vergütungs- und Nominationsausschuss verfügen..."
IV. Oberleitungsorgan Rz 38	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.	Gemäss Rz. 38 soll die FINMA Erleichterungen gewähren können. Dies würde eine Genehmigungspflicht voraussetzen. Im Hinblick auf mögliche Erleichterungen ist zudem klarzustellen, dass die FINMA nicht nur im Hinblick auf die Unabhängigkeit der Mitglieder, sondern auch im Hinblick auf das Erfordernis weiterer Ausschüsse insgesamt Erleichterungen gewähren kann. Gerade in komplexeren Finanzgruppen sind nicht auf allen Ebenen alle Ausschüsse erforderlich. Ebenso wenig besteht unseres Erachtens gesetzliche Genehmigungspflicht. Zudem ist fraglich, ob "ausgewiesene Kenntnisse" vorliegen müssen bzw. was darunter zu verstehen ist. Weiter sollte für den Nominationsschuss der Präsident des Oberleitungsorgans als Vorsitzender zugelassen sein. Änderungsantrag: Die Mehrheit der Mitglieder des Prüf-, Risiko- und Nominationsausschusses muss grundsätzlich unabhängig (vgl. Rz. 20ff) sein. Die FINMA kann bei Finanzgruppen Erleichterungen sowohl im Hinblick auf die erforderlichen Ausschüsse als auch auf die Unabhängigkeit der Mitglieder gewähren. Der Präsident des Oberleitungsorgans soll grundsätzlich weder dem Prüfungsausschuss angehören noch Vorsitzender eines anderen Ausschusses sein, mit Ausnahme des Nominationsausschusses. Die Mitglieder sämtlicher Ausschüsse müssen insgesamt über hinreichende ~~ausgewiesene~~ Kenntnisse und Erfahrung im Aufgabenbereich des entsprechenden Ausschusses verfügen.
IV. Oberleitungsorgan Rz 42	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;	Änderungsantrag: Überwachung und Beurteilung der finanziellen Berichterstattung und der Integrität der Finanzabschlüsse; einschliesslich deren Besprechung mit dem für das Finanz- und Rechnungswesen verantwortlichen Geschäftsleitungsmitglied und mit dem leitenden Revisor ~~sowie dem Leiter der internen Revision~~. Der Prüfausschuss bespricht mit

		dem Leiter der internen Revision seine Beurteilung der Zuverlässigkeit der internen Kontrollsysteme.
IV. Oberleitungsorgan Rz 43	- Überwachung und Beurteilung der Wirksamkeit der internen Kontrolle, namentlich auch der Risikokontrolle und der Compliance-Funktion, und der internen Revision;	Unserer Ansicht nach obliegen die Überwachung und die Beurteilung der Wirksamkeit der internen Kontrollen nicht dem Audit-Komitee sondern dem Risikoausschuss. Änderungsantrag: Zuteilung der Funktion an das Oberleitungsorgan, d) Aufgaben des Risikoausschusses.
V. Geschäftsleitung Rz 61	den Erlass von Vorschriften zur Regelung des operativen Geschäftsbetriebs;	Wir erachten diese Rz. als sinnvoll, kollidiert jedoch mit der Rz. 13. Siehe entsprechender Kommentar bei Rz. 13.
V. Geschäftsleitung Rz 65	Die Geschäftsleitung ist insgesamt je nach geographischer Geschäftsausrichtung mit den lokalen, regionalen, nationalen und internationalen Märkten und dem entsprechenden regulatorischen Umfeld hinreichend vertraut.	Unserer Ansicht nach wird in dieser Rz. erneut ins Aufsichtsrecht aufgenommen, was im Privatrecht ohnehin schon gilt. Im Sinne der Rechtssicherheit ist darauf zu verzichten und die privatrechtliche Regel muss im Sinne der Verhältnismässigkeit genügen. Änderungsantrag: Streichen.
VI. Rahmenkonzept für das institutsweite Risikomanagement Rz 70	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.	Änderungsantrag: 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~~ materieller Risikokategorien eingesetzt werden.
VII. Internes Kontrollsystem Rz 79	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.	Der dritte Satz „Im Weiteren sind Kontrollen vorzusehen, um insbesondere Verletzungen der Risikolimiten und Abweichungen von der festgelegten Risikopolitik frühzeitig zu erkennen" dupliziert die Bestimmung unter Rz. 72. Änderungsantrag: Streichen des erwähnten Satzes.
VII. Internes Kontrollsystem Rz 87	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.	Siehe Kommentar unter der Rz. 88. Änderungsantrag: Die Institute der Aufsichtskategorien 1 bis 3 verfügen über ~~eine~~ ei-

		genständige Risikokontroll- und Compliance-Funktionen. ~~als unabhängige Kontrollinstanzen~~. ~~Sie bestimmen einen CRO, der für die Risikokontrolle zuständig ist~~. Sie bestimmen einen CRO der sowohl für die Risikokontrolle- als auch für die Compliance-Funktion zuständig sein kann.
VII. Internes Kontrollsystem Rz 88	Systemrelevante Banken bestimmen einen CRO, der Mitglied der Geschäftsleitung und ausschliesslich für die Risikokontrolle zuständig ist.	Der Rundschreibentwurf schreibt für systemrelevante Funktionen vor, dass ein CRO als Mitglied der Geschäftsleitung ausschliesslich für die Risikokontrolle zuständig sein darf. Dies entspricht nicht der neueren Praxis und ist auch sachlich nicht zu rechtfertigen. Die Funktionen von Compliance und Risikokontrolle ergänzen sich in der Praxis gut. Ein Interessenkonflikt, der eine funktionale Trennung von Compliance und Risikokontrolle erfordern würde, ist nicht ersichtlich. Im Gegenteil mit dem Zusammenführen dieser Funktionen unter eine gemeinsame Leitung können Synergien (z.B. spezialisiertes Finanzwissen und rechtliche Expertise) genutzt werden, um schädliche Risiken zu erkennen und entsprechend zu entschärfen. Aus diesem Grund muss es weiterhin möglich sein die Risikokontrolle und die Compliance-Funktion in einer Geschäftseinheit unter der Leitung des CRO zu führen. Änderungsantrag: Systemrelevante Banken bestimmen einen CRO, der Mitglied der Geschäftsleitung ist ~~und ausschliesslich für die Risikokontrolle zuständig ist~~. Die Risikokontrollfunktion kann mit der Compliance-Funktion eine Geschäftseinheit unter der Leitung des CRO bilden.
VII. Internes Kontrollsystem Rz 93	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.	Gemäss Rz. 93 muss jedes neue Produkt von der Risikokontrolle begutachtet werden. Dies könnte einen erheblichen Mehraufwand bedeuten, insbesondere bei gleichartigen Produkten derselben Produkteklasse (z.B. bei allen neuen Strukturierten Produkten). Hier ist eine Vereinfachung anzustreben. Änderungsantrag: Die Risikokontrolle nimmt bei der Entwicklung von neuen oder erweiterten Produktekategorien, Dienstleistungen, Geschäfts- oder Marktbereichen sowie bei wesentlichen oder komplexen Transaktionen am Entwicklungsprozess bzw. an der Sorgfaltsprüfung (Due Diligence) teil.
VII. Internes Kontrollsystem Rz 98	Die Risikokontrolle berichtet dem Oberleitungsorgan mindestens jährlich über die Entwicklung des Risikoprofils des Instituts und seine Tätigkeit gemäss Rz 89ff. Im Weiteren	Aus unserer Sicht sollte die Geschäftsleitung und nicht das Oberleitungsorgan unverzüglich über Verletzungen der Risikolimiten informiert werden.

	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.	Änderungsantrag: 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~~ die Geschäftsleitung 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.
VII. Internes Kontrollsystem Rz 100	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;	Obschon bei den Aufgaben und Verantwortlichkeiten der Compliance-Funktion das Compliance-Risiko mehrfach genannt wird – findet sich keine Definition dieser Risiken im Rundschreiben. Änderungsantrag: Das Compliance-Risiko bezeichnet das Finanz- oder Reputationsrisiko des Instituts, wenn geltende Gesetze, Regeln und Bestimmungen, lokale oder internationale Best Practices (einschliesslich ethischer Standards) oder die eigenen internen Standards des Instituts nicht befolgt werden.
VIII. Interne Revision Rz 109	einem unabhängigen Dritten, vorausgesetzt die Prüfgesellschaft bestätigt dessen professionelle Kompetenzen und angemessene technische und personelle Ressourcen.	Unseres Erachtens sollte es zulässig sein, die interne Revision in einer zur Finanzgruppe gehörenden Service Company anzusiedeln. Änderungsantrag: ... an eine Gesellschaft innerhalb der Gruppe oder an einen ~~einem~~ unabhängigen Dritten, vorausgesetzt die Prüfgesellschaft bestätigt dessen professionelle Kompetenzen und angemessene technische und personelle Ressourcen.
VIII. Interne Revision Rz 115	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).	Änderungsantrag: Die Arbeit der internen Revision richtet sich nach ~~Standards~~ den International Standards for the Professional Practice of Internal Auditors des Institute of Internal Auditors (IIA)
VIII. Interne Revision Rz 119	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.	Wir sind der Meinung, dass die Begriffe Prüfziele und Prüfplanung nicht mehr aktuell sind und sich die FINMA enger an die International Standards for the Professional Practice of Internal Audit anlehnen sollte. Änderungsantrag: ... legt die interne Revision die Prüfziele und die risikobasierte Prüfplanung für die nächste Prüfperiode fest...

VIII. Interne Revision Rz 124	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.	Unseres Erachtens sollte die Ausführung im ersten Satz dieser Bestimmung präzisiert werden. Änderungsantrag: Im Weiteren informiert die interne Revision das Oberleitungsorgan oder dessen Prüfausschuss mindestens halbjährlich über die Beseitigung wesentlicher ~~festgestellter~~ Mängel und die Zuverlässigkeit ~~bzw. den Stand~~ der Umsetzung von Empfehlungen der internen Revision und der Prüfgesellschaft.
X. Offenlegung Rz 128 ff.	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.	Die Bestimmung fordert weitere und umfassende Publikationen. Es fehlen diesbezüglich die gesetzlichen Grundlagen welche solche Publikationen erfordern, des Weiteren sind die Offenlegungsvorschriften der Banken bereits detailliert geregelt. Änderungsantrag: Streichen.
X. Offenlegung Rz 135- 143	Folgende Informationen der Richtlinie der SIX Exchange betreffend Informationen zur Corporate Governance sind von Instituten der Aufsichtskategorien 1 - 3 öffentlich zu publizieren: (...)	Wir gehen davon aus dass sich die Offenlegungsrichtlinien auf die Finanzgruppe und nicht auf die entsprechenden Tochtergesellschaften mit Banklizenz beziehen.
X. Offenlegung Rz. 140	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.)	Rz. 142: Betreffend Grundlagen der Entschädigungen (Rz. 140) steht die Bestimmung im Widerspruch zur Bestimmung im FINMA Rundschreiben 2010/1 Rz. 71, welche besagt, dass die Offenlegung sich nach Bekanntgabe des Geschäftsberichts (OR, BankG) und somit nicht in jedem Fall nach den Richtlinien der SIX Exchange richtet. Änderungsantrag: Streichen.

Konsultation FINMA Rundschreiben 2008/21 Operationelle Risiken Banken

Referenz	Originaltext	Kommentar UBS
IV. Qualitative Anforderungen Rz. 135.1	Die Geschäftsführung stellt sicher, dass das IT-Konzept in Anlehnung an die internationalen Standards das Vorhandensein der folgenden minimalen Aspekte gewährleistet: a. Aktuelle und vollständige Übersicht über die wesentlichsten Bestandteile der IT Netzwerkumgebung mit Schnittstellen zwischen Systemen und Applikationen, b. Vorgaben und Prozesse, die eine explizite Identifikation und Beurteilung von inhärenten IT-Risiken sowie die	Unseres Erachtens ist die Rz. 135.1 a) bis g) zu detailliert und entspricht nicht dem gewünschten prinzipienorientierten Ansatz. Wir empfehlen daher die Überarbeitung dieser Bestimmung.

	Überwachung der Risikominderung und einen angemessenen Umgang mit den IT-Residualrisiken sicherstellen, c. Systematischer Prozess im Hinblick auf die Identifikation und Beurteilung von IT Risiken im Rahmen der Sorgfaltsprüfung (Due Diligence) insbesondere bei Akquisitionen resp. Auslagerungen im IT-Bereich, d. Eindeutige Festlegung von Rollen, Aufgaben und Verantwortlichkeiten in Bezug auf Daten- und Prozessverantwortliche, e. Überwachungsprozess, der die Einhaltung von regulatorischen und institutsinternen Vorgaben für IT-Systeme und -Prozesse sicherstellt, f. Prozesse zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Verantwortung zur Reduktion von IT-Risiken sowie Einhaltung der IT-Sicherheit und – Verfügbarkeit, g. Technologie- und Investitionsplanung zur Sicherstellung einer angemessenen IT Kapazität sowohl unter normalen Geschäftsbedingungen wie auch in Stressperioden sowie zur Reduktion der Komplexität und Fragmentierung der IT-Infrastruktur.	
IV. Qualitative Anforderungen Rz. 135.2	Die Geschäftsführung hat zudem ein Konzept für den Umgang mit Cyberrisiken zu implementieren. Dieses Konzept hat mindestens die folgenden Aspekte abzudecken und eine effektive Umsetzung durch geeignete Prozesse sowie eine eindeutige Festlegung von Aufgaben, Rollen und Verantwortlichkeiten zu gewährleisten: a. Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyberattacken, insbesondere in Bezug auf besonders schützenswerte Daten und Systeme, b. Schutz der Technologieinfrastruktur vor Cyberattacken, insbesondere im Hinblick auf die Verfügbarkeit der Systeme und die Integrität resp. Vertraulichkeit von Daten, c. Erfassung von Cyberattacken auf Basis einer systematischen Überwachung der Technologieinfrastruktur, d. Reaktion auf Cyberattacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyberattacken in Abstimmung mit dem BCM, und e. Sicherstellung einer zeitnahen Wiederherstellung des	Unseres Erachtens ist die Rz. 135.2 a) bis e) zu detailliert und entspricht nicht einem prinzipienorientierten Ansatz. Wir empfehlen daher die Überarbeitung dieser Bestimmung. Weiter erscheint die Beschreibung „besonders schützenswerte Daten und Systeme" unklar. Wir empfehlen eine klare Definition der Daten und Systeme, die identifiziert werden müssen.

	normalen Geschäftsbetriebs nach Cyberattacken durch geeignete Massnahmen.	
IV. Qualitative Anforderungen Rz. 135.3	Die Geschäftsführung lässt insbesondere in Bezug auf die Sicherstellung eines angemessenen Schutzes der besonders schützenswerten Daten und Systemen vor Cyberattacken regelmässig Vewundbarkeitsanalysen und Penetration Testings durchführen. Diese müssen grundsätzlich durch geeignete externe Dienstleister durchgeführt werden, können bei Vorhandensein von qualifiziertem Personal und Ressourcen jedoch auch durch interne Stellen vollzogen werden.	Änderungsantrag: Diese ~~müssen~~ können ~~grundsätzlich durch geeignete externe Dienstleister durchgeführt~~ von qualifiziertem Personal und Ressourcen durch interne Stellen vollzogen werden, ~~können bei Vorhandensein von qualifiziertem Personal und Ressourcen jedoch auch durch interne Stellen vollzogen werden,~~ ansonsten durch geeignete externe Dienstleister.
IV. Qualitative Anforderungen Rz 136 ff.		Das vorliegende RS regelt operationelle Risiken i.S. von Art. 89-94 ERV. Die operationellen Risiken sind in Rz. 2 definiert. Die Sicherstellung der Fortführung von systemrelevanten Funktionen (SIFs) gehört nicht zu diesen operationellen Risiken und damit nicht zum vorliegenden Themenbereich. Bei den SIFs geht es dagegen um die Verminderung der von systemrelevanten Banken ausgehenden Risiken für die Stabilität des Finanzsystems (Art. 7 BankG), d.h. um die Verminderung der wirtschaftlichen und finanziellen Auswirkungen im Fall einer Insolvenz eines systemrelevanten Instituts. Die Anforderungen sind im Gesetz (Art. 9 BankG und Art. 60ff BankV) und mittels Verfügung (SNB) bereits geregelt. In den Ziffern 136 ff. werden die Frage und Regelung von operationellen Risiken und die Anforderungen an die Systemrelevanz in unzulässiger und unnötiger Weise vermischt. Wir beantragen daher, Grundsatz 5 und Rz. 136-136.3 zu überarbeiten und auf *„Operational Continuity of Critical Shared Services"* bzw. die *"kritischen gemeinsamen Dienstleistungen"* im Sinne der FSB Konsultation *"Guidance on Arrangements to Support Operational Continuity in Resolution"* vom 5. November 2015 zu konzentrieren.(vgl. auch PRA Konsultationspapier ‚CP38/15; 15. Oktober 2015). Gemäss Erläuterungen soll im vorliegenden RS lediglich einer von drei Fällen abgebildet werden, d.h. wenn diese Critical Shared Services innerhalb der gleichen legal entity erbracht werden (‚in-house service provisioning'; FSB Paper Ziff. 3.1.(i)). Dies müsste im Text selbst klargestellt werden. Da noch keine finale FSB Guidance vorliegt, käme als Alternative in

		Frage, diesen Bereich erst bei Vorlage der FSB Guidelines in einem separaten RS zu regeln. Damit könnten zum einen unnötige Abweichungen vom FSB Standard vermieden werden. Zum anderen liesse sich die Materie auch vollständig in einem RS abhandeln, mit entsprechenden Definitionen, Prinzipien und Anforderungen. So sagen die vorliegenden Bestimmungen nichts zur Definition der kritischen Dienstleistungen aus oder der Prinzipien, die in diesem Zusammenhang einzuhalten sind. Zudem ist aufgrund der Aufteilung der verschiedenen Modelle des Service provisioning auf unterschiedliche Rundschreiben nicht mehr klar, dass die drei Service Provisioning Modelle gleichwertig sind (so wie dies auch das FSB festhält). Eine Regelung der ganzen Materie in einem separaten Rundschreiben wäre daher eine gangbare Alternative. Seitens UBS würden wir uns dabei gerne aktiv einbringen. Die nachfolgenden Ausführungen beziehen sich auf den Fall, dass kein gesondertes RS erstellt wird und hier die *Critical Shared Services innerhalb* der *gleichen* Entity erbracht werden.
Rz. 136	Überschrift: Grundsatz 5:.....	Der Inhalt des Grundsatzes sollte aufgeteilt werden. Ziffer 136 bezieht sich auf die Kontinuität bei der Geschäftsunterbrechung und ist klar von der Aufrechterhaltung der kritischen Dienstleistungen abzugrenzen. Kontinuität von kritischen Dienstleistungen bei Abwicklung und Sanierung betrifft bei systemrelevanten Banken die systemrelevanten Funktionen. Änderungsantrag: Entsprechend wäre die Überschrift zu ändern ...Kontinuität bei Geschäftsunterbrechung ~~und Kontinuität von kritischen Dienstleistungen bei der Abweichung und Sanierung von (systemrelevanten) Banken~~
Rz. 136	Die Geschäftsführung hat über Pläne zur Fortführung der Geschäfte der Bank zu verfügen, welche die Kontinuität der Tätigkeiten und die Schadensbegrenzung im Falle einer schwerwiegenden Geschäftsunterbrechung gewährleisten.	Mit der oben beantragten Änderung in der Überschrift wäre sichergestellt, dass sich diese Anforderung nur auf den Fall der Kontinuität bei einer Geschäftsunterbrechung bezieht und nicht auf die kritischen gemeinsamen Dienstleistungen oder gar die SIFs.
Rz. 136.1	Die Geschäftsführung von systemrelevanten Banken hat überdies sicherzustellen, dass institutsspezifische Funktionen, deren plötzlicher Ausfall oder Unterbruch Auswirkungen auf die Finanzstabilität, die Restrukturierung oder die Abwicklung der jeweiligen systemrelevanten Bank gefährden könnten („kritische Funktionen"), im Insolvenzfall aufrecht erhalten werden können. Zu diesem Zweck hat	Der erste Satz bezieht sich auf die systemrelevanten Funktionen (SIF) und versucht diese und die Voraussetzungen für den Anwendungsfall neu zu definieren ("institutsspezifische Funktionen"). Dies ist weder notwendig noch zulässig, da die SIFs durch Gesetz, Verordnung und Verfügung der SNB im konkreten Anwendungsfall festgelegt sind. Der Umfang der SIFs und die diesbezügliche Nachweispflicht der Bank kann nicht auf diese Weise erweitert werden.

	die Geschäftsführung von systemrelevanten Banken sicherzustellen, dass auch die für die kritischen Funktionen notwendigen Dienstleistungen („kritische Dienstleistungen") im Insolvenzfall fortgeführt werden können.	Änderungsantrag: Streichen. Soweit unter "kritischen Funktionen" etwas anderes verstanden wird als die SIFs (vgl. auch oben, zum Begriff des FSB), sollte dies hier ausdrücklich klargestellt werden. Die FINMA verwendet in ihrem RRP Guidance Plan den Begriff der "Critical Operations", d.h. andere, wichtige Funktionen, die aber nicht SIFs darstellen und für welche der gesetzliche Nachweis für den Notfallplan entsprechend auch nicht gilt. Critical functions haben ihre Bedeutung vor allem im internationalen Kontext und der globalen Abwicklungsplanung. (Betreffend des FINMA RRP Guidance Plan ist aber noch anzufügen, dass es das Verständnis der UBS ist, dass dieses Dokument keine Gültigkeit mehr hat). Änderungsantrag: Streichen. Mit den "kritischen Dienstleistungen" werden die sog. "Critical Shared *Services*" angesprochen. Diese sind vor allem im Rahmen der Verbesserung der globalen Abwicklungsfähigkeit zu sehen (grenzüberschreitende Aspekte). Ein formeller Bezug zu den entsprechenden FSB Standards wäre sinnvoll. Dies scheint uns der Hauptbestandteil der Regeln zu bilden, die hier abgebildet werden sollen, in Anlehnung an das Konsultationsdokument des FSB "Guidance on Arrangements to Support Operational Continuity in Resolution" vom 3. November 2015. Diese kritischen Dienstleistungen bedürfen einer Definition und Konkretisierung (vgl. auch FSB Paper, Ziff. 2.2., S. 9: "Critical services" bzw. "Critical shared services")."
Rz. 136.2	Die systemrelevanten Banken treffen die hierfür erforderlichen Massnahmen im Rahmen der Notfallplanung (Art. 9 Abs. 2 lit. d BankG i.V.m. Art. 60 ff. BankV). Bestehen zu diesem Themengebiet international anerkannte Standards, so sind diese ebenfalls zu berücksichtigen.	Satz 1 kann sich nur auf solche "Critical Shared Services" beziehen, welche für die Erbringung einer SIF notwendig und erforderlich sind. Wie soeben aufgeführt können nicht über Art. 9 Abs. 2 Buchstabe d BankG hinaus zusätzliche Anforderungen an den Notfallplan gestellt werden, deren Aufrechterhaltung im Insolvenzfall sicherzustellen wäre. Änderungsantrag: Präzisierung und Ergänzung wie folgt. "Soweit eine systemrelevante Bank die für die Weiterführung von systemrelevanten Funktionen notwendigen kritischen Funktionen selbst innerhalb der Bank erbringt, sorgt sie für die angemessene Transparenz, vertragliche Dokumentation der Dienstleistungen, welche bei Einhaltung der Zahlungsverpflichtungen die Weiterführung

		der Dienstleistung in der Abwicklung ermöglicht und Einhaltung des "Arm's length" Grundsatzes und trifft Vorkehrungen für die Beibehaltung von Schlüsselpersonen ("Key staff") und Zugang zu IP-Rechten, die von anderen Gruppengesellschaften gehalten werden." Die einzelnen Anforderungen in Bezug auf MIS, finanzielle Ressourcen, Preisstrukturen, etc. müssten hier ebenfalls aufgeführt werden (oder ggf. in einem Anhang hierzu). Der Begriff der "international anerkannten Standards" erscheint uns zu wenig präzis. Es sollte ausdrücklich klargestellt werden, dass es sich um die FSB Standards handelt und nicht um Anforderungen, die lediglich in gewissen Staaten (wie z.B. UK) gelten. Änderungsantrag: Präzisieren wie folgt. "Die diesbezüglichen internationalen Standards des FSB sind ebenfalls zu berücksichtigen."
Rz. 136.3	Zur Vereinfachung einer allfälligen Abwicklung oder Restrukturierung haben auch nicht systemrelevante Banken ein Inventar über die aus ihrer Sicht wichtigsten Dienstleistungen zu erstellen und regelmässig zu aktualisieren. Das Inventar enthält Angaben zu (i) Anbieter und Empfänger der Dienstleistung (Geschäftseinheit), (ii) Preis(gestaltung) / interne Gebührenerhebung, (iii) Berichterstattungslinien des Dienstleistungserbringers, sowie (iv) die für die Dienstleistung nötigen personellen Ressourcen (quantitativ und qualitativ).	Für nichtsystemrelevante Institute bestehen zur Zeit keine gesetzlichen Anforderungen in Bezug auf die Abwicklung oder Restrukturierungen. Etwas anderes ergibt sich auch nicht aus der Bankenverordnung. Entsprechend entbehrt Rz. 136.3 unserer Ansicht nach einer genügenden Grundlage. Änderungsantrag: Streichen.
Anhang 3 Rz 33	Die Bank muss über klare Sicherheitsanforderungen für Mitarbeitende, die auf CID zugreifen, verfügen. Es ist regelmässig zu überprüfen, ob die Anforderungen für einen angemessenen Umgang mit CID weiterhin erfüllt sind. Erhöhte Sicherheitsanforderungen müssen für privilegierte IT-Benutzer und Anwender mit funktionalem Zugriff[26] auf Massen-CID („Schlüsselmitarbeitenden") gelten. Diese erhöhte Sicherheitsanforderungen sind auch auf privilegierte Anwender mit Zugriff auf höchst vertrauliche Unterkategorien von CID (z.B. chiffrierte Konten) anzuwenden. [26] Insbesondere auch bei erweiterten Zugriffsrechten wie z.B. die Abfrage und Extraktion/Migration von grossen Datenmengen.	Es werden zahlreiche Begriffe (z.B. „Massen-CID", „Extraktion", „höchstvertrauliche Unterkategorien von CID") verwendet, welche nicht eindeutig definiert sind und erheblichen Interpretationsspielraum lassen. Änderungsantrag: Wir empfehlen die Begriffe mit klaren Definitionen zu ergänzen oder zu umschreiben.

Konsultation FINMA Rundschreiben 2010/1 Vergütungssysteme

Referenz	Originaltext	Kommentar UBS
II. Geltungsbereich Rz 4 und Rz 6	Rz. 4 Adressaten des Rundschreibens sind alle der schweizerischen Finanzmarktaufsicht unterstellten Banken, Effektenhändler, Finanzgruppen und Finanzkonglomerate, Versicherungsunternehmen, Versicherungsgruppen und Versicherungskonglomerate sowie Bewilligungsträger nach Art. 13 Abs. 2 und 4 des Kollektivanlagengesetzes (KAG; SR 951.31). Diese werden nachfolgend als Finanzinstitute bezeichnet. Rz. 6 Banken, Effektenhändler, Finanzgruppen und Finanzkonglomerate, die als Einzelinstitut oder auf Stufe der Finanzgruppe oder des Finanzkonglomerats erforderliche Eigenmittel (Mindestanforderungen gemäss Art. 7 ff. bzw. Art. 42 der Eigenmittelverordnung [ERV; SR 952.03]) von mindestens CHF 10 Milliarden halten müssen.	Es ist unklar, ob die Bestimmung nur für die Finanzgruppe oder auch für die Tochtergesellschaften in der Schweiz (mit Banklizenz und den erforderlichen Eigenmitteln von CHF 10 Milliarden) gelten soll. Da die FINMA gemäss Ihrer Medienmitteilung vom 1. März 2016 von den beiden Grossbanken spricht, nehmen wir jedoch an, dass das Rundschreiben an die Finanzgruppe und nicht an einzelne Tochtergesellschaften adressiert ist. Zudem besteht insbesondere für Vorschriften für ausländische Töchter auf Solobasis keine genügende gesetzliche Grundlage. Änderungsantrag: Ergänzung wie folgt. Ausgenommen sind Tochtergesellschaften einer Finanz- oder Versicherungsgruppe, sofern die Finanz- oder Versicherungsgruppe Adressat des Rundschreibens ist und die Vergütungspolitik gruppenweit anwendet.
IV. Grundsätze Rz 20	Der Verwaltungsrat genehmigt jährlich die Vergütungen der Geschäftsleitung, der Leiter der Kontrollfunktionen sowie den Gesamtpool für das Finanzinstitut.	Auf Stufe Finanzgruppe erachten wir diese Ergänzung als sinnvoll. Auf Stufe Tochtergesellschaften wäre eine solche Genehmigung kaum praktikabel, da bestimmte Leiter von Kontrollfunktionen auf Gruppenstufe vergütet werden. Änderungsantrag: Siehe Kommentar zu Rz. 4 und Rz. 6.
IV. Grundsätze Rz 21	Der Verwaltungsrat setzt einen Entschädigungsausschuss ein. Dieser soll eine unabhängige und fachkundige Unterstützung des Verwaltungsrats sicherstellen.	Für börsenkotierte Finanzinstitute steht die Regelung im Widerspruch zu den Bestimmungen der Verordnung gegen übermässige Vergütungen, wonach der Vergütungsausschuss von der Generalversammlung gewählt wird. Falls das Rundschreiben auch auf Tochtergesellschaften Anwendung finden soll (siehe Kommentar zu Rz. 4 und Rz. 6), könnte ein zusätzlicher Vergütungsausschuss auf dieser Stufe die einheitliche, gruppenweite Anwendung der Vergütungspolitik erheblich erschweren. Änderungsantrag: Streichen oder eventualiter Verweis auf Verordnung gegen übermässige Vergütungen.
IV. Grundsätze	Der schwerwiegende Verstoss gegen interne oder externe	Unseres Erachtens sollte diese Bestimmung auf das Senior Manage-

Rz 46	Vorschriften führt zu einer Reduktion oder einer Verwirkung der variablen Vergütung („Malus"). Verträge sind so auszugestalten, dass eine Rückforderung von bereits ausbezahlten variablen Vergütungen grundsätzlich möglich ist (Claw-back).	ment mit vergleichsweise hohen Gesamtvergütungen beschränkt werden. Änderungsantrag: Wir empfehlen die Rz. zu ergänzen, mit der Definition der Mitarbeiter, die von den Rückforderungen der Vergütungen betroffen sind. Aus Gründen der Rechtssicherheit sollten zudem die folgenden Punkte präzisiert werden: • Der Tatbestand für eine Rückforderung sollte möglichst genau umschrieben werden. • Es sollte bestimmt werden, wer die Rückforderungen auslöst (FINMA oder Finanzinstitut). • Die Frist, innert welcher eine Rückforderung möglich ist, muss bestimmt sein. Wir schlagen eine Frist von drei Jahren vor. • Mit der Bezeichnung "bereits ausbezahlten variablen Vergütungen" wird zudem eine mit der Rechtsordnung kaum vereinbare Rückwirkung auf sämtliche in früheren Jahren geleisteten Vergütungen geschaffen, welche aufgrund fehlender vertraglicher Vereinbarungen nicht durchsetzbar wäre.

Forschungsinstitut für Arbeit
und Arbeitswelten

Universität St.Gallen

Universität St. Gallen
FAA-HSG
Tellstrasse 2
CH-9000 St. Gallen

Telefon +41 (0)71 224 28 00
Telefax +41 (0)71 224 28 07
Roland.Müller@unisg.ch
www.faa.unisg.ch

Per E-Mail

Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
CH 3003 Bern
peter.ruetschi@finma.ch

St. Gallen, 13. April 2016 RM/rm

Stellungnahme zum FINMA-Rundschreiben 2016/x „Corporate Governance – Banken“

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit zur Mitwirkung im Rahmen der Anhörung zum FINMA-Rundschreiben 2016/x „Corporate Governance – Banken“. Nach umfangreichen Abklärungen nehmen wir gerne die Gelegenheit wahr, zum vorgeschlagenen Rundschreiben innert offener Frist Stellung zu nehmen.

Allgemeine Anmerkungen

Der vorliegende Entwurf des Rundschreibens 2016/xx Corporate Governance – Banken ist sehr zu begrüssen, da es den Versuch unternimmt a) Anpassungen bei den bestehenden Grundlagen zur Corporate Governance anhand der aus der Finanzkrise gewonnen Erkenntnisse und den überarbeiteten internationalen Standards vorzunehmen und b) den Themenblock Corporate Governance, Risikomanagement, Compliance und interne Kontrolle bei Banken kompakt zusammenzufassen.

Der vorliegende Entwurf weist jedoch auch eine Anzahl von Defiziten auf, die wir im Folgenden näher erörtern wollen. In der Übersicht handelt es sich um folgende Punkte:

a) Es fehlt der grundsätzliche Bezug zu den zugrundeliegenden internationalen Standard, konkret zu den Standards ISO 31000 (Risiko Management) und zum ISO 19600 (Compliance)

b) In der Folge ergeben sich daher Unschärfen und Ungenauigkeiten, die dazu führen, dass wesentliche konzeptionelle Elemente eines nach internationalen Standards gängigen integrierten Corporate Governance und Risikomanagements vergessen gehen.

c) Damit wird die Praxistauglichkeit, die Effektivität und Effizienz sowie der tatsächliche Mehrwert eines nach den vorliegenden Vorgaben konzipierten Corporate Governance und Risiko Managements in Frage gestellt.

Wir regen daher eine grundlegende Überprüfung der vorgebrachten Entwürfe an, um Corporate Governance, Risikomanagement, Compliance-Management und IKS nicht nur papier-, sondern auch praxistauglich und entsprechend den gängigen internationalen Standards auszugestalten.

Den nachfolgenden Erläuterungen liegen die Standards ISO 31000, ISO 19600 bzw. die entsprechende ONR zu Grunde, sofern nicht anderweitig referenziert. Sie werden grossteils wörtlich wiedergegeben.

I. RUNDSCHREIBEN 2016/XX CORPORATE GOVERNANCE - BANKEN

1. Top Down- und Bottom Up-Ansatz

Ein modernes integriertes Risikomanagement besteht sowohl aus der Innensicht der Unternehmung, den Prozessen und Verfahren, als auch aus der Aussensicht, den Verpflichtungen der obersten Leitung und der Führungskräfte im Rahmen der Grundsätze der Führung der Organisation und im Sinne der Zielerreichung (Corporate Governance). Die Risikobeurteilung und Risikobewältigung aus Innenperspektive erfolgt nach dem Bottom-Up Ansatz, aus der Aussenperspektive nach dem Top-Down Ansatz. Ein integriertes Risikomanagement verbindet und koordiniert sowohl den Top-down als auch den Bottom-Up Ansatz.

Im Rundschreiben 2016/xx Corporate Governance – Banken findet sich kein Hinweis auf diese konzeptionelle Grundlage eines integrierten Risikomanagements. Es ist zu empfehlen diesen Ansatz entsprechend aufzunehmen.

2. Risikomanagement-System mit Rahmen und Prozess

Voraussetzung für ein wirksames Risikomanagement ist die Ausrichtung auf die Politik, das heisst auf die Ziele und Strategien der Organisation, sowie der Auftrag und die Verpflichtung der obersten Leitung und Führungskräfte, den Risikomanagement-Prozess bei der Führungstätigkeit anzuwenden.

Ein wirksames Risikomanagement erfordert das Vorhandensein eines Risikomanagement-Systems, welches den organisatorischen Rahmen und die Tätigkeit

des Managements für den Umgang mit den Risiken festlegt. Das Risikomanagement-System schliesst den Risikomanagement-Prozess mit ein.

Das Rundschreiben 2016/xx Corporate Governance – Banken führt ab Rz 66 ein „Rahmenkonzept für das institutsweite Risikomanagement“ an, versäumt jedoch das Risikomanagement-System, welches den organisatorischen Rahmen und die Tätigkeit des Managements für den Umgang mit Risiken festlegt sowie den Risikomanagement-Prozess zu unterscheiden bzw. aufzuführen. Das vorgelegte „Rahmenkonzept“ vermischt gar die Elemente Risikomanagement-Rahmen und Risikomanagement-Prozess. Diese Unschärfe führt dazu, dass der organisatorische Rahmen der Risikomanagements, sprich die Verpflichtung der obersten Leitung und der Führungskräfte, die Risikopolitik, die Rollen und Verantwortungen von Risikoeignern und Risikomanagern sowie das Management der Ressourcen festzulegen, mit dem operativen Handling von Risiken im Rahmen des Risikomanagement-Prozesses (das „DO“ von Plan, Do, Check Act) vermengt wird. Dies ist einerseits verwirrend und anderseits nicht konform mit gängigen Standards. Das Funktionieren des vorgeschlagenen „Rahmenkonzeptes“ ist daher zu hinterfragen.

Es ist zu empfehlen eine saubere Trennung des Risikomanagement-Rahmens und des Risikomanagement-Prozesses vorzunehmen und die Begrifflichkeiten entsprechend den internationalen Standards zu definieren. Das vorgelegte Rahmenkonzept ist vollständig zu überarbeiten.

3. Risikomanagement-Prozess

Der Risikomanagement-Prozess umfasst die Tätigkeiten, die darauf ausgerichtet sind, eine Organisation bezüglich Risiken zu steuern und zu überwachen und besteht aus den Kernprozessen: Zusammenhang herstellen, Risiken identifizieren, Risiken analysieren, Risiken bewerten und Risiken bewältigen. Er wird von folgenden weiteren Prozessen begleitet: Risiken überwachen / überprüfen sowie Risiken kommunizieren und Informationen austauschen.

Wie oben aufgeführt fehlt der Risikomanagement-Prozess. Es ist zu empfehlen diesen separat aufzunehmen und in den Kontext des Gesamt-Risikosystems zu bringen.

4. Notfall-, Krisen- und Kontinuitätsmanagement

Ein vollständiges Risikomanagement beinhaltet auch ein Notfall-, Krisen- und Kontinuitätsmanagement. Auf dieses geht das Rundschreiben 2016/xx Corporate Governance – Banken nicht und das Rundschreiben 2008/21 – Operationellen Risiken Banken nur auszugsweise und in Teilen ein. Auf Ausführungen in Zusammenhang mit dem Notfall- und Krisenmanagement wird gänzlich verzichtet.

Um ein ganzheitliches Risikomanagement zu gewährleisten, sind sowohl das Notfall, als auch das Krisenmanagement zwingend aufzunehmen sowie weitergehende Ausführungen zum Kontinuitätsmanagement zu integrieren.

5. Risikokultur

Erst die geeignete Umsetzung des Risikomanagements, mit all seinen Elementen führt zu einer gelebten Risikokultur in der Organisation.

Auf die Risikokultur wird in den Rundschreiben überhaupt nicht eingegangen.

RZ 3 müsste neu wie folgt lauten:

„Das Risikomanagement umfasst die organisatorischen Strukturen sowie die Methoden und Prozesse, die der Schaffung einer Risikokultur und der Festlegung von Risikostrategien und Risikosteuerungsmassnahmen sowie der Identifikation […].“

Es ist zwingend zu empfehlen, der Risikokultur den nötigen Raum im Rundschreiben zu gewähren. Kein Risikomanagement kann ohne die zu Grunde liegende Risikokultur existieren. Es droht gar zu einem reinen Papiertiger zu avancieren. Nur eine gelebte Risikokultur erlaubt ein sinnvoller Umgang mit Risiken.

6. Compliance-Management

Ein funktionierendes Corporate Governance, Risikomanagement und Compliance Management System weist neben dem Risikomanagement-System und dem Internen Kontroll-System auch ein Compliance Management System auf.[1] Im Rundschreiben sollte klargestellt werden, dass es sich um drei "Systeme" handelt, die insbesondere personell völlig unabhängig vom Internal Audit sein müssen.

Obgleich der Vorschlag zum Rundschreiben in Teilen auf die Compliance Funktion eingeht (Rz 8), wird diese nicht angemessen berücksichtigt. Einerseits werden Definitionen zum Compliance Management gemäss ISO 19600 nicht richtig wiedergegeben, andererseits fehlt an vielen Stellen der Bezug zum Compliance Management-System.

So wird bspw. in Rz 5 der Begriff „Risikoappetit“ verwendet, welcher gemäss ISO 31000 korrekterweise mit „Risikoeinstellung“ bezeichnet wird. Der Begriff „Risikoappetit“ ist entsprechend zu streichen.

Die Einbindung, Integration und geeignete Abstimmung der unterschiedlichen Management-Systeme in den Bereichen Risiko, Compliance und interne Kontrolle ist von entscheidender Bedeutung. Die entsprechenden Verweise und Bezüge zum Compliance Management sind im Rundschreiben an verschiedenen Stellen nachzuführen.

Konkret werden daher folgende Anpassungen vorgeschlagen.

Rz 1 müsste neu wie folgt lauten:

„Das vorliegende Rundschreiben erläutert die Anforderungen an die Corporate Governance, das interne Kontrollsystem und das Risiko- und Compliance-Management bei Banken […].“

Rz 5 müsste neu wie folgt lauten:

[1] Vinay Kalia, Roland Müller: Risk Management at Board Level, Haupt-Verlag, 2nd edition, S. 68, mit entsprechender Graphik.

„Die Risikoeinstellung beinhaltet sowohl quantitative wie qualitative Überlegungen hinsichtlich […].“

Rz 8 müsste neu wie folgt lauten:

„Die Compliance-Funktion unterstützt und überwacht die Einhaltung aller bindenden Verpflichtungen.“

Rz 10 müsste neu wie folgt lauten:

„Das Organ für die Oberleitung, Aufsicht und Kontrolle bezeichnet die Werte, entwikkelt die strategischen Ziele, legt die Mittel fest, um diese Ziele zu erreichen und kontrolliert die Geschäftsleitung im Hinblick auf die Einhaltung der Werte und die Verfolgung dieser Ziele

Rz 12 müsste neu wie folgt lauten:

„Das Oberleitungsorgan entscheidet auf Antrag der Geschäftsleitung über die Geschäftsstrategie, die wesentlichen Unternehmensziele und das Unternehmensleitbild und erlässt Leitsätze zur Unternehmenskultur und den Unternehmenswerten und legt die Compliance Strategie fest.“

Rz 16 müsste neu wie folgt lauten:

„[…].Das Oberleitungsorgan oder sein zuständiger Ausschuss überwacht und beurteilt die intern Revision, das Risikomanagement und das Compliance-Management und vergewissert sich periodisch, dass diese über angemessene Ressourcen und Kompetenzen sowie Unabhängigkeit und Objektivität verfügt, um ihre Prüfaufgaben beim Institut wahrzunehmen.“

Rz 36 müsste neu wie folgt lauten:

„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 Risiko- und Compliance-Ausschuss einrichten. […]“

Rz 46 bis 52 müsste neu wie folgt lauten:

d) Aufgaben des Risiko- und Compliance-Ausschusses

Die Aufgaben umfassen insbesondere die:

- *Prüfung des Rahmenkonzepts für das institutsweite Risikomanagement-System und Unterbreitung der entsprechenden Empfehlungen an das gesamte Oberleitungsorgan;*

- *Prüfung des Rahmenkonzepts für das institutsweite Compliance Management System und Unterbreitung der entsprechenden Empfehlungen an das gesamte Oberleitungsorgan;*
- *Würdigung der Kapital- und Liquiditätsplanung und diesbezügliche Berichterstattung an das gesamte Oberleitungsorgan;*
- *Mindestens jährliche Beurteilung des Rahmenkonzepts, der Wirksamkeit und der Anwendung der Regeln der Kunst für das institutsweite Risikomanagement und Veranlassung der notwendigen Anpassungen;*
- *Kontrolle, ob das Institut ein geeignetes Risikomanagement mit wirksamen Prozessen unterhält, die der jeweiligen Risikolage und den Compliance Zielen des Instituts gerecht werden;*
- *Überwachung der Umsetzung der Risikostrategien, insbesondere im Hinblick auf deren Übereinstimmung mit dem vorgegebenen Risikoappetit und den Risikolimiten gemäss Rahmenkonzept für das institutsweite Risikomanagement.*

Der Risikoausschuss erhält vom Chief Risk Officer (CRO, dem Chief Compliance Officer und andern relevanten Funktionsträgern regelmässig aussagekräftige Berichte zu den jeweiligen Aspekten des Rahmenkonzepts für das institutsweite Risiko- und Compliance Management (gemäss Rz 66ff.) und dessen Einhaltung.

Zwischen Prüfausschuss und Risikoausschuss sind geeignete Informationsflüsse einzurichten, welche eine wirksame gegenseitige Abstimmung und eine angemessene Reaktion auf Veränderungen im Risikoprofil und den bindenden Verpflichtungen des Instituts ermöglichen.

Rz 53 müsste neu wie folgt lauten:

„Die Geschäftsleitung ist zuständig für die operative Geschäftstätigkeit im Einklang mit den Werten, der Geschäftsstrategie, dem Rahmenkonzept für das institutsweite Risikomanagement, dem Rahmenkonzept für das institutsweite Compliance Management sowie den weiteren vom Oberleitungsorgan verabschiedeten Grundlagen, Geschäfts- und Organisationsvorschriften. Sie vollzieht die Beschlüsse des Oberleitungsorgans und ist für die Einhaltung der bindenden Verpflichtungen im Rahmen der operationellen Geschäftstätigkeit verantwortlich.“

Rz 56 müsste neu wie folgt lauten:

„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 Rahmenkonzepts für das institutsweite Compliance Managements, des Unternehmensleitbildes und der Unternehmensziele;“

Rz 63 müsste neu wie folgt lauten:

„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 bindenden Verpflichtungen inkl. der aufsichtsrechtlichen Vorschriften und internen Vorgaben entsprechen.“

Rz 99 bis 143 sind analog den oben aufgeführten Vorschlägen konzeptionell und bezüglich Terminologie an ISO 19600 anzupassen. Im Weiteren sind folgende Anpassungen vorzunehmen:

Rz 99 bis 103 müsste neu wie folgt lauten:

„c) Aufgaben und Verantwortlichkeit der Compliance-Funktion

Die Aufgaben und Verantwortlichkeiten der Compliance-Funktion als unabhängige Kontrollinstanz umfassen ~~in der Regel~~ folgende Tätigkeiten:

- *Mindestens jährliche Einschätzung der Wirksamkeit des Compliance Managements und 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;*
- *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;*
- *Jährliche Berichterstattung an das Oberleitungsorgan über die Umsetzung des Regelwerks, die Wirksamkeit des Compliance Managements, 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.*

[2]Nebst den Aufgaben und Verantwortlichkeiten der Compliance-Funktion in ihrer Rolle als unabhängige Kontrollinstanz unterstützt und beratet die Compliance-Funktion die Geschäftsleitung sowie die Mitarbeiter bei der Ausarbeitung, Durchsetzung und Überwachung der bindenden Verpflichtungen und unterstützt die Geschäftsleitung bei der Ausbildung und Information der Mitarbeiter bezüglich Werte und Compliance.“

Rz 111 müsste neu wie folgt lauten:

„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 und finanziell adäquat dotiert sein und über die nötigen Fachkompetenzen verfügen, damit sie ihr Mandat erfüllen kann“

Rz 117 müsste neu wie folgt lauten:

„Die interne Revision liefert wichtige Entscheidungsgrundlagen für die Beurteilung, ob das Institut ein seinem Risikoprofil und seinen Compliance Zielen, angemessenes und wirksames internes Kontrollsystem besitzt.“

[2] Ohne der Verpflichtung zu einem Regelwerk ist der Inhalt der Aufgaben und Verantwortlichkeiten völlig unbestimmt; ISO 19600 nennt die (allgemeinen) Aufgaben und Verantwortlichkeiten präzise; s. 5.3.4

7. Internes Kontrollsystem

In Rz 87 wird aufgeführt, dass nur Institute der Aufsichtskategorien 1 bis 3 über eine eigenständige Risikokontrolle und Compliance-Funktion als unabhängige Kontrollinstanzen verfügen sollen.

Diese Einschränkung ist zwar im Sinne der Grössenverträglichkeit löblich, jedoch nicht zielführend, entspricht nicht dem ISO Standard und ist auch im internationalen, insbesondere im europäischen Vergleich nicht vorgesehen. Auch kleinere Institute haben zwingend über die entsprechenden unabhängigen Kontrollinstanzen zu verfügen. Die Einschränkung auf Institute der Kategorie 1 bis 3 ist zu streichen.

Ergänzend zum Chief Risk Officer (CRO) ist unter dem Rz 87 und Rz 88 auch der Chief Compliance Officer (CCO) aufzuführen.

Rz 87 müsste neu wie folgt lauten:

„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 und einen CCO, der für das Compliance Management zuständig ist“

Im Weiteren ist die Begrifflichkeit der „Risikokontrolle“ in Verbindung mit dem CRO bzw. den unabhängigen Kontrollinstanzen nicht eindeutig. Im Entwurf des Rundschreibens ist unklar, welche Verantwortlichkeit nun effektiv dem CRO zukommt. Der Begriff der Risikokontrolle wird erst unter Rz 89 erstmals aufgeführt und wird nicht näher definiert. Es ist daher zu empfehlen den Abschnitt der Rz 87/88 i.V.m. Rz 89ff. besser zu gruppieren, allenfalls zusammenzuführen und ausführlicher zu definieren.

Darüber hinaus wird eine grundlegende, konzeptionelle Überarbeitung des Rundschreibens in Bezug auf die Compliance-Funktion vorgeschlagen, welches die Compliance als eigenes Hauptkapitel behandelt und auch die Wichtigkeit von Compliance-Schulungen unterstreicht.

II. RUNDSCHREIBEN 2008/21 OPERATIONELLE RISIKEN BANKEN UND 2010/21 VERGÜTUNGSSYSTEME

Auf die Anpassungen der Rundschreiben 2008/1 Operationelle Risiken Banken und 2010/1 Vergütungssysteme wird nicht weiter eingegangen. Querverweise aus den oben aufgeführten Vorschlägen zur Anpassung des Rundschreibens 2016/xx Corporate Governance – Banken sind entsprechend nachzuzeichnen. Diesbezüglich verweisen wir auf unsere Stellungnahme vom 13. August 2009.

* * * * * * *

Wir bedanken uns für die Gelegenheit Stellung nehmen zu können und stehen Ihnen für weitere Rückfragen selbstverständlich zur Verfügung.

Mit freundlichen Grüssen

Prof. Dr. Roland Müller

Präsident der Fördergesellschaft
des FAA-HSG

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Eidgenössische Finanzmarktaufsicht
FINMA
Herr Peter Rütschi
Laupenstrasse 27
CH-3003 Bern

peter.ruetschi@finma.ch

Datum 20. April 2016
Kontaktperson Michele Vono
Direktwahl 061 206 66 29
E-Mail m.vono@vskb.ch

Stellungnahme des VSKB zu den FINMA-Rundschreiben 2016/xx «Corporate Governance – Banken», 2008/21 «Operationelle Risiken Banken» und 2010/01 «Vergütungssysteme»

Sehr geehrter Herr Rütschi
Sehr geehrte Damen und Herren

Am 1. März 2016 hat die Eidgenössische Finanzmarktaufsicht FINMA die Anhörung zu den Rundschreiben 2016/xx «Corporate Governance – Banken», 2008/21 «Operationelle Risiken Banken» und 2010/01 «Vergütungssysteme» eröffnet. Wir danken Ihnen für die Gelegenheit zur Stellungnahme. Gerne übermitteln wir Ihnen nachfolgend unsere Einschätzungen zu den drei Rundschreiben.

Zusammenfassung

Grundsätzlich ist das Bestreben der FINMA zu begrüssen, die aktualisierten internationalen Richtlinien für Corporate Governance und die Regeln für ein effektives Risikomanagement auf Ebene Rundschreiben übergreifend zu regeln. Die vorliegenden Entwürfe weisen allerdings erhebliche Defizite auf, die es zu korrigieren gilt:

- Den politischen und rechtlichen Realitäten der Kantonalbanken und damit auch den Anforderungen der Public Governance wird im Rundschreiben «Corporate Governance – Banken» zu wenig Rechnung getragen. Einige Bestimmungen im Rundschreiben (Rz 16, Rz 36 ff.) würden gar die rechtlichen Vorgaben auf kantonaler Ebene tangieren, ohne

dass dazu eine Notwendigkeit besteht noch ein Beitrag zur Lösung eines Problems bzw. eines Missstandes geleistet würde.

- Dem erklärten Grundsatz der Prinzipienorientierung wird in den Rundschreiben unzureichend nachgelebt. Zahlreiche Regelungen sind zu detailliert und lassen den Banken keinen ausreichenden Spielraum für eine verhältnismässige und flexible Umsetzung. Auch ist eine völlige Abkehr vom Prinzip des «Comply or explain» unter diesem Gesichtspunkt verfehlt und folgerichtig zu unterlassen.

- Das Proportionalitätsprinzip muss ebenfalls konsequenter und sachgerechter umgesetzt werden (Rz 9). Die zugrundeliegende Kategorisierung muss auch relevante Kriterien wie Komplexität, Struktur oder Risikoprofil berücksichtigen. Ein pauschaler Einbezug aller Banken der Aufsichtskategorie 3 in den Anwendungsbereich des Rundschreibens geht klar zu weit und ist abzulehnen.

- Das Unterlaufen der Gewaltentrennung zwischen dem Oberleitungsorgan und der Geschäftsleitung (Liquiditätsmanagement [Rz 14], Besetzung von Schlüsselpersonen [Rz 15], Bestimmung externe Prüfgesellschaft [Rz 16], Strukturveränderungen und Investitionen [Rz 17], direkte Reporting Lines unter Umgehung der Geschäftsleitung [Rz 35]) ist nicht sachgerecht und wird abgelehnt. Es darf nicht sein, dass dem Oberleitungsorgan – welches für die Aufsicht und Kontrolle zuständig ist – auch noch operative Kompetenzen zugeordnet werden.

- Mit der Anforderung, dass Institute der Aufsichtskategorie 1 bis 3 einen Risiko- und Prüfausschuss einrichten und ein detailliertes Pflichtenheft umsetzen müssen (Rz 36 ff.), übertrifft die FINMA internationale Empfehlungen und betreibt damit ein inakzeptables «Gold Plating». Mit Verweis auf die Grundsätze der Proportionalität und Prinzipienorientierung sind die Regelungen betreffend Ausgestaltung der Ausschüsse zwingend nur für systemrelevante Banken vorzusehen. Zudem besteht kein bankenaufsichtsrechtlicher Grund, wieso der Präsident des Oberleitungsorgans nicht auch Vorsitzender eines Ausschusses sein kann (Rz 38).

1. Allgemeine Bemerkungen

Die FINMA will mit den vorliegenden Revisionen die aktualisierten internationalen Richtlinien für Corporate Governance (vgl. v.a. BCBS Guidelines «Corporate Governance Principles for Banks», 2015) und die Regeln für ein effektives Risikomanagement auf Ebene Rundschreiben regeln. Dagegen ist aus Sicht der Kantonalbanken prinzipiell nichts einzuwenden. Die Kantonalbanken unterstützen ein modernes Aufsichtsrecht, das auf der Höhe der internationalen Anforderungen steht und an die schweizerischen Verhältnisse angepasst ist. Die vorliegenden Entwürfe zu den Rundschreiben weisen in ihrer Konzeption und Systematik allerdings einige grundsätzliche Defizite auf, die es zwingend zu korrigieren gilt. Nachfolgend umreissen wir zunächst unsere allgemeinen Kernanliegen in Bezug auf die besondere Eigentümerstruktur der Kantonalbanken, die Grundsätze der Prinzipienorientierung und der

Proportionalität sowie die begriffliche Systematik und Konsistenz in den Rundschreiben. Die konkreten Anmerkungen zu den verschiedenen Rundschreiben bzw. Randziffern finden Sie im Anschluss daran in Kapitel 2.

a) Der besonderen rechtlichen und politischen Situation der Kantonalbanken muss besser Rechnung getragen werden

Mit Blick auf die besondere Eigentümerstruktur und die rechtlichen Voraussetzungen der Kantonalbanken geben wir zu bedenken, dass insbes. das Rundschreiben 2016/xx «Corporate Governance – Banken» massgebliche und einschneidende Auswirkungen auf Prozesse und Strukturen der Governance der Banken haben wird, die sich in manchen Fällen nicht ohne Weiteres mit den bestehenden gesetzlichen Regelungen auf kantonaler Ebene vereinbaren lassen bzw. partiell mit diesen im Widerspruch stehen. Einige Bestimmungen des Rundschreibens würden bei einzelnen Kantonalbanken Änderungen der rechtlichen Vorgaben auf kantonaler Ebene (auf Stufe Gesetz, möglicherweise gar Verfassung) nötig machen, ohne dass dabei aus Sicht der betroffenen Kantonalbank eine Notwendigkeit noch aus gesamtheitlicher Sicht ein (wesentlicher) Beitrag zur Lösung eines Problems oder eines konkret vorhandenen Missstandes geleistet würde. Zudem berücksichtigen einzelne der neu vorgeschlagenen Vorgaben des Rundschreibens die Gegebenheiten und Realitäten einer Kantonalbank nur ungenügend. Die Regelung der Governance einer Kantonalbank kann sich aufgrund ihrer rechtlichen und politischen Voraussetzungen (Eigentümerstruktur, Leistungsauftrag u.a.) nicht allein an Erfordernissen eines Privatunternehmens ausrichten. Manche Regelungen, die für ein Privatunternehmen sinnvoll und geboten sein mögen, machen für eine Kantonalbank mit dem Kanton als alleinigem oder zumindest mehrheitlichem Eigentümer wenig Sinn und lassen sich so nicht vernünftig umsetzen. Beispielhaft sei hier auf die Vorgaben zur Bestimmung der Prüfgesellschaft durch das Oberleitungsorgan (Rz 16) oder die personelle Ausgestaltung der Ausschüsse des Oberleitungsorgans (Rz 36 ff.) verwiesen (vgl. dazu auch unsere spezifischen Bemerkungen unten).
Diesen Realitäten und damit auch den Anforderungen der Public Governance muss besser Rechnung getragen werden. Gefordert ist grundsätzlich mehr Flexibilität und Spielraum bei der Umsetzung der Vorgaben durch konsequentere Prinzipienorientierung (vgl. nächsten Abschnitt).

b) Der Grundsatz der Prinzipienorientierung muss konsequent umgesetzt werden

Die FINMA bezeichnet die Prinzipienorientierung explizit als wichtige «Zielvorstellung» (vgl. RS 2016/xx «Corporate Governance – Banken», Rz 9; FINMA-Erläuterungsbericht, S. 8). Die Kantonalbanken unterstützen diesen Grundsatz ausdrücklich und begrüssen das klare Bekenntnis der FINMA. Mit Blick auf die Revisionsentwürfe müssen wir allerdings feststellen, dass dem Grundsatz der Prinzpienorientierung unzureichend nachgelebt wird. Zahlreiche Regelungen sind ausgesprochen detailliert und lassen den Banken keinen ausreichenden Spielraum für eine, auf die jeweilige Situation abgestimmte, verhältnismässige und flexible Umsetzung. Wenn die FINMA ihren eigenen Grundsatz ernst nimmt, muss hier dringend mehr Flexibilität bei der Umsetzung gewährleistet werden. Dies erachten wir insbesondere bei der Regelung zur Ausgestaltung der Ausschüsse und des Oberleitungsorgans für zwingend. Dies kann bspw. durch eine vermehrte Verwendung von Kann-Formulierungen erfolgen. Vor diesem Hintergrund erachten wir auch die völlige Abkehr vom Prinzip des «Comply or explain» für ungerechtfertigt und verfehlt. Dieses bewährte Prinzip ermöglicht es den Instituten, die aufsichtsrechtlichen Vorgaben im Rahmen eines vernünftigen Ermessensspielraums, angepasst an die konkreten Verhältnisse, differenziert nach Grösse, Komplexität der Organisationsstruktur sowie nach sachlichem und geographischem Geschäftskreis, um-

zusetzen (vgl. bisher FINMA-RS 2008/24, Rz 9 und ferner Rz 101 und Rz 114). Ein vernünftiger Ermessenspielraum bei der Umsetzung ist auch insofern angezeigt, als die umfassend beaufsichtigten Institute nach Bankenrecht eine jederzeitige Gewähr für eine optimale Organisation und eine einwandfreie Geschäftsführung sicherzustellen haben (Art. 3 Abs. 2 lit. a u. c BankG). Die FINMA will dieses bewährte und sachlich angemessene Prinzip nun zu Gunsten eines unnötig komplizierten Systems von detaillierten Kategorisierungen und Ausnahmebewilligungen zu allen möglichen Themen ersetzen. Entgegen erklärtem Anspruch der FINMA produziert gerade dieses neue System allzu detaillierte Regelungen, welche den in Aussicht gestellten und auch wünschenswerten prinzipienorientierten Ansatz beeinträchtigen. Die Kantonalbanken fordern deshalb, dem Prinzip der Prinzipienorientierung stärker Rechnung zu tragen, den Grundsatz «Comply or explain» beizubehalten und vermehrt mit Kann-Formulierungen zu arbeiten (vgl. die spezifischen Bemerkungen unten).

c) Das Proportionalitätsprinzip ist umfassend im Rahmen einer ergänzten Bankenkategorisierung sicherzustellen

Ähnlich wie der Grundsatz der Prinzipienorientierung muss auch der Grundsatz der Proportionalität konsequent und sachgerecht umgesetzt werden. Denn die Bedeutung dieses Prinzips ist mit Blick auf eine differenzierte und verhältnismässige Regulierung gerade für kleine und mittelgrosse Banken nicht hoch genug einzuschätzen. Im Rahmen der Entwürfe zum Rundschreiben «Corporate Governance – Banken» orientiert sich die FINMA dabei an der Aufsichtskategorisierung nach FINMA-RS 2011/02 «Eigenmittelpuffer und Kapitalplanung Banken». Diese primär grössenorientierte Kategorisierung mag für Zwecke der Eigenmittel- und Liquiditätsregulierung sachgerecht und ausreichend sein. Für Zwecke der Risikokontrolle und Corporate Governance ist sie jedoch unzureichend, da sie massgebliche Kriterien wie die Komplexität oder das Risikoprofil eines Instituts nicht angemessen abbildet. Wie die FINMA im Rundschreiben «Corporate Governance – Banken» in Rz 9 in Anlehnung an die Basler Principles selbst betont, muss sich das Proportonalitätsprinzip neben der Grösse insbesondere auch an der Komplexität, der Struktur und dem Risikoprofil der Institute ausrichten. Mit anderen Worten: Die Gewährung von generellen Ausnahmen oder Erleichterungen soll sich nicht nur an der Grösse der Institute orientieren, sondern auch an deren Komplexität und Risikoprofil. Es ist insofern nicht sachgerecht und auch nicht nachvollziehbar, dass eine mittelgrosse, regional tätige Retailbank der Kategorie 3, die ein konservatives, risikoarmes und auch für Dritte nachvollziehbares Geschäftsmodell verfolgt, die gleichen Anforderungen an Risikokontrolle und Compliance erfüllen muss wie eine international agierende, systemrelevante Grossbank – zumal sich die entsprechenden Anforderungen an internationalen Empfehlungen orientieren, die für international systemrelevante Grossbanken (mit Rechtsform Aktiengesellschaft) gedacht sind. Insbesondere lehnen wir den pauschalen Einbezug aller Banken der Aufsichtskategorie 3 in den Anwendungsbereich des Rundschreibens ab.

Für das Rundschreiben «Corporate Governance – Banken» bräuchte es aus den oben genannten Gründen eigentlich eine eigene ausgewogene Kategorisierung, die die Kriterien Komplexität und Risikoprofil ebenso umfasst wie die Grösse. Da die Schaffung einer eigenen Kategorisierung mit einem (zeitlichen) Aufwand zur Erarbeitung verbunden sein dürfte und daher zum jetzigen Zeitpunkt nicht verfügbar ist, fordern wir, dass das Rundschreiben «Corporate Governance – Banken» zwar grundsätzlich für alle Institute gilt, dabei jedoch sachgerecht zwischen systemrevanten Banken (SIFIs) einerseits und den restlichen Banken (Non-SIFIs) andererseits differenziert (so dass die Abgrenzung grundsätzlich zwischen die Aufsichtskategorien 2 und 3 zu liegen kommt). Der FINMA sollte es mit einer entsprechenden «Kann-Formulierung» vorbehalten sein, im Einzelfall Verschärfungen anzuordnen, wenn Non-

SIFIs bzw. Institute der Aufsichtskategorie 3 bis 5 aus Sicht der FINMA ein komplexes Geschäftsmodell verfolgen oder ein hohes Risikoprofil aufweisen (oder fallweise aus anderen Gründen).
Aus Gründen der Rechtssicherheit ist sodann sicherzustellen, dass die Anwendbarkeit einer konkreten Bestimmung für bestimmte Bankenkategorien unmissverständlich und in positiver Weise (nicht *ex negativo*) in den Randziffern vermerkt werden. Mit anderen Worten: Es muss nicht nur explizit festgehalten werden, für welche Banken die Regel gilt, sondern auch, welche Banken davon ausgenommen sind.

d) Die begriffliche Systematik und Konsistenz in den Rundschreiben ist zu verbessern
Schliesslich erachten wir die Rundschreiben hinsichtlich der Begriffsdefinitorik und -systematik für stark verbesserungsbedürftig. Kernbegriffe wie «Risikoappetit», «Risikotoleranz», «Compliance-Funktion» etc. werden unzureichend definiert und nicht angemessen von anderen relevanten Kategorien bzw. Konzepten abgegrenzt. Ebenso zeigen sich an verschiedenen Stellen Widersprüche oder Inkonsistenzen zur Begriffsverwendung in anderen Rechtstexten (Verordnungen, Rundschreiben).
Es ist aus Gründen der Rechtssicherheit und der praktischen Umsetzbarkeit unabdingbar, dass die relevanten Kernbegriffe klar, konsistent und trennscharf definiert werden. Zudem sollte ein Glossar zu den relevanten Kernbegriffen zur Verfügung gestellt werden.

2. Spezifische Bemerkungen zu den Rundschreiben

2.1 Rundschreiben 2016/xx «Corporate Governance – Banken»

II. Begriffe

Rz 5
Die in Rz 5 verwendeten Begriffe «Risikoappetit» und «Risikotoleranz» sind nicht konsistent zu anderen FINMA-Rundschreiben (bspw. 2008/21, 2008/15, 2008/32). Weiter wird im aktuellen Rundschreiben der Begriff «Risikoappetit» nicht richtig verwendet, denn dieser entspricht viel eher der «Risikotoleranz». Die «Risikotoleranz» entspricht dem Risiko, welches ein Unternehmen zu tragen bereit ist bzw. tragen kann. Sie diktiert damit die Risikolimiten des Oberleitungsorgans. Der «Risikoappetit» hingegen entspricht demjenigen Risiko, das ein Unternehmen im Rahmen seiner Möglichkeiten eingehen will. Dies wird exemplarisch im FINMA-Rundschreiben 2008/32 «Corporate Governance Versicherer» deutlich, wo es bei Rz 17 heisst: «Das Unternehmen legt seiner Grösse und Komplexität angemessene Risikostrategien fest, wobei der Risikoappetit und die Risikotoleranz zu berücksichtigen sind. Die Risikotoleranz begrenzt sich durch die ökonomische Wertverminderung, die ein Unternehmen zu tragen bereit ist oder aufgrund geeigneter Massnahmen tragen kann. Sie hängt ab von den vorhandenen Ressourcen (Kapital, HR, IT) und diktiert die Risikolimiten. Der Risikoappetit umfasst das Risiko, das ein Unternehmen im Rahmen seiner Möglichkeiten eingehen will.»

Rz 8
Rz 8 steht im Widerspruch zu den Aufgaben und Verantwortlichkeiten der Compliance-Funktion in Rz 99 ff. In Rz 8 fehlen eine klare Definition der Compliancerisiken, eine Abgrenzung zur Funktion der Risikokontrolle sowie zur Geschäftsleitung. Die auf dieser unklaren Basis geregelten Folgen für die Compliance-Funktion sind dementsprechend lückenhaft,

missverständlich und teilweise auch falsch geregelt (vgl. dazu Stellungnahme der Zürcher Kantonalbank). Wir fordern daher eine ersatzlose Streichung von Rz 8.

III. Geltungsbereich (Proportionalitätsprinzip)

Rz 9
Mit der zugrunde gelegten Aufsichtskategorisierung kann dem Proportionalitätsprinzip nicht angemessen entsprochen werden, da sie relevante Kriterien wie Komplexität oder Risikoprofil zu wenig berücksichtigt (vgl. Anmerkungen in Kap. 1 oben). Das Konzept ist für den vorliegenden Regulierungs- und Aufsichtszweck entsprechend zu ergänzen. Von Erleichterungen und Ausnahmen sollen nicht nur kleine Institute der Kategorien 4 und 5, sondern auch risikoarme und wenig komplexe, mittelgrosse Institute der Aufsichtskategorie 3 profitieren können. Dementsprechend fordern wir eine sachgerechte Differenzierung zwischen systemrevanten Banken (SIFIs bzw. Aufsichtskategorie 1 und 2) einerseits und den restlichen Banken (Non-SIFIs bzw. Aufsichtskategorie 3 bis 5) andererseits. Der FINMA sollte es mit einer entsprechenden «Kann-Formulierung» vorbehalten sein, im Einzelfall Verschärfungen anzuordnen, wenn Non-SIFIs bzw. Institute der Aufsichtskategorie 3 bis 5 aus Sicht der FINMA ein komplexes Geschäftsmodell verfolgen oder ein hohes Risikoprofil aufweisen (oder fallweise aus anderen Gründen). Schliesslich erachten wir es aus Gründen der Rechtssicherheit für wichtig, dass die Anwendbarkeit einer konkreten Bestimmung für bestimmte Bankenkategorien unmissverständlich und in positiver Weise (nicht *ex negativo*) in den Randziffern vermerkt werden. Es muss nicht nur explizit festgehalten werden, für welche Banken die Regel gilt, sondern auch welche Banken davon ausgenommen sind.

IV. Oberleitungsorgan

A. Aufgaben und Verantwortlichkeiten

Rz 10
Das Oberleitungsorgan sollte die Geschäftsleitung auch weiterhin «beaufsichtigen» und nicht auch noch «kontrollieren». Weiter schlagen wir vor, dass das Wort «entwickelt» durch «legt fest» ersetzt wird.

b) Organisation

Rz 13
Der Begriff «Weisungen» als Unterbegriff der «Reglemente» ist missverständlich, da damit kaum einzelfallbezogene Anweisungen gemeint sein können. Ausserdem geht die FINMA hier von einer Zuordnung der Kompetenz zum Erlass von Weisungen an das Oberleitungsorgan aus. Diese Zuordnung stimmt jedoch nicht zwangsläufig mit den Richtlinien von Banken überein. Der Begriff «Weisungen» ist daher ersatzlos zu streichen.

c) Finanzen

Rz 14
Gemäss Rz 14 soll das Oberleitungsorgan die von der Geschäftsleitung erstellte Liquiditätsplanung periodisch genehmigen. Die Anforderung ist inkonsistent zum Rundschreiben 2015/2 «Liquiditätsrisiken Banken». Dort steht, dass das Oberleitungsorgan die Liquiditätsrisikotoleranz festlegen soll. Die Liquiditätsplanung ist eine operative Tätigkeit, welche in hoher Kadenz erfolgen muss (unter Umständen in Krisensituationen täglich). Das Oberleitungsorgan soll nicht in die operative Steuerung eingreifen. Es muss genügen, wenn das Oberleitungsor-

gan die Liquiditätsrisikotoleranz festlegt. Die Bestimmung sollte entsprechend angepasst werden.

d) Personelle und weitere Ressourcen
Rz 15
Die Wahl resp. Abberufung von Personen in Schlüsselfunktionen durch das Oberleitungsorgan erachten wir mit Blick auf die Trennung von Verantwortlichkeiten als kritisch. Da diese Personen oft Geschäftsleitungsmitgliedern unterstellt sind, kann dies zu Interessenskonflikten führen. Die sehr offene Formulierung «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) [Hervorhebungen d. Verf.]» kann dazu führen, dass das Oberleitungsorgan das ganze Management bestimmen müsste. Vor diesem Hintergrund besteht zudem die Gefahr, dass bei Interessenkonflikten zwischen Oberleitungsorgan und Geschäftsleitung die Personen in leitenden Kontroll- und Schlüsselfunktion zur taktischen «Manövriermasse» werden. Aus diesem Grund erachten wir Rz 15 für problematisch. Die Wahl resp. Abberufung von Personen in Schlüsselfunktionen soll weiterhin der Geschäftsleitung vorbehalten sein. Zudem sollten die unter Rz 15 erwähnten Schlüsselfunktionen (bspw. «Head IT», etc.) näher beschrieben werden.

e) Überwachung und Kontrolle
Rz 16
Gemäss Rz 16 muss das Oberleitungsorgan die externe Prüfgesellschaft bestimmen. Diese Bestimmung steht im Widerspruch einerseits zu Art. 698 Abs. 2 OR und andererseits zu gewissen Kantonalbanken-Gesetzen (z.B. Gesetz über die Thurgauer Kantonalbank Art. 12.). Die Wahl der externen Prüfgesellschaft sollte weiterhin durch die Eigentümer des Instituts erfolgen können.

f) Strukturveränderungen und Investitionen
Rz 17
Wir sind der Meinung, dass das Oberleitungsorgan nur über wesentliche bzw. bedeutende Änderungen der Unternehmensstruktur entscheiden sollte. Ausserdem sollten die Kompetenzen für allfällige Funktionsauslagerungen bei der Geschäftsleitung verbleiben.

B. Mitglieder des Oberleitungsorgans
a) Allgemeine Voraussetzungen
Rz 18 und Rz 19
Im Sinne des Proportionalitätsgrundsatzes erachten wir es als wichtig, dass die fachlichen Anforderungen an die Mitglieder des Oberleitungsorgans mindestens im Fall von kleineren Instituten nicht an den Anforderungen an eine Grossbank ausgerichtet werden. Es ist kaum möglich, dass bei einer regional tätigen Bank sämtliche Mitglieder des Oberleitungsorgans über vertiefte Kernkompetenzen in den banktechnischen Belangen verfügen.
Darüber hinaus sollten keine konkreten «zentralen Bereiche» vorgegeben werden, die im Oberleitungsorgan vertreten sein müssen. Wichtig sind angemesse diversifizierte Kompetenzen im Oberleitungsorgan, welche in Bezug auf die Geschäftsfelder und Risiken des Instituts adäquat sind. Hier wäre mehr Prinzipienorientierung angezeigt. Rz 18 und Rz 19 sind entsprechend anzupassen.

b) Unabhängigkeit
Rz 25
Gemäss Rz 25 dürfen die Mitglieder des Oberleitungsorgans keine geschäftlichen Beziehungen zum Institut unterhalten, welche aufgrund ihrer Art oder ihres Umfangs zu einem Interessenkonflikt führen. Für kleine und mittlere Banken mit lokaler und regionaler Ausrichtung ist hier eine Ausnahmebestimmung vorzusehen oder es muss sichergestellt sein, dass diesbezüglich die Ausstandspflicht (vgl. Rz 33) zur Anwendung kommen kann.

C. Grundsätze der Mandatsführung
Rz 31
Analog zu Rz 15 weisen wir auch hier auf einen möglichen Interessenkonflikt im Rahmen der Festlegung des Anforderungsprofils für Schlüsselpersonen hin. Die Anforderungsprofile von Schlüsselpersonen, welche der Geschäftsleitung unterstellt sind, sollten auch von dieser definiert werden können.

Rz 32
An Mitglieder des Oberleitungsorgans kleiner und mittlerer, lokal und regional tätiger Banken sollten nicht die gleichen Anforderungen an Weiterbildung, Kenntnis der Regulatorien etc. gestellt werden wie an solche von international tätigen Grossbanken. Im Sinne der Proportionalität fordern wir hier eine Ausnahmeregelung oder Erleichterungen (z.B. im Sinne einer Kann-Formulierung).

D. Arbeitsteilung und Ausschüsse
a) Rolle des Präsidenten
Rz 35
Bei kleinen und mittleren, lokal und regional orientierten Instituten soll der Dialog zu den Personen in leitenden Kontrollfunktionen über die Geschäftsleitung laufen können und nicht direkt über den Präsidenten des Oberleitungsorgans. Eine entsprechende Ausnahmeregelung oder Erleichterungen sind vorzusehen.

b) Ausschüsse
Rz 36 ff.
In Rz 36 ff. werden auf Stufe Oberleitung konkrete Ausschüsse (Risiko- und Prüfausschuss) für Institute der Aufsichtskategorie 1 bis 3 definiert und diesen zudem detaillierte Pflichtenhefte zugewiesen. Der von der FINMA im Erläuterungsbericht «Corporate Governance – Banken» erwähnte Anspruch der prinzipienorientierten Regulierung (Ziff. 2 Abs. 2) wird in Rz 36 ff. klar zu wenig nachgekommen. Mit den vorgeschlagenen Anforderungen geht die FINMA sogar über die internationalen Empfehlungen des Basler Ausschuss hinaus. Denn dieser hält explizit fest (S. 19 ff.): «A audit committee and risk committee should be required for systemically important banks and is strongly recommended for other banks based on an organisation's size, risk profile or complexity[1]». Wir gehen davon aus, dass die Kantonalbanken der Kategorie 3 mit ihrem vergleichsweise risikoarmen, inlandorientierten und wenig komplexen Geschäftsmodells nicht zwingend in den Geltungsbereich der empfohlenen Richtlinien des Basler Ausschusses fallen, womit sich auch keine entsprechende Anforderungen an deren Ausschüsse aufdrängen.
Mit Blick auf die realen Verhältnisse sind die im Entwurf zum Rundschreiben gestellten Anforderungen betr. Prüf- und Risikoausschuss für die allermeisten Kantonalbanken der Auf-

[1] Basel Committee on Banking Supervision – Guidelines - Corporate governance principles for banks (July 2015)

sichtskategorie 3 nicht oder nur mit unverhältnismässigem Aufwand umzusetzen. Insbesondere die Anforderung, die Ausschüsse auch personell hinreichend zu differenzieren, ist aus Sicht der betroffenen Kantonalbanken nicht praktikabel. Es hätte zur Folge, dass bei gewissen Instituten das Oberleitungsorgan personell erweitert werden müsste, was einzelnen Kantonalbanken aufgrund der gesetzlichen Vorgaben nicht möglich ist.
Weiter hält das Rundschreiben fest, dass der Präsident des Oberleitungsorgans grundsätzlich weder dem Prüfungsausschuss angehören noch Vorsitzender eines anderen Ausschusses sein solle. Aus unserer Sicht gibt es keinen bankenaufsichtsrechtlichen Grund, weshalb der Präsident nicht auch Vorsitzender eines Ausschusses sein kann. Es besteht zudem keine FINMA-Kompetenz, solches hier einschränkend zu regeln. Der Präsident des Oberleitungsorgans bei Kantonalbanken nimmt vielfach wichtige Aufgaben innerhalb der Ausschüsse wahr und fungiert oftmals gemeinsam mit dem CEO als erste Kontaktperson für die Eigner der Bank bzw. für den Regierungsrat. Schliesslich ist festzuhalten, dass die Formulierung im Rundschreiben, wonach die Mehrheit der Mitglieder des Prüf-, Risiko- und Nominationsausschusses unabhängig sein müsse (Rz 38), im Ergebnis dazu führt, dass der Spielraum für die sinnvolle Besetzung sämtlicher Ausschüsse massiv eingegrenzt wird. Auch wird mit dieser Formulierung Rz 21 tangiert, welche besagt, dass mindestens 1/3 des Oberleitungsorgans unabhängig sein muss.
Im Verweis auf die Grundsätze der Proportionalität und Prinzipienorientierung fordern wir, dass die vorgeschlagenen Regelungen betr. Ausgestaltung der Ausschüsse (Rz 36) nur für systemrelevante Banken gelten und für die übrigen Banken Ausnahmen bzw. Erleichterungen bei der Umsetzung (z.B. durch Kann-Formulierungen) vorgesehen werden. Ausserdem fordern wir, dass Rz 37 und Rz 38 ersatzlos gestrichen werden.

V. Geschäftsleitung

A. Aufgaben und Verantwortlichkeiten

Rz 62

Gemäss Rz 15 ist das Oberleitungsorgan für Ressourcen wie beispielsweise Infrastruktur oder IT verantwortlich. Gemäss Rz 62 trägt jedoch die Geschäftsleitung diese Verantwortung. Dieser Widerspruch sollte korrigiert werden.

VI. Rahmenkonzept für das institutsweite Risikomanagement

Rz 70

Aufgrund der aktuellen Formulierung bleibt unklar, wo die erwähnten «aufsichtsrechtlichen Definitionen» zu finden sind. Dies sollte entsprechend präzisiert werden.

VII. Internes Kontrollsystem

Rz 79

Gemäss Rz 79 hat das Institut 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. Aus unserer Sicht kann realistischerweise nicht sichergestellt werden, dass sämtliche Arbeitsprozesse erfasst werden. Die Formulierung sollte dahingehend angepasst werden, dass lediglich «wesentliche Arbeitsprozesse» zu erfassen sind. Das Rundschreiben 2008/32 «Corporate

Governance Versicherer» hält ebenfalls fest, dass beim Risikomanagement und beim Internen Kontrollsystem wesentliche Risiken im Fokus stehen. Das Ziel sollte aus Gründen der Praktikabilität und Umsetzbarkeit insofern nicht auf Vollständigkeit, sondern Wesentlichkeit gelegt werden. Nutzen und Aufwand stehen sonst in keinem angemessenen Verhältnis. Die Formulierung von Rz 79 sollte entsprechend angepasst werden.

Rz 80 und Rz 81
Der Begriff der «ertragsorientierten Geschäftseinheit» ist unklar und sollte präzisiert werden. Aktuell verlangen die Rz 80 und Rz 81, dass «nicht-ertragsorientierte Geschäftseinheiten» (bspw. Backoffice, IT, etc.) ihre Risiken nicht bewirtschaften müssen. Falls diese Interpretation nicht richtig ist, müssten die Rz 80 und Rz 81 entsprechend angepasst bzw. präzisiert werden.

B. Unabhängige Kontrollinstanzen
b) Aufgaben und Verantwortlichkeiten der Risikokontrolle
Rz 93
Aus unserer Sicht muss es für kleine und mittlere, lokal und regional orientierte Banken genügen, wenn sich die Risikokontrolle auf die Kontrolle von Bestehendem beschränkt und nicht bereits schon bei der Entwicklung von Dienstleistungen/Produkten ansetzen muss. Die geringeren personellen Kapazitäten lassen bei diesen Banken eine entsprechende Ausweitung der Funktion nicht oder nur schwer zu.

Rz 95
Gemäss Rz 95 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. Die Setzung der wichtigsten Risikolimiten liegt in der Kompetenz des Oberleitungsorgans. Mit den Risikolimiten bestimmt das Oberleitungsorgan den Risikoappetit. Es ist deshalb die Aufgabe des Oberleitungsorgans zu gewährleisten, dass die Risikolimiten im Einklang zum Risikoappetit stehen. Die Formulierung ist entsprechend anzupassen.

Rz 97
Gemäss Rz 97 muss die Risikokontrolle der Geschäftsleitung mindestens halbjährlich einen Bericht über die Risiken bzw. die Risikopositionen erstatten. Aus unserer Sicht reicht eine jährliche Berichterstattung aus.

C) Aufgaben und Verantwortlichkeiten der Compliance-Funktion
Rz 99 ff.
Im vorliegenden Entwurf findet sich weder eine Definition der Compliance-Risiken noch eine klare Abgrenzung gegenüber operationellen Risiken. Entsprechend unklar bleibt die Abgrenzung zwischen der Compliance-Funktion und der Funktion der Risikokontrolle. Daraus resultieren wiederum diverse Probleme. Es ist zu erwähnen, dass die Aufgaben, Verantwortlichkeiten und Abgrenzung von der Compliance und der Risikokontrolle im FINMA-Rundschreiben 2008/24 «Überwachung und interne Kontrolle Banken» deutlich besser beschrieben werden. Eine klare Trennung der erwähnten Funktionen ist für die Banken massgebend und sollte deshalb fortgeführt werden. Wir verweisen in diesem Zusammenhang auf die Stellungnahme der Zürcher Kantonalbank und schliessen uns den entsprechenden Schlussfolgerungen an.

VII. Interne Revision

C. Aufgaben und Verantwortlichkeiten

Rz 121

Gemäss Rz 121 muss die interne Revision sicherstellen, dass sämtliche risikorelevanten Geschäftsaktivitäten im Rahmen einer Mehrjahresplanung einer Prüfung durch sie selbst oder durch die Prüfgesellschaft unterliegen. Aus unserer Sicht sollte auf diese unnötige Forderung verzichtet werden, da die Mehrjahresplanung offensichtlich weder einem Standard noch einer «best practice» entspricht (siehe nachfolgende Ausführungen):

Standards:

- Basel Committee on Banking Supervision (Juni 2012 ; Ziff. 31): « The internal audit function in banks: annual audit plan that can be part of a multi year plan. (…) plan should be updated at least annually (or more frequently) »
- The Insitute of Internal Auditors (PS 2010.A.1): Die Prüfplanung der internen Revision muss auf Basis einer dokumentierten Risikobeurteilung erfolgen, die mindestens einmal pro Jahr durchzuführen ist. Der Input der leitenden Führungskräfte, der Geschäftsleitung und des Überwachungsorgans müssen dabei berücksichtigt werden.

Best practice:

- Schweizerischer Verband für Interne Revision (2015): In der Enquete 2011 war ein mittelfristiger Prüfplan noch ein Kriterium für die Ausrichtung der jährlichen Prüfplanung. Die aktuelle Bedeutung war zwar noch gegeben, die künftige Bedeutung nahm aber ab. In der Enquete 2014 war eine mittelfristige Planung bereits kein Kriterium mehr. 2011 erfolgte bei 79% die Prüfplanung mit einem Jahr oder weniger. 2014 war dieser Wert bereits 82%.
- PwC – State of the IA profession study (2015): Es findet sich kein Hinweis, dass die Mehrjahresplanung einen relevanten Beitrag liefert.

X. Offenlegung

Rz 128 ff.

Aus Konsistenzgründen sind wir der Meinung, dass alle Offenlegungspflichten im entsprechenden FINMA-Rundschreiben 2016/01 «Offenlegung Banken» publiziert und nicht in verschiedenen Rundschreiben verteilt werden sollten. Eine entsprechende Anpassung ist vorzunehmen.

Rz 133

Während das Wahlverfahren für die Mitglieder des Oberleitungsorgans gesetzlich oder statutarisch festgelegt ist, weist der Rekrutierungsprozess für Geschäftsleitungsmitglieder eine grosse situative Komponente auf. Eine Auflistung aller Möglichkeiten (interne und externe Ausschreibung, Executive Search, etc.) macht aus unserer Sicht wenig Sinn. Die Richtlinie zur Publikation ist daher für die Geschäftsleitung zu streichen.

Rz 134

Für kleine und mittlere Banken, die lokal und regional tätig sind, hat die Risikoausrichtung und die Risikoeinschätzung nicht die gleich ausgeprägte Bedeutung wie bei grossen nationa-

len oder internationalen Banken. Entsprechend sollten bei der öffentlichen Publikation Ausnahmen für kleine und mittlere Banken vorgesehen werden.

Rz 143
Die Informationen über die weiteren Tätigkeiten und die Interessenbindungen der Mitglieder des Oberleitungsorgans und der Mitglieder der Geschäftsleitung (Rz 139) basieren auf manuellen Erhebungen. Die Nachführung auf der Internetseite innerhalb eines Monats – wie in Rz 143 verlangt – ist deshalb kaum praktikabel. Die First von einem Monat sollte angepasst werden.

XI. Inkrafttreten und Übergangsbestimmungen

Rz 145
Die Institute brauchen für eine seriöse Umsetzung der neuen Vorgaben Ressourcen und genügend Zeit. Für einige aufgeführte Themen (bspw. für die Erarbeitung des Rahmenkonzepts) wird im Rundschreiben ein Jahr für die Umsetzung eingeräumt, was zu begrüssen ist. Wir schlagen vor, dass alle Anforderungen bis spätestens nach einem Jahr umgesetzt werden müssen. Konkret könnten die neuen Offenlegungen im nächsten Geschäftsbericht vorgenommen werden und es müssten keine aufwändigen Zwischenlösungen durch zusätzliche Publikationen erarbeitet werden. Sollten die neuen Richtlinien – entgegen unserer Forderungen – auf die Zusammensetzung des Oberleitungsorgans relevante Auswirkungen haben, müsste den Kantonalbanken eine deutlich längere Übergangsfrist eingeräumt werden.

2.2 Rundschreiben 2008/21 «Operationelle Risiken Banken»

Generell

Für die Kantonalbanken fehlt im Rundschreiben 2008/21 «Operationelle Risiken Banken» die Angabe einer angemessenen Übergangsfrist. Dies müsste unbedingt nachgeholt werden. Weiter ist unklar, ob das von der FINMA am 22. Oktober 2010 veröffentlichte Positionspapier zu den Risiken im grenzüberschreitenden Finanzdienstleistungsgeschäft durch das Rundschreiben 2008/21 «Operationelle Risiken Banken» ersetzt bzw. abgelöst wird. Eine entsprechende Präzisierung ist nötig.

IV. Qualitative Anforderungen an den Umgang mit operationellen Risiken

B. Qualitative Grundanforderungen
a) Grundsatz 1: Kategorisierung und Klassifizierung von operationellen Risiken
Rz 122
Gemäss Rundschreiben soll das Oberleitungsorgan die Risikobeurteilung entlang der Dimensionen «Eintrittswahrscheinlichkeit» und «Schadensausmass» im Rahmenkonzept vornehmen. Die Beurteilung der operationellen Risiken in diesem Detaillierungsgrad als Teil des Rahmenkonzepts ist aus unserer Sicht nicht stufengerecht. Sinnvollerweise erfolgt die Einschätzung der «Eintrittswahrscheinlichkeit» und des «Schadensausmasses» laufend durch die operativen Einheiten (wie bei anderen Risikoarten auch). Die Oberleitung sollte lediglich die Vorgaben für die Klassifizierung und die Risikotoleranz festlegen und die Risikokontrolle

und/oder Geschäftsleitung über die wesentlichen operationellen Risiken regelmässig informieren. Rz 122 ist entsprechend anzupassen.

b) Grundsatz 2: Identifizierung, Begrenzung und Überwachung
Rz 130
Wir erachten den Hinweis auf risikobasierte interne Preisfestsetzung (Pricing) resp. Performance Messung als nicht zielführend. Die Grobheit der entsprechenden «Op-Risk»-Modelle mit entsprechend hohem Modellrisiko lassen eine detaillierte Steuerung kaum zu. Zusätzlich besteht die Möglichkeit zu Fehlallokationen, indem zum Beispiel höhere Eigenmittelkosten in Kauf genommen werden, anstatt Investitionen in Prozessverbesserungen zu machen. Rz 130 ist entsprechend anzupassen.

c) Grundsatz 3: Interne und externe Berichterstattung
Rz 133
Gemäss Rz 133 muss eine Bank über eine formelle, vom Oberleitungsorgan genehmigte Offenlegungspolitik verfügen, aus der hervorgeht, wie die Bank ihre operationellen Risiken offenlegt und welche Kontrollprozesse bezüglich Offenlegung anzuwenden sind. Während die Motivation für Rz 133 grundsätzlich nachvollziehbar ist, halten wir eine Anwendung im konkreten Fall für schwierig. Insbesondere besteht die Gefahr, dass geschäftsrelevante Informationen an die Öffentlichkeit und somit auch an die Mitbewerber gelangen. Die FINMA sollte diese Richtlinie entsprechend überdenken.

d) Grundsatz 4: Technologieinfrastruktur
Rz 135 ff.
Gerade bei mittleren und kleinen Banken werden IT-Dienstleistungen oft gesamtheitlich an einen Anbieter vergeben («Outsourcing»). Dies betrifft auch die in Rz 135.1 ff. genannten Anforderungen. Aus unserer Sicht ist es sinnvoll, die Möglichkeit und Zulässigkeit des «Outsourcing» explizit im Rundschreiben festzuhalten.
Während der Inhalt der Punkte in Rz 135 ff. grundsätzlich zu begrüssen ist, halten wir das explizite Festhalten von detaillierten Vorgaben für einen spezifischen Risikobereich für nicht zweckmässig. Gerade mit Blick auf rasch ändernde Gebiete wie die Informatik wäre ein grundsätzlicher Verweis auf entsprechende Standards / Organisationen hilfreicher. Auch hier wäre mithin mehr Prinzipienorientierung angezeigt. Rz 135 ff. sollte entsprechend angepasst werden.
Schliesslich ist unklar, ob die regelmässig durchzuführenden Verwundbarkeitsanalysen und Penetration Testings (vgl. dazu Rz 135.3) für sämtliche Systeme oder nur für CID-relevante Systeme gelten. Zudem wäre zu präzisieren, ob es sich bei den «besonders schützenswerten Daten» um «besonders schützenswerte Personendaten» gemäss Datenschutzgesetz (DSG) oder um «Kundenidentifikationsdaten» gemäss Anhang 3 handeln.

e) Grundsatz 5: Kontinuität bei Geschäftsunterbrechung und Kontinuität von kritischen Dienstleistungen bei der Abwicklung und Sanierung von (systemrelevanten) Banken
Rz 136.3
Im Erläuterungsbericht der FINMA (vgl. dazu Ziffer 4.4) wird zum Grundsatz 5 erwähnt, dass neben den nur für systemrelevante Banken verbindliche Regeln einzelne Vorschriften, wo sinnvoll, auch auf nicht-systemrelevante Banken anwendbar sind. Es ist unklar, welche «einzelnen» Vorschriften dies konkret sind. Eine klare Trennung der Anforderungen für systemrelevante und nicht-systemrelevante Banken wäre zu begrüssen.

In diesem Zusammenhang fällt uns auf, dass zur Vereinfachung einer allfälligen Abwicklung oder Restrukturierung auch nicht-systemrelevante Banken ein Inventar über die aus ihrer Sicht wichtigsten Dienstleistungen zu erstellen und regelmässig zu aktualisieren haben. Wir erachten die Erstellung eines solchen Inventars in diesem Umfang (insbesondere in Bezug auf die Punkte personelle Ressourcen, Preis(-gestaltung) und interne Gebührenerhebung) weder für nötig noch für zielführend. Das Kosten-/ Nutzenverhältnis ist unausgewogen.
Rz 136.3 sollte entweder gestrichen oder es sollten zumindest Erleichterungen für nicht-systemrelevante Banken vorgesehen werden (z.B. als Kann-Formulierung).

f) Grundsatz 6: Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft
Rz 136.4
Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft ergeben sich zumeist aus Regelverstössen. Solche Risiken stellen selbst bei Zugrundelegung der gemäss FINMA-Entwurf (Rz 2) offenen Umschreibung der operationellen Risiken klarerweise Compliance-Risiken dar. Demzufolge erfolgt die Regelung am falschen Ort. Wir verweisen in diesem Zusammenhang auf die Stellungnahme der Zürcher Kantonalbank. Rz 136.4 soll ersatzlos gestrichen werden.

Anhang 3 Umgang mit elektronischen Kundendaten

Grundsätzlich sollte bei der Anwendung der entsprechenden Randziffern das Proportionalitätsprinzip besser berücksichtigt werden. So haben beispielsweise globale Institute mit grenzüberschreitenden Aktivitäten höhere Standards bezüglich Zugriffsrechten und Logverfahren zu gewährleisten als lokal und regional tätige Institute. Dementsprechend sollten für diese Institute Erleichterungen vorgesehen werden. Dies trifft insbesondere auf die folgenden Punkte zu:

C. Grundsatz 3: Datenspeicherort und -zugriff
a) Datenspeicherort und -zugriff allgemein
Rz 17 ff.
Der hohe Detaillierungsgrad von Rz 17 bis Rz 19 stellt aus unserer Sicht eine problematische Abkehr vom prinzipienbasierten Ansatz dar, was wir bereits in der Anhörung im Jahr 2013 kritisiert haben.
Der Zusatz «...entlang der CID-Kategorien und den daraus resultierenden Sicherheitsvorkehrungen» wird nicht benötigt. Die Inventare wurden seitens der Banken in den letzten Jahren erstellt. Der Mehraufwand für die zusätzliche Dokumentation bringt keinen weiteren Nutzen. Die Banken sind mit der Umsetzung der bestehenden Anforderungen ausreichend sensibilisiert. Rz 17 bis 19 sollten ersatzlos gestrichen oder es sollten Erleichterungen / Ausnahmen für kleine und mittlere Banken vorgesehen werden.

E. Grundsatz 5: Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben
d) Liste von Schlüsselmitarbeitenden
Rz 35
Wir halten das explizite Loggen von Massen-CID-Abfragen für unnötig, solange die Daten nicht aus der Systemumgebung heraustransferiert werden können, resp. der Transfer (bspw. via E-Mail) nicht bereits automatisch geloggt wird. Rz 35 ist entsprechend anzupassen.

G. Grundsatz 7: Risikominderung in Bezug auf die CID-Vertraulichkeit
b) Test für die Entwicklung, Veränderungen und Migration von Systemen
Rz 41.1
Solange Entwicklungs-, Test- und Produktionsanlagen im selben geschützten Bereich liegen, ist die Migration von Daten zwischen den Systemen unproblematisch. Eine separate Anonymisierung etc. ist in diesem Zusammenhang unnötig, da vorhandene Zugriffkonzepte die Sichtbarkeit der Daten genügend einschränken. Rz 41.1 ist entsprechend anzupassen.

2.3 Rundschreiben 2010/01 «Vergütungssysteme»

Generell

Grundsätzlich halten wir den Zeitpunkt für substantielle Anpassungen des Rundschreibens 2010/01 «Vergütungssysteme» für verfrüht. Bei der Überführung der «Verordnung gegen übermässige Vergütungen bei börsenkotierten Aktiengesellschaften» (VegüV) in das Gesetz können zum jetzigen Zeitpunkt substantielle Änderungen am Inhalt nicht ausgeschlossen werden. Aufgrund des ergänzenden Charakters des RS 2010/01 zum erwähnten Gesetz ist zu erwarten, dass das Rundschreiben 2010/01 «Vergütungssysteme» wieder angepasst werden muss. Um den Aufwand in Grenzen zu halten, schlagen wir vor, Anpassungen am Rundschreiben erst nach Vorliegen des entsprechenden Gesetzestextes vorzunehmen. Weiter kritisieren wir, dass im vorliegenden Entwurf zum Rundschreiben die Regelung einer Übergangsfrist fehlt. Dies müsste zwingend ergänzt werden.
Schliesslich begrüssen wir die Anhebung der für die primäre Anwendung dieses Rundschreibens genannten Kapitalgrenze auf CHF 10 Mrd. Hingegen halten wir die Ausdehnung des Geltungsbereichs via «Best Practice» für problematisch (vgl. spezifische Bemerkungen).

IV. Grundsätze

Grundsatz 1: Der Verwaltungsrat ist für die Ausgestaltung und Umsetzung der Vergütungspolitik verantwortlich und erlässt ein Vergütungsreglement
Rz 20
Wie bereits bei Rz 15 im Rundschreiben 2016/xx «Corporate Governance – Banken» bezüglich Abgrenzung von Verantwortlichkeiten zwischen Oberleitungsorgan und Geschäftsleitung angemerkt, halten wir die Genehmigung der Vergütungen für den Leiter der Kontrollfunktionen durch den Verwaltungsrat für problematisch. Dies sollte der Geschäftsleitung vorbehalten sein.

Grundsatz 2: Das Vergütungssystem ist einfach, transparent und umsetzbar ausgestaltet sowie langfristig ausgerichtet
Rz 24
Der Ausschluss von Absicherungsgeschäften, welche die Wirksamkeit von Elementen des Vergütungssystems ausser Kraft setzen, halten wir in dieser allgemeinen Form für nicht umsetzbar. Einerseits können «Hedges» durch Personen getätigt werden, welche mit den begünstigten Person eine wirtschaftliche Einheit bilden, aber vom Vergütungssystem nicht erfasst werden. Andererseits können volle oder partielle «Hedges» unbeabsichtigt eingegangen werden. In der gegebenen allgemeinen Formulierung besteht somit die erhebliche Gefahr unbeabsichtigter Verstösse gegen Rz 24. Die Rz 24 sollte unbedingt angepasst werden.

Grundsatz 6: Die Zuteilung der variablen Vergütung erfolgt anhand nachhaltiger Kriterien

Rz 46

Die Ergänzung der Rz 46 mit der Pflicht von «Clawback»-Regelungen ist hinsichtlich rechtlicher Durchsetzbarkeit (insbes. aus arbeits- und steuerrechtlichen Gründen) erheblich in Frage gestellt. Rechtlich kaum durchsetzbare zivilrechtliche Regeln zu neuen aufsichtsrechtlichen Pflichten zu erheben, ist kontraproduktiv und setzt falsche Signale. Demzufolge ist diese Pflicht zu streichen. Sollte die FINMA wider Erwarten auf die Streichung dieser neuen Pflicht verzichten, müsste konsequenterweise eine grosszügige Übergangsfrist gewährt werden. Einschneidende Regeln dieser Art lassen sich nämlich nur rechtsgültig implementieren, nachdem den betroffenen Mitarbeitenden nach vorgängiger Zustellung der Regelung Gelegenheit eingeräumt wurde, bei Nichteinverständnis unter Einhaltung der vereinbarten Kündigungsfrist das Arbeitsverhältnis durch Kündigung aufzulösen. Zahlreiche Segmente von Mitarbeitenden weisen relativ lange Kündigungsfristen von z.B. 6 Monaten auf. Vor Zustellung der geänderten Regelung wäre diese zusammen mit weiteren allfälligen Anpassungen sorgfältig koordiniert mit der bestehenden Regelungsarchitektur auszuformulieren und von sämtlichen Kompetenzträgern bis hin zu den obersten internen Gremien zu verabschieden. Bei Konzernstrukturen müsste die Umsetzung mehrstufig in sämtlichen Konzernteilen erfolgen. Die Übergangsfrist müsste demzufolge wesentlich länger als die längsten Kündigungsfristen sein. Eine Frist von rund 2 Jahren wäre angemessen.

Wir bitten Sie um Berücksichtigung unserer Anliegen und danken Ihnen für Ihre Bemühungen. Gerne stehen wir Ihnen bei Bedarf für eine Erläuterung unserer schriftlichen Ausführungen zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Dr. Adrian Steiner
Leiter Public Affairs

Vereinigung Schweizerischer Assetmanagement- und Vermögensverwaltungsbanken
Association de Banques Suisses de Gestion
Associazione di Banche Svizzere di Gestione Patrimoniale ed Istituzionale
Association of Swiss Asset and Wealth Management Banks

VAV
ABG

Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstrasse 27
3003 Bern
Per E-Mail: peter.ruetschi@finma.ch

Zürich, 20. April 2016

Stellungnahme zu den FINMA-Rundschreiben „Corporate Governance - Banken", Operationelle Risiken Banken" & „Vergütungssysteme"

Sehr geehrter Herr Rütschi

Die Vereinigung Schweizerischer Assetmanagement und Vermögensveraltungsbanken (VAV) ist Ihnen für die Einladung dankbar, zu den Entwürfen und zum Erläuterungsbericht betreffend den oben genannten Rundschreiben Stellung zu nehmen.

Unsere Antwort beschränkt sich auf einige wenige Elemente des Rundschreibens „Corporate Governance - Banken". Für die übrigen Aspekte und die zwei anderen Rundschreiben verweisen wir auf die detaillierte Stellungnahme der Schweizerischen Bankiervereinigung, an deren Ausarbeitung wir aktiv mitgewirkt haben und die wir grundsätzlich unterstützen. Besonders möchten wir den ***geforderten Verzicht auf eine Trennung von Risiko- und Prüfungsausschuss, insbesondere für Banken der Aufsichtskategorie 3, bekräftigen***.

Allgemein:
Corporate Governance und Risk Governance sind zentrale Elemente für den Erfolg, die Bonität, die nachhaltige Entwicklungsfähigkeit und die Krisenresistenz eines Finanzinstituts. Somit bildet die Vorgabe der grundlegenden Prinzipien einen wichtigen Bestandteil der Regulierung. Damit die erwünschte Wirkung besteht, ist allerdings eine spezifische Ausgestaltung und Implementierung entscheidend, abhängig von Kultur, Grösse, Eigentümerstruktur, Organisation und Marktstellung. So hält auch der Erläuterungsbericht fest (S. 9/23): „Die Anforderungen im Rundschreiben sind grundsätzlich prinzipienorientiert. … Corporate Governance und Risikomanagement sind Aufsichtsthemen, welche sich nicht mit einem „one size fits all"-Ansatz prüfen und überwachen lassen". In zentralen Teilen wird jedoch dieser „prinzipienorientierte Grundsatz" nicht konsequent befolgt und die vorgeschlagenen Regeln beschränkten die Institute in der Ausgestaltung von Organisation und Prozessen mehr, als dies zur Zielerreichung erforderlich wäre.

Separation von Risiko- und Prüfungsausschuss:
Eine Abkehr vom „prinzipienorientierten Ansatz" stellt insbesondere Rz 36 dar, die verlangt, dass Institute der Aufsichtskategorie 1-3 einen separaten Prüfausschuss und Risikoausschuss einrichten müssen. Wie im Erläuterungsbericht festgehalten, sieht auch der Basler Ausschuss diese Separierung

nur für systemrelevante Banken zwingend vor, für die übrigen grösseren Banken handelt es sich nur um eine Empfehlung (Erläuterungsbericht S. 11/23). Wichtig ist, dass auf Stufe des Oberleitungsorgans die fachlichen Qualifikationen betreffend Risikomanagement und -kontrolle sowie Prüfwesen vorhanden sind und somit ein kompetent zusammengesetzter Ausschuss die zugewiesenen Aufgaben erfüllen kann. Dass inhaltlich insbesondere betreffend die Themen IKS, operationelle Risiken und Risikokontrolle Überschneidungen bestehen, verdeutlichen die folgenden Randziffern:

- Aufgaben Prüfausschuss, Rz 43: *„Überwachung und Beurteilung der Wirksamkeit der internen Kontrollen, namentlich auch der Risikokontrolle und der Compliance-Funktion, und der internen Revision;"*
- Aufgaben Risikoausschuss, Rz 49: *„Kontrolle, ob das Institut ein geeignetes Risikomanagement mit wirksamen Prozessen unterhält …"*

Die Verwendung des Begriffs „Kontrolle" im Aufgabenkatalog des Risikoausschusses suggeriert zudem eine aktive, operative Kontrolltätigkeit des Risikoausschusses, welche nicht adäquat ist. Auch der Risikoausschuss überwacht interne Kontrollen und Risikokontrollen und stellt damit deren Adäquanz und Wirksamkeit sicher, keinesfalls führt er diese jedoch aus. Somit erfüllt letztlich der Risikoausschuss bezogen auf das IKS und insbesondere die unabhängigen Kontrollfunktionen die gleichen Funktionen wie der Prüfungsausschuss, nämlich die Sicherstellung resp. Überwachung und Beurteilung der Wirksamkeit der internen Kontrollen. Diese inhaltliche Überschneidung kann dazu führen, dass ein integrierter Risiko- und Prüfungsausschuss für ein einzelnes Institut eine adäquatere Lösung darstellt, als die Führung von zwei separaten Ausschüssen.

Vorgaben für die unabhängigen Kontrollinstanzen vs. Vorgaben für die Risikokontrolle i.e.S.:
Die Rz 82ff. definieren die Einrichtung und Unterstellung der unabhängigen Kontrollinstanzen. Sinnvollerweise wird dabei die exakte organisatorische Ausprägung und Eingliederung der Kontrollinstanzen offen gelassen. In den Randziffern 89 jedoch werden verschiedene Aufgaben der Funktion „Risikokontrolle" zugewiesen, die abhängig von der gewählten Organisationsform auch anderen unabhängigen Kontrollinstanzen zugewiesen werden können. So hat z.B. die „Überwachung von Systemen für die Einhaltung von aufsichtsrechtlichen Vorschriften" (Rz 92) nicht zwingend durch die Risikokontrollfunktion zu erfolgen, sondern kann einer anderen unabhängigen Kontrollinstanz wie der Finanzkontrolle oder Compliance zugewiesen werden.

Um dies zu verdeutlichen, wird vorgeschlagen, folgende Formulierung aus dem Erläuterungsbericht (S. 15/23) in das Rundschreiben aufzunehmen, zB als Rz 84a:
„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 werde, bspw. für Sicherheitsthemen, eine unabhängige Finanzkontrolle etc."

Die Rz 87 wäre zudem sinngemäss anzupassen:
„Die Institute der Aufsichtskategorie 1 bis 3 verfügen über eine eigenständige Risikokontrolle, eine Compliance-Funktion sowie allenfalls über weitere Funktionen als unabhängige Kontrollinstanzen. Sie bestimmen einen CRO, einen Chief Compliance Officer und allenfalls weitere Verantwortliche, die für die Kontrollen zuständig sind~~, der für die Risikokontrolle zuständig ist~~."

Aus Konsistenzgründen wäre schliesslich auch die Rz 51 zu ergänzen:
„Der Risikoausschuss erhält vom Chief Risk Officer (CRO) und andern relevanten Funktionsträgern wie insbesondere dem Chief Compliance Officer, dem Head Legal/General Counsel, dem Chief Information Officer und dem Chief Security Officer regelmässig aussagefähige Berichte zu den jeweiligen Aspekten des Rahmenkonzeptes für das institusweite Risikomanagement (gemäss Rz 66ff.) und dessen Einhaltung.“

Zur Verdeutlichung des Grundprinzips der unabhängigen Kontrollinstanzen wird zudem vorgeschlagen, den Begriff der „unabhängigen Kontrollsinstanzen“ unter Abschnitt II. Begriffe zu ergänzen:
„Die unabhängigen Kontrollinstanzen überwachen die Risiken sowie die Einhaltung regulatorischer und interner Vorschriften sowie die Beachtung von marktüblichen Standards. Institutsspezifisch können verschiedene unabhängige Kontrollinstanzen definiert werden.“

Weitere inhaltlich Anpassungsvorschläge:

- Rz 15: Abhängig vom Risikoprofil und der Organisationsform stellt auch jene des Head Legal/General Counsel eine Schlüsselfunktion dar. Dieser sollte somit in der Aufzählung ergänzt werden “(*z.B. Chief Risk Officer, Chief Compliance Officer, Head Legal/General Counsel, Head IT)*”
- Rz 16: Das Oberleitungsorgan richtet das Kontrollsystem (abgesehen von wenigen strukturellen Vorgaben im Rahmenkonzept) nicht ein, sondern stellt dessen Einrichtung sicher. Eine Formulierung die dies berücksichtigt wäre z.B.: *„~~Es richtet ein wirksames internes Kontrollsystem ein…~~Es definiert die Grundsätze zur Kontrolle im Rahmenkonzept, stellt sicher, dass ein wirksames internes Kontrollsystem eingerichtet wird,….“*
- Rz 17: Auch im Falle von Funktionsauslagerungen sollten lediglich wesentliche Auslagerungen im Oberleitungsorgan entschieden werden: *„Das Oberleitungsorgan entscheidet über …., wesentliche Funktionsauslagerungen,…“*
- Rz 18: Die Aufzählung der im Oberleitungsorgan erwähnten Bereiche ist zu ergänzen um HR sowie Legal: *„ ….so dass nebst den Hauptgeschäftsfeldern sämtliche weitere zentralen Bereiche wie Finanz- und Rechnungswesen, Risikomanagement, Controlling, Compliance, Legal, HR und IT kompetent vertreten sind“*
- Dem Informationsfluss zwischen den Ausschüssen kommt wichtige Bedeutung zu, dies sollte jedoch nicht auf den Prüfausschuss und den Risikoausschuss beschränkt werden: *„Zwischen Prüfausschuss und Risikoausschuss sowie weiteren relevanten Ausschüssen sind geeignet Informationsflüsse einzurichten, …“*

Für die Kenntnisnahme und wohlwollende Prüfung unserer Ausführungen möchten wir uns im Voraus bedanken.

Freundliche Grüsse

Dr. Pascal Gentinetta
Geschäftsführer

Simon Binder
Public Policy Manager

Zuger Kantonalbank

Per Email: peter.ruetschi@finma.ch
Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Ruetschi
Laupenstrasse 27
CH-3003 Bern

Zuger Kantonalbank
Baarerstrasse 37, Postfach 1158
6301 Zug
Telefon +41 41 709 11 11
Fax +41 41 709 15 55
www.zugerkb.ch

Kontakt: Dr. Adrian Andermatt
T Direkt: +41 (41) 709 12 60
F Direkt: +41 (41) 725 12 60
adrian.andermatt@zugerkb.ch

Zug, 8. April 2016

Stellungnahme zum FINMA-Rundschreiben 2016/x «Corporate Governance – Banken»

Sehr geehrter Herr Ruetschi

Die Zuger Kantonalbank dankt der Eidg. Finanzmarktaufsicht FINMA für die Einladung zur Stellungnahme in Sachen FINMA-Rundschreiben 2016/x «Corporate Governance – Banken» und verzichtet auf Stellungnahmen zu den sich ebenfalls in Revision befindenden FINMA-Rundschreiben 2008/21 «Operationelle Risiken Banken» und FINMA-Rundschreiben 2010/01 «Vergütungssysteme». Im Weiteren verweist die Zuger Kantonalbank auf die Stellungnahme des Verbands Schweizerischer Kantonalbanken (VSKB).

Die Zuger Kantonalbank nimmt zum FINMA-Rundschreiben 2016/x «Corporate Governance – Banken» (Rundschreiben) innert Frist gerne wie folgt Stellung.

Die Zuger Kantonalbank ist eine an der SIX Swiss Exchange kotierte spezialgesetzliche Aktiengesellschaft nach kantonalem Recht im Sinne von Art. 763 OR, an welcher der Kanton Zug von Gesetzes wegen mindestens 50 % des Aktienkapitals hält. Die Rechtsform der spezialgesetzlichen Aktiengesellschaft, die gesetzliche Einbindung des Kantons Zug in die Corporate Governance der Bank – so insbesondere der Regierungsrat, welcher einerseits Genehmigungsinstanz bezüglich der Entschädigung des Bankrates ist und im Bankrat mit einem Mitglied direkt vertreten wird – und die strategische Ausrichtung der Bank führen dazu, dass die nachfolgenden Regelungen gemäss Rundschreiben aus Sicht der Zuger Kantonalbank überdacht werden sollten:

- Separater Prüfungs- und Risikoausschuss
- Unvereinbarkeit der Funktionen Präsident Bankrat und Vorsitzender des Entschädigungsausschusses
- Kalibrierung von Kategorie 3-Banken

Vorab kann jedoch festgehalten werden, dass die neuen Corporate Governance-Anforderungen der FINMA aus Sicht der Zuger Kantonalbank grundsätzlich in die richtige Richtung zielen. Im Gegensatz zum bisherigen FINMA-Rundschreiben 08/24 «Überwachung und interne Kontrolle Banken» behandelt das neue Rundschreiben die Governance- und Risikoaspekte umfassender, systematischer und integrierter. Die Ausführungen über Verantwortlichkeiten, Aufgaben und Anforderungen betreffend Oberleitungsorgan und Geschäftsleitung, über das Rahmenkonzept Risikomanagement, IKS, Interne Revision und Offenlegung machen aus unserer Sicht ebenfalls Sinn und werden von uns begrüsst. Nun zu den Kritikpunkten.

a) Separater Prüfungs- und Risikoausschuss

Nicht einverstanden ist die Zuger Kantonalbank mit der vorgesehenen Anforderung, dass bereits bzw. sämtliche Banken der Risikokategorie 3 je einen separaten Prüfungs- und Risikoausschuss einzurichten haben, welche unter einander wie auch gegenüber anderen Ausschüssen personell hinreichend getrennt sein müssen. Diese Regelung mag bei grossen und komplexen Instituten allenfalls Sinn machen. Bei der Zuger Kantonalbank macht diese vorgesehene Regelung – unter der Annahme, dass wir auf dem Weg zu einer Kategorie 3-Bank sind - aber aus verschiedenen Gründen keinen Sinn. Einerseits, weil diese Regelung an eine Kantonalbank mit geringer Komplexität unverhältnismässige Anforderungen an entsprechende Ressourcen auf Stufe Oberleitungsorgan stellt. Andererseits, weil trotz der im Rundschreiben relativ klar definierten Aufgaben für die beiden Ausschüsse es unvermeidliche Überschneidungen, so beispielsweise bezüglich operationeller Risiken und Reputationsrisiken, gibt, welche eine ressourcenintensive gegenseitige Abstimmung und einen laufenden Informationsaustausch erfordern. Nebst einer unnötigen Doppelbelastung für die involvierten Mitglieder der Geschäftsleitung führt dies auch zu den genannten Ineffizienzen innerhalb des Oberleitungsorgans sowie auch bei der internen Revision, ohne dass ein Mehrwert für die Bank und ihre Stakeholders erkennbar ist.

Abschliessend zu diesem Thema gilt es festzuhalten, dass die Aufgaben- und Verantwortungsbereiche der beiden Ausschüsse ohne weiteres fachgerecht und auf effiziente Art und Weise durch einen kombinierten Prüfungs- und Risikoausschuss wahrgenommen werden können. Die Zuger Kantonalbank ist heute auch so aufgestellt. Eine Aufteilung in zwei separate Ausschüsse des Bankrates mit personellen Unvereinbarkeiten bedürfte unseres Erachtens einer besonderen Begründung, welche jedoch nicht substantiiert vorliegt.

b) Unvereinbarkeit der Funktionen Präsident Bankrat und Vorsitzender des Entschädigungsausschusses

Im Rundschreiben wird weiter festgehalten, dass der Präsident des Oberleitungsorgans grundsätzlich weder dem Prüfungsausschuss angehören noch Vorsitzender eines andern Ausschusses sein soll. Die Gründe, warum er insbesondere nicht dem Entschädigungsausschuss vorstehen kann, sind nicht bekannt bzw. substantiiert dargelegt worden.

Der Präsident des Bankrates der Zuger Kantonalbank amtet seit mehreren Jahren auch als Vorsitzender des Entschädigungsausschusses (EA). Dies ist auch aus Governance-Sicht aus den nachfolgenden Gründen unproblematisch bzw. begrüssenswert:

- Gemäss Gesetz über die Zuger Kantonalbank genehmigt der Regierungsrat die Vergütung des Bankrates. Entsprechend hat der Bankrat als Oberleitungsorgan im Sinne des Rundschreibens in der Vergangenheit jeweils bei einer beabsichtigten Änderung der Vergütung des Bankrates einen Antrag an den Regierungsrat gestellt, über welchen dieser unabhängig entschieden hat.
- Gemäss Reglement des Entschädigungsausschusses der Zuger Kantonalbank hat der EA keine abschliessenden Kompetenzen, diese liegen allesamt beim Bankrat. Der EA hat somit nur eine Unterstützungsfunktion.

Für die Zuger Kantonalbank ist es weiter auch von Vorteil, dass der Präsident des Bankrates zugleich als Vorsitzender des Entschädigungsausschusses amtet. Zusammen mit dem Präsidenten der Geschäftsleitung ist der Bankpräsident die Kontaktperson zum Regierungsrat und erörtert mit diesem Themen wie Staatsgarantie, Gesetzesänderungen, Finanzabschlüsse, Dividendenpolitik etc. In dieser Konstellation wurde in den letzten Jahren auch die VegüV in enger Zusammenarbeit mit der Zuger Regierung bei der Zuger Kantonalbank auf freiwilliger Basis weitestgehend und im Rahmen des gesetzlich Zulässigen eingeführt.

Da der Kanton mit einem Aktienanteil von gut 50 % der grösste und einflussreichste Aktionär ist, ist eine kompetente, auf Vertrauen basierende Zusammenarbeit auf Augenhöhe mit dem Regierungsrat entscheidend. Es wäre für ein anderes Mitglied des Bankrates schwierig, diese Position einzig in Bezug auf Entschädigungsfragen wahrzunehmen. Auf der andern Seite erwartet auch der Regierungsrat, dass der Bankpräsident die primäre Ansprechperson von Seiten Bank in Bezug auf die genannten Themen ist.

Zusammenfassend kann festgehalten werden, dass es keine guten Gründe dafür gibt, dass der Bankpräsident nicht auch Vorsitzender des EA bei der Zuger Kantonalbank sein sollte, es aber sehr gute Gründe dafür gibt.

c) Kalibrierung von Kategorie 3-Banken

Aus Sicht der Zuger Kantonalbank sollte eine Kategorisierung nicht oder zumindest nicht in erster Linie nach der Grösse einer Bank erfolgen, sondern diese sollte insbesondere auch nach deren Risikoprofil ausgerichtet werden. Die Zuger Kantonalbank beispielsweise unterhält keine Niederlassungen oder Tochtergesellschaften ausserhalb des Kantons oder gar im Ausland, keine Investment Banking Aktivitäten und keinen Eigenhandel und hat auch keine Zielmärkte im Ausland. Die angebotenen Produkte im Aktivgeschäft sind zudem standardisiert. So werden beispielsweise keine Kredite an Gegenparteien mit unübersichtlichen Strukturen vergeben, keine nennenswerten Exportfinanzierungen und keine internationalen Projektfinanzierungen, Leasing oder Factoring gemacht.

Auch wenn die Zuger Kantonalbank das Grössenkriterium von CHF 15 Mia. Bilanzsumme in einiger Zeit erfüllen wird, wird sich am Risikoprofil der Bank nichts Grundlegendes ändern. Umgekehrt ist es durchaus möglich, dass eine Bank, welche das Grössenkriterium bei weitem nicht erfüllt, ein exponierteres Risikoprofil als die Zuger Kantonalbank aufweist. Auch stimmt die Kalibrierung nicht mit den von der FINMA festgehaltenen Eigenschaften überein. Beispielsweise wird eine Kategorie 3-Bank, zu welcher eine Bank mit einer Bilanzsumme von mindestens CHF 15 Mia. bereits zugehört, als grossen und komplexen Marktteilnehmer mit einem bedeutenden Risiko umschrieben. Auf die Zuger Kantonalbank trifft jedoch, auch wenn sie die zuvor genannte Schwelle von CHF 15 Mia. Bilanzsumme überschreiten wird, die Umschreibung eines Marktteilnehmers mittlerer Grösse mit durchschnittlichem Risiko zu, was gemäss FINMA-Beschreibung den Eigenschaften einer Kategorie 4-Bank entspricht.

Aus Sicht der Zuger Kantonalbank wäre es somit angezeigt, dass der Bilanzsummengrenzwert für die Qualifikation als Kategorie 3-Bank von aktuell CHF 15 Mia. auf beispielsweise mindestens CHF 30 Mia. angehoben oder der genannte Grenzwert in Kombination mit einem qualitativen Element, so insbesondere dem Risikoprofil der Bank, kombiniert wird. Sollte an der vorgesehenen Kalibrierung festgehalten werden, wäre zumindest die Pflicht zur Einrichtung von getrennten Prüfungs- und Risikoausschüssen auf Kategorie 2-Banken zu reduzieren.

Besten Dank für die wohlwollende Prüfung unserer Anliegen.

Freundliche Grüsse
Zuger Kantonalbank

Bruno Bonati
Präsident des Bankrates

Heinz Leibundgut
Vorsitzender des Prüfungs- und Risikoausschusses

Recht Steuern & Compliance

Kontakt Werner W. Wyss, VRR
Telefon 044 292 34 71
Fax 044 292 24 54

Briefadresse: Postfach, 8010 Zürich

Per e-Mail
Eidgenössische Finanzmarktaufsicht FINMA
Herr Peter Rütschi
Laupenstr. 27
CH-3003 Bern

Zürich, 20. April 2016

Neues FINMA-RS 2016/xx Corporate Governance-Banken sowie Anpassung der FINMA-RS 2008/21 Operationelle Risiken Banken und 2010/1 Vergütungssysteme

Sehr geehrter Herr Rütschi

Sehr geehrte Damen und Herren

In genannter Sache danken wir für die Gelegenheit an dieser Anhörung teilzunehmen und reichen Ihnen innert angesetzter und mit E-Mail vom 23. März 2016 bis 20. April 2016 erstreckten Frist hiermit unsere Stellungnahme ein.

Die Zürcher Kantonalbank begrüsst ein modernes Aufsichtsrecht, welches einerseits internationale Anforderungen berücksichtigt und andererseits auf die Verhältnisse der Schweiz zugeschnitten ist. Die vorliegenden Entwürfe des neuen bzw. der beiden angepassten Rundschreiben weisen allerdings in Konzeption und Systematik noch einige grundsätzliche Defizite auf, welche zwingend zu korrigieren sind. Mit Bezug auf den Entwurf des neuen Rundschreibens Corporate Governance Banken sind wir der Ueberzeugung, dass die Beibehaltung zumindest der wesentlichen Regelungen gemäss altbewährter Vorgängerfassung FINMA-RS 2008/24 eine bessere Regulierung darstellt.

Nachfolgend fassen wir vorab unsere Hauptanliegen zusammen und begründen diese sodann einlässlich.

Wunschgemäss senden wir Ihnen unsere Stellungnahme per E-Mail, liefern sie aber falls von ihnen gewünscht auch noch mit normaler Post nach.

Zusammenfassung der Forderungen der Zürcher Kantonalbank

I. Generell

1. *Klare Definitionen und Abgrenzungen der wesentlichen Organe und Funktionen sowie weiterer Schlüsselbegriffe in einem Glossar*
2. *Konsequente Verwirklichung der auch von der FINMA gewollten prinzipienorientierten Regulierung unter Weglassung umfangreicher und aufwendiger Kategorisierungen gemäss Rahmenkonzept*
3. *Festhalten am Grundsatz ‚Comply or explain' statt aufwendigen Ausnahmebewilligungen*
4. *Ausreichende Uebergangsfristen, je nach Thema bis zu 2 Jahren*

II. Neues FINMA-RS 2016/xx Corporate Governance-Banken

1. *Klare und widerspruchsfreie Abgrenzung der Aufgaben, Kompetenzen und Verantwortlichkeiten von Oberleitungsorgan und Geschäftsleitung sowie von diesen Organen einerseits sowie den Funktionen Risikokontrolle u. Compliance andererseits, insb. Wiedereinführung einer klaren Umsetzungsverantwortung der Geschäftsleitung (i.S.v. FINMA-RS 2008/24, Rz 99)*
2. *Klare und in sich widerspruchsfreie Regelung der Compliancefunktion, insb. ersatzlose Streichung von Rz 8, und bessere Abgrenzung zur Funktion Risikokontrolle*
3. *Respektierung zwingender gesellschaftsrechtlicher Regelungen und im Uebrigen Spezifizierung des Gesellschaftsrecht konsequent nur, soweit aus Sicht Bankenaufsichtsrecht zwingend erforderlich*
4. *Bei organisatorischen Regelungen zusätzliche angemessene Ausnahmen auch für Institute der Gruppe 3*

III. Anpassung FINMA-RS 2008/21 Operationelle Risiken Banken

1. *Ergänzung der Definition der operationellen Risiken und klare Abgrenzung von Compliance-Risiken (Rz 2)*
2. *Konsequente Rückführung auf prinzipienorientierte Regulierung, insb. der Grundsätze 4 (Technologieinfrastruktur, Rz 135 ff.) und 5 (Kontinuität, Rz 136 ff.)*
3. *Ersatzlose Streichung der Regelung zu Risiken aus grenzüberschreitendem Dienstleistungsgeschäft (Rz 136.4)*

IV. Anpassung FINMA-RS 2010/1 Vergütungssysteme

1. *Ersatzlose Streichung der neuen Pflicht zur Implementierung von ‚Clawback'-Regelungen (Rz 46)*
2. *Reduktion der minimalen Aufschubfrist für Teile der variablen Entschädigung von 3 auf 2 Jahre (Rz 52)*
3. *Bei organisatorischen Regelungen zusätzliche angemessene Ausnahmen auch für Institute der Gruppe 3*

I. Generelles

1. Generelle **Vorbemerkung**: Soweit diese Stellungnahme keine (abweichenden) Ausführungen zu bestimmten Themen enthält, schliesst sich die Zürcher Kantonalbank ergänzend den **Stellungnahmen der SBVg und des VSKB** an.

2. Der Wechsel von einem vom IKS dominierten Regulierungsansatz des Risikomanagements (FINMA-RS 2008/24) hin zu einem **Risk Governance-Ansatz** ist **nicht gelungen**. Insbesondere belässt das neue, von bewährter Normenhierarchie losgelöste **Institut des Rahmenkonzepts** zu viel **Offenheit** insbesondere **mit Bezug auf die grundsätzliche Verteilung der Verantwortlichkeiten** innerhalb eines Instituts.

3. Auf Basis des neuen Risk Governance-Ansatzes wird mit dem **Ansatz eines Rahmenkonzepts** ein **kompliziertes System von vorgegebener Kategorisierung und Ausnahmebewilligungen** hochgefahren. Dieses produziert viel zu detaillierte Regulierung und läuft damit dem von der FINMA formulierten Anspruch einer **prinzipienorientierten Regelung** unter **Verzicht auf Detailausführungen** gerade entgegen.

4. Die vorgeschlagenen Regelungen lassen vielfach eine klare und rechtssichere Basis vermissen. Insbesondere werden viele verwendete **Schlüsselbegriffe nicht definiert**. Umgekehrt werden teilweise **neue Begriffe** eingeführt, welche **nicht mit den einschlägigen gesetzlichen Regelungen abgestimmt** sind. Wir fordern deshalb ein **Glossar** mit untereinander klar abgegrenzten Definitionen der wesentlichen Schlüsselbegriffe.

5. **Operationelle Risiken werden weiter gefasst** als bisher, während **Compliancerisiken nicht mehr definiert** sind. Auch **fehlt** eine klare **Abgrenzung zwischen Funktion Risikokontrolle und Compliancefunktion**. Dies führt zu zahlreichen unklaren Bestimmungen mit Bezug auf die Aufgaben, Kompetenzen und Verantwortlichkeiten der beiden Funktionen.

6. Der Trend unnötig detaillierter Regulierung kombiniert mit der fehlenden klaren Abgrenzung zwischen Funktion Risikokontrolle und Compliancefunktion führt zu einem massiven **Ausbau von operationellen Risiken**. Materiell ist dies **teilweise sogar falsch**, z.B. mit Bezug auf die Risiken aus grenzüberschreitendem Dienstleistungsgeschäft.

7. Umgekehrt ist die **Regelung der Compliancefunktion nur noch bruchstückhaft** und deshalb mit Bezug auf ihre Aufgaben, Kompetenzen und Verantwortlichkeiten teilweise **unvollständig und unklar**, teilweise sogar **widersprüchlich und schlicht falsch**.

8. Auch die mit Bezug auf ein **gesamheitliches und effizientes Risikomanagement** besonders wichtige Abgrenzung von Kompetenzen, Aufgaben und Verantwortlichkeiten von **Oberleitungsorgan** einerseits (**Gesamtverantwortung**) und **Geschäftsleitung** andererseits (**Umsetzungsverantwortung**) ist generell sehr schlecht gelungen und produziert zahlreiche vermeintliche „Doppelspurigkeiten", Unklarheiten und Fehler.

9. Im Bereich der Organisationsregeln wird der Grundsatz verletzt, **Spezifizierungen des Gesellschaftsrecht** nur vorzunehmen, soweit dies **aufgrund eindeutiger bankaufsichtsrechtlicher An-**

forderungen zwingend nötig ist und gleichzeitig **keine zwingenden Regeln des Zivilrechts** entgegenstehen. Teilweise werden gemäss OR zwingend dem Oberleitungsorgan zustehende Aufgaben, Kompetenzen und Verantwortlichkeiten „nach unten delegiert". Umgekehrt besteht auch ein Trend, generell „nach oben zu delegieren", typischerweise gleich ans Oberleitungsorgan. (Auch) dies führt zu einer **Verwischung der klaren Grenzen zwischen Oberleitungstätigkeiten und operativen Tätigkeiten**. Im Ergebnis verliert dadurch das Oberleitungsorgan seine vom operativen Geschäft unabhängige Oberleitungs- und Kontrollfunktion. Im Gegenzug besteht die Gefahr der Ueberlastung des Oberleitungsorgans.

10. Der bewährte **Grundsatz ‚Comply or Explain'**, welcher abgeschafft werden soll, ermöglicht jedem Institut, die Vorgaben gestützt auf vernünftiges Ermessen mit Blick auf die konkreten Verhältnisse umzusetzen. Wir empfehlen, diesen Grundsatz **wieder einzuführen**, zumal dadurch **kein Widerspruch weder zum Proportionalitätsprinzip noch zum prinzienorientierten Ansatz** besteht, sondern vielmehr eine sinnvolle Ergänzung und Präzisierung.

11. Die zahlreichen Neuerungen und Anpassungen stellen zusammen ein **komplexes Gesamtkonzept** dar und produzieren **erheblichen Analyse- und Umsetzungsbedarf**. Insbesondere sind mit Blick auf ein effizientes Risikomanagement zahlreiche **IT-gestützte Lösungen** umzubauen oder neu zu schaffen. Die Implementierung von IT-gestützten Lösung dauern von Konzeptanalyse bis finaler Inbetriebnahme regelmässig 2 Jahre. Deshalb sind unter allen drei betroffenen Rundschreiben generell **längere Uebergangsfristen** von **erfahrungsgemäss 2 Jahren** zu gewähren.

II. Zum neuen FINMA-RS 2016/xx Corporate Governance Banken

1. Generelle Bemerkungen

1.1. Es fällt auf, dass viele Ausführungen für sich allein richtig sind. Zahlreiche ebenfalls **notwendige Ausführungen fehlen** aber, was **Lücken und Unklarheiten** produziert. Ueberdies bestehen zahlreiche **Widersprüche**, teilweise zu grundsätzlichsten Grundregeln wie z.B. zur Abgrenzung des Oberleitungsorgans zur Geschäftsleitung oder zu den Aufgaben, Kompetenzen und Verantwortlichkeiten der Compliancefunktion. Insgesamt **fehlt ein vollständiges, widerspruchsfreies und aus sich selbst heraus in jeder Hinsicht verständliches Gesamtsystem**.

1.2. Im Bereich **Corporate Governance** soll die FINMA in zurückhaltender Weise nur solche Regeln aufstellen, welche aus **bankspezifischer aufsichtsrechtlicher Sicht zwingend gefordert** sind. Folgerichtig ist insbesondere auf allgemeine Ausführungen zu den Aufgaben des Oberleitungsorgans und der Geschäftsleitung zu verzichten. Solche Ausführungen sind nicht nötig und können im Gegenteil kontraproduktiv sein. Beispielsweise wird jede Aenderung des Zivilrechts auch eine Anpassung des FINMA-Rundschreibens erforderlich machen. Im schlechtesten Fall wird durch Formulierungen im FINMA-Rundschreiben, welches nicht identisch wie das Zivilrecht formuliert ist, für Banken im Ergebnis ohne Not sogar das anwendbare Zivilrecht abgeändert. Soweit das Zivilrecht zwingender Natur ist, z.B. die unentziehbaren Aufgaben, Kompetenzen und Verantwortlichkeiten des Oberleitungsorgans gemäss Art. 716 u. 716a OR, ist dies gar nicht zulässig. In den andern Fällen würde unnötige **Rechtsunsicherheit** produziert. Eine gesetzliche Grundlage für solche Regelungen besteht ohnehin nicht, da sich die FINMA funktionsgemäss auf zwingende aufsichtsrechtliche Aspekte zu beschränken hat.

2. Bemerkungen zur Titelseite

2.1. Entsprechend den im neuen Rundschreiben verwendeten Schlüsselbegriffen muss der Untertitel besser lauten „Corporate Governance, Risikomanagement und interne**s** Kontroll**system** bei Banken".

2.2. Unter „Konkordanz" muss der Titel des Rundschreiben „Ueberwachung und interne Kontrolle" heissen.

3. Bemerkungen zu Abschnitt I Gegenstand (Rz 1 f.)

3.1. Der **Begriff „Checks and Balances"** gehört in die Politik, nicht aber in ein Regelwerk in Zusammenhang mit Unternehmensführung. Unternehmen sind auf die Erzielung eines unternehmerischen Erfolgs ausgerichtete Zusammenschlüsse von Personen mit hierarchisch geregelten Aufgaben, Kompetenzen und Verantwortlichkeiten, die im materiellen Recht grossmehrheitlich im Zivilrecht geregelt sind. Die Zürcher Kantonalbank untersteht als selbständige Anstalt des kantonalen Zürcher Rechts zwar mit Bezug auf ihre „Betriebsverfassung" primär dem vom Zürcher Kantonsrat erlassenen ZKB-Gesetz und den vom Bankrat als Oberleitungsorgan, genehmigt vom Zürcher Kantonsrat, gestützt auf das ZKB-Gesetz erlassenen Reglementen (Organisationsreglement, Reglement über die Generaldirektion, etc.). Diese Regelungen orientieren sich aber am OR und an internationalen Standards. Im Uebrigen untersteht die Zürcher Kantonalbank mit Bezug auf ihre Geschäftstätigkeit dem Zivilrecht. „Corporate Governance" bedeutet nichts anderes als Grundsätze der Unternehmensführung. Das Oberleitungsorgan hat sich richtigerweise auf Festlegung von Geschäftspolitik und Vorgaben für Betriebsorganisation, Geschäftsführung und Verhalten zu beschränken. In diesem Rahmen ist das Oberleitungsorgan letztlich dafür verantwortlich, dass sich das Unternehmen gesetzeskonform verhält (vgl. Art. 716a Abs. 1 Ziff. 1, 2 u. 5 OR; für die Zürcher Kantonalbank § 15 Abs. 3 Ziff. 1 u. 2 ZKB-Gesetz). Die **FINMA** muss sich kompetenzgemäss darauf beschränken, welche **organisatorischen Eckpfeiler** zu beachten sind, damit die **aus Sicht Bankenaufsichtsrecht relevanten Aspekte** zwingend erfüllt werden können. Die anderweitig insbesondere gemäss Zivilrecht bereits gültigen Rechtsgrundsätze sind demzufolge lediglich soweit nötig aus Sicht Bankenaufsichtsrecht zu **spezifizieren**. Die Aufzählung bekannter allgemeiner Prinzipien samt unnötigen Einschränkungen sind wegzulassen.

3.2. Da die Formulierung von Rz 2 eine Begriffsumschreibung darstellt, empfehlen wir aus systematischen Gründen, diese **Rz neu in den Abschnitt II Begriffe zu verschieben**.

4. Bemerkungen zu Abschnitt II Begriffe (Rz 3 ff.)

4.1. **Zu Rz 3 ff.**: Im Vernehmlassungsentwurf werden verschiedene Begriffe ohne klare Definition verwendet, namentlich „Risikomanagement", „Risikoappetit", „Risikoprofil", „Risikostrategie" und „Risikopolitik". Andere Schlüsselbegriffe wie „operationelle Risiken" werden (im RS 2008/21, Rz 2) unvollständig und weitere solche Begriffe wie „Compliance-Risiken" gar nicht (mehr) definiert. Die Formulierungen im Erläuterungsbericht sind nur teilweise weiterführend und bleiben im Ergebnis ebenfalls vage und teilweise inkonsistent. Ein FINMA-Rundschreiben muss mit Bezug auf solche Schlüsselbegriffe aus sich selbst heraus **Klarheit schaffen**. Im **FINMA-RS 2010/1** besteht bereits ein solcher Katalog von klaren Begriffsbestimmungen (vgl. dort Rz 11 ff.).Für die Schlüsselbegriffe sind deshalb auch in diesem neuen **Rundschreiben zu Corporate Governance präzise Definitionen** vorzusehen. Wir fordern,

dass für sämtliche Schlüsselbegriffe, wozu über vorstehende Liste hinaus noch weitere Begriffe zählen (vgl. z.B. nachstehend Ziff. 4.2), in einem Anhang 1 ein **Glossar** erstellt wird (vgl. z.B. BCBS-Corporate Governance Principles for Banks, Glossary S. 4 f.). Dieses muss mit untereinander klar abgegrenzten Definitionen Klarheit schaffen.

4.2. **Zu Rz 4/8**: (Auch) diese Formulierungen zu „Risikokontrolle" und „Compliancefunktion" sind keine präzisen Definitionen, sondern bloss Zuweisungen von Verantwortlichkeiten. Dies ist ebenfalls im Glossar zu klären (vgl. vorstehend Ziff. 4.1). Beim **Begriff der Risikokontrolle** ist zudem zu unterscheiden zwischen der **Funktion Risikokontrolle** (als Abgrenzung zur Compliancefunktion) und der Risikokontrolle als Umschreibung der **Aufgabe,** welche **analog auch von der Compliancefunktion wahrgenommen** wird (vgl. unten Ziff. 4.3 lit. d u. 8.6).

4.3. **Zu Rz 8**: Diese Regelung ist schlicht **falsch** und setzt sich in Widerspruch mit verschiedenen anderweitigen Regeln im Rundschreiben und überdies mit allgemein anerkannten Prinzipien:

a) Rz 8 steht systematisch am falschen Ort und setzt sich in **Widerspruch** mit dem Umschrieb der Aufgaben, Kompetenzen und Verantwortlichkeiten der **Compliancefunktion in Rz 99 ff.** Dieser Befund dürfte Folge davon sein, dass die Compliancefunktion im Entwurf der FINMA nur noch bruchstückhaft geregelt ist. Eine Definition der Compliance-Risiken fehlt ebenso wie eine klare Abgrenzung einerseits zur Funktion Risikokontrolle und andererseits zur Geschäftsleitung. Die auf dieser schwachen Basis geregelten Folgen für die Compliancefunktion sind dementsprechend lückenhaft, missverständlich und teilweise falsch geregelt.

b) Der generelle **Begriff der „Risikokontrolle" im weitesten Sinne** ist **mehrstufig** und zwischen ertragsorientierten Geschäftseinheiten gemäss Rz 81 und unabhängigen Kontrollfunktionen wie insbesondere der Compliancefunktion gemäss Rz 99 ff. aufgeteilt. Die **ertragsorientierten Geschäftseinheiten** haben **als Risikobewirtschafter** die primäre Verantwortung für die Einhaltung aller Regeln und müssen deshalb gemäss Rz 81 auch selbst das operative Geschäft und die damit verbundene Einhaltung externer wie interner Regeln des Rechts und der Ethik überwachen (BCBS-Corporate Governance Principles for Banks vom 8. Juli 2015, Prinzip 9, Ziff. 133 f.; Othmar Strasser, Zur Entwicklung der Funktion Legal und Compliance unter dem Aspekt von Corporate Governance - ein Plädoyer für eine integrierte Funktion Recht, in: Susan Emmenegger (Hrsg.), Schweiz. Bankrechtstagung 2011, Corporate Governance, Basel 2011, S. 93-164, S. 126 f.). Soweit dabei Regelverstösse oder andere Missstände erkannt werden, kann und muss die entscheidkompetente Linienstelle auch selbst Massnahmen zur Behebung der Missstände, zur Disziplinierung allfälliger fehlbarer Mitarbeitender und zur besseren Steuerung der Risiken anordnen. In Uebereinstimmung mit den **Vorgaben anerkannter internationaler Standards** (insb. bereits erwähnter BCBS-Corporate Governance Principles for Banks u. G20/OECD-Principles of Corporate Governance vom 25. November 2015; vgl. Erläuterungsbericht, S. 6) erfüllen die ertragsorientierten und entscheidkompetenten Geschäftseinheiten damit eine **genuine ihnen zugeordnete Aufgabe** im Rahmen der 1. ‚Line of Defence', wie dies Rz 81 richtigerweise anordnet.

c) Demgegenüber können der Compliancefunktion nur ausnahmsweise **einzelne Kontroll- und Ueberwachungsaufgaben** zugeordnet werden. Dies ist dann richtig und sinnvoll, wenn für die Wahrnehmung einer bestimmten Ueberwachungskompetenz ausgesprochen **hohe Anforderungen an Fachkompetenz und funktionale Unabhängigkeit** zu stellen sind. Damit die

wichtige hauptsächliche Beratungs- und Unterstützungsaufgabe der Compliancefunktion (Rz 103) nicht verwässert oder aufgehoben wird, müssen sich solche Kontroll- und Ueberwachungsaufgaben aber auf wenige sachlich eng umrissene Sachverhalte mit **von der Geschäftsleitung klar und abschliessend definiertem Kontrollrahmen** beschränken. Dieser Kontrollrahmen hat klar und abschliessend zu regeln, was zu kontrollieren ist, was mit den Kontrollergebnissen zu geschehen hat und wem daraus eine Handlungspflicht entsteht. Solche **Ausnahmen von der Regel** sind **in einschlägigen institutsinternen Regelwerken klar und abschliessend zu regeln** (vgl. bei der Zürcher Kantonalbank § 13 Abs. 2 u. § 15 Compliance-Reglement Konzern und Stammhaus; Othmar Strasser, a.a.O., Integrierte Funktion Recht, S. 117 f. u. 126 f.).

d) Neben den hauptsächlichen **Beratungs- und Unterstützungsaufgaben** gemäss Rz 103 (2. ‚Line of Defence') hat die Compliancefunktion auch **Aufgaben der Risikokontrolle** gemäss Rz 99-102 (3. ‚Line of Defence'). Letzteres ist einerseits die **periodische Ueberwachung des Risikoprofils der Compliancerisiken verbunden mit der Empfehlung allfälliger Massnahmen** zur besseren Risikosteuerung und andererseits die **periodische Kontrolle der Wirksamkeit** der von den verantwortlichen und entscheidkompetenten Linienverantwortlichen i.d.R. auf Empfehlung der Compliancefunktion angeordneten Risikosteuerungsmassnahmen (insb. Rz 100, entspr. FINMA-RS 2008/24, Rz 109). Diese Aufgabe der Risikokontrolle ist **dieselbe, welche auch die Funktion Risikokontrolle gestützt auf Rz 97 ausübt**. Die beste Umschreibung dieser Tätigkeit findet sich im **altbewährten FINMA-RS 2008/24, Rz 122**, welche schon bisher auf die Compliancefunktion **analog anwendbar** war. Diese Formulierung ist deshalb **auch ins neue Rundschreiben zu übernehmen** (oben Ziff. 4.1 u. unten Ziff. 8.6).

   Solche Aufgaben der Compliancefunktion wirken - im Gegensatz zu Ueberwachungsfunktionen im Rahmen der 1. ‚Line of Defence' (vgl. oben lit. c) - **ex-ante** und sind damit ein äusserst effizientes Mittel der Risikosteuerung. Insbesondere können sie die Realisierung eines Risikos und damit den **Eintritt von Schäden und andern Nachteilen im Interesse des Unternehmens zum vornherein verhindern** (zum Ganzen Urteil des Bundesverwaltungsgerichts Nr. B-3625/2014 vom 6. Oktober 2015, E 3.1; Othmar Strasser, a.a.O. Integrierte Funktion Recht, S. 117 ff. u. 144 f.; ders., Antwort einer Bank auf die erhöhte Verantwortlichkeit im Unternehmen aus zivil-, straf- und verwaltungsrechtlicher Sicht - oder Management von Compliance Risiken als Aufgabe von Unternehmensjuristen, in: M.A. Niggli/Marc Amstutz (Hrsg.), Verantwortlichkeit im Unternehmen, Zivil- und strafrechtliche Perspektiven, Basel 2007, S. 245 ff., insb. S. 257 f. u. 267 ff.). Die Wahrnehmung solcher **Aufgaben schliesst funktionsgemäss grundsätzlich aus**, dass die Compliancefunktion gleichzeitig **Anordnungskompetenz** hat. Vielmehr steht es der Compliancefunktion unter Vorbehalt klar und abschliessend geregelter Ausnahmen von der Regel (vgl. oben lit. c) nur zu, ein bestimmtes Verhalten zu **empfehlen**, nicht aber, ein solches durchzusetzen (Strasser, a.a.O. Integrierte Funktion Recht, S. 117). Im Falle der Nichtbeachtung einer Empfehlung muss der Compliancefunktion korrelativ ein **Interventionsrecht** (Rz 83) sowie ein **Eskalationsrecht** zustehen (Rz 86 u. unten Ziff. 8.2).

e) Im **Datenschutz** ist dieses **Gesamtkonzept der Compliancefunktion sogar gesetzlich bzw. auf Verordnungsstufe normiert** worden (vgl. Art. 11a Abs. 5 lit. e u. Abs. 6 DSG i.V.m. Art. 12a u. 12b VDSG u. dazu Werner Wyss, in: Handbücher für die Anwaltspraxis, Datenschutzrecht, Nicolas Passadelis/David Rosenthal/Hanspeter Thür, Basel 2015, § 11 Rz 11.8 ff. m.w.V.).

f) Nach dem Gesagten **beschränkt Rz 8 auch in ungerechtfertigter Weise den Handlungs- und Ermessensspielraum der Geschäftsführung** für die in ihrer Verantwortung liegenden Festlegung der umzusetzenden Organisationsstruktur (BCBS Corporate Governance Principles, Prinzip 9, Ziff. 132 f.; Othmar Strasser, a.a.O., Integrierte Funktion Recht, S. 126 f.; ders., a.a.O. Management von Compliance Risiken, S. 269 f.). Insbesondere ist die Geschäftsleitung im Rahmen vernünftigen Ermessens frei, mit einer solchen Kompetenz auch eine **andere Stelle** zu betrauen, welche für das bestimmte zu regelnde Thema **aufgrund ihrer organisatorischen und funktionalen Stellung** über **ausreichenden Grad an Unabhängigkeit und Fachwissen** verfügt (Othmar Strasser, a.a.O. Integrierte Funktion Recht, S. 126 f.). Auch solche Fälle sind als Ausnahmen von der Grundregel (Rz 81) in institutsinternen Regelwerken klar und abschliessend zu regeln (vgl. bei der Zürcher Kantonalbank § 20 Abs. 3 Compliance-Reglement Konzern und Stammhaus). Damit steht Rz 8 auch im **Widerspruch zu Rz 57**.

g) Demzufolge fordern wir, **Rz 8 ersatzlos zu streichen** und die **Compliancefunktion im vorgenannten Sinne umfassend richtig und klar zu regeln**. Andernfalls besteht ein ernsthaftes Risiko, dass entgegen bewährten Grundsätzen von ‚good' Corporate Governance die Compliancefunktion im Rahmen dieser lückenhaft formulierten Regulierung und/oder des offen formulierten Rahmenkonzepts sogar weit über die heutige Rechtslage hinaus (BGE Nr. 6B 901/2009 vom 3. November 2010 betr. Verurteilung eines Leiters Rechtsdienst; BGE Nr. 6B 907/2009 vom 3. November 2010 betr. Verurteilung eines Leiters Compliance) ungerechtfertigterweise **in uferloser Weise strafrechtlich verantwortlich** wird, z.B. neu auch für das Nichtunterbinden eines Regelverstosses und dies sogar ohne dahingehende betriebsintern festgelegte Handlungspflichten (vgl. BGH-Urteil Nr. 5 StR 394/08 vom 17. Juli 2009 betr. Verurteilung eines Leiters Rechtsdienst; zum Ganzen Othmar Strasser, a.a.O. Integrierte Funktion Recht, S. 102 f. u. 161 ff.).

4.4. Der **Grundsatz ‚Comply or explain'** ermöglicht jedem Institut unter Zugrundelegung eines vernünftigen Ermessens die Umsetzung **prinzipienorientierter** aufsichtsrechtlicher Vorgaben angepasst auf die konkreten Verhältnisse insbesondere differenziert nach Grösse, Komplexität, Struktur und Risikoprofil (bisher FINMA-RS 2008/24, Rz 9, 101 u. 114). Der **Grundsatz der Proportionalität** (Rz 9) ist eine blosse Konkretisierung der Prinzipienorientierung. Der Grundsatz ‚Comply or explain' widerspricht somit dem prinzipienorientierten Ansatz nicht, sondern ergänzt diesen vielmehr optimal. Der damit einhergehende Ermessenspielraum ist den **nach Bankenrecht umfassend beaufsichtigten** Instituten zuzugestehen, haben sie doch nach Bankenrecht immerhin jederzeitige Gewähr für optimale Organisation und einwandfreie Geschäftsführung sicherzustellen (Art. 3 Abs. 2 lit. a u. c BankG) und müssen innerhalb dieser Leitplanken in der Lage sein, vernünftige, sachlich wohlbegründete Entscheide zu treffen. Der Grundsatz ist demzufolge beizubehalten. Demgegenüber bleiben beim beabsichtigten **System eines Rahmenkonzepts mit detaillierten Kategorisierungen und Ausnahmebewilligungen** die **Aufgaben, Kompetenzen und Verantwortlichkeiten auf allen Stufen völlig offen** und die **wesentlichen Organe und Funktionen** wie insbesondere Oberleitungsorgan, Geschäftsleitung, Funktion Risikokontrolle und Compliancefunktion werden **nicht eindeutig definiert und abgegrenzt** (vgl. z.B. Rz 13 mit Rz 57, Rz 8 mit Rz 99 ff. od. Rz 98 mit Rz 102 sowie unsere jeweiligen Kommentare). In der Praxis würden von Institut zu Institut völlig unterschiedlichen Lösungen implementiert. Grosses Ermessen bei der Umsetzung ist wünschenswert und angemessen. Zur Vermeidung von erheblicher **Rechtsunsicherheit bei zentralen Themen** sollte ein FINMA-Rundschreiben, welches die Regulierung von Corporate Governance-Grundsätzen in Anspruch nimmt, aber zumindest vorstehend skizzierte grundsätzlichste Definitionen und Regelungen selbst in klarer Form vornehmen. Umgekehrt **beschränkt das System** durch zahlreiche unnötige Detailregelungen trotzdem in mannig-

faltiger Weise die **Autonomie der Institute** quasi am falschen Ort. Ohne Zusatznutzen zu schaffen werden mit diesem Ansatz im Gegenteil unnötiger Aufwand und kontraproduktive Zeitverzögerungen produziert. Für solche unnötigen Einschränkungen des Ermessens beaufsichtigter Institute besteht keine gesetzliche Grundlage. Ueberdies widerspricht das System der erklärten Absicht der FINMA, das **Proportionalitätsprinzip** bzw. den **prinzipienorientierten Ansatz** verwirklichen zu wollen (vgl. Rz 9; FINMA-Medienmitteilung, S. 1; FINMA-Erläuterungsbericht, S. 8 u. 10).

4.5. **Zu Rz 5**: Erforderlich ist nicht eine umfassende Regelung, sondern nur sofern relevant. Die Formulierung von Rz 5 ist demzufolge **am Ende zu ergänzen mit „sofern relevant"**.

4.6. **Zu Rz 7/79**: Die hier und in Rz 79 verwendete **Definition des internen Kontrollsystems (IKS)** ist gegenüber der aktuellen Fassung gemäss FINMA-RS 2008/24, Rz 2 **deutlich enger gefasst**. Während die Definition in FINMA-RS 2008/24 - in Anlehnung an den etablierten IKS-Standard COSO ERM - auch Prozesse für Risikomanagement und Einhaltung der anwendbaren Normen (Compliance) als Teil der internen Kontrolle festhält, sind diese im vorliegenden Entwurf Teil des Rahmenkonzepts für das institutsweite Risikomanagement. Damit lehnt sich die neue IKS-Definition im Kern an den COSO-IC Standard an. Das so definierte IKS ist kein Riskmanagement-Regelwerk mehr, sondern **reines Kontroll-Regelwerk**. Konsequenterweise haben Finanzdienstleister **zusätzlich** zum IKS ein aufwendiges und wenig zielführendes **Rahmenkonzept für das institutsweise Risikomanagement** zu unterhalten. Die Separierung von Risikomanagement und Kontrolle ist zwar grundsätzlich möglich, sollte aber wenn schon konsistent angewendet werden. Wir lehnen diesen Ansatz allerdings aus grundsätzlichsten Ueberlegungen generell ab. Insbesondere ist dieser Ansatz **notwendigerweise mit einem komplexen, unnötig detaillierten und aufwendigen System von Kategorisierungen und Ausnahmebewilligungen verbunden** und **widerspricht dem von der FINMA selbst gewünschten prinzipienorientierten Ansatz** (vgl. oben Ziff. 4.4). Wir empfehlen deshalb, die **bisherige altbewährte Formulierung gemäss FINMA-RS 2008/24, Rz 2 weiterhin** zu übernehmen. Zudem ist zum besseren Verständnis der nur noch bruchstückhaft geregelten Compliancefunktion auch die **Definition der Compliancerisiken** an geeigneter Stelle entsprechend **altbewährter Regulierung in FINMA-RS 2008/24, Rz 98** wieder aufzunehmen (vgl. oben Ziff. 4.1 u. unten Ziff. III.1.2).

4.7. Soweit die FINMA diesem Hauptstandpunkt wider Erwarten nicht folgt, ist zu berücksichtigen, dass das **IKS gemäss Rz 79** auch organisatorische Strukturen (z.B. das System der 3 ‚Lines of Defence; vgl. oben Ziff. 4.3 lit. b-d) erfasst. Der Standard COSO-IC enthält die Kontrolldimension „Operations", „Financial Reporting" und „Compliance". Diese sind in Rz 7 zwar abgebildet, die Dimension „Compliance" aber ungenügend. Dies ist zu präzisieren. Sodann zielt die von Rz 7 verwendete Kontrolldimension „Minderung der Risiken" nach unserer Lesart auf das Management finanzieller Risiken ab. Diese Kontrolldimension wird manchmal separat aufgeführt, mitunter aber auch unter der Dimension „Operations" subsummiert. Aus Gründen von Klarheit und Präzision empfehlen wir, auch diese Dimension ausdrücklich separat und klar formuliert aufzuführen. Als **Eventualstandpunkt** empfehlen wir folgende **Aenderungen/Ergänzungen der Formulierung von Rz 7**, welche aus Gründen der Klarheit gleichwohl auch die wesentlichen Aspekte gemäss **Rz 2 von FINMA-RS 2008/24** übernehmen sollte (Aenderungen/Ergänzungen von Rz 7 unterstrichen):

„Das interne Kontrollsystem umfasst die Gesamtheit der organisatorischen Strukturen sowie die vom Institut definierten Vorgänge, Methoden und Massnahmen, die dazu dienen, eine angemessene Sicherheit in Bezug auf die Wirksamkeit von operativen Geschäftsprozessen, des Risikomanagements, die Zuverlässigkeit der finanziellen Berichterstattung und die Befolgung von Gesetzen zu gewährleis-

ten. Von besonderer Bedeutung sind dabei Kontrollstrukturen und -prozesse, welche auf allen Ebenen des Instituts die Grundlage für die Erreichung der geschäftspolitischen Ziele und einen ordnungsgemässen Institutsbetrieb bilden. Dabei beinhaltet das interne Kontrollsystem nicht nur Aktivitäten der nachträglichen Kontrolle, sondern auch solche der Planung und Steuerung. Eine wirksame interne Kontrolle umfasst u.a. in die Arbeitsabläufe integrierte Kontrollaktivitäten, Prozesse für Risikomanagement und Einhaltung der anwendbaren externen und internen Normen des Rechts und der Ethik (Compliance), eine von der Risikobewirtschaftung unabhängige Risikokontrolle sowie die Compliancefunktion. Die interne Revision prüft und beurteilt die interne Kontrolle und trägt dadurch zu deren laufenden Verbesserung bei."

4.8. Im Rahmen des vorstehend formulierten Eventualstandpunkts wäre die (geänderte) Definition von Rz 7 konsistent auch in Rz 79 zu verwenden. Die aktuelle Formulierung von Rz 79 verwendet Elemente aus dem Risikomanagement-Regelwerk und lehnt sich damit an die alte IKS-Definition gemäss aktuellem FINMA-RS 2008/24, Rz 2 an. Dies ist gemäss unserem Hauptstandpunkt nicht zu beanstanden (vgl. oben Ziff. 4.6), gemäss Eventualstandpunkt aber **inkonsistent mit der Definition von Rz 7**. Konsequenterweise sind diesfalls bei Spezifizierung die Komponenten gemäss COSO-IC Standard zu verwenden. Im **Eventualstandpunkt** empfehlen wir folgende kurze und klare Formulierung von Rz 79:

„Das Institut hat über ein adäquates, dokumentiertes internes Kontrollsystem gemäss Rz 7 zu verfügen." (Nachfolgende Passagen ersatzlos zu streichen)

4.9. **Zu Rz 9**: Das **Proportionalitätsprinzip** ist zu begrüssen, indessen noch auszubauen, damit insbesondere auch **Banken der Kategorie 3** in angemessener Weise davon direkt profitieren (vgl. insb. unten Ziff. 5.15, 8.3 u. IV.3.2). Das Proportionalitätsprinzip ist eine **Konkretisierung des prinzipienbasierten Ansatzes**. Ueber das Proportionalitätsprinzip hinaus muss deshalb weiterhin auch der von der FINMA ausdrücklich gewünschte **prinzipienorientierte** Ansatz (vgl. Medienmitteilung, S. 1; Erläuterungsbericht, S. 8) anwendbar sein und zu diesem Zweck ausdrücklich **zu regulieren** (vgl. oben Ziff. 4.4). Als Formulierung drängt sich die Uebernahme der **altbewährten Regulierung gemäss FINMA-RS 2008/24, Rz 9, 101 u. 114** auf. Die konsequente Verwirklichung des prinzipienbasierten Ansatzes ist **besonders wichtig für** alle diejenigen **Kantonalbanken**, welche strukturgemäss über eine Governance verfügen, welche entweder wie bei der Zürcher Kantonalbank mit kantonalem Gesetz geregelt ist, bei welcher kantonale Behörden in anderer Form z.B. als Organe mitwirken oder bei der Kanton eine Aktienmehrheit hält (vgl. Art. 762 OR). Solche Kantonalbanken sind bei Umsetzung neuer Anforderungen zur Corporate Governance jedenfalls auf die tatkräftige Mithilfe des Kantons bzw. der kantonalen Behörden, Organe, etc. angewiesen (vgl. z.B. unten Ziff. 5.7).

5. Bemerkungen zu Abschnitt IV Oberleitungsorgan (Rz 10 ff.)

5.1. Generell sind die Ausführungen auf die Bereiche **Risikomanagement, IKS und Compliance** zu beschränken. Die postulierte zwingende Zuständigkeit des Oberleitungsorgans für Strukturveränderungen und Investitionen ist ein unzulässiger Eingriff in die zivilrechtlich gewährten Selbstgestaltungsrechte eines Unternehmens und demzufolge zu streichen.

5.2. **Zu Rz 10**: Diese Regelung ist aus Klarheitsgründen am Ende zu ergänzen mit (Ergänzung in Fettdruck): „... Verfolgung dieser Ziele **und der Einhaltung gesetzlicher, regulatorischer und interner Vor-**

schriften. Es versteht die Unternehmensstrukturen und Risiken der einzelnen Geschäftsfelder des Instituts".

5.3. **Zu Rz 12**: Die Festlegung der Grundsätze und Vorgaben für die in Ziff. 12 genannten Themen, insbesondere für die **Geschäftsstrategie**, obliegt als **unentziehbare Kompetenz** dem **Oberleitungsorgan** (vgl. nachfolgend Ziff. 5.4 u. unten Ziff. 6.2; bei der Zürcher Kantonalbank § 15 Abs. 3 Ziff. 1 u. 2 ZKB-Gesetz). Solche Grundsätze und Vorgaben muss das Oberleitungsorgan selbständig festlegen (können), z.B. in Form von den Weisungen der Geschäftsleitung übergeordneten **Reglementen**. Die Kompetenz, auf Antrag der Geschäftsleitung bloss generell „Ja" oder „Nein" zum ganzen Paket entscheiden zu dürfen, reicht nicht aus. Demgegenüber ist **Rz 56 bereits richtig formuliert**, indem die Ausarbeitung der Geschäftspolitik dem Oberleitungsorgan obliegt und nicht in die Kompetenz bzw. Verantwortung der Geschäftsleitung für Anträge fällt. Die Formulierung von Rz 12 ist demgemäss im Sinne vorstehender Ausführungen mit Rz 56 in Einklang zu bringen. Aus Gründen von Klarheit und Systematik ist zudem hier der **letzte Satz** zu streichen und als **Ergänzung bei Rz 10** anzufügen (vgl. vorstehend Ziff. 5.2). Stattdessen ist der **zweitletzte Satz** wie folgt **anpassen**: (Aenderung im Fettdruck): „... Einrichtung und Ueberwachung **durch ein wirksames Risikomanagement.**"

5.4. **Zu Rz 13**: Die **Grundordnung eines Finanzinstituts** wird in Form von **Reglementen** erlassen. Weisungen sind demgegenüber operative Detailregelungen, welche die generellen in den Reglementen festgelegten Vorgaben konkretisieren. Die Weisungskompetenz gehört deshalb richtigerweise der Funktion Geschäftsleitung (so richtigerweise auch Rz 61 u. unten Ziff. 6.5). Deshalb sind hier **„Weisungen" zu streichen**. Das Oberleitungsorgan hat sich funktionsgemäss auf Erlass der Grundordnung zu beschränken, welche die **grundsätzlichen Vorgaben** für Unternehmenspolitik, Leitbild, Geschäftsstrategie und Organisation des Instituts (inkl. Eckpfeiler für Mitarbeitende zur Einhaltung von externen und internen Vorschriften und zu weiteren Verhaltensregeln) beinhaltet.

5.5. **Zu Rz 14**: (Auch) für Wirksamkeit von **Rechnungswesen und Finanzkontrolle** sollen sowohl Oberleitungsorgan als auch Geschäftsleitung (vgl. Rz 57 u. 59) zuständig sein. Richtigerweise hat das **Oberleitungsorgan** (auch) hier die **Gesamtverantwortung**, während der **Geschäftsleitung Umsetzungsverantwortung** zukommt.

Nach neuem Rechnungslegungsrecht ist zudem nicht mehr der Jahresbericht, sondern der **Lagebericht** zu genehmigen.

Schliesslich geht die Pflicht des Oberleitungsorgans, darüber hinaus auch **Geschäftsbericht, Jahresbudget, Zwischenabschlüsse und finanzielle Jahresziele** zu verabschieden, weit über das gesetzlich Vorgeschriebene und sinnvoll Praktikable hinaus. Gängige Praxis ist, dass das Oberleitungsorgan in Uebereinstimmung mit gesetzlichen Bestimmungen lediglich den Jahresabschluss verabschiedet. Es gibt keinen ersichtlichen Grund, weshalb die Zuständigkeiten nur für Banken im vorgeschlagenen Umfang zwingend zu erweitern. Die Folge wären **beträchtliche Mehraufwendungen** in organisatorischer Hinsicht (z.B. zusätzliche Sitzungen des Oberleitungsorgans vor einem Quartalsabschluss). Aber auch in materieller Hinsicht hätten solche Zusatzpflichten einen wesentlichen Einfluss auf die zeitlichen Kapazitäten der Mitglieder des Oberleitungsorgans. Entsprechend weniger Zeit stünde dem Oberleitungsorgan für seine Hauptaufgabe Unternehmensführung zur Verfügung. Wir empfehlen deshalb **Verzicht** auf diese Regelung.

5.6. **Zu Rz 15**: Die Kompetenz ist zu weit gefasst. Wahl und Abberufung auch **„weiterer Personen in leitenden Kontroll- und Schlüsselfunktionen"** sind **operative Tätigkeiten**, welche im Rahmen der vom Oberleitungsorgan gesetzten geschäftspolitischen Eckpfeiler von der **Geschäftsleitung** wahrzunehmen sind. Dies ergibt sich schon daraus, dass ein grosses Institut mehrere hundert Schlüsselfunktionen bzw. -personen haben kann. Das Oberleitungsorgan verfügt hier zumindest über die **Delegationskompetenz**, welche es mit vernünftigem Ermessen wahrnehmen kann. Mehr ist nicht erforderlich.

5.7. **Zu Rz 16**: Die Pflicht zur Einrichtung eines **wirksamen Internen Kontrollsystems (IKS)** steht im Widerspruch zur Pflicht der Geschäftsleitung nach Rz 59, welche (ebenfalls) für Ausgestaltung und Unterhalt eines IKS zuständig ist. Richtigerweise hat das **Oberleitungsorgan** die **Gesamtverantwortung** dafür, dass geeignete Massnahmen zur Risikosteuerung (wozu auch ein IKS gehört) implementiert werden. Dessen Umsetzung liegt demgegenüber in der Verantwortung der **Geschäftsleitung (Umsetzungsverantwortung**; vgl. oben Ziff. 5.4). Diese Abgrenzung ist abzubilden.

Zudem weist **Satz 2 von Rz 16** sachfremde Begriffe auf und ist deshalb der richtigen Terminologie entsprechend wie folgt anzupassen (Aenderungen in Fettdruck): „... Es **sorgt für ein geeignetes Konzept für das institutsweite Risikomanagement**".

Die **Bestimmung der aufsichtsrechtlichen Prüfgesellschaft** obliegt bei Aktiengesellschaften der Generalversammlung (Art. 730 V Ziff. 1 Abs. 1 OR). Damit liegt insbesondere **keine unentziehbare Kompetenz des Oberleitungsorgans** vor (Art. 716a OR e contrario). Im Fall der **Zürcher Kantonalbank** obliegt die Pflicht gemäss gesetzlicher Anordnung auf Antrag des Bankrats dem **Kantonsrat** (§ 15 Abs. 3 Ziff. 5 ZKB-Gesetz). Es gibt keinen Grund, in diesem Punkt für Banken weiter zu gehen als das OR bzw. das sich am OR orientierende ZKB-Gesetz und auf diesem Weg bewährte Regeln unnötigerweise einzuschränken (vgl. oben Ziff. 3.1). Im Falle der Zürcher Kantonalbank wäre die Anpassung der Governance in diesem Punkt wie dargelegt ohne kooperative Mitwirkung des Kantonsrats auch gar nicht möglich (vgl. oben Ziff. 4.9). Die Pflicht zur Bestimmung der aufsichtsrechtlichen Prüfgesellschaft durch das Oberleitungsorgan ist demzufolge in Rz 16 **ersatzlos zu streichen**.

5.8. **Zu Rz 17**: Der hier aufgelistete zwingende Katalog ist zu weitgehend und insbesondere zu offen formuliert, z.B. „Projekte von strategischer Bedeutung". Jedes Institut hat die relevanten Themen in Würdigung der konkreten Verhältnisse, mithin insbesondere von Grösse, Komplexität, Struktur und Risikoprofil des Instituts (vgl. FINMA-RS 2008/24, Rz 9), vernünftig festzulegen. In Anwendung des prinzipienorientierten Ansatzes ist demzufolge der ganze **Katalog und damit Rz 17 ersatzlos zu streichen**.

5.9. **Zu Rz 18**: Die Regelung macht im Prinzip Sinn. Der allzu offene **Begriff „Kernkompetenz"** ist aber zu präzisieren.

5.10. **Zu Rz 20 ff.**: Die Bestimmungen zur **Zusammensetzung und Unabhängigkeit des Oberleitungsorgans entbehren einer gesetzlichen Grundlage**. Abwegig ist **Rz 26**, welche ohne nähere Begründung ausdrücklich die **Gläubigerinteressen über die Eigentümerinteressen** stellt. Gläubigerschutz ist ein wichtiges Anliegen, das seinen Niederschlag aber in zivilrechtlichen Normen und in einer reichen Gerichtspraxis gefunden hat. Ein solches abstraktes Primat von Gläubigerinteressen in einem FINMA-Rundschreiben ist weder sinnvoll noch nötig und ändert im Gegenteil ohne Not etablierte gesellschaftsrechtliche Grundsätze massiv und nur für Banken ab.

5.11. **Zu Rz 28**: Das Kriterium der **Unabhängigkeit** muss hier mit Blick auf grosse Unterschiede von Institut zu Institut **präziser** gefasst werden. Die erforderliche Unabhängigkeit ist insbesondere dann gefährdet, wenn die betr. Person **Mitglied des Wahlorgans** ist. Eine Interessenkollision und damit auch eine Gefährdung der Unabhängigkeit kann sich darüber hinaus allenfalls auch bei weiteren **höchsten kantonalen Funktionen** wie z.B. des Regierungsrates oder höchster kantonaler Gerichte oder Steuerbehörden ergeben (vgl. Formulierung in § 14 Abs. 3 ZKB-Gesetz). Ist das Wahlorgan für das Oberleitungsorgan (bei der Zürcher Kantonalbank Bankpräsidium und Bankrat) ausschliesslich der Kantonsrat (vgl. § 11 Abs. 2 Ziff. 1 ZKB-Gesetz), haben Kommunalpolitiker wie z.B. Gemeindepräsidenten oder Vertreter kommunaler Körperschaften als unabhängig im Sinne von Rz 28 zu gelten.

5.12. **Zu Rz 31**: Der Katalog ist zu weitgehend. Insbesondere soll das Oberleitungsorgan nicht mit zu viel Administrativaufwand belastet werden, damit sich dessen Mitglieder prioritär auf die Hauptaufgabe der Führung der Gesellschaft (oder Gruppe) konzentrieren können. Die Festlegung der konkreten **Anforderungsprofile der „übrigen Mitglieder der Geschäftsleitung sowie weiterer Schlüsselpersonen"** muss **funktionsgemäss** der **Geschäftsleitung** obliegen.

5.13. **Zu Rz 33**: Das **Institut des Ausstands** ist sinnvoll und mitunter nötig. Ausstand ist aber auch nicht immer das beste Mittel, um Interessenkonflikten sinnvoll zu begegnen, zumal bei Konzernverhältnissen. **Alternativlösungen** können z.B. Vorschriften sein, wonach eine bestimmte Anzahl unabhängiger Mitglieder dem betr. Traktandum zustimmen müssen. Ultima ratio ist aber zweifellos der Ausstand. Die (richtige) Pflicht des Präsidenten, den Umgang mit solchen Konflikten zu regeln, ist deshalb dahingehend zu ergänzen, dass **neben dem Institut des Ausstandes auch andere Lösungen möglich** sind.

5.14. **Zu Rz 34**: Es gibt Institute, welche gerade aus Gründen der Corporate Governance **als Präsidium ein Kollektivorgan** einsetzen, so etwa die Zürcher Kantonalbank ein 3er-Gremium. Auch wenn innerhalb dieses Gremiums eine bestimmte Person als Präsident und die andern beiden als Vizepräsidenten amten (§ 16 Abs. 1 ZKB-Gesetz), kommen doch dem Präsidialgremium als ganzes zahlreiche wichtige Kompetenzen zu (vgl. z.B. § 16 Abs. 3 Ziff. 1-5). In solchen Fällen müssen die Anforderungen an den Präsidenten sachlogisch auch für die beiden Vizepräsidenten gelten. Dies ist in Rz 34 **zu präzisieren** („Der Präsident oder ein als Gremium konstituiertes Präsidium"). Nur am Rande sei erwähnt, dass der 1. Satz von Rz 34 nicht stricte iuris überprüfbar ist und deshalb reines „Programm" ist.

5.15. **Zu Rz 36**: Die organisatorische **Aufgliederung in separate Ausschüsse, insbesondere Prüf- und Risikoausschüsse**, macht **für grosse Institute** Sinn (zu den Aufgaben, Kompetenzen u. Verantwortlichkeiten vgl. aber unten Ziff. 5.17). Bei mittleren und kleineren Instituten ist eine derart feingliedrige Struktur weder nötig noch sinnvoll. Hier müssen innerhalb bewährter Governance, mit Blick auf Geschäftsmodell und Personalbestand und unter Zugrundelegung von vernünftigem Ermessen auch einfachere Lösungen möglich bleiben. Demzufolge ist es in Anwendung des **Proportionalitätsprinzips** angemessen, die Grenzziehung nicht erst zwischen den Aufsichtskategorien 3 und 4 zu ziehen, sondern bereits die **Kategorie 3 auszunehmen**. Analoges fordern wir auch für den Entschädigungsausschuss (unten Ziff. IV.3.2).

5.16. Zu **Rz 36-38**: Das Zusammenspiel dieser Regeln, insbesondere die Regel, dass auch die Ausschüsse „unabhängig" sein müssen, führt dazu, dass im **Ergebnis sehr wenig Spielraum für die sinnvolle Besetzung sämtlicher Ausschüsse** insbesondere **mit der Ausschuss-spezifisch notwendigen Fachkompetenz möglich** ist (vgl. Erläuterungsbericht, S. 12). Ist die Hauptregel gemäss Rz 21, dass nur 1/3 des Oberleitungsorgans unabhängig sein muss, ernst gemeint, wovon auszugehen ist, darf sie

nicht durch andere Regeln de facto aufgehoben werden. Die Herausforderung ist sachlogisch dadurch zu lösen, dass die **Unabhängigkeit** als eigenständiges Kriterium **nur auf Stufe Gesamt-Oberleitungsorgan** gefordert werden darf, nicht auch auf Stufe Einzelausschuss. Es gibt auch keinen bankenaufsichtsrechtlichen Grund, weshalb der **Präsident** nicht **auch Vorsitzender eines Ausschusses** sein kann. Es besteht keine FINMA-Kompetenz, solches hier einschränkend zu regeln. Rz 38 ist demzufolge ersatzlos zu streichen od. erheblich im Sinne der Ausführungen anzupassen.

5.17. **Zu Rz 40 ff. (Prüfungsausschuss) und 46 ff. (Risikoausschuss):** Die Aufgaben, Kompetenzen und Verantwortlichkeiten dieser beiden **Ausschüsse** können **je nach Grösse, Komplexität, Struktur und Risikoprofil eines Instituts** (vgl. FINMA-RS 2008/24, Rz 9) massiv variieren. Demzufolge kann ein bestimmtes Thema z.B. bei einem Institut als hohes Risiko eingeschätzt sein, was die Zuordnung zum Risikoausschuss nahelegt. Bei einem andern Institut kann mangels hohem Risiko Exposure bei demselben Thema die Zuordnung zum Prüfungsausschuss angemessen sein. Die Zürcher Kantonalbank hat die Gremien Prüfungs- und Risiko- (Management-) Ausschüsse (ebenso wie einen Entschädigungs- und Personalausschuss; vgl. FINMA-RS 2010/1, Rz 21 u. unten Ziff. IV.3) bereits implementiert, deren Aufgaben aus vorstehend dargelegten Gründen aber teilweise anders geregelt als gemäss Rz 40 ff. vorgesehen. So ist z.B. bei der Zürcher Kantonalbank entgegen Rz 47 das Thema „**Kapital- und Liquiditätsplanung**" dem Pflichtenheft des Prüfungsausschusses zugeteilt (vgl. § 2 Abs. 1 Ziff. 1 der Richtlinien über die Aufgaben und Befugnisse des Prüfungsausschusses der Zürcher Kantonalbank). Umgekehrt gehört z.B. das Thema „**Ueberwachung- und Beurteilung der Wirksamkeit der internen Kontrolle**" entgegen Rz 43 zum Pflichtenheft des **Risiko- (Management-) Ausschusses** (vgl. § 2 Abs. 1 Ziff. 2 der Richtlinien über die Aufgaben und Befugnisse des Risikomanagement-Ausschusses der Zürcher Kantonalbank).

Diese Thematik ist demzufolge richtigerweise dadurch zu lösen, dass die Vorgaben der FINMA in Nachachtung des **prinzipienorientierten Ansatzes** strikte generell bleiben müssen. Jedes Institut ist zu verpflichten, die **gemäss vernünftiger Ermessenseinschätzung wichtigen Themen unter Würdigung der konkreten Verhältnisse**, mithin unter Würdigung insbesondere von Grösse, Komplexität, Struktur und Risikoprofil des Instituts (vgl. FINMA-RS 2008/24, Rz 9), dem **Pflichtenheft des einen oder andern Ausschusses** zuzuteilen. Für diese Lösung spricht auch die vorgesehene Pflicht zur Implementierung geeigneter Informationsflüsse zwecks Abstimmung zwischen den beiden Ausschüssen (Rz 52). Gestützt auf diese **Abstimmungspflicht** kommt der Frage, welches Thema welchem Ausschuss zugeteilt wird, nur noch untergeordnete Bedeutung zu.

Wenn schon fälschlicherweise eine allgemein verbindliche Regelung der Pflichtenhefte der beiden Ausschüsse erfolgt, wäre jedenfalls die implementierte **Lösung der Zürcher Kantonalbank überzeugender**. Einerseits bringt sie bereits formell Bezeichnungen und Verantwortlichkeiten der Ausschüsse besser in Einklang und führt überdies zu einer **Konzentration von spezifischen Risikothemen beim Risikoausschuss** und von **Kapital- und Liquiditätsthemen beim Prüfungsausschuss**. Dies wiederum erleichtert die anspruchsvolle Aufgabe der richtigen Zuteilung der Mitglieder des Oberleitungsorgans entsprechend ihrer Fachkompetenz zum einen oder andern Ausschuss (vgl. oben Ziff. 5.16).

6. Bemerkungen zu Abschnitt V Geschäftsleitung (Rz 53 ff.)

6.1. Der Geschäftsleitung kommen diejenigen Aufgaben, Kompetenzen und Verantwortlichkeiten zu, welche im Fall der Zürcher Kantonalbank teilweise der Zürcher Kantonsrat im ZKB-Gesetz und im Uebrigen

der Bankrat als Oberleitungsorgan, genehmigt vom Zürcher Kantonsrat, insbesondere im Organisationsreglement und im Reglement über die Generaldirektion an diese delegiert hat. Die FINMA ist nicht befugt, mit Bezug auf „Corporate Governance" in solche rechtskonform und sinnvoll geregelten Gesellschaftsstrukturen einzugreifen. Allfällige Vorschriften der FINMA haben sich auf die **aus bankenaufsichtsrechtlicher Sicht zwingenden Aspekte betr. Risikomanagement, IKS und Kontrollfunktionen** zu beschränken und müssen **prinzipienorientiert** bleiben (vgl. vorne Ziff. 4.4).

6.2. In diesem Abschnitt V **fehlt eine Regelung**, welche die **Verantwortung der Geschäftsleitung** zur Umsetzung der notwendigen Risikoorganisation klar festhält. Dies ist zur Schaffung von **Rechtssicherheit mit Bezug auf die grundsätzlichen Aufgaben, Kompetenzen und Verantwortlichkeiten der wesentlichen Organe und Funktionen** elementar (vgl. oben Ziff. 4.4). Wir fordern deshalb, die **Formulierung gemäss altbewährter Vorfassung in FINMA-RS 2008/24, Rz 99** ausdrücklich auch in dieses Rundschreiben zu übernehmen. Wesentlich ist insbesondere die klare Unterscheidung zwischen der Verantwortung der mit Anordnungskompetenz ausgestatteten Geschäftsleitung zur Umsetzung der Risikoorganisation und der Verantwortung der Compliancefunktion (und anderer Risikokontrollfunktionen) zur Risikokontrolle (vgl. oben Ziff. 4.3).

6.3. **Zu Rz 57 u. 59**: Die **Doppelzuständigkeiten** von Geschäftsleitung und Oberleitungsorgan (gemäss Rz 14 u. 16) sind durch Präzisierung der Formulierung (vgl. oben Ziff. 5.5 u. 5.7) **zu korrigieren**.

6.4. **Zu Rz 60**: Wir empfehlen zur Klärung folgende Ergänzung (Ergänzung in Fettdruck): „... Bilanzstrukturmanagement **und Liquiditätsmanagement**."

6.5. **Zu Rz 61**: Die **Weisungskompetenz** gehört richtigerweise zur Funktion Geschäftsleitung. Deshalb ist sie hier stehen zu lassen, aber bei Rz 13 zu streichen (vgl. oben Ziff. 5.4).

6.6. **Zu Rz 62**: Die Geschäftsleitung soll verantwortlich für eine „Technologieinfrastruktur" sein, welche Sicherheit, Integrität und Verfügbarkeit der Daten und Systeme bietet. Im Entwurf zum geänderten FINMA-RS 2008/21 ist demgegenüber in Rz 135.2 lit. b von „Schutz der Technologieinfrastruktur vor Cyberattaken, insbesondere im Hinblick auf die Verfügbarkeit der Systeme und die Integrität respektive Vertraulichkeit von Daten" die Rede, in Rz 135.1 Ziff. f von „Prozessen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Verantwortung zur Reduktion von IT-Risiken sowie Einhaltung der IT-Sicherheit und -Verfügbarkeit". In Rz 1 von Anhang 3 von FINMA-RS 2008/21 wiederum steht: „Die Grundsätze sind hauptsächlich auf das Risiko von Vorfällen in Bezug auf die Vertraulichkeit von Kundenmassendaten durch Verwendung elektronischer Systeme zugeschnitten. Sie gehen nur am Rande auf Sicherheitsüberlegungen für physische Daten sowie auf Fragen der Integrität und Verfügbarkeit von Daten ein." Wir empfehlen, alle diese Abschnitte besser aufeinander abzustimmen und dabei durchwegs die **drei wichtigen Anforderungen „Vertraulichkeit, Integrität und Verfügbarkeit"** zu verwenden, welche sachlich zusammengehören. Gestützt darauf wird im Ergebnis auch eine **prinzipienorientierte Regelung** erreicht (vgl. oben Ziff. 4.4 u. unten Ziff. III.4).

7. Bemerkungen zu Abschnitt VI Rahmenkonzept (Rz 66 ff.)

7.1. Das FINMA-Rundschreiben hat sich **auf bankenrechtlich zwingend geforderte Vorschriften zu Risikomanagement, IKS und Kontrollfunktionen zu beschränken** und dabei den **prinzipienorientierten Ansatz zu verwirklichen**. Die Regeln gemäss Entwurf sind zu detailliert und greifen teilweise

in Aufgaben, Kompetenzen und Verantwortlichkeiten anderer Organe ein, die gegenüber Dritten zivilrechtlich haftbar werden können. Damit werden bewährte bestehende **Prinzipien zur unternehmerischen Verantwortlichkeit** auf den Kopf gestellt. Ueberdies wird der **Grundsatz prinzipienbasierter Regulierung** missachtet (vgl. Ziff. 4.4). Der Katalog ist demzufolge wenn schon **auf die wesentlichsten Kernthemen zu reduzieren**.

7.2. Im **Eventualstandpunkt** empfehlen wir, die **Aufzählung der Aspekte** wenigstens **sachlich präziser mit veränderter Reihenfolge** grundsätzlich wie folgt vorzunehmen: Rz 69, 70, 73, 71, 74, 72, 75, 78, 77 und 76.

7.3. **Zu Rz 70**: Ebenfalls als **Eventualstandpunkt** empfehlen wir folgende Ergänzung (Ergänzung in Fettdruck): „Präzisierung der **materiellen** institutsspezifischen ..."

7.4. **Zu 73 u. 75**: Bei beiden Rz empfehlen wir ebenfalls als **Eventualstandpunkt** zur Klärung folgende Ergänzung (Ergänzung in Fettdruck): „... auf sämtliche **materiellen** Risikokategorien ..."

7.5. Dass der von uns geforderte **prinzipienorientierte Ansatz** (vgl. oben Ziff. 4.4) mit vorliegendem Entwurf noch nicht realisiert ist, zeigt sich auch darin, dass statt einer Beschränkung auf **generelle Grundsätze** stattdessen **auch Aspekte der Umsetzung** geregelt werden. Dies ist, wie nachfolgend aufgezeigt wird, insbesondere mit Bezug auf Rz 67, 71 und 72 der Fall.

7.6. **Zu Rz 67/71**: Das Rahmenkonzept, welches wir ohnehin ablehnen (vgl. oben Ziff. 4.4) soll Risikopolitik, Risikoappetit sowie **Risikolimiten** festlegen. Indessen ist das Festlegen konkreter Limiten als risikosteuernde Massnahme sachlogisch bereits **Umsetzung**. Kommt dazu, dass Limiten nicht bei allen Arten von Risiken bzw. Geschäftsfeldern sinnvolle Massnahmen zur Risikosteuerung darstellen. In diesem Zusammenhang ist deshalb bei **Rz 67** jedenfalls der Begriff Risikolimiten zu streichen. Bei **Rz 71** werden neben der Pflicht zu Risikolimiten zudem **Definitionen von Risikominderungsstrategien und Risikominderungsinstrumenten** festgelegt. Letztere stellen ebenfalls Umsetzungsmassnahmen dar. Deshalb ist die ganze **Rz 71 ersatzlos zu streichen**. Falls sich die FINMA wider Erwarten gegen diese Streichung stellt, müsste im Eventualfall zumindest dieselbe Ergänzung wie bei Rz 73 u. 75 vorgenommen werden (Präzisierung der **materiellen** institutsspezifischen ...; vgl. oben Ziff. 7.4).

7.7. **Zu Rz 72**: Die geforderte **Definition von Massnahmen**, um Verletzungen der Risikolimiten rechtzeitig zu erkennen, ist ebenfalls bereits einer **Umsetzung** und deshalb **ersatzlos zu streichen**.

7.8. Soweit vorstehend kritisierte Regelungen wider Erwarten beibehalten werden, müsste die Anforderung nach dem Gesagten jedenfalls auf ein **Rahmen- und Umsetzungskonzept** für das institutsweite Risikomanagement ausgedehnt werden.

7.9. Mindestens die **Rz 121, 122, 128 u. 130 von FINMA-RS 2008/21** enthalten weitere Regelungen hinsichtlich der im Rahmenkonzept abzudeckenden Aspekte. Dieser Zusammenhang muss durch entsprechende **Querverweise** evident gehalten werden. Dies aber nur noch, soweit diese Regelungen im Rahmen einer **prinzipienorientierten Regelung** überhaupt noch nötig sind.

7.10. Aus dem Vernehmlassungstext geht nicht hervor, inwiefern das **Management von Compliance-Risiken** ebenfalls Teil des Rahmenkonzepts für das institutsweite Risikomanagement ist. Mit Blick auf das Ziel eines **in sich stimmigen Gesamtkonzepts** für das Risikomanagement ist klar davon auszu-

gehen. Für den **Eventualfall**, dass am System eines Rahmenkonzeptes entgegen unserer Forderung überhaupt festgehalten wird (vgl. oben Ziff. 4.4), wäre dies aus Klarheitsgründen **zu präzisieren** (vgl. auch oben Ziff. 4.6 f.).

8. Bemerkungen zu Abschnitt VII Internes Kontrollsystem (Rz 79 ff.)

8.1. Zu **Rz 79**: Aus systematischen Gründen sollten die **Sätze 2 und 3** („Diese soll namentlich ... Risikostrategien zu implementieren") hier **gestrichen und am Ende von Rz 89 eingefügt** werden (vgl. oben Ziff. 4.6 ff. zu Rz 7). Teilweise ist die Formulierung der Sätze 2 und 3 auch nicht auf **Compliance-Risiken** zugeschnitten. Letztere sind i.d.R. **nicht klar „messbar", sondern lediglich steuerbar** (vgl. Othmar Strasser, Management von Compliance Risiken, S. 262 f.). Dies rechtfertigt ebenfalls die systematische Umteilung.

8.2. **Zu Rz 86**: Die **notwendigerweise mit einer effizienten Compliancefunktion verbundenen Aufgaben, Kompetenzen und Verantwortlichkeiten** werden unvollständig, damit missverständlich und teilweise (insb. in Rz 8) schlicht falsch geregelt (vgl. oben Ziff. 4.3). Wichtig ist hier unter Rz 86 insbesondere, dass die Compliancefunktion ein **uneingeschränktes Eskalationsrecht** ans Oberleitungsorgan haben muss, und zwar in formeller Hinsicht **an dieses Gremium als Ganzes** und nicht bloss wie in Rz 86 geregelt nur an einen Ausschuss desselben. Diese Einschränkung wiederspricht den zwingenden Vorschriften von Art. 716 u. Art. 716a Ziff. 1, 2 u. 5 OR (nichtdelegierbare Kompetenz des Oberleitungsorgans zur Festlegung von Organisation und Erlass von Vorgaben, u.a. zur Einhaltung von externen und internen Vorschriften). Das Eskalationsrecht darf **auch nicht in zeitlicher Hinsicht eingeschränkt** werden wie dies Rz 86 tut („regelmässig"). Nicht ausreichend ist ein bloss periodisches Informationsrecht in Form von Berichterstattung, wie dies Rz 86 suggeriert. Erforderlich ist vielmehr ein **jederzeitiges** Eskalationsrecht **im Einzelfall**, damit die Compliancefunktion, wenn nach ihrer Einschätzung z.B. hohe Risiken in Frage stehen, im Interesse des Instituts das Oberleitungsorgan umgehend informieren kann (vgl. für Zürcher Kantonalbank § 17 Compliance-Reglement Konzern und Stammhaus; zum Ganzen Othmar Strasser, a.a.O. Integrierte Funktion Recht, S. 153 f.). Dementsprechend ist Rz 102 zu präzisieren und zu ergänzen (analog Rz 98, vgl. unten Ziff. 8.10 f.).

Als eine Art Vorstufe zum Eskalationsrecht muss die Compliancefunktion auch über das Recht verfügen, **wichtige Informationen gleichzeitig parallel** der **Geschäftsleitung und dem Oberleitungsorgan** zur Kenntnis zu bringen, z.B. periodische Berichte über die Einschätzung der Risiken (vgl. Rz 99-102). Damit wird das Risiko gesteuert, dass das Oberleitungsorgan aus Sicht Compliancefunktion wichtige Informationen jedenfalls **ungefiltert** erhalten muss (vgl. Othmar Strasser, a.a.O. Integrierte Funktion Recht, S. 138 ff.).

8.3. **Zu Rz 87**: Eine **eigenständige Risikokontrolle (CRO)** macht **für grosse Institute** Sinn. Bei mittleren und kleineren Instituten ist eine solche formale Anforderung weder nötig noch sinnvoll. Hier müssen innerhalb bewährter Governance, mit Blick auf Geschäftsmodell und Personalbestand und unter Zugrundelegung von vernünftigem Ermessen auch einfachere Lösungen möglich bleiben, ganz im Sinne des **Proportionalitätsprinzips** (vgl. Rz 9). Demzufolge ist es angemessen, von dieser Regelung auch die Institute gemäss **Aufsichtskategorie 3 auszunehmen**.

8.4. **Zu Rz 88**: Die Forderung nach einem **CRO**, welcher **ausschliesslich für die Risikokontrolle** (i.S.v. Rz 89-98) **zuständig** sein soll, erachten wir als **kontraproduktiv**. Abgesehen von Compliance-Risiken

werden unter der Funktion CRO typischerweise sämtliche Risikobereiche zusammengefasst. Dies muss möglich sein, solange die unterstellten Funktionen **nicht ertragsorientiert** sind und überdies **Fachkompetenz** im Bereich Risikomanagement aufweisen. Dies wird auch **vom Erläuterungsbericht bestätigt** (vgl. S. 15). Die Kompetenz des CRO allein auf Risikokontrolle zu beschränken wäre ebenfalls kontraproduktiv, würde doch damit ein schlagkräftiges zentrales Risk Management organisatorisch und personell auseinandergerissen. Wir ersuchen Sie, diese Regelung im Sinne der Ausführungen abzuändern und zu präzisieren. Eine aus unserer Sicht zielführende Neuformulierung von Rz 88 lautet wie folgt:

„Systemrelevante Banken bestimmen einen CRO, der Mitglied der Geschäftsleitung und mindestens für die Risikokontrolle i.S.v. Rz 89-98 zuständig ist."

8.5. **Zu Rz 88/89**: Gemäss Rz 85 bestimmt jedes Institut innerhalb der Geschäftsleitung die Person(en), welche für die unabhängigen Kontrollinstanzen zuständig ist/sind. Dies gilt gemäss systematischer Gliederung dieses Abschnitts nur für die in Rz 80 genannten, „von den ertragsorientierten unabhängigen Kontrollinstanzen", nicht auch für die interne Revision. Letztere wird erst im nachfolgenden VIII. Abschnitt (Rz 104 ff.) geregelt. Zur Klärung empfehlen wir, den Titel entsprechend anzupassen.

8.6. **Zu Rz 89 ff.**: Der wichtige **Schlüsselbegriff der Risikokontrolle** im Sinne der Aufgabe (nicht der Funktion) wird im Entwurf nicht mehr griffig definiert, sondern in zahlreiche Einzelaspekte zerrissen. Der Begriff ist **zu definieren** (vgl. oben Ziff. 4.3 lit. a) und zwar im von uns geforderten Glossar (vgl. oben Ziff. 4.1 f.). Eine präzise Formulierung findet sich in der altbewährten Regelung gemäss **FINMA-RS 2008/24, Rz 122**. Diese Formulierung ist somit auch ins neue Rundschreiben zu übernehmen, die Formulierungen gemäss Rz 89 ff. des Entwurfs entsprechend anzupassen. Die Aufgabe **Risikokontrolle wird auch von der Compliancefunktion wahrgenommen**. Die Formulierung von FINMA-RS 2008/24, Rz 122 ist demzufolge auch bei der Compliancefunktion zu regeln (Rz 99 ff.). Andernfalls wäre die Regelung - wie bisher - analog auf die Compliancefunktion anwendbar (vgl. oben Ziff. 4.3 lit. d).

8.7. **Zu Rz 89**: Hier sind zusätzlich die in Rz 79 gestrichenen Sätze 2 und 3 neu einzufügen (vgl. oben Ziff. 8.1). In der Formulierung von Rz 89 ist im Uebrigen (ebenfalls) klarzustellen, dass auch der Risikokontrolle **keine generelle uferlose Ueberwachungspflicht** zukommt, sondern wie bei der Compliancefunktion **nur im Rahmen der von der Geschäftsleitung festgelegten Umsetzung** einer in sich stimmigen Risikoorganisation (vgl. oben Ziff. 4.3 u. 6.2 u. unten Ziff. 8.10 ff.).

8.8. **Zu Rz 91**: Wir empfehlen folgende Umformulierung (Aenderungen in Fettdruck): „Die Risikokontrolle **legt** die für ... notwendigen Informationen **fest**."

8.9. **Zu Rz 92**: Gemäss bewährtem Setup in zahlreichen Instituten liegt die Verantwortung für die Ueberwachung von Systemen für die Einhaltung aufsichtsrechtlicher Pflichten in Zusammenhang mit **Eigenmittel-, Risikoverteilungs- und Liquiditätsbewirtschaftung** statt beim CRO beim CFO. Deshalb empfehlen wir folgende Umformulierung (Aenderungen in Fettdruck): „... **Die** Ueberwachung von Systemen für die Einhaltung von aufsichtsrechtlichen Vorschriften (insbesondere Eigenmittel-, Risikoverteilungs- und Liquiditätsvorschriften) **liegt in der Verantwortung des CRO oder des CFO**.

8.10. **Zu Rz 95**: Es stimmt, dass die **Risikokontrolle aktiv in den Prozess der Festlegung der Risikolimiten eingebunden** ist. Die Risikokontrolle hat aber formal **weder Antrags- noch Entscheidkompetenz**. Demzufolge kann sie auch **nicht gewährleisten**, dass sämtliche in Rz 95 aufgeführten Parame-

ter tatsächlich richtig gesetzt werden. Eine solche Gewährleistungspflicht würde, wie bereits unter Rz 89 falsch formuliert, zu einer generellen uferlosen Ueberwachungspflicht der Risikokontrolle führen (vgl. oben Ziff. 8.7). In der Formulierung von Rz 95 ist deshalb **klarzustellen**, dass die Risikokontrolle mangels Antrags- und Entscheidkompetenz **weder eine allgemeine Ueberwachungspflicht noch die Pflicht, die Richtigkeit der festgelegten Regeln zu gewährleisten**, hat.

8.11. **Zu Rz 98**: Die allgemeine **periodische Berichterstattung** ist klar von der **Information über eine konkrete Regelverletzung** zu unterscheiden (vgl. oben Ziff. 8.2). Bei Regelverstössen kann die Geschäftsleitung wesentlich schneller handeln als das Oberleitungsorgan. Im **Normalfall** genügt deshalb selbst bei schwerwiegenden Regelverstössen die **sofortige Information der Geschäftsleitung** zwecks Anordnung der notwendigen Massnahmen (vgl. FINMA-RS 2008/24, Rz 111). Unter Vorbehalt des Eskalationsrechts unabhängiger Kontrollfunktionen (vgl. oben Ziff. 8.2) genügt diesfalls die **nachträgliche Information des Oberleitungsorgans** über den Missstand und seine Behebung, entweder nach Behebung des Missstandes oder im Rahmen der ohnehin erfolgenden periodischen Berichterstattung. In gewissen Fällen drängt sich zumindest eine **zeitgleiche Information des Oberleitungsorgans auf, z.B. bei presseträchtigen Vorfällen**. Nur, aber immerhin **in ausgesprochenen Ausnahmefällen**, z.B. bei Regelverstössen durch die Geschäftsleitung selbst oder in Ausübung des Eskalationsrechts, ist sachlogisch direkt das **Oberleitungsorgan** zu informieren, damit dieses **anstelle der Geschäftsleitung** die notwendigen Massnahmen entscheiden kann. Die Regelung von Rz 98 ist entsprechend im Sinne vorstehender Ausführungen anzupassen (ebenso wie Rz 102; vgl. nachstehend Ziff. 8.12).

8.12. **Zu Rz 102**: „Risikokontrolle" findet auch im Bereich der Compliancefunktion statt (vgl. oben Ziff. 4.3 lit. d). Das **Recht auf jederzeitigen unbeschränkten Zugang zum Oberleitungsorgan (Eskalationsrecht)** ist folgerichtig hier ebenfalls im Sinne unserer Ausführungen zu Rz 86 (oben Ziff. 8.2) und zu Rz 98 (vorstehend Ziff.8.11) zu präzisieren und zu ergänzen.

9. Bemerkungen zu Abschnitt VIII Interne Revision (Rz 104 ff.)

9.1. Entsprechend der Systematik mit (mindestens) drei Kontrollinstanzen (ertragsorientierte Geschäftseinheiten, von den ertragsorientierten Geschäftseinheiten unabhängige Kontrollinstanzen u. interne Revision) drängt es sich auf, den Abschnitt „VIII Interne Revision" neu im Abschnitt „VII Kontrollinstanzen" als neues Kapitel „C" zu führen.

10. Bemerkungen zu Abschnitt IX Gruppenstrukturen (Rz 125 ff.)

10.1. Dieser Abschnitt ist im Prinzip zu begrüssen. Gemäss **BCBS-Principles Corporate Governance for Banks**, Prinzip 5 (‚Governance of group structures'), Ziff. 95 gilt aber **zusätzlich**, dass „the board of the parent company should be aware of the material risks and issues that might affect both the bank as a whole and its subsidiaries". Es ist daher sinnvoll und nötig, **Prinzipien zur Führung der Gruppe** zu implementieren (z.B. Informationsfluss und -austausch, Vereinheitlichung von Dokumenten, etc.)

10.2. **Zu Rz 126**: Das Zusammenspiel der ersten beiden Sätze ist verwirrend und bedarf einer klärenden Neuformulierung.

11. Bemerkungen zu Abschnitt X Offenlegung (Rz 128 ff.)

11.1. Die Offenlegungspflichten gehen zu weit, insbesondere weiter als derzeitige gesetzliche Regelungen samt anerkannten internationalen Standards. Insbesondere sind Anliegen des **Anlegerschutzes auf dem Weg entsprechender Gesetzgebung** (z.B. im FIDLEG) zu regeln und nicht durch die Hintertür eines rechtlich grundsätzlich nicht verbindlichen FINMA-Rundschreibens, dem aber in der Praxis faktisch weitreichende Wirkung zukommt. Die Formulierung ist somit **zu redimensionieren**.

11.2. **Zu Rz 133**: **Grundsätze des Wahlverfahrens für das Oberleitungsorgan und des Rekrutierungsprozesses für Mitglieder der Geschäftsleitung** sollen nicht offengelegt werden müssen. Dies ginge weit über bewährte gesetzliche Regelungen und internationale Standards hinaus. Deshalb ist diese Bestimmung **ersatzlos zu streichen**.

11.3. **Zu Rz 138**: Die Publikation der Organisation des Oberleitungsorgans genügt. Deshalb ist **„Arbeitsweise"** zu **streichen**.

11.4. **Zu Rz 143**: Ein Monat ist zu kurz, um materielle Aenderungen, z.B. nach einem Strategiewechsel, auf der Internetseite nachzuführen. Deshalb ist **„innerhalb eines Monats" streichen**.

12. Bemerkungen zu Abschnitt XI Inkrafttreten und Uebergangsbestimmungen (Rz 144 f.)

Zu Rz 145: Die **Umsetzungsfrist** muss **2 Jahre** betragen (vgl. oben Ziff. I.11)

III. Zur Anpassung des FINMA-RS 2008/21 Operationelle Risiken Banken

1. Bemerkungen zu Rz 2

1.1. Bei der Umschreibung der operationellen Risiken soll neu die **Ausnahme für strategische Risiken und Reputationsrisiken gestrichen** werden (bisherige Formulierungen gemäss Satz 3 von Rz 1 u. Rz 2.1). Dies ist insofern richtig, als auch solche Risiken Auswirkungen auf die Reputation eines Instituts haben können.

1.2. Wichtig für das Gesamtverständnis ist, dass zur Schaffung eines in sich stimmigen Gesamtkonzepts und von klaren Abgrenzungen zwischen der Funktion Risikokontrolle und der Compliancefunktion auch die **Compliance-Risiken ausdrücklich definiert** werden, und zwar durch Uebernahme der **altbewährten Formulierung gemäss FINMA-RS 2008/24, Rz 98** (vgl. oben Ziff. II.4.3 lit. a u. II.4.6). Dies hat im von uns geforderten **Glossar** zu erfolgen (vgl. oben Ziff. II.4.1).

1.3. Compliance-Risiken erfassen als **Verhaltensrisiken**, welche zu **Rechtsverletzungen** führen, eine Gemengelage von Konsequenzen, welche immer auch mehr oder weniger grosse **Reputationsschäden, finanzielle Verluste und überdies rechtliche Sanktionen** generieren (FINMA-RS 2008/24, Rz 98). Letztere erfassen z.B. Nachteile wie Bewilligungsentzug, Kündigung vorteilhafter Vertragsbeziehungen,

Ausschluss, Lizenzverlust, Gefängnisstrafen, u.ä., welche wiederum immer mehr oder weniger grosse Reputationsschäden, finanzielle Verluste und (weitere) rechtliche Sanktionen nach sich ziehen (Othmar Strasser, a.a.O. Management von Compliance Risiken, S. 261 ff. m.w.V.; vgl. auch unten Ziff. 8.1).

1.4. Demgegenüber bleibt die **Definition der operationellen Risiken gemäss vorgeschlagener Formulierung von Rz 2 unklar**. Durch die ausdrückliche Eingrenzung der Risikokategorie auf Gefahr von „Verlusten" ist davon auszugehen, dass von der Umschreibung „sämtliche" rechtlichen Risiken die **Kategorie rechtlicher Sanktionen** (vgl. vorstehend Ziff. 1.3) **nicht erfasst** ist. Zusätzlich unklar wird die Umschreibung dadurch, dass zwar „Sanktionen" erwähnt werden, aber ausdrücklich auf „Bussen von Aufsichtsbehörden" und damit wiederum auf Verluste eingeschränkt. Diese Formulierung schafft überdies unnötige Verwirrung, weil das aktuelle Bankenaufsichtsrecht bekanntlich die Sanktionierung mit Busse gar nicht vorsieht. Wir empfehlen, die Koordination zwischen operationellen und Compliance-Risiken im Sinne der Ausführungen klarer zu regeln.

1.5. Unter Mitberücksichtigung der Tatsache, dass Compliance-Risiken i.d.R. nicht klar messbar, aber immerhin steuerbar sind (vgl. oben Ziff. II.8.1) könnte eine klarere **Abgrenzung zwischen operationellen und Compliance-Risiken** durch **Umformulierung von Art. 89 ERV** erfolgen, wonach vom Begriff operationelle Risiken **Rechtsrisiken** „nur erfasst werden, soweit sie **messbar** sind" (was beim oben in Ziff. 1.3 genannten Katalog i.d.R. nur auf finanzielle Verluste zutrifft).

2. Bemerkungen zum Grundsatz 1 Kategorisierung und Klassifizierung (Rz 119 ff.)

2.1. Die neu eingeführte Pflicht zur Kategorisierung und Klassifizierung von operationellen Risiken (Rz 121 f. u. Anhang 2) macht im Sinne eines **Gesamtkonzepts** im Prinzip Sinn, weil damit dem Risikomanagement eine **besser strukturierte Basis für ein effizientes Risikomanagement** gegeben wird. Entsprechend dem Proportionalitätsprinzip bzw. **prinzipienorientierter Regulierung** (Rz 117) ist die Kategorisierung indessen genereller mit weniger Detailgrad zu fassen (vgl. oben Ziff. II.4.4)

2.2. Zu präzisieren ist in **Rz 121**, auf welcher **Basis** die „Risikobereitschaft gemessen an inhärenten Risiken" und „Risikotoleranz gemessen an den Residualrisiken" zu ermitteln sind.

3. Bemerkungen zum Grundsatz 3 Interne und externe Berichterstattung (Rz 131 ff.)

3.1. Es fällt auf, dass betr. interne und externe Offenlegungspflichten keinerlei Hilfestellung mit Bezug auf die **Materialitätsgrenze**, welche eine solche Pflicht auslöst, formuliert wird (vgl. insb. Rz 132). Ohne solche Präzisierung obliegt es der auf vernünftigem Ermessen basierenden **Einschätzung jedes Instituts**, ob ein Fall von Offenlegung gesetzt vorliegt.

4. Bemerkungen zum Grundsatz 4 Technologieinfrastruktur (Rz 135 ff.)

In Nachachtung des erklärten Anspruchs einer **prinzipienorientierten Regelung** unter Verzicht auf Detailausführungen (Rz 117 u. oben Ziff. II.4.4) erachten wir die Reduzierung des ganzen Abschnitts lediglich auf Rz 135 als sachgerecht. Bei den thematisch nachfolgend in **Rz 135.1-135.3** aufgezählten Aspekten handelt es sich ohnehin nicht um Prinzipien, sondern um **operative Umsetzungsmass-**

nahmen. Solche sind abhängig vom konkreten Geschäftsmodell und daraus abgeleiteten Risikoexposures jedes einzelnen Instituts. Unabhängig davon die Anforderungen von Rz 135.1-135.3 als Minimalstandard zu fordern, ist in Anwendung **prinzipienorientierter Regulierung** weder sinnvoll noch nötig. Folgerichtig sind die **Rz 135.1-135.3 ersatzlos zu streichen** (vgl. oben Ziff. II.6.6).

5. Bemerkungen zu Rz 135

Die Formulierung von Rz 135 gemäss Entwurf impliziert, dass sowohl ein IT-Konzept und ein integriertes und umfassendes Risikomanagement zu implementieren ist. Richtigerweise ist selbstverständlich nur schon aus Gründen der Konsistenz ein kombiniertes **IT-Risikomanagement-Konzept** gemeint. Zudem ist es nicht stufengerecht, wenn die Geschäftsleitung ein solches Konzept zu erstellen hat. Die **Zuständigkeit auf tieferer Stufe**, je nach Organisation des Instituts z.B. beim Leiter IT, ist angemessen. Die Geschäftsleitung hat im Rahmen ihrer generellen Verantwortung zur Umsetzung einer geeigneten Risikoorganisation nur, aber immerhin dafür zu sorgen, dass damit (auch) das IT-Risikomanagement abgedeckt wird (vgl. oben Ziff. II.5.7 u. 6.2). Die Formulierung in Rz 135 ist im Sinne der Ausführungen entsprechend anzupassen.

6. Bemerkungen zu Rz 135.1-135.3

6.1. Die Ausführungen unter dieser Ziff. 6 erfolgen nur für den **Eventualfall**, dass die FINMA wider Erwarten unserer Forderung gemäss oben Ziff. 2.1 und Ziff. 4 nicht folgt.

6.2. **Zu Rz 135.1**: Das OpRisk-Konzept beinhaltet das IT-Risikomanagement-Konzept und das IT-Risikomanagement-Konzept umfasst wiederum das Cyber-Risikomanagement-Konzept. Analog zu Rz 135 (vgl. oben Ziff. 5) ist auch hier der kombinierte Begriff **„IT-Risikomanagement-Konzept"** zu verwenden.

6.3. Die ausführlichen Minimalanforderungen gemäss **Rz 135.1 lit. a-g** lehnen sich gemäss Erläuterungsbericht an einschlägige internationale Standards an. Werden die Anforderungen von Rz 135.1 lit. a-g erfüllt, sind demzufolge auch die internationalen Standards (z.B. gemäss Security Standards im COBIT-Rahmenwerk von ISACA; vgl. FN 15 des Rundschreibens) erfüllt. Dies genügt für eine erklärtermassen **prinzipienorientierte Regulierung** (vgl. oben Ziff. II.4.4) vollauf. Die ausdrücklichen **Hinweise im Ingress von Rz 135.1 und in FN 15 sind demzufolge ersatzlos zu streichen**. Andernfalls müsste der Finanzdienstleister gegenüber der Revisionsstelle nicht nur die Einhaltung von Rz 135.1, sondern darüber hinaus immer auch die Einhaltung der internationalen Standards nachweisen.

6.4. Unter **lit. a von Rz 135.1** ist **keine „Vollständigkeit"** erforderlich. Wie in allen andern Bereichen eines effizienten Risikomanagements auch muss die risikoorientierte Konzentration auf das Wesentliche genügen, welche bei jedem Institut entsprechend dem konkreten Geschäftsmodell unterschiedlich sein kann (Rz 117; vgl. oben Ziff. II.4.4). Der Wortlaut ist anzupassen.

6.5. (Auch) bei **lit. b und c von Rz 135.1** sind die bewährten **Prinzipien des generellen Risikomanagements** anwendbar. Nur schon aus Gründen allgemeiner Kohärenz müssen dieselben Verfahren und Methoden wie in allen andern Bereichen (ausserhalb der IT) zur Anwendung gelangen. Diese beiden lit. sind demzufolge zu streichen od. mit Bezug auf die Formulierung anzupassen.

6.6. **Zu Rz 135.2**: Nach unserem Verständnis (vgl. oben Ziff. 6.2) **muss** das IT-Risikomanagement-Konzept auch die Cyber-Risiken mitenthalten. Demzufolge ist FN 16 dahingehend anzupassen („Die Cyber-Risiken sind Bestandteil des IT-Risikomanagement-Konzepts").

6.7. Zudem sind (auch) bei Cyber-Risiken dieselben bewährten **Grundsätze des generellen Riskiomanagements** und dementsprechend dieselben Verfahren und Methoden wie in allen andern Bereichen anwendbar (vgl. oben Ziff. 6.5). Die Detailregelungen gemäss lit. a-e sind demzufolge ersatzlos zu streichen od. mit Bezug auf die Formulierung anzupassen.

6.8. **Zu Rz 135.3**: Die „Sicherstellung eines angemessenen Schutzes" verlangt bereits implizite, dass dies durch **qualifizierte Personen mit entsprechenden Hilfsmitteln** zu erfolgen hat. Eine beaufsichtigte Bank hat jederzeit **Gewähr für einwandfreie Geschäftsführung** und eine **optimale Organisation** zu bieten (vgl. Art. 3 Abs. 2 lit. a u. c BankG). Zur Organisation gehört auch Auswahl, Einsatz und und laufende Aus- und Weiterbildung von persönlich integren und fachlich kompeteten Angestellten (sog. **„Fit- and Proper-Rule"**). Bei dieser Sachlage ist nicht einsehbar, weshalb in diesem Bereich eine Pflicht zum Beizug von „geeigneten externen Dienstleistern" bestehen soll. Eine beaufsichtigte Bank muss in der Lage sein, solche Pflichten mit eigenem Personal zu erfüllen. Der letzte Satz von Rz 135.3 ist deshalb **ersatzlos zu streichen**.

7. Bemerkungen zum Grundsatz 5 BCM und TBTF (Rz 136.1/136.2)

7.1. Die **gesetzlichen Bestimmungen** zur Systemrelevanz (‚Too-big-to-fail', TBTF) leiten sich aus **Art. 8 f. BankG** ab. Die Bestimmungen zur Sicherstellung systemrelevanter Funktionen werden auf Verordnungsstufe in **Art. 60 ff. BankV** konkretisiert. TBTF-Bestimmungen auf Stufe FINMA-Rundschreiben müssen sich jedenfalls innerhalb des von BankG und BankV gesetzten Rahmens bewegen.

7.2. Die Regelung von Rz 136.1 ist gemäss unserer Ansicht **weder formal noch inhaltlich** eine **konsistente Umsetzung von TBTF**. Formal verwendet Rz 136.1 andere Begrifflichkeiten als die Bankengesetzgebung (z.B. „kritische Funktion" und „kritische Dienstleistung"). Diese neuen Begriffe werden nicht definiert und stehen auch in keinem erkennbaren Zusammenhang mit systemrelevanten Funktionen. Wenn schon wären **Systematik und Begriffe an die geltende Bankengesetzgebung anzupassen**. Zu überlegen ist, ob die TBTF überhaupt in diesem Rundschreiben geregelt werden soll.

7.3. Inhaltlich legt Rz 136.1 eine **sachliche Nähe von BCM zur Sicherstellung systemrelevanter Funktionen** nahe, welche **nicht gegeben** ist. Die Sicherstellung systemrelevanter Funktionen im **TBTF-Kontext orientiert sich allein am Thema der drohenden Insolvenz (PONV)**, welches gemäss Art. 25 BankG Auslöser für einen Notfall unter TBTF ist. Demgegenüber **setzt BCM bereits deutlich früher ein** und kennt das PONV-Konzept nicht. Die kritischen Geschäftsprozesse gemäss BCM sind zudem weitgehend anders definiert als die systemrelevanten Funktionen. Damit ist der Begriff des Business Contingency Plan im BCM ein anderer als der TBTF-Notfallplan.

7.4. Zusammenfassend ist die im Entwurf vorgeschlagene kombinierte Regelung der Themen **BCM** und **TBTF/Insolvenz** in den Rz 136.1 und 136.2 unglücklich herausgekommen. Wir empfehlen stattdessen, im Sinne **prinzipienorientierter Regulierung** (vgl. Rz 117) die Rz 136.1 und 136.2 in eine **gemeinsame neue Rz 137** mit folgendem Wortlaut zusammen zu fassen (und damit die Regelung gemäss Entwurf massiv zu vereinfachen):

„Systemrelevante Banken berücksichtigen im Rahmen ihrer Notfallplanung (Art. 9 Abs. 2 lit. d BankG i.V.m. Art. 60 ff. BankV) auch operationelle Risiken. Dabei zeigen sie auf, welche dieser zur Insolvenzgefahr nach Art. 25 BankG führen können und inwieweit sie für die Weiterführung systemrelevanter Funktionen kritisch sind."

7.5. Der Klarheit und besseren Uebersichtlichkeit willen ist diesfalls folgerichtig die Regelung zu den Risiken bei grenzüberschreitenden Dienstleistungen (Rz 136.4), sofern sie überhaupt als nötig erachtet wird (vgl. dazu unten Ziff. 8) neu als Rz 138 zu führen.

7.6. Für den **Eventualfall**, dass die FINMA vorstehenden Vorschlägen wider Erwarten nicht folgen will, sind nachfolgend in Ziff. 7.7/8 aufgeführten **Eckpfeiler** zu beachten:

7.7. Bei der Pflicht systemrelevanter Banken, geeignete Massnahmen im Rahmen der Notfallplanung vorzukehren, sollen gemäss **Rz 136.2** auch international anerkannte Standards berücksichtigt werden. Diese Formulierung ist in zweifacher Hinsicht unklar. Zum einen ist in der Rechtspraxis regelmässig **unklar, ob ein bestimmter Standard tatsächlich „international anerkannt"** ist oder eben gerade nicht. Diesen Begriff unkommentiert stehen zu lassen würde erhebliche **Rechtsunsicherheit** produzieren. Als „anerkannt" kann eine Regelung zum Vornherein nur dann gelten, wenn sie einen breit abgestützten Konsens findet, und zwar weit über den Rechtskreis hinaus, für welchen die Regelung ohnehin Geltung beansprucht. Vor diesem Hintergrund darf z.B. nicht jede EU-weite Regelung auch gleich als „anerkannter internationaler Standard" gelten. Zum andern sollten international anerkannte Standards sachlogisch jedenfalls nur soweit anwendbar sein, wie dies tatsächlich ihrem **Anwendungsbereich** entspricht. Es gibt z.B. Standards, welche sich ausdrücklich nur auf grenzüberschreitende Sachverhalte beziehen. Für eine bloss „domestic" systemrelevante Bank wie die Zürcher Kantonalbank ist die dahingehende **Präzisierung der Formulierung in Rz 136.2** besonders wichtig.

7.8. Ueberdies bleibt teilweise unklar, welches der genaue **Anwendungsbereich einer bestimmten Regelung** sein soll. Bezieht sich z.B. die Formulierung „hierfür" in Rz 136.2 Absatz 1 nur auf Rz 136.1 oder auch auf Rz 136? Aus Gründen von Klarheit und Verständlichkeit schlagen wir vor, die Regelung von Rz 136.2 **je Thema in einer eigenen Randziffer** zu regeln (z.B. BCM in Rz 136, TBTF/Insolvenz in Rz 137 und folgerichtig die Risiken bei grenzüberschreitenden Finanzdienstleistungen, soweit überhaupt nötig, in Rz 138). Ueberdies ist ausdrücklich **klarzustellen, dass sich Rz 136.2 nur auf Rz 136.1 bezieht**.

8. Bemerkungen zum Grundsatz 6 Risiken bei grenzüberschreitendem Geschäft (Rz 136.4)

8.1. Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft sind solche, welche sich aus **Regelverstössen** ergeben. Solche Risiken stellen selbst bei Zugrundelegung der gemäss FINMA-Entwurf (Rz 2) sehr offenen Umschreibung der operationellen Risiken gemäss altbewährtem FINMA-RS 2008/24, Rz 98, klassische Erscheinungsformen von **Compliance-Risiken** dar (vgl. oben Ziff. 1.3). Dies steht in Einklang mit den **Anforderungen des Basler Ausschusses** (vgl. BCBS Compliance and the Compliance Function in Banks vom 29. April 2005, Einleitung, Ziff. 3). Mit dieser Regelung würde deshalb der **Anwendungsbereich von operationellen Risiken zu Unrecht massiv ausgedehnt**.

8.2. Die FINMA-Aeusserungen aus dem Jahre 2010, welche Grundlage für den heutigen Regulierungsentwurf sind, wiesen als blosses **Positionspapier von Oktober 2010** lediglich eine formell nicht vorgesehene Erlassform auf und waren demzufolge rein formell als unverbindliche Meinungsäusserung der FINMA zu qualifizieren. Dieses FINMA-Positionspapier enthielt indessen detaillierte Ausführungen, welche trotz der informellen Erlassform in der Praxis Beachtung fanden und sich bewährt haben. Demgegenüber wird die Kurzdarstellung in Rz 136.4 den **komplexen Herausforderungen und Risiken des grenzüberschreitenden Geschäfts** nicht gerecht. Demzufolge wird diese Regelung in der Praxis wenig hilfreich sein und höchstens noch zu Missverständnissen und falschen Schlüssen führen.

8.3. Die breite Thematik ist auch **nicht auf rein aufsichtsrechtlichen Regulierungsbereich beschränkt**. Mit Ueberführung in ein formelles **FINMA-Rundschreiben** würde sich die FINMA demzufolge dem Vorwurf aussetzen, hier ohne ausreichende gesetzliche Grundlage zu regulieren.

8.4. Aus all diesen Gründen empfehlen wir, **Rz 136.4 ersatzlos zu streichen** und stattdessen das **Positionspapier von Oktober 2010 beizubehalten**.

8.5. Selbst wenn fälschlicherweise von operationellen Risiken ausgegangen würde, wäre die Regelung jedenfalls unvollständig, da sie nur den **engen Fokus auf das Verhältnis des Instituts zum Kunden** als Person legt. Dieses Verhältnis ist indessen mehrdimensional. Neben den relevanten **Aspekten zum Kunden** (wie z.B. Domizil, Steuerstatus, Anlegerstatus, etc.) müssten überdies mindestens noch folgende drei **weiteren Dimensionen** vorgängig abgeklärt werden:

(a) **Spezifische Aspekte der Anlagezielmärkte**, z.B. mit Bezug auf allfällige Lizenzpflichten, Offenlegungspflichten, etc.;

(b) **Produkte- bzw. Dienstleistungsspezifische Aspekte**, z.B. Zugangsrestriktionen, Lock up-Klauseln, Nachschusspflichten, Segregierungspflichten, etc.; und

(c) **Transaktionsspezifische Aspekte (inkl. Finanzmarkinfrastruktur-Aspekte)**, z.B. börsenrechtliche Lizenz-, Offenlegungs- und Meldepflichten vor Ort, etc.

Daraus ergibt sich, dass der Begriff **„grenzüberschreitendes Dienstleistungsgeschäft" auch Kunden mit Domizil Schweiz erfasst**, z.B. einen Kunden mit Domizil Schweiz, für welchen das Institut japanische Government Bonds kaufen soll (was u.a. erst nach Vorliegen einer japanischen Lizenz zulässig ist).

8.6. Schlicht **falsch** ist die Aussage am Ende von Rz 136.4, **externe Vermögensverwalter** seien **Beauftragte der Bank**. Vielmehr handelt es sich um **Kunden** der Bank, welche mit Blick auf ihr spezifisches Geschäftsmodell (mit eigenen Endkunden) besondere Dienstleistungen der Bank in Anspruch nehmen. Die Bank hat auf dieses Geschäftsmodell adaptierte besonderen **Anforderungen und Prozesse** zu implementieren, welche geeignet sind, die Risiken bei Geschäftstätigkeit mit externen Vermögensverwaltern angemessen zu steuern. Dazu gehört, dass die Bank nur solche externen Vermögensverwalter als Kunden akzeptiert, welche die von der Bank gesetzten **Anforderungen an guten Ruf und Fachkompetenz erfüllen**. Eine eigentliche **Schulungspflicht ist daraus keinesfalls abzuleiten**. Dies wäre schon deshalb verfehlt, weil die Endkunden eines externen Vermögensverwalters freiwillig diesen und nicht eine Bank als Finanzdienstleister gewählt haben. Es wäre wirtschaftlich eine verkehrte Welt, die Banken zu verpflichten, durch **unentgeltlichen aktiven Zusatzaufwand** die Qualität der externen Vermögensverwalter anzuheben und damit deren **Attraktivität für die Endkunden zu Lasten der Banken zu erhöhen**. Vielmehr wird die Bank mit externen Vermögensverwaltern, welche die von der Bank gesetzten Anforderungen nicht erfüllen, keine Geschäftsbeziehungen eröffnen. Für den Even-

tualfall, dass Rz 136.4 wider Erwarten nicht ersatzlos gestrichen wird, ist demzufolge auch die Regelung bezüglich externen Vermögensverwaltern im Sinne der Ausführungen anzupassen.

Diese Thematik wird durch das pendente **Gesetzgebungsprojekt FIDLEG/FINIG** in absehbarer Zeit ohnehin entschärft. Demgemäss werden externe Vermögensverwalter dem **Grundprinzip ‚Same Business Same Rules'** folgend sowohl am **‚Point of Sale'** (mit FIDLEG) als auch mit Bezug auf **aufsichtsrechtliche Bewilligungsanforderungen** (mit FINIG) **gleich langen Spiessen** unterstellt, wie sie für alle andern bisher bereits beaufsichtigten Finanzdienstleister heute schon gelten. Auf der Basis gleich langer Spiesse wird sich mit Bezug auf das Kundensegment externe Vermögensverwalter eine **Schulungspflicht der Banken umso weniger** ableiten lassen (vgl. Werner Wyss, in: René Bösch/ François Rayroux/Christoph Winzeler/Eric Stupp (Hrsg.), Basler Kommentar KAG, 2. A., Basel 2016, Art. 10 KAG N 144h ff.).

9. Bemerkungen zu Anhang 3 Rz 35

Diese Regelung stellt entgegen dem Erläuterungsbericht keine geringfügige Anpassung dar, sondern vielmehr eine **massive Verschärfung der Sicherheitsvorgaben für Massen-CID**. Die Folge davon wären enorme finanzielle und anderweitige Aufwendungen. Eine überzeugende Begründung dafür findet sich weder im Erläuterungsbericht noch an anderer Stelle. Folgerichtig ist der **2. Satz von Anhang 3 Rz 35** („Dabei sind einzelne Transaktionen bzw. Zugriffe den einzelnen Benutzern zuzuordnen") **ersatzlos zu streichen**.

IV. Zur Anpassung des FINMA-RS 2010/1 Vergütungssysteme

1. Bemerkungen zu Rz 6/7

1.1. Wir begrüssen den Ansatz, dass künftig nur noch die grössten Finanzdienstleister diesem Rundschreiben unterstehen sollen. Das Kriterium, auf die regulatorisch geforderten Eigenmittel abzustellen und dabei für Banken und weitere Finanzdienstleister (ausgenommen Versicherungen) gemäss neuer Rz 6 die **Grenze bei CHF 10 Mia.** festzulegen, erscheint uns sinnvoll.

1.2. Wir nehmen zur Kenntnis, dass uns die Herren Dr. Thomas Bauer, Verwaltungsratspräsident, und Mark Branson, Direktor, anlässlich des kürzlichen High Level-Meetings vom 16. März 2016 in Bern bestätigt haben, dass die Zürcher Kantonalbank diesem Rundschreiben trotz der Möglichkeit gemäss Rz 9 künftig nicht mehr unterstehen wird.

2. Bemerkungen zu Rz 20

2.1. Die bisherige Regelung von Rz 20, wonach das Oberleitungsorgan die **Vergütungen der Geschäftsleitung**, sowie den **Gesamtpool für das Finanzinstitut** genehmigt, entspricht bewährter und etablierter ‚good' Governance. Im Kern handelt es sich dabei um unentziehbare Aufgaben des Oberleitungsorgans in Zusammenhang mit Oberleitung, Organisation und Festlegung von Regeln zur Befol-

gung von Gesetzes und internen Vorschriften (vgl. Art. 716a Abs. 1 Ziff. 1, 2 u. 5 OR; für die Zürcher Kantonalbank § 15 Abs. 3 Ziff. 1 u. 2 ZKB-Gesetz). Demgemäss kann diese Kompetenz auch nicht delegiert werden, z.B. an einen Ausschuss des Oberleitungsorgans (vgl. oben Ziff. II.8.2).

2.2. Dass dies **jährlich** geschehen soll, ist sachlogisch nachvollziehbar, zumal variable Vergütungsteile je nach Geschäftsergebnis des Finanzinstituts und persönlicher Leistung des konkreten Mitarbeitenden **von Jahr zu Jahr erheblich variieren** können. Unter **arbeitsrechtlichen Aspekten** ist dies nicht nur hilfreich, sondern sogar nötig. Das Prozedere der jährlichen Genehmigung ist ein wichtiger Beleg für die Würdigung der im betreffenden Geschäftsjahr relevanten **konkreten Verhältnisse**, insbesondere der individuellen Leistungskomponente des betroffenen Mitarbeitenden. Dieses Verfahren unterstützt somit erheblich die rechtlich durchsetzbare Begründung für die Qualifikation der variablen Vergütung als **freiwilligen Bonus (Gratifikation)**.

2.3. Nicht einzusehen ist demgegenüber, weshalb auch die Vergütungen der **„Leiter der Kontrollfunktionen"** jährlich vom Verwaltungsrat genehmigt werden sollen.

2.4. Zum einen legt das Rundschreiben selbst ausreichend klar die relevanten **Eckpfeiler** für eine angemessene Gesamtvergütung ohne falsche Anreize fest (vgl. insb. Rz 57 ff.). Auch die „Leiter der Kontrollfunktionen" sind aber im Uebrigen in die **unternehmensweite Organisation, Struktur der Personalprozesse und Vergütungspolitik** des Finanzinstituts eingebunden. Davon losgelöste individuelle Entscheide mit Bezug auf die „Leiter der Kontrollfunktionen" könnten zu sachlich nicht gerechtfertigten **Verzerrungen** in die eine oder andere Richtung führen. Im Extremfall könnte z.B. die Gesamtvergütung eines „Leiters" ohne sachlichen Grund tiefer ausfallen als die Gesamtvergütung einzelner seiner ihm unterstellten Mitarbeitenden. Solche Resultate sind selbstredend zu verhindern.

2.5. Zum andern bleibt mit dem **offenen Begriff „Leiter der Kontrollfunktionen"** trotz Rz 58 unklar, welche konkreten Mitarbeitenden von dieser Regelung erfasst sein sollen, zumal mit Bezug auf die Risikoorganisation **von Finanzinstitut zu Finanzinstitut sehr grosse Unterschiede** bestehen. Sind nur die höchsten Leiter gemeint, z.B. der CRO, oder sind es auch die ihm unterstellten Leiter von Teilbereichen, z.B. die Leiter Market Risk, Operational Risk, etc.? (vgl. oben Ziff. II.8.4). Sind bei Instituten mit getrennten Bereichen Compliance und Legal beide Leiter erfasst? Solche und andere Fragen würden im praktischen Alltag zu grosser Unsicherheit führen. Eine abschliessende Aufzählung sämtlicher „Leiter der Kontrollfunktionen" ist mit Blick auf die von Institut zu Institut unterschiedlichen Organisationsformen weder möglich noch zielführend. Besser ist es, diese Funktionen generell **von der Regel von Rz 20 auszunehmen** und demzufolge gar nicht zu erwähnen.

2.6. Die **Festlegung konkreter Vergütungen** ist überdies eine **operative Tätigkeit**, während sich der Verwaltungsrat auf die Festlegung der generellen Vergütungspolitik und gestützt darauf auf generischen Vorgaben (in Form von Reglementen) zu beschränken hat (vgl. Rz 17-19; oben Ziff. II.5.4 u. II.6.1). Im Falle der **Mitglieder der Geschäftsleitung** ergibt sich die Kompetenz des Verwaltungsrats als **Ausnahme von der Regel** aufgrund der hierarchischen Stufe.

2.7. Wir empfehlen deshalb, die **„Vergütungen der Leiter der Kontrollfunktionen"** von der jährlichen Genehmigung durch den Verwaltungsrat und damit **vom Anwendungsbereich von Rz 20 auszunehmen**.

3. Bemerkungen zu Rz 21

3.1. Wir lesen diese Regelung so, dass der **Entschädigungsausschuss** per definitionem aus dem Kreis der Verwaltungsräte zu besetzen ist. Demzufolge dürfen an die Mitglieder des Entschädigungsausschusses keine höheren Anforderungen an die Unabhängigkeit und Fachkunde gestellt werden. Im Gegenteil muss es genügen, wenn das **Ausschussmitglied die Unabhängigkeitsanforderung auf Stufe Oberleitungsorgan erfüllt**, weil beim Einsitz in einen Ausschuss primär die **Ausschuss-spezifische Fachkompetenz entscheidend** ist und andernfalls die Ausschüsse unter Einhaltung der 1/3-Regelung kaum mehr vernünftig besetzt werden könnten (vgl. Entwurf FINMA-RS 2016/xx Corporate Governance - Banken, Rz 18 ff. und unsere Ausführungen dazu oben Ziff. II.5.11 u. insb. II.5.16).

3.2. Analog zu den Prüf- und Risiko- (Management-) Ausschüssen (vgl. oben Ziff. II.5.15) ist es beim Entschädigungsausschuss angemessen, in Anwendung des Proportionalitätsprinzips bereits die **Kategorie 3 auszunehmen**.

4. Bemerkungen zu Rz 46

4.1. Am ersten Satz dieser geänderten Randziffer ist nichts zu beanstanden.

4.2. Der Zusatz **„Malus"** kann zu unnötiger Verwirrung führen. In diesem sensiblen Bereich der Behandlung von Vergütungsregeln werden von Institut zu Institut **höchst unterschiedliche Formulierungen** verwendet. Demgemäss hat auch der Begriff „Malus" bei verschiedenen Instituten unterschiedliche Bedeutung. Er wird teilweise z.B. eingeschränkt bloss auf den Wegfall aufgeschobener, aber noch nicht definitiv zugeteilter variabler Vergütungsteile verwendet. Diesen Begriff am Schluss des 1. Satzes in Klammer anzufügen ist aber gar nicht nötig, da der **Satz aus sich selbst heraus verständlich** ist. Wir empfehlen, den in Klammern gesetzten Begriff **„Malus" ersatzlos zu streichen**.

4.3. Der zweite Satz (‚Clawbacks') ist demgegenüber **arbeitsrechtlich nicht durchsetzbar**. Die FINMA selbst hat bereits in Zusammenhang mit Erlass von FINMA-RS 2010/1 Vergütungssysteme 2009 das **Spannungsfeld** zwischen aufsichtsrechtlich wünschenswerten Massnahmen und zwingenden Regeln gemäss Schweizerischem **Arbeitsrecht** erkannt, mit Bezug auf die Möglichkeit des Aufschubs von Teilen der Gesamtvergütung gesetzgeberischen Handlungsbedarf im Schweizer Arbeitsrecht geortet und entsprechend Anpassungen im OR gefordert (vgl. FINMA-Erläuterungsbericht Rundschreiben Vergütungssysteme vom 3. Juni 2009, insb. Ziff. 3.2 S. 27 ff.). Neben den von der FINMA in diesem Erläuterungsbericht bereits analysierten Aspekten sind darüber hinaus nach Schweizerischem Arbeitsrecht insbesondere auch alle Arten von arbeitsrechtlichen Vergütungen grundsätzlich am Ende des Monats, spätestens mit Beendigung des Arbeitsverhältnisses und im Falle von Beteiligungen am Geschäftsergebnis allerspätestens 6 Monate nach Ablauf des Geschäftsjahres fällig (Art. 323 Abs. 1 u. 3 u. Art. 339 Abs. 1 OR; vgl. statt Vieler Ullin Streiff/Adrian von Kaenel/Roger Rudolph, Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7. A., Zürich 2012, Art. 323 OR N 2 ff., Art. 339 OR N 2 ff.). Der Schweizerische Gesetzgeber ist seither zu diesem Thema **nicht** tätig geworden. Somit bestehen heute wie bisher auch weiterhin **erhebliche Risiken**, dass sich bereits jede Art von Aufschub von arbeitsrechtlich begründeten Vergütungen im Streitfall vor Gericht nicht durchsetzen lässt.

4.4. Nur am Rande sei erwähnt, dass sich die Rechtslage im **Steuerrecht analog** darstellt. Ein aufsichtsrechtlich motivierter Aufschub von Teilen der Gesamtentschädigung führt höchstens dann nicht zur so-

fortigen Steuerpflicht, wenn zweifelsfrei (a) noch kein durchsetzbarer Anspruch, sondern erst eine Anwartschaft vorliegt, (b) die Umwandlung der Anwartschaft in einen durchsetzbaren Anspruch von zukünftigen nicht völlig unwahrscheinlichen Ereignissen abhängt und (c) das Ausbleiben oder der Eintritt solcher Ereignisse nicht vom Anwartschaftsbegünstigten beeinflusst werden kann. Erschwerend kommt dazu, dass im Steuerrecht der Natur der Sache nach sogar **von Kanton zu Kanton unterschiedliche Regelungen** bestehen. Ueberdies hat der betroffene Mitarbeiter für bereits ausbezahlte Vergütungen selbstverständlich bereits Steuern bezahlt. In Zusammenhang mit der allfälligen Rückzahlung solcher Vergütungsteile an den Arbeitgeber bei Vollzug von ‚Clawback'-Regelungen stellen sich deshalb auch hochkomplexe Fragen der angemessenen **Berücksichtigung der Steuerfolgen**. Auch all dies hat die FINMA bereits in Zusammenhang mit Erlass von FINMA-RS 2010/1 Vergütungssysteme erkannt und vom Gesetzgeber Klärung der Rechtslage gefordert (vgl. FINMA-Erläuterungsbericht Rundschreiben Vergütungssysteme vom 3. Juni 2009, insb. Ziff. 3.3 S. 29 ff.). Auch hier ist seither der Gesetzgeber **nicht** tätig geworden.

4.5. Ist nur schon der aufsichtsrechtlich motivierte Aufschub von Teilen der Vergütung über die Beendigung des Arbeitsverhältnisses hinaus mit Bezug auf die rechtliche Durchsetzbarkeit erheblich in Frage gestellt, trifft dies **umso mehr** auf das Recht des Arbeitgebers zu, bereits an den Mitarbeitenden ausbezahlte Vergütungsteile nachträglich wieder zurückzufordern. Neben den **ganz erheblichen rechtlichen Risiken** (vgl. vorstehend Ziff. 4.3 f.) kommen bei dieser Konstellation noch **hohe wirtschaftliche Risiken** dazu, dass nämlich der betreffende (ehemalige) Mitarbeitende den geschuldeten Betrag bereits konsumiert oder in wenig liquide Werte investiert hat.

4.6. Gleichwohl sollen nun aber gemäss neuer Rz 46 ‚Clawback'-Regelungen aufsichtsrechtliche Pflicht werden. Eine rechtlich nicht durchsetzbare Regelung darf nur schon deshalb nicht zur Pflichtregelung erklärt werden, weil die **Nichtdurchsetzbarkeit der Pflicht** bei den Mitarbeitenden **falsche Signale und Anreize** setzt. Solches gilt es im Gegenteil zu vermeiden (vgl. Rz 51).

4.7. Sollte die FINMA wider Erwarten an der Pflicht zu ‚Clawback'-Regelungen festhalten, müsste sie gleichzeitig noch klarere **Regeln für die Umsetzung** bereitstellen. Wichtig wäre beispielsweise zu wissen, ob für die „grundsätzliche" Möglichkeit der Rückforderung auch eine zeitlich beschränkte Regelung (sichergestellt z.B. mittels zweijähriger Option) genügt oder wie sich „Malus" und ‚Clawback' gegenseitig ausschliessen und/oder ergänzen sollen. Sodann brauchen die Institute diesfalls eine **grosszügige Uebergangsfrist** für die rechtsgültige arbeitsvertragliche Implementierung. Bei wichtigen Aenderungen dieser Tragweite muss den Mitarbeitenden die eindeutig und detailliert formulierte Regelung vorgängig zugestellt werden und jeder Mitarbeitende muss bei Nichteinverständnis Gelegenheit haben, vor Inkrafttreten der neuen Regelung unter **Einhaltung der vereinbarten Kündigungsfrist** das Arbeitsverhältnis durch Kündigung zu beenden (statt Vieler Ullin Streiff/Adrian von Kaenel/Roger Rudolph, a.a.O., Art. 320 OR N 2 ff.). Bei manchen Instituten beträgt die vereinbarte Kündigungsfrist für verschiedene Segmente von Mitarbeitenden 6 Monate. Vor Zustellung der geänderten Regelung an die Mitarbeitenden müsste diese, zusammen mit weiteren allfälligen Aenderungen sorgfältig koordiniert mit der bestehenden Regelungsarchitektur, ausformuliert und von sämtlichen Kompetenzträgern bis hin zu den obersten internen Gremien eines jeden Instituts verabschiedet werden. Bei Konzernstrukturen müsste die Umsetzung in der Folge noch mehrstufig in sämtlichen Konzernteilen erfolgen, wobei in jedem Einzelfall noch allfälliges entgegenstehendes zwingendes Recht vor Ort zu berücksichtigen wäre (vgl. Rz 5). Die **Uebergangsfrist** müsste deshalb wesentlich länger als die Kündigungsfrist sein, mithin sicher **2 Jahre**.

4.8. Generell sind zusätzliche Hinweise für die **intertemporale Umsetzung** nötig, z.B. zur Frage der Behandlung von Fällen, bei welchen es um die Beurteilung von Fehlverhalten vor der Aenderung des Rundschreibens geht, das erst nach der Aenderung entdeckt wird.

5. Bemerkungen zu Rz 52

5.1. Die Pflicht zum Aufschub eines Teils der Gesamtvergütung i.S.v. Rz 49 ist Ausfluss der Ratio, den aufgeschobenen Teil der Vergütung auch dann zurückbehalten zu können, wenn im Verantwortungsbereich eines Mitarbeitenden Verluste erwirtschaftet werden, nachdem dieser verantwortliche Mitarbeitende das Unternehmen bereits verlassen hat (Rz 55). Im dynamischen Finanzbereich zeigt die Erfahrung, dass sich Verluste dieser Art bereits innert **2 Jahren** materialisieren und erkannt werden. Zudem ist jede Art von Aufschub von **arbeitsrechtlich** begründeten Entschädigungen mit dem erheblichen Risiko behaftet, dass sich dies im Streitfall vor Gericht arbeitsrechtlich **nicht durchsetzen** lässt. Dieses **Risiko nimmt mit zunehmender Länge der Aufschubfrist stetig zu**. Die FINMA selbst hat das **Spannungsfeld** zwischen aufsichtsrechtlich wünschenswertem Aufschub von Teilen der Gesamtvergütung und zwingenden Regeln des Schweizerischen Arbeits- und Steuerrechts bereits in Zusammenhang mit Erlass von FINMA-RS 2010/1 Vergütungssysteme 2009 erkannt, gesetzgeberischen Handlungsbedarf im Schweizer Arbeitsrecht geortet und entsprechend gesetzliche Anpassungen gefordert. Der Schweizerische Gesetzgeber ist aber seither **nicht** tätig geworden (vgl. oben Ziff. 4.3 f.). Eine dreijährige Frist ist somit weder sinnvoll noch nötig und im Gegenteil kontraproduktiv. Demgegenüber erhöht eine bloss zweijährige Frist die Chancen, dass ein Arbeitgeber die mit den Mitarbeitenden vereinbarten Regelungen im Streitfall vor Gericht tatsächlich auch erfolgreich durchsetzen kann. Wir empfehlen deshalb, für die Frist zum Aufschub als **Minimalstandard zwei Jahre** festzulegen.

5.2. Selbstverständlich soll jedes Institut **nach freiem Ermessen** berechtigt sein, mit Blick auf die konkreten Verhältnisse, insbesondere gewählte Geschäftsstrategie und Risikopolitik i.S.v. Rz 51, gleichwohl **längere Fristen** von 3 oder mehr Jahren vorzusehen.

Für allfällige Rückfragen und für ein persönliches Gespräch stehen Ihnen die Unterzeichneten jederzeit gerne zur Verfügung.

Freundliche Grüsse
Zürcher Kantonalbank

Prof. Dr. Othmar Strasser
General Counsel

RA lic.iur Werner Wyss, M.B.L.-HSG
Head Regulatory Affairs