ASSOCIATION DES BANQUIERS PRIVÉS SUISSES

VEREINIGUNG SCHWEIZERISCHER PRIVATBANKIERS

SWISS PRIVATE BANKERS ASSOCIATION

Par e-mail et par courrier

Autorité fédérale de surveillance des
marchés financiers (FINMA)
Alessandro Lana
Einsteinstrasse 2
3003 Bern

Genève, le 25 juin 2013

Circ.-FINMA 2008/21 « Risques opérationnels - banque » - révision partielle

Monsieur,

Nous nous référons aux documents relatifs à l'audition susmentionnée, publiés en date du 23 mai 2013 par votre Autorité.

Après analyse des modifications proposées, l'Association des Banquiers Privés Suisses (ABPS) renonce à établir une détermination spécifique, car elle se rallie entièrement aux propositions et aux conclusions qui seront exprimées par la prise de position de l'Association suisse des banquiers (ASB).

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

ASSOCIATION DES BANQUIERS
PRIVES SUISSES
Le Secrétaire général:

Michel Y. Dérobert

Copie : M. Claude-Alain Margelisch, ASB

12, RUE DU GÉNÉRAL-DUFOUR, CASE POSTALE 5639, CH-1211 GENÈVE 11, TÉL +41 (0)22 807 08 04, FAX +41 (0)22 320 12 89

Email: info@swissprivatebankers.com www.swissprivatebankers.com

CREDIT SUISSE

Eidgenössische Finanzmarktaufsicht FINMA
Herrn Alessandro Lana
Geschäftsbereich Risikomanagement
Einsteinstrasse 2

3003 Bern

Zürich, 28. Juni 2013

FINMA-RS 2008/21 „Operationelle Risiken Banken" – Teilrevision

Sehr geehrter Herr Lana

Wir beziehen uns auf die Anhörung zur Teilrevision des FINMA Rundschreibens 2008/21 „Operationelle Risiken Banken" und bedanken uns für die Möglichkeit, Ihnen unsere Stellungnahme einreichen zu können.

Unsere Stellungnahme gliedern wir in die beiden überarbeiteten Kernbereiche des Rundschreibens, d.h. 1) Kapitel IV. „Qualitative Anforderungen" und 2) Anhang 3 „Umgang mit elektronischen Kundendaten".

1) Kapitel IV. Qualitative Anforderungen

Grundsätzliches

Wir unterstützen das Vorhaben der FINMA, die „Principles for the Sound Management of Operational Risk" des Basel Committee on Banking Supervision (BCBS) in das oben genannte Rundschreiben aufzunehmen.

Ferner begrüssen wir die neuen bzw. überarbeiteten Vorgaben, würden jedoch bei einzelnen Randziffern Konkretisierungen empfehlen, um spätere Missverständnisse sowohl bei Banken als auch bei Prüfgesellschaften zu vermeiden.

Bemerkungen zu den Bestimmungen

- **Randziffer 116**

  Gemäss dieser Randziffer dürfen die Mindesteigenmittelanforderungen für Banken, die operationelle Risiken nach dem AMA unterlegen, nicht tiefer als 80% jener Anforderungen betragen, welche die Bank theoretisch unter dem Mindeststandard von Basel I gehabt hätte. Eine Berechnung nach Basel I ist nicht möglich, weil wir diese seit 1. Januar 2011 nicht mehr durchführen. Wir empfehlen daher, diese Randziffer zu streichen.

CREDIT SUISSE

- **Randziffer 120/124**

  Wir empfehlen, die Verantwortlichkeit für die Bewilligung des Rahmenkonzeptes für das Management von operationellen Risiken anstelle des Verwaltungsrats der Geschäftsleitung zuzuweisen. Der Verwaltungsrat sollte für die Festlegung von Risikobereitschaft und Risikotoleranz zuständig sein. Basierend auf diesen Parametern ist es die Aufgabe der Geschäftsleitung, das Rahmenkonzept für operationelle Risiken zu definieren.

- **Randziffer 122**

  Bei diesem Paragraphen empfehlen wir eine Präzisierung, um zu verdeutlichen, dass die Geschäftsleitung eindeutige und wirksame Verantwortlichkeiten für das Management von operationellen Risiken definiert. Des Weiteren ist eine zuständige Einheit für operationelle Risiken für die Aufrechterhaltung und die laufende Weiterentwicklung des Rahmenkonzepts für das Management von operationellen Risiken verantwortlich. [...] Konsistent zu weiteren Risikofunktionen soll eine zuständige Einheit für operationelle Risiken adäquat in relevanten Gremien vertreten sein.

  Diese Verantwortlichkeiten decken sich insbesondere mit den Paragraphen 14, 15 sowie 32 bis 36 der vom BCBS publizierten „Principles for the Sound Management of Operational Risk".

- **Randziffer 128**

  Gemäss Erläuterungsbericht der FINMA sind unter den Anforderungen zur Preisfestsetzung und Performancemessung die Verfahren zur Allokation der Eigenmittelanforderungen für operationelle Risiken auf Geschäftsbereiche zu verstehen. Wir würden vorziehen, wenn dieser Sachverhalt direkt in das Rundschreiben aufgenommen wird.

Fragenliste zur Anhörung

Das Inkrafttreten dieses Kapitels ist im Entwurf für den 1. Januar 2015 vorgesehen. Wie beurteilen Sie die Möglichkeit, das Inkrafttreten des Kapitels IV.B „Qualitative Grundanforderungen" bereits auf den 1. Juli 2014 festzusetzen?

Wir erachten ein Inkrafttreten per 1. Juli 2014 als nicht praktikabel, insbesondere im Hinblick auf nötig werdende interne Anpassungen.

2) Umgang mit elektronischen Kundendaten

Grundsätzliches

Eine Regelung betreffend Umgang mit Kundendaten wird grundsätzlich begrüsst, da wir der Meinung sind, dass die Vertraulichkeit von Kundenangaben auch in Zukunft von Bedeutung für den Schweizer Finanzplatz bleiben wird.

Nichtsdestotrotz sollte insbesondere Anhang 3 „Umgang mit elektronischen Daten" im breiteren Kontext betrachtet und das politische Umfeld und dessen Entwicklung (MiFID, FATCA, Informationsaustausch, FSB Initiative usw.) mitberücksichtigt werden. Ferner empfehlen wir Anhang 3 in einer separaten Regelung ausserhalb des Rundschreibens 2008/21 abzubilden.

Wir erachten es auch als wichtig, dass die Ziele und die generellen Anforderungen aufgezeigt werden. Wir empfehlen aber die Grundsätze allgemeiner zu halten und mehr auf risikobasierte Prinzipien abzustützen, die es in den Einzelheiten den Instituten überlässt, wie diese umgesetzt werden, denn

a. die einzelnen Finanzinstitute sind technisch und organisatorisch unterschiedlich ausgerichtet;

b. Technologien ändern sich rapide; und

CREDIT SUISSE

c. Lebenszyklen von Kundendaten sind variabel.

Insbesondere erachten wir die Kostenfolge der starr vorgegebenen und detaillierten Grundsätze als unverhältnismässig, bzw. das Aufwand-/Nutzenverhältnis erscheint uns als sehr unausgewogen.

Basierend auf diesen grundsätzlichen Vorbehalten lehnen wir den Anhang 3 in der jetzigen Form ab und empfehlen, den Anhang 3 nochmals zu hinterfragen und eine gründliche Überarbeitung mit Einschluss aller betroffenen Kreise durchzuführen. Wir stehen dazu für weitere Unterstützung gerne zur Verfügung.

Bemerkungen zu den Bestimmungen

- **Scope / Gültigkeitsbereich**

  Wie bereits in unserem Schreiben vom November 2012 ausgedrückt, wünschen wir eine sehr klare Definition des Gültigkeitsbereiches.

  Wichtig ist jedoch dabei, dass die Bank für weniger sensitive Kundengruppen (z.B. Financial Institutions, Gegenparteien, Broker, Kunden mit Waivern) nicht genau dieselben Aufwände betreiben muss; somit sollten Vereinfachungen möglich sein. Ein solcher Passus könnte z.B. lauten „Die erwähnten Grundsätze gelten für alle Kundensegmente, die konkrete Umsetzung kann aber risikobasiert erfolgen, z.B. in Abhängigkeit von Kundenart und dem Vertraulichkeitsbedürfnis."

  Die Terminologie "in oder von der Schweiz aus betreut" [...] ist zu wenig genau. Die Nennung der Buchungsplattform würde Missverständnisse vermeiden, z.B. in der Schweiz gebucht/gespeichert und betreut.

  Eine Ausweitung auf im Ausland betreute oder geführte Kundenbeziehungen lehnen wir ab, dies würde weitere Abstimmungen mit Anforderungen anderer Aufsichtsbehörden und Regulatoren (insbesondere US SEC und MAS) erfordern und somit die Komplexität in Bezug auf Zeitrahmen, Ressourcen und Kosten massiv erhöhen.

- **Bestehende Regelungen / Grundlagen**

  Da einige der formulierten Grundsätze auf bereits bestehenden Vorschriften basieren (Bankgesetz, Datenschutzbestimmungen, Bestimmungen Outsourcing Banken, etc.) empfehlen wir diese nicht weiter zu konkretisieren, sondern lediglich mittels Querverweis darauf zu referenzieren.

  Die bestehenden Bestimmungen haben teilweise bewusst auf mehr einschränkende Massnahmen verzichtet, um den unterworfenen Instituten eine flexible, auf ihre Organisation angepasste Handhabung zu gewährleisten – trotzdem werden diese Bestimmungen entsprechend eingehalten.

  Eine weitergehende Konkretisierung von Vorgaben ist a) verwirrend (was ist nun gültig und zwingend) und b) käme einer versteckten Gesetzesrevision nahe, welche auf solchem Weg nicht statthaft ist.

- **Eignung der Grundsätze**

  Neben der Gesetzeskonformität stellen wir die Eignung von detaillierten und konkreten Grundsätzen zur Erreichung der gesetzten Ziele in Frage. Eingestandenermaßen anzustreben ist ein erhöhter Schutz im Umgang mit Kundendaten. Eine 100% Sicherheit, dass solche Daten nicht zweckentfremdet werden können (absichtlich und/oder fahrlässig) lässt sich aber auch mit detaillierten Anforderungen nie erreichen.

  Um eine kunden- und institutsgerechte Umsetzung zu gewährleisten, muss ein auf die effektiven Risiken abgestützter und prinzipienbasierter Ansatz mit entsprechendem Ausgestaltungsfreiraum auf Einzelfallbasis gewählt werden.

  Manche der in den Grundsätzen verlangten Anforderungen sind zum Vornherein ungeeignet zur Zielerreichung oder nur mit enormem Aufwand umsetzbar – unter anderem:

  a. wichtigste Aktiven einer Bank sind die Kunden und entsprechend ihre Daten. Diese sind unbestritten vor unberechtigtem Zugriff zu schützen und zwar in Bezug auf Data-at-rest (Speicherung/Lagerung) sowie Data-in-motion (e-mail, etc.). Es ist jedoch eminent wichtig zu erkennen und zu beachten, dass

innerhalb einer Bank Kundendaten umfassend bearbeitet werden müssen (z.B. Front, BackOffice/Operations, Accounting/Controlling, IT). Damit sind auf allen Stufen und in vielen Bereichen sehr viele Mitarbeitende befasst, und zwar unter allen möglichen Blickwinkeln (direkte Kundenbetreuung, Verarbeitung von Kundenaufträgen, Verbuchung von Kundentransaktionen, Einfordern von Kundenformalitäten, Überwachung von Kundenbeziehungen und Kundenpositionen (Kreditüberwachung), Abwicklung von Kundenanlässen, etc.). Bei der Credit Suisse Schweiz haben ca. 75% der Mitarbeitenden in irgendeiner Form Zugriff auf Kundendaten um ihre Aufgaben erfüllen, die Kunden der CS betreuen bzw. deren Aufträge bearbeiten zu können.

b. Rz 20ff: Eine umfassende „Pseudonymisierung" oder „Anonymisierung" der Kundendaten, die ausserhalb der Schweiz gespeichert oder auf die vom Ausland aus zugegriffen werden, wie die Grundsätze dies vorsehen, würde zahlreiche im Interesse der Kunden notwendige Tätigkeiten erschweren. Soweit der Kunde seine vorherige ausdrückliche Zustimmung erteilt hat (Waiver), muss es – gerade auf Wunsch und im Interesse des Kunden – nach wie vor möglich sein, von den geforderten rechtlichen, technischen und organisatorischen Sicherheitsmassnahmen im Einzelfall abzusehen (siehe dazu auch Sektion „Scope/Geltungsbereich").

c. Der Grundsatz, dass die Bank wissen muss, wo Kundendaten gespeichert werden und von welchen Anwendungen verarbeitet werden und wo elektronisch auf sie zugegriffen werden kann (Rz 15ff), geht von einer systemtechnisch und prozessual einfachen Struktur aus, welche mittels detaillierten Vorgaben geregelt werden kann. Die über Zeit gewachsenen Infrastrukturen und Datenverwendungen sind aber sehr vielseitiger und komplexer: somit kann mit fixen Vorschriften keine erhöhte Datensicherheit erreicht werden.

d. Wir empfehlen, nicht Listen (Mitarbeiter mit Zugriffen auf CID / Applikationsinventar) zu verlangen (Rz 15ff), sondern eine rollen- und funktionsbasierte Zugriffsregelung vorzuschreiben, welche a) das need-to-know Prinzip (Reichweiten-Beschränkung, Segments-Eingrenzungen, etc.) berücksichtigen soll und b) periodische Reviews und Bewilligungen/Bestätigungen ermöglicht. Diese Formulierung würde es den Instituten erlauben, eine auf ihre Organisation und Grösse zugeschnittene Lösung zu implementieren.

e. Zuordnung einer „end-to-end" Daten-Ownership an eine zentrale Stelle (Rz 8ff) bringt für grössere Institute erhöhte Aufwände mit sich, da Kundendaten - wie vorstehend schon erwähnt - an diversen Stellen erfasst und verarbeitet werden. Eine overall-Verantwortung bläht die Organisation auf, ist kostenintensiv und bringt vor allem keine zusätzliche Sicherheit. Wir empfehlen, anstelle eines Data-Owners, die Rollen und Verantwortlichkeiten zu definieren, z.B.

   - Governance Verantwortlicher
   - Design- & Quality Verantwortliche (Business, IT, Legal)
   - Controlling (Risk)
   - Processes & Services/Accesses (Business, IT)
   - Data Management (Business, Legal, IT)

f. Risikominderungen (Rz 46ff) wie Logging, Doppelfunktionen, etc. (Rz 46ff) sollten nicht zu detailliert definiert werden, da solche Massnahmen stark von Organisation und Systemen und Prozessen abhängen. Neben den rein technischen Möglichkeiten und Kontrollen ist zu beachten, dass ein detailliertes Logging nur Sinn macht, wenn auch Ressourcen für Monitoring und Investigations eingeplant sind, d.h. ein „flächendeckendes" Logging ist nur mit beachtlichem finanziellem und personellem Aufwand realisierbar.

g. U.E. sollten keine detaillierten Vorgaben zur Meldung/Kommunikation von Vorfällen in Bezug auf die Vertraulichkeit von CID gemacht werden (Rz 49ff): a) gelten entsprechende Erwartungen für alle Arten von schwerwiegenden Vorfällen, b) sind die meisten Vorfälle in Grund und Auswirkung sehr unterschiedlich und müssen demzufolge auch nach individuellen Regeln bearbeitet werden können.

CREDIT SUISSE

h. Die weitgehenden Forderungen nach Einflussnahme bei 3. Firmen in Bezug auf Rekrutierung, Anstellung, Schulung und Überwachung (Rz 54ff) ist in der Realität aufwändig und nur schwer durchsetzbar, insbesondere in einem internationalen Umfeld.

- **Realisierbarkeit: Aufwand – Kosten – Zeit**

  Im Weiteren wünschen wir, dass den Aspekten der Machbarkeit und der Verhältnismäßigkeit (d.h. Kosten-Nutzen-Prinzip) ausreichend Rechnung getragen wird. Die Umsetzung der vorliegenden Grundsätze zum Anhang 3 würde für eine Bank wie die Credit Suisse zu sehr hohen Kosten führen und im Vergleich zum Nutzen unverhältnismässig sein. Die Implementierung wird mehrere Monate benötigen, für einzelne Anforderungen Jahre, d.h. eine Realisierung der Anforderungen per 1. Januar 2015 ist unrealistisch.

Fragenliste zur Anhörung

Wie beurteilen Sie die Möglichkeit einer Ausweitung des Anwendungsbereichs auf natürliche Personen („Privatkunden"), deren Geschäftsbeziehungen im Ausland betreut oder geführt werden?

Eine Ausweitung auf im Ausland betreute oder geführte Kundenbeziehungen lehnen wir ab – dies würde weitere Abstimmungen mit Anforderungen anderer Aufsichtsbehörden und Regulatoren (insbesondere US SEC und MAS) erfordern.

Da insbesondere bei grossen, international tätigen Banken, die technischen aber auch ablauf- und aufbauorganisatorischen Begebenheiten regional unterschiedlich sind, wären diesbezüglich länderspezifische Anpassungen und Implementationen nötig. Die obengenannten Gründe würden die Komplexität in Bezug auf Zeitrahmen, Ressourcen und Kosten exponentiell erhöhen.

Wie beurteilen Sie die Möglichkeit einer Ausweitung des Anwendungsbereichs auf juristische Personen (z.B. „Firmenkunden")

Wie vorgängig erwähnt, ist eine Differenzierung nach Sensitivität der Kundengruppen (z.B. Privat-Banking-Kunden, Retail-Kunden, Financial Institutions, Gegenparteien, Broker, Kunden mit Waivern) anzustreben, da die Bedürfnisse dieser Segmente unterschiedlich sein können. Mit einem prinzipien- bzw. risikobasierten Ansatz kann dies erreicht werden. Ein solcher Passus könnte z.B. lauten „Die erwähnten Grundsätze gelten für alle Kundensegmente, die konkrete Umsetzung kann aber risikobasiert erfolgen, z.B. in Abhängigkeit von Kundenart und dem Vertraulichkeitsbedürfnis."

Für weitere Erläuterungen und für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüssen

CREDIT SUISSE AG

Andreas Manz

Head Bank Operational Risk Oversight,
Business Continuity Management and
Technology Risk Management

Michel Ruffieux

COO General Counsel Division & Head Corporate Legal Group

Cc: FINMA, Dr. Michael Loretan, Leiter Aufsicht CS Group

Messieurs,

Nous vous remercions de bien vouloir trouver ci-après un complément à notre réponse que nous vous avons fait parvenir ce matin.

1. Chapitre IV.B « Exigences qualitatives de base »
Si cette date butoir correspond au respect de la nouvelle circulaire pour tous les nouveaux cas initiés à partir du 1er janvier 2015, cela nous semble raisonnable.
Par contre, une mise en conformité des cas existants pourrait impliquer la mise en place de changements organisationnels importants, voire des systèmes d'information en place. De plus, il faut également tenir compte de nombreux projets régulatoires déjà en cours dans la même période. Nous proposons donc d'examiner dans quelle mesure il serait possible de coordonner la date d'entrée en vigueur de l'annexe 3 avec les délais de BCBS (Basel Committee for Banking Supervision) pour la mise en place de "Principles for effective Risk data aggregation and risk reporting" qui partage un certain nombre de principes avec la nouvelle circulaire.

En vous remerciant par avance de l'attention que vous voudrez bien porter à notre prise de position.
Meilleures salutations.

Françoise Védy
Business Project Manager | GPB Change Delivery Switzerland
HSBC Private Bank (Suisse) SA, Route de Pré-Bois 6, PO Box 3580, CH-1216 Vernier
T +41 (0) 58 705 40 31 | francoise.vedy@hsbcpb.com
www.hsbcprivatebank.com
----- Forwarded by Francoise VEDY/PBRS/HSBC on 02.07.2013 15:27 -----

From: Francoise VEDY/PBRS/HSBC
To: alessandro.lana@finma.ch
Cc: Guy PHARAO/PBRS/HSBC@HSBC
Date: 02.07.2013 11:32
Subject: Audition relative à la révision partielle de la circulaire "Risques opérationnels – banques" - Réponse HSBC

Messieurs,

Nous nous référons au projet de révision de la circulaire "Risques opérationnels - banques" et vous remercions de nous avoir donné l'occasion de vous faire part de nos commentaires à son égard.

Nos commentaires sont les suivants:

Commentaire 1

B. Principe 2 : données d'identification du client (*client identifying data*, CID)
c) Responsabilité des CID
Extrait du chiffre 13: "Les unités responsables des CID (« Data Owners ») doivent assumer la surveillance de la totalité du cycle de vie des données des clients, incluant la validation des droits d'accès ainsi que la suppression et le retraitement des systèmes opérationnels et de sauvegarde"

Nous estimons que les activités mentionées ci-dessus devraient pouvoir être déléguées à des unités dotées des compétences et d'une organisation appropriée (p.ex. les services informatique, sécurité informatique, les opérations, le front office, etc).
Les responsabilités des "Data Owners" doivent ainsi pouvoir s'incrire dans le contexte plus général d'une politique de gestion des données de l'entreprise définissant les standards et principes de gestion avec des rôles et responsabilités cohérents et adaptés à la structure et la complexité de

chaque banque.

Commentaire 2

C. Principe 3 : lieu de stockage et accès aux données
b) Lieu de stockage et accès aux données depuis l'étranger
Extrait du chiffre 23: 'L'obligation d'informer le client est caduque lorsque les données disponibles hors de Suisse ne permettent pas de remonter à l'identité des clients concernés."

A cet égard, nous considérons que les techniques de pseudonymisation et anonymisation décrites sous chiffres 65 et 66 doivent être traitées de manière semblables, en particulier au chiffre 23, si le processus de pseudonymisation est conduit intégralement en Suisse et que la "table de concordance" est également conservée de manière sécurisée en Suisse. En effet, dans un tel cas de la pseudonymisation, un tiers ne dispose, sur la seule base de l'information finale, d'aucun lien logique ou algorythmique permettant, même théoriquement, de remonter à l'information initiale.
Ainsi, la dernière phrase du chiffre 66 ("En vertu de la définition... à la LPD) devrait purement et simplement être supprimée cas amenant une certaine confusion sur l'admissibilité d'autres solutions de traitement des données.

Commentaire 3

II. Glossaire
Chiffre 65: Techniques réversibles de traitement des données
Chiffre 66: Techniques irréversibles de traitement des données

Nous estimons que les techniques de traitement devrait préciser leur contexte de mise en application et leur sensibilité (soit Direct, Indirect, potentiellement Indirect). Nous proposons le système suivant:
Règle 1: Lorsque les données sont stockées et traitées en Suisse (le système d'information reste en Suisse), et les données sont seulement transférées, les deux techniques de traitement sont autorisées (voir également commentaire 2)
Règle 2 :Lorsque les données sont stockées et traitées à l'étranger (le système d'information est en dehors de Suisse),
- la nécessité d'une technique irréversible devrait être limitée aux données identifiant directement le client.
- la technique réversible (par opposition à irréversible) devrait pouvoir s'appliquer aux données qui n'identifient qu'indirectement le client
- dans le cas des données d'identification potentiellement indirecte, une technique de traitement (réversible ou pas) ne devrait s'imposer que pour autant que l'on puisse raisonnablement s'attendre à ce que leur combinaison conduise concrètement à une possible identification du client.

Commentaire 4
III. Exemple de données d'identification des clients
A : Données d'identification directe des clients
B : Données d'identification indirecte des clients
C : Données d'identification potentiellement indirecte des clients

Nous considérons que les catégories et éléments de données doivent rester un exemple mais en aucun cas une ligne stricte, la banque pouvant proposer et mettre en place une structure de classification et de traitement de CID adaptés à son modèle de fonctionnement, celle-ci étant sujette au contrôle du réviseur externe.

Par ailleurs, nous émettons un avis défavorable sur une possible applicabilité de l'annexe 3 aux relations bancaires suivies et gérées à l'étranger. En effet, il est fortement à craindre que l'extension à l'étranger de cette réglementation suisse impliquerait d'importants problèmes en matière d'organisation et de compatibilité avec la réglementation locale en plus de constituer un possible désavantage concurrentiel.

Enfin, nous relevons que la distinction qui pourrait être faite entre clientèle privée-commerciale ne se recoupe que partiellement avec celle de particuliers-personnes morales. Ainsi, à titre d'exemple, un client UHNWI peut très bien traiter ses affaires sous son nom propre et des sociétés commerciales remettre en gestion les liquidités dont elles n'ont pas un besoin immédiat comme le ferait n'importe quel particulier fortuné. Si un tel critère d'applicabilité devait être retenu, il conviendrait que celui-ci soit parfaitement clair de ce point de vue.

En vous remerciant par avance de l'attention que vous voudrez bien accorder à la présente prise de position.

Meilleures salutations.

Françoise Védy
Business Project Manager | GPB Change Delivery Switzerland
HSBC Private Bank (Suisse) SA, Route de Pré-Bois 6, PO Box 3580, CH-1216 Vernier
T +41 (0) 58 705 40 31 | francoise.vedy@hsbcpb.com
www.hsbcprivatebank.com

PostFinance

PostFinance AG
Risikokontrolle
Mingerstrasse 20
3030 Bern

Telefon +41 79 595 57 75
www.postfinance.ch

P.P. 502301236 CH-4808 Zofingen

A-PRIORITY

Eidgenössische Finanzmarktaufsicht FINMA
Alessandro Lana
Einsteinstrasse 2
CH-3003 Bern

Datum 26. Juni 2013
Ihre Nachricht FINMA-RS 2008/21: Operationelle Risiken Banken - Teilrevision
Kontaktperson Lukas Brütsch, Leiter Risikokontrolle PostFinance AG
E-Mail lukas.bruetsch@postfinance.ch
Direktwahl +41 79 595 57 75

Stellungnahme der PostFinance AG zur Anhörung zum FINMA-Rundschreiben 2008/21: Operationelle Risiken Banken - Teilrevision

Sehr geehrter Herr Lana
Sehr geehrte Damen und Herren

Mit Datum vom 23. Mai 2013 haben Sie die Anhörung zur Teilrevision des FINMA-Rundschreibens 2008/21: Operationelle Risiken Banken eröffnet. Wir danken Ihnen für die Möglichkeit eine Stellungnahme zur Teilrevision einreichen zu können, welche wir gerne annehmen und Ihnen vorliegend unsere Stellungnahme im Rahmen der Anhörung zur Verfügung stellen.

1. Stellungnahme zu einzelnen Randziffern

Rz 120
i. Die Begriffe „Art", „Typ" und „Ebene" der operationellen Risiken sind unklar. Wir empfehlen, diese Begriffe in einem Glossar zu beschreiben.

ii. Wir sind der Meinung, dass die Festlegung einer Risikobereitschaft und deren Steuerung weder praktikabel noch zielführend ist. Die Risikobereitschaft definieren Sie als die inhärenten Risiken, die eine Bank *a priori* einzugehen bereit ist und grenzen diese ab gegenüber Residualrisiken, das heisst gegenüber jenen Risiken, die durch geeignete Massnahmen beschränkt werden. Im Umkehrschluss entspricht die Risikobereitschaft den eingegangen Risiken vor irgendwelchen risikominimierenden Massnahmen. Eine Quantifizierung dieser Grösse ist kaum praktikabel, weil bei der Risikobeurteilung sämtliche risikomindernden Massnahmen weggedacht werden müssen. Wir empfehlen stattdessen, die Höhe der Risikotoleranz zu steuern und gleichzeitig regelmässig die Wirksamkeit der Massnahmen zu überprüfen. Massnahmen die an Wirkung einbüssen, haben einen direkten Einfluss auf das Residualrisiko. Das entspricht unserer Ansicht nach Ihrem Beispiel zum Umgang mit Exceptions to Policy im Erläuterungsbericht.

Rz 122
Der Begriff „solide Führungsstruktur" ist unklar. Wir empfehlen, diesen Begriff in einem Glossar zu beschreiben.

Rz 125 Bst. c
Im Zusammenhang mit dem Kommentar zu Rz 120: Da der Begriff der „Arten" von operationellen Risiken unklar ist, ist nicht klar, worauf sich die diesbezügliche Risikobereitschaft und Risikotoleranz und allfällige Limiten beziehen sollen.

Rz 130 Bst. c
Was verstehen Sie unter relevanten externen Ereignissen? Sind hiermit Ereignisse bei Dritten oder Externe Ereignisse im Sinne von externem Betrug, Elementarereignissen etc. gemeint? Wir empfehlen, diesen Begriff zu erläutern.

Anhang 3, Rz 9 (Definition CID)
Es wird bei der Definition von CID nicht erwähnt, dass der Geheimhaltungsbereich über zivilrechtlich gültige Einschränkungen mit spezifischen Konsequenzen eingeschränkt werden kann. Die FINMA hat aber selber in der Mitteilung 3 (2009) vom 17. Juni 2009 Einschränkungen der Geheimhaltung in den AGB der Banken und Effektenhändler verlangt. Derartige Einschränkungen müssen im Interesse der Institute weiterhin möglich sein. Insbesondere müssen auch besondere Bearbeitungsmodalitäten vereinbart werden können (z.B. Inkasso, Zahlungsverkehr etc.). Auf nicht-geheime CID wird die Regelung nicht vollumfänglich Anwendung finden. Ein präzisierender Hinweis auf diese Einschränkung wäre hilfreich, weil das Rundschreiben ansonsten (namentlich auch über die Beispiele in Rz 87) den Eindruck vermittelt, die getroffene Regelung müsse ausnahmslos auf alle CID Anwendung finden.

Anhang 3, Rz 11 (Klassifizierung und Vertraulichkeitsstufen) **und Rz 48** (Tests für die Entwicklung, Veränderung und Migration von Systemen)
Die Charakterisierung der Massnahmen Anonymisierung, Pseudonymisierung und Verschlüsselung als Beispiele ist sachgerecht. Sie entspricht der in vielen Passagen des Rundschreibens zum Ausdruck gebrachten Rücksichtnahme auf Unterschiede der Banken bezüglich ihrer Grösse, Struktur und Komplexität.
Das Fehlen der Einschränkung in Form der Exemplifikation fehlt in Rz 48. Die Ausfassung des Texts lässt offen, ob die Massnahmen auch in Rz 48 Beispielcharakter haben sollen, was aber dringend zu fordern ist. Die in Rz 48 genannten Vorgänge sind Anwendungsfälle des Bearbeitens von CID, weshalb eine Verschärfung der allgemeinen Regel in Rz 11 nicht angezeigt ist. Der Text in Rz 48 muss an die Regelung in Ziff. 11 angepasst werden („zum Beispiel Anonymisierung, Pseudonymisierung oder Verschlüsselung").

Anhang 3, Rz 25 („Need-to-know"-Grundsatz)
Die in Rz 25 erfolgte Konkretisierung des „Need-to-know"-Prinzips scheint zu signalisieren, dass die Minimierung des Kreises der Zugriffsberechtigten und des Bestands der ihnen zur Verfügung stehenden CID nicht ausreichend ist. Die Verpflichtung zur Unterscheidung von Kundengruppen verhindert (bei enger Auslegung) den Betrieb von Abrufsystemen zur gesamten Kundschaft. Da nicht vorstellbar ist, dass die Regelung die nationale Kundenbetreuung unterbinden will (Front Office und/oder Back Office), ist der Text in diesem Punkt missverständlich. Der Text muss dahingehend präzisiert werden, dass das „Need-to-know" nicht zwingend im Rahmen der Unterscheidung von Kundenuntergruppen erfolgen muss, sondern dass dies auch in insgesamt sachgerechter Art und Weise geschehen kann.

2. Spezifische Rückmeldung zu Kapitel IV.B. „Qualitative Grundanforderungen"

a. Wie beurteilen Sie die Möglichkeit, das Inkrafttreten des Kapitels IV.B „Qualitative Grundanforderungen" bereits auf den 1. Juli 2014 festzusetzen?

Wir empfehlen, das gesamte revidierte Rundschreiben wie vorgesehen per 1.1.2015 in Kraft zu setzen. Einzelne im Kapitel aufgeführte Randziffern – z.B. Rz 133 – benötigen erfahrungsgemäss ausreichende Fristen für die Evaluation, Implementierung und Etablierung.

3. Spezifische Rückmeldung zu Anhang 3 „Umgang mit elektronischen Kundendaten"

a. Ausweitung des Anwendungsbereichs auf natürliche Personen, deren Geschäftsbeziehungen im Ausland betreut oder geführt werden

Die Fragestellung ist für PostFinance nicht relevant.

b. Ausweitung des Anwendungsbereichs auf juristische Personen

Die im Rundschreiben vorgesehenen Massnahmen werden sich in den meisten Punkten auch auf Geschäftskunden auswirken (Governance, Prozesse). Eine ausdrückliche Ausdehnung des Anwendungsbereich ist nicht erforderlich.

Wir danken Ihnen für die wohlwollende Prüfung unserer Anliegen und stehen selbstverständlich jederzeit und gerne für allfällige Fragen zur Verfügung.

Freundliche Grüsse

PostFinance AG
Leiter Sicherheit

Martin Hofer

PostFinance AG
Leiter Risikokontrolle

Lukas Brütsch

RAIFFEISEN

Raiffeisen Schweiz

Raiffeisenplatz
9001 St. Gallen
Telefon 071 225 88 88
Telefax 071 225 88 87
www.raiffeisen.ch
beat.hodel@raiffeisen.ch

A - Post
Eidgenössische Finanzmarktaufsicht
FINMA
Alessandro Lana
Einsteinstrasse 2
CH-3003 Bern

Für Sie zuständig:
Beat Hodel - 071 225 83 76

St. Gallen, 30. Juni 2013

Anhörung zur Teilrevision des Rundschreibens 2008/21 "Operationelle Risiken Banken"

Sehr geehrte Damen und Herren

Wir beziehen uns auf die eröffnete Anhörung der Eidgenössischen Finanzmarktaufsicht (FINMA) zur Teilrevision des Rundschreibens 2008/21 "Operationelle Risiken Banken".

Die Raiffeisen Gruppe unterstützt die Stellungnahme der Schweizerischen Bankiervereinigung (SBVg). Wir empfehlen der FINMA die darin erwähnten Punkte zu berücksichtigen. Nachfolgend möchten wir einige Punkte hervorheben, welche aus unserer Sicht besonders wichtig sind:

Aufgaben des Verwaltungsrates
Die revidierte Version spezifiziert die Aufgaben und Kompetenzen des Verwaltungsrats. Wir begrüssen dies, soweit damit eine zweckmässige Aufgaben- und Kompetenzverteilung erreicht und Klarheit geschaffen wird. Diese Voraussetzungen sind im teilrevidierten Rundschreiben allerdings nicht in jedem Fall erfüllt.
Einige Vorgaben bezüglich der Aufgaben des Verwaltungsrates erachten wir als nicht verhältnismässig. Es handelt sich dabei teilweise um Aufgaben mit operativem Charakter. Hinzu kommen Widersprüche zu andern FINMA-Rundschreiben, welche in einer Gesamtsicht der Klarheit abträglich sind.

- Gemäss Erläuterungsbericht zur Teilrevision des Rundschreibens 2008/21 besteht „eine wichtige Anforderung für die Ausgestaltung von sinnvollen Konzepten für die Definition von Risikobereitschaft und -toleranz für operationelle Risiken darin, dass diese individuell für jedes materielle Risiko zu definieren sind."
  Demgegenüber erachten wir es als nicht zweckmässig, die Festlegung der Risikobereitschaft zu diversen inhärenten Einzelrisiken dem Verwaltungsrat zu übertragen. Dieser sollte vielmehr die Risikopolitik und -strategie festlegen. Zudem wird damit ein Widerspruch zu FINMA-RS 2008/24 geschaffen: Gemäss FINMA-RS 2008/24 führt der Verwaltungsrat eine systematische Risikoanalyse durch und stellt sicher, dass alle wesentlichen Risiken im Institut erfasst, begrenzt und überwacht werden. Diese Vorgabe ist unseres Erachtens für die Stufe des Verwaltungsrates angemessen.
  Eine zweckmässige Lösung besteht unseres Erachtens darin, dass die Geschäftsleitung die Risikobereitschaft und -strategie für wesentliche operationelle Einzelrisiken festlegt und dies dem Verwaltungsrat für die grössten Risiken rapportiert.

- Das Rahmenkonzept ist gemäss Anhörungsentwurf vom Verwaltungsrat zu genehmigen. Unseres Erachtens sind nicht alle im Rundschreiben erwähnten Inhalte für die Bewilligung auf Verwaltungsratsstufe geeignet. Die Verantwortung für die Etablierung von Risikoberichterstattungs- und Manage-

mentinformationssystemen (Ziffer e) sollte beispielsweise nicht dem Verwaltungsrat zugewiesen werden, da

dies dem FINMA-RS 2008/24 widerspricht. Gemäss Rz 83 des FINMA-RS 2008/24 hat die Geschäftsführung sicherzustellen, dass „alle relevanten Informationen über das betriebliche Geschehen erhoben, verteilt und bearbeitet werden (Management Informationssystem)". Auch die Festlegung einer einheitlichen Klassifizierung (Ziffer f) auf Stufe Verwaltungsrat erachten wir als nicht zweckmässig.

Qualitative Anforderungen

Wir stellen fest, dass in die Formulierung qualitativer Anforderungen im revidierten Rundschreiben vermehrt Begriffe aus den quantitativen Ansätzen Eingang gefunden haben. Für eine wirksame Steuerung und Kontrolle operationeller Risiken erachten wir die qualitativen Aspekte als weitaus bedeutender als die quantitativen Ansätze. Begriffe wie Schwellenwerte, Limiten, Risikotoleranz und Messung des Verlustpotenzials bergen die Gefahr, dass die qualitative Auseinandersetzung durch Modellgläubigkeit abgelöst wird. Unsere Befürchtung ist, dass durch die entsprechenden Begriffe und Konzepte aus der quantitativen Welt regulatorische Anreize entstehen, die Weiterentwicklung des op. Risk Frameworks in eine Richtung zu fördern, die wir als unzweckmässig erachten, da quantitativ orientierte Ansätze Gefahr laufen, wesentliche Aspekte der operationellen Risiken zu vernachlässigen. Wir empfehlen daher, im Rahmen der qualitativen Anforderungen auf Begriffe zu verzichten, welche quantitativen Konzepten entstammen.

Umgang mit elektronischen Kundendaten (Anhang 3)

Wir erachten den Detaillierungsgrad der Vorschriften als zu hoch. Ungeachtet des Entwicklungsstandes einer Bank im Umgang mit elektronischen Kundendaten bedingt die detaillierte Regelung per se einen hohen Abstimmungs- und Umsetzungsaufwand um volle Compliance zu gewährleisten.

Auf der einen Seite würden wir uns daher wünschen, dass sich der Anhang 3 auf die Formulierung von Prinzipien beschränkt. Sofern diesem Anliegen nicht Rechnung getragen wird, erachten wir die Frist als zu kurz bemessen. Der Anhang 3 tritt gemäss Anhörungsentwurf am 01.01.2015 in Kraft. Da die Umsetzung des Anhangs 3 aufwändige und kostenintensive Anpassungen an die detaillierten Vorschriften zur Folge hat, erachten wir eine Übergangsfrist bis mindestens 01.01.2016 als angemessen.

Spezifische Situation der Raiffeisen Gruppe

Wir gehen davon aus, dass die Inhalte des Rundschreibens bei Raiffeisen mehrheitlich konsolidiert auf Gruppenebene anzuwenden sind. Die Umsetzung bei den Raiffeisenbanken wird im Rahmenkonzept der Raiffeisen Schweiz und / oder dem Reglement Risikopolitik für die Raiffeisen Gruppe beschrieben und über interne Regulatorien bei den Raiffeisenbanken umgesetzt werden.

Fragenliste zur Anhörung

Frage 1 der FINMA: Wie beurteilen Sie die Möglichkeit, das Inkrafttreten des Kapitels IV.B „Qualitative Grundanforderungen" bereits auf den 1. Juli 2014 festzusetzen?

Antwort: Der Anhörungsentwurf sollte, basierend auf der Stellungnahme der SBVg und der einzelnen Institute, umfassend überarbeitet werden. Wir gehen davon aus, dass dieser Prozess Zeit in Anspruch nimmt und die Inkraftsetzung des Rundschreibens verzögern wird. Anders als etwa im Markt- oder Kreditrisikomanagement hat sich im op. Risk Bereich eine Best Practice erst in Teilbereichen herauskristallisiert. Die Regulierung ist daher ein Balanceakt, der im besten Fall das op. Risk Management der Branche auf ein Minimalniveau anhebt und im schlechtesten Fall die Weiterentwicklung der Disziplin op. Risk Management behindert.
Das Ziel einer vorgezogenen Einführung schafft unnötigen Druck auf diesen heiklen regulatorischen Prozess und birgt die Gefahr, dass die Qualität der Regulierung leidet.
Deshalb sollte am bisherigen Zieltermin festgehalten werden.

Frage 2 der FINMA: Wie beurteilen Sie die Möglichkeit einer Ausweitung des Anwendungsbereichs

a) *auf natürlichen Personen („Privatkunden"), deren Geschäftsbeziehungen im Ausland betreut oder geführt werden?*
b) *auf juristische Personen (z.B. „Firmenkunden")?*

Antwort: Es gelten die vorgenannten grundsätzlichen Punkte zum Anhang 3.

Die Ausweitung erhöht die Betriebskosten ohne zusätzlichen Nutzen zu stiften. Der Schutz der genannten Kundengruppen ist bereits durch andere Bestimmungen (schweizerisches Datenschutzgesetz und lokale Datenschutzgesetze) gewährleistet.
Wir empfehlen daher dringend, auf eine Ausweitung zu verzichten.

Wir danken Ihnen im Voraus für die Berücksichtigung unserer Stellungnahme. Gerne stehen wir Ihnen für weitergehende Erklärungen zu unserer Stellungnahme zur Verfügung.

Freundliche Grüsse

Raiffeisen Schweiz

Marcel Zoller
Leiter Departement Finanzen
Mitglied der Geschäftsleitung

Dr. Beat Hodel
Leiter Gruppen-Risikosteuerung
Mitglied der erweiterten Geschäftsleitung

SwissBanking

Eidgenössische Finanzmarktaufsicht FINMA
Alessandro Lana
Einsteinstrasse 2
3003 Bern

alessandro.lana@finma.ch

Basel, 27. Juni 2013
J.4.6/J.2/A.045.2/SLO/FHA/AAR

Anhörung zur Teilrevision des FINMA Rundschreibens 2008/21 „Operationelle Risiken Banken“

Sehr geehrte Frau Präsidentin
Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 23. Mai 2013 eröffnete Anhörung betreffend die Teilrevision des FINMA-Rundschreibens (RS) 2008/21 „Operationelle Risiken Banken“ und bedanken uns für die Gelegenheit zur Stellungnahme. Ebenso möchten wir der FINMA unseren Dank für die Organisation des Workshops vom 8. März 2013 aussprechen. Dieser bot eine gute Gelegenheit zum direkten Austausch, den wir sehr schätzen. Leider sind sowohl die Vorlaufzeit für gewisse Traktanden des Workshops als auch die aktuelle Anhörungsfrist sehr kurz ausgefallen, was eine vertiefte Vorbereitung bzw. die Erarbeitung dieser Stellungnahme entlang unserer Governance erheblich erschwert. Wir bitten Sie daher erneut, der Zeitplanung künftig mehr Beachtung zu schenken und uns bei Anhörungen angemessene Fristen einzuräumen.

Grundsätzlich begrüssen wir es, dass die FINMA Vorgaben zum Management von operationellen Risiken macht und sich dabei an internationalen Standards orientiert.

Dabei gilt es jedoch zu gewährleisten, dass kleinere und mittlere Banken ohne bedeutende operationelle Risiken mittels einer angemessenen Differenzierung der Anforderungen (Proportionalitätsprinzip) vor unverhältnismässigen Anforderungen bewahrt werden. Die Kriterien für die Differenzierung sollten unseres Erachtens nochmals überdacht und derart ausgestaltet werden, dass sie einen möglichst grossen Risikobezug aufweisen.

Sowohl in Bezug auf die qualitativen Anforderungen (Kapitel IV) als auch auf den Umgang mit vertraulichen Kundendaten (Anhang 3) erachten wir den Anhörungsentwurf derzeit noch als inhaltlich und formell ungenügend. Insbesondere enthält der Text an mehreren Stellen unverhältnismässige oder ungenaue und unklar formulierte Bestimmungen.

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

Betreffend Anhang 3 zum Umgang mit vertraulichen Kundendaten beantragen wir, die Anforderungen stärker prinzipien-basiert auszugestalten und die Detail-regelungen zu streichen. Die voraussichtlichen Kostenfolgen, welche durch die detaillierten Regelungen anfallen würden, erscheinen uns unverhältnismässig im Vergleich zum zu erwartenden Nutzen. Des Weiteren wirft der Entwurf verschiedene Fragen im Zusammenhang mit der schweizerischen Datenschutz-gesetzgebung auf.

Vor diesem Hintergrund erachten wir eine nochmalige gründliche Überarbeitung des Rundschreibens als notwendig und würden es daher sehr begrüssen, wenn die FINMA die betroffenen Kreise nach der Auswertung der Anhörung und der Überarbeitung zumindest mündlich nochmals informieren und über die wichtigsten Anpassungen anhören würde.

Da die Anhörung zum Rundschreiben zwei grundsätzlich unterschiedliche und jeweils in sich geschlossene Themen beinhaltet, ist unsere Stellungnahme ebenso in zwei Kapitel aufgeteilt, wobei das erste hauptsächlich die qualitativen Anforderungen behandelt und das zweite den Anhang 3 des Rundschreibens betreffend Umgang mit vertraulichen Kundendaten.

1. Qualitative Anforderungen an das Risikomanagement von operationellen Risiken

1.1 Grundsätzliches

Grundsätzlich begrüssen wir es, dass die FINMA Vorgaben zum Management von operationellen Risiken macht und sich dabei an internationalen Standards wie beispielsweise den „Principles for the Sound Management of Operational Risk“ orientiert. Dabei gilt es jedoch zu beachten, dass Best Practices für international tätige Banken, wie sie der Basler Ausschuss für Bankenaufsicht formuliert hat, nicht telquel und flächendeckend als Mindeststandards für alle Banken in der Schweiz angewendet werden können. Stattdessen muss mittels einer angemessenen Differenzierung der Anforderungen (Proportionalitätsprinzip) gewährleistet werden, dass insbesondere kleinere und mittlere Banken ohne bedeutende operationelle Risiken nicht unverhältnismässig belastet werden (vgl. auch Kapitel 1.3).

Obwohl wir die neuen Vorgaben grundsätzlich unterstützen, können wir den Entwurf des Rundschreibens in seiner jetzigen Version noch nicht vollumfänglich gutheissen. Insbesondere enthält der Text an vielen Stellen noch sehr ungenaue und unklar formulierte Bestimmungen, die bei der Umsetzung durch die Banken sowie bei der anschliessenden Prüfung durch die Prüfgesellschaften unweigerlich zu grossen Problemen und Diskussionen führen würden. Da dies weder im Sinne der Regulierung noch der Adressaten der Regulierung ist, erlauben wir uns, Sie in den folgenden Kapiteln auf die entsprechenden kritischen Stellen hinzuweisen und alternative Vorschläge anzubringen.

Wir nehmen enttäuscht zur Kenntnis, dass die Regulierungsfolgenabschätzung in Kapitel 5 des Erläuterungsberichtes einmal mehr sehr rudimentär ausgefallen ist und keine ernsthafte Auseinandersetzung mit den Auswirkungen der Regulierung enthält. Auch wenn eine Quantifizierung dieser Auswirkungen schwierig sein dürfte, so hätten wir zumindest eine differenzierte Analyse erwartet, welche die organisatorischen, technischen und finanziellen Auswirkungen für die verschiedenen Bankengruppen aufzeigt.

Des Weiteren haben wir den Eindruck, dass der Rundschreiben-Entwurf Begriffe und Konzepte aus einer Vielzahl unterschiedlicher Fachbereiche und Risikomanagement-Ansätze enthält, die derzeit noch ungenügend aufeinander abgestimmt sind. Die Bedeutung von Begriffen, die nicht im Rundschreiben selbst definiert werden, sollte mittels Referenzierungen auf andere Rechtstexte und Regulierungsvorgaben erklärt werden.

Bezüglich Begrifflichkeiten weisen wir darauf hin, dass in jüngeren Beispielen von Rundschreiben hauptsächlich der Begriff „Geschäftsleitung“ verwendet wird (z.B. FINMA-RS 2013/6 „Liquidität Banken“ und 2011/2 „Eigenmittel-Puffer und Kapitalplanung Banken“), während das FINMA-RS 2008/24 „Überwachung und interne Kontrolle Banken“ den Begriff „Geschäftsführung“ verwendet. Eine einheitliche Handhabung der Begriffe wäre für die Verständlichkeit und Konsistenz der FINMA-Regulierung wünschenswert.

Im Vergleich zu anderen Rundschreiben und Rechtstexten enthält der Entwurf derzeit noch zahlreiche Fussnoten, welche die Lesbarkeit des Rundschreibens unnötig erschweren. Grundsätzlich sollten Fussnoten lediglich Verweise oder Definitionen enthalten (beispielsweise Fussnoten 4, 5, 6, 12, 13). Die anderen Fussnoten sind entweder überflüssig (Fussnoten 7, 8, 9, 10) oder sollten direkt in den Text des Rundschreibens integriert werden (Fussnote 11). Die Fussnote 8 enthält zudem noch einen sprachlichen Fehler: Am Schluss des Satzes sollte es „werden“ statt „wird“ heissen.

1.2 Mindesteigenmittel und Untergrenze (Floor)

In der neuen **Randziffer 116*** wird festgehalten, dass Banken, die operationelle Risiken nach dem AMA unterlegen, das sogenannte „Floor-Regime“ des Basler Ausschusses anwenden müssen und ihre Eigenmittel auf Gesamtbankstufe nicht weniger als 80% der erforderlichen Eigenmittel unter dem Mindeststandard von Basel I betragen dürfen. Im Wissen darum, dass eine Berechnung nach dem alten Basel I Regime heute kaum noch sinnvoll bzw. gar obsolet ist und die Banken zudem vor erhebliche praktische Probleme stellt, kann die FINMA unter Anwendung von Art. 47 ERV im Einzelfall regeln, wie eine „angemessene approximative Berechnung der theoretischen Basel-I-Anforderungen“ vorgenommen werden kann.

Wir begrüssen diese Flexibilität ausdrücklich. Allerdings fehlt in Rz 116* – im Gegensatz zu Rz 381.1* von FINMA-RS 2008/19 „Kreditrisiken Banken“ – ein Hinweis darauf, was eine „angemessene approximative Berechnung“ in den Augen der FINMA sein könnte. Wir schlagen daher vor, die Rz 116* analog zu RS 2008/19 um folgenden Satz

zu ergänzen: „Für operationelle Risiken orientiert sie sich dabei am Basisindikatoransatz gemäss Art. 92 bzw. am Standardansatz gemäss Art. 93 ERV."

1.3 Proportionalitätsprinzip (Kapitel IV.A)

Wir begrüssen das Vorhaben der FINMA sehr, wonach die qualitativen Anforderungen von Kapitel IV des Rundschreibens von den Banken unter Anwendung des Proportionalitätsprinzips umgesetzt werden können. Hingegen verstehen wir nicht, weshalb die Differenzierung lediglich aufgrund des Kriteriums der Grösse einer Bank (**Randziffer 117***) erfolgen soll. Wir würden es begrüssen, wenn die Differenzierung nicht nur entlang der Grösse der Bank, sondern analog zum Proportionalitätsprinzip in FINMA-RS 2013/6 „Liquidität Banken" (Rz 10) auch entlang den Kriterien von „Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten" angewendet werden könnte. Wir beantragen daher, diese Randziffer entsprechend zu ergänzen.

Des Weiteren begrüssen wir auch die Möglichkeit von Ausnahmen für kleine Banken gemäss **Randziffer 118*** ausdrücklich. Jedoch sind wir auch hier der Ansicht, dass die Definition einer „kleinen" Bank entlang der Kategorisierung gemäss FINMA-RS 2011/2 „Eigenmittelpuffer und Kapitalplanung Banken" zu eng und – gerade mit Bezug auf operationelle Risiken – zu wenig risikosensitiv ist. Der äusserst vage formulierte dritte Punkt dieser Randziffer („Geschäftsaktivitäten ohne bedeutende Komplexität") vermag diesen Makel nicht zu beheben.

Wir beantragen stattdessen, für die Definition einer kleinen Bank den am Workshop vom 8.3.2013 vorgeschlagenen Ansatz mit zwei Dimensionen zu verwenden und neben der Kategorisierung gemäss FINMA-RS 2011/2 auch den Anteil der erforderlichen Eigenmittel für operationelle Risiken im Vergleich zum Gesamtkapital zu verwenden (vgl. auch FINMA-Folien vom 8.3.2013, Seite 9 f).

1.4 Qualitative Grundanforderungen (Kapitel IV.B)

Die in **Randziffer 119*** aufgeführten Ausnahmen für kleine Banken sind unserer Ansicht nach grundsätzlich sinnvoll und richtig und daher ausdrücklich zu begrüssen.

In diesem Zusammenhang scheint uns jedoch die Ausnahme von der Anwendung von Rz 127 Bst. c bis i überflüssig zu sein. Da in Rz 127 Bst. a bis i lediglich „*Beispiele* von Instrumenten und Methoden", die „eingesetzt werden *können*" aufgeführt sind, ist es nicht nötig, gewisse Banken davon auszunehmen. Es könnte sogar im Gegenteil eher verwirrend sein und Unsicherheit schüren bezüglich des Status von Bst. a und b für kleine Banken bzw. von Bst. a bis i für die restlichen Banken.

Der Verweis auf die „Principles for the Sound Management of Operational Risk" könnte unseres Erachtens gut in einer Fussnote untergebracht werden, da er bezüglich der konkreten Anforderungen für die Banken in der Schweiz keine zusätzlichen Informationen oder konkreten Hinweise liefert. Falls die FINMA jedoch den Verweis im Rundschreibentext zu belassen gedenkt, würden wir eine eigene Randziffer vorschlagen, da keinerlei Zusammenhang zu den Ausnahmen für kleine Banken besteht.

1.4.1 Grundsatz 1: Verantwortlichkeiten

Die vorgeschlagene Regelung bezüglich Verantwortlichkeiten erscheint uns weder klar abgegrenzt und formuliert noch verhältnismässig zu sein und bedarf unseres Erachtens einer gründlichen Überarbeitung. So ist beispielsweise gänzlich unklar, was in welchem Detaillierungsgrad von welchem Organ bzw. von welcher hierarchischen Stufe in einem sogenannten Rahmenkonzept gemäss Rz 120* zu regeln ist. Ausserdem scheint es uns nicht angemessen zu sein, dem Verwaltungsrat die Verantwortung über die Festlegung von Details des Managements von operationellen Risiken zu übertragen. Dies wäre weder praktikabel noch verhältnismässig.

Weiter haben wir grundsätzlich Vorbehalte gegenüber den Konzepten der „Risikobereitschaft" („Risk-Appetite" gemäss Erläuterungsbericht, S. 11) und der „Risikotoleranz" im Zusammenhang mit operationellen Risiken. Insbesondere die Vorstellung, dass eine Bank bereit ist, inhärente Risiken (d.h. ohne jegliche Kontrollen) bewusst einzugehen, erachten wir als unrealistisch. Eine Bank sucht in der Regel die operationellen Risiken im Vergleich zu anderen Risikotypen nicht aktiv bzw. mit einer konkreten Renditeerwartung, sondern sie erwachsen ihr im Sinne eines Nebeneffektes aus ihrer Geschäftstätigkeit. Diesen Unterschied in der ökonomischen Natur der Risiken gilt es zu berücksichtigen. Daher plädieren wir dafür, die Konzepte der „Risikobereitschaft" und der „inhärenten Risiken" gänzlich aus dem Rundschreiben zu streichen.

Basierend auf obenstehenden Kommentaren würden wir vorschlagen, die Festlegung und Abgrenzung der Verantwortlichkeiten – in Anlehnung an FINMA-RS 2013/6 „Liquidität Banken" – wie folgt zu formulieren:

Randziffer 120*

- *Das Organ für die Oberleitung, Aufsicht und Kontrolle (nachfolgend „Verwaltungsrat") ist für die Festlegung der Risikotoleranz für operationelle Risiken zuständig. Der Verwaltungsrat überprüft diese bei Bedarf, d.h. im Falle einer wesentlichen Veränderung der Risikosituation, oder aber mindestens jährlich.*

  Die vom Verwaltungsrat festgelegte Risikotoleranz bildet den Ausgangspunkt für die Operationalisierung des bankinternen Rahmenkonzeptes zur Bewirtschaftung der operationellen Risiken, des entsprechenden Weisungswesens sowie der Risikoidentifikations- und steuerungsprozesse.

Randziffer 121*

- *Die Geschäftsleitung oder ein ihr direkt unterstellter Ausschuss entwickelt und setzt, in Übereinstimmung mit der festgelegten Risikotoleranz, das Rahmenkonzept zur Bewirtschaftung des operationellen Risikos um. Dieses enthält Art, Typ und Ebene der operationellen Risiken, welchen die Bank ausgesetzt ist und welche sie einzugehen bereit ist. Dabei sind Massnahmen vorzusehen, die es erlauben, Verletzungen der Risikotoleranz rechtzeitig zu erkennen und Gegenmassnahmen zu ergreifen.*

  Zum Rahmenkonzept zur Bewirtschaftung des operationellen Risikos zählt insbesondere der Erlass von internen Weisungen und/oder Richtlinien zum Management von operationellen Risiken.

Randziffer 122*

- *Die Geschäftsleitung definiert eindeutige und wirksame Verantwortlichkeiten für das Management von operationellen Risiken. Des Weiteren ist eine klar bezeichnete Einheit für die Aufrechterhaltung und die laufende Weiterentwicklung des Rahmenkonzeptes für das Management von operationellen Risiken verantwortlich. Diese Einheit muss über genügend qualifiziertes Personal verfügen, um ihre Verantwortlichkeiten wirkungsvoll wahrnehmen zu können. Konsistent zu analogen Risikoeinheiten soll die Einheit für operationelle Risiken adäquat in relevanten bankinternen Gremien vertreten sein.*

In **Randziffer 123*** muss gemäss unserem Dafürhalten das Kriterium der Wesentlichkeit sowohl auf bestehende als auch auf neue Produkte etc. angewandt werden. Daher schlagen wir vor, den Satz wie folgt zu ändern: *„[…] dass das Rahmenkonzept bezogen auf alle wesentlichen neuen und bestehenden Produkte […]“*.

1.4.2 Grundsatz 2: Rahmenkonzept und Kontrollsystem

Gestützt auf unseren Kommentar zum Grundsatz 1 (vgl. oben) sind wir der Ansicht, dass der Erlass von internen Vorschriften (d.h. Weisungen und/oder Richtlinien) nicht in die Kompetenz des Verwaltungsrates, sondern der Geschäftsleitung gehört. Wir schlagen daher vor, die **Randziffer 124*** wie folgt abzuändern: *„Das Rahmenkonzept ist in internen Weisungen und/oder Richtlinien angemessen festzuhalten […].“*

Bezüglich Inhalt des Rahmenkonzeptes gemäss **Randziffer 125*** haben wir zudem folgende Bemerkungen:

- Unserer Ansicht nach muss nicht das Rahmenkonzept die in Rz 125* aufgeführten Aspekte abdecken, sondern die auf Basis des Rahmenkonzeptes von der Geschäftsleitung erlassenen Weisungen und/oder Richtlinien.
- Allgemein ist die Verwendung der Begriffe und Konzepte in diesem Grundsatz derzeit noch sehr uneinheitlich und daher verwirrend. Während in Bst. b) von „*Identifikation, Messung, Beurteilung und Steuerung*“ die Rede ist, werden in Bst. f) die „*Risikobewertung*“ und in Fussnote 8 die „*Überwachung, Kontrolle und Minderung*“ zusätzlich aufgeführt. Des Weiteren stimmen die in Grundsatz 2 verwendeten Begriffe auch nicht mit denen von Grundsatz 3 („*Identifizierung, Begrenzung und Überwachung*“) überein.
- Auch sind wir der Ansicht, dass gewisse der verwendeten Begriffe (z.B. Schwellenwerte, Limiten, Messung) sehr eng an das quantitative Management anderer Risikotypen (z.B. Kredit-, Markt- oder Liquiditätsrisiken) angelehnt sind und für das qualitative Management von operationellen Risiken nicht geeignet sind.
- Wir bitten Sie daher, die Begrifflichkeiten in diesem Rundschreiben-Entwurf und insbesondere in den Grundsätzen 2 und 3 nochmals zu überprüfen und sich dann auf eine klare, einheitliche und konsistente Verwendung der Begriffe und Konzepte festzulegen.

b) Gemäss oben stehender Bemerkung beantragen wir, in Bst. b analog zu Grundsatz 3 von Instrumenten für die „Identifizierung, Begrenzung und Überwachung“ zu sprechen.

   Da die Komponente „Berichterstattung“ unter Punkt e) separat aufgeführt ist, regen wir an, den entsprechenden Hinweis in Punkt b) zu streichen.

c) Gemäss unserem Vorschlag für die Formulierung von Grundsatz 1 (vgl. oben) sollte die Festlegung der Risikotoleranz in der Verantwortung des Verwaltungsrates liegen und daher hier nicht mehr aufgeführt werden.

   Bezüglich der Festlegung von Limiten / Schwellenwerten für operationelle Risiken sind wir grundsätzlich sehr kritisch. Zentral scheint dabei insbesondere, dass solche Limiten oder Schwellenwerte nicht wie bei anderen Risikotypen als Erlaubnis zur Verwendung der Limite gesehen werden, sondern eher als maximal tolerierbare Schwellenwerte, bei deren Überschreiten vorher definierte Gegenmassnahmen und Berichterstattungsmechanismen ausgelöst werden.

d) Wie bereits weiter oben ausgeführt, sind wir der Ansicht, dass das Konzept der inhärenten Risiken im Zusammenhang mit operationellen Risiken problematisch ist und daher gestrichen werden sollte.

f) Wir würden vorschlagen, den Begriff „materiell“ durch den geläufigeren Begriff „wesentlich“ zu ersetzen. Des Weiteren sollte vor „Zielsetzung“ der Artikel („der“) eingefügt werden, um den Sinn der Bestimmung zu verdeutlichen.

g) Soll hiermit tatsächlich die Überprüfung und Beurteilung von operationellen Risiken sichergestellt werden (was ja eigentlich bereits in Punkt b) sowie in Grundsatz 3 festgehalten ist) oder soll sichergestellt sein, dass das *Management* von operationellen Risiken von unabhängiger Seite überprüft und beurteilt wird?

h) Der Buchstabe „h)“ fehlt derzeit in der deutschen Version der Anhörungsunterlagen noch. In der französischen Version wurde „zeitnah“ mit „en temps réel“ übersetzt, was jedoch „in Echtzeit“ bedeutet und nicht mit „zeitnah“ gleichzusetzen ist. Wir würden für die französische Übersetzung den Ausdruck „dans les meilleurs délais“ bevorzugen.

In **Randziffer 126*** sollte unseres Erachtens auf das FINMA-RS 2008/24 „Überwachung und interne Kontrolle Banken“ verwiesen werden, damit klar wird, dass das Kontrollsystem bezüglich operationeller Risiken auf das allgemeine Kontrollsystem der Bank aufbauen und nicht als davon losgelöst betrachtet werden soll.

1.4.3 Grundsatz 3: Identifizierung, Begrenzung und Überwachung

In **Randziffer 127*** wird zuerst von der „Identifizierung, Begrenzung und Überwachung“ von Risiken als Grundlage des Risikomanagements gesprochen, während danach aber nur von „Identifizierung und Beurteilung“ die Rede ist und zu Begrenzung und Überwachung keine weiteren Hinweise gegeben werden. Wir bitten Sie, die Begrifflichkeiten nochmals zu überprüfen und gegebenenfalls anzupassen (beispielsweise Streichung von „Beurteilung“).

Bei den Beispielen von Instrumenten und Methoden (Bst. a bis i) sehen wir folgende Schwierigkeiten:

a) Risiko- und Kontrollbeurteilungen sollten gerade das Resultat der Instrumente und Methoden in Bst. a bis i sein und daher u.E. nicht in dieser Liste aufgeführt werden.

e) Uns scheint nicht klar, wie eine Analyse der Zusammenhänge zwischen den Risiken, den Prozessen und den Kontrollen bei der Identifikation eben derselben Risiken hilfreich sein könnte.

f) In diesem Punkt besteht ein sprachliches Problem: Es geht aus dem Text nicht klar hervor, wie der Satzbaustein „die Wirksamkeit des internen Kontrollsystems“ mit dem ersten Teil des Satzes in Verbindung steht.

Die **Randziffer 128*** ist in der jetzigen Formulierung sehr knapp gehalten und sollte unseres Erachtens im Sinne des Erläuterungsberichtes (S. 14) konkretisiert werden, so dass zumindest festgehalten ist, dass unter „interner Preisfestsetzung“ die Allokation der erforderlichen Eigenmittel auf verschiedene Geschäftsbereiche und -einheiten zu verstehen ist. Des Weiteren würden wir Sie bitten zu erläutern, wie diejenigen Banken, die nicht den AMA anwenden, diese Allokation der Eigenmittelanforderungen vornehmen sollen.

1.4.4 Grundsatz 4: Interne und Externe Berichterstattung

Der erste Satz von **Randziffer 129*** scheint uns redundant zu sein und sollte daher gestrichen werden. Der Prozess zur Überwachung der operationellen Risiken wird bereits in Grundsatz 3 definiert.

Wir anerkennen, dass geeignete Berichterstattungsmechanismen benötigt werden, jedoch ist uns nicht klar, was mit dem „proaktiven“ Risikomanagement gemeint ist. Unseres Erachtens sollte das Management von (operationellen) Risiken grundsätzlich proaktiv sein. Wir beantragen daher, den Begriff „proaktiv“ zu streichen, da ansonsten fälschlicherweise der Eindruck entstehen könnte, dass an anderen Stellen im Rundschreiben von einem reaktiven Management die Rede ist.

In **Randziffer 130*** würden wir anregen, das Wort „Entscheidungsfindung“ durch „Identifizierung, Begrenzung und Überwachung“ zu ersetzen, damit klar wird, welchem Zweck die Berichterstattung dient.

Bezüglich Punkt a) dieser Randziffer verweisen wir auf unseren Kommentar zu Grundsatz 1 und schlagen vor, den Begriff „Risikobereitschaft“ zu streichen.

In Punkt b) ist unklar, was mit „signifikant“ gemeint ist. Besser wäre wahrscheinlich der Begriff „wesentlich“.

Die **Randziffer 131***, wonach die Banken über eine „formelle, vom Verwaltungsrat genehmigte Offenlegungspolitik“ verfügen müssen, ist unserer Ansicht nach überflüssig und daher zu streichen. Die Offenlegung von Risikoinformationen jeglicher Art wird in der Regel nicht von der Unternehmung selbst bestimmt, sondern im Rahmen des

Rechnungslegungsstandards (z.B. FINMA-RS 2008/2 „Rechnungslegung Banken“, Rz 149) oder aufgrund von aufsichtsrechtlichen Anforderungen (z.B. FINMA-RS 2008/22 „EM-Offenlegung Banken“) verlangt. Dabei sind jeweils auch Inhalt, Frequenz und Überprüfung der Offenlegungen geregelt.

Eine über die bestehenden aufsichtsrechtlichen und rechnungslegungstechnischen Anforderungen hinausgehende, separate Offenlegung zum Management von operationellen Risiken würden wir klar ablehnen. Eine solche wäre, insbesondere im Vergleich zu anderen Risiken (z.B. Kredit- oder Liquiditätsrisiken), unverhältnismässig und würde zu Redundanzen mit anderen Offenlegungen führen.

Zudem wäre es unangemessen und unsachgemäss, den Erlass einer solchen Offenlegungspolitik auf Stufe des Verwaltungsrates anzusiedeln. Falls eine Bank einen Prozess betreffend ihre Risikooffenlegungen festhalten möchte, so ist es ihr selbst zu überlassen, wie und auf welcher Stufe sie dies regelt.

In **Randziffer 132*** werden die von den Banken offen zu legenden Informationen angesprochen. Wir gehen davon aus, dass damit die aufsichtsrechtlichen Anforderungen bzw. die Vorgaben der jeweiligen Rechnungslegungsstandards zur Offenlegung von Risikoinformationen gemeint sind. Des Weiteren nehmen wir an, dass unter dem Begriff „Anspruchsgruppen“ die Investoren, Gläubiger, Einleger und die interessierte Öffentlichkeit gemeint sind und das „Konzept“ mit dem „Rahmenkonzept“ gemäss Rz 120* gleichzusetzen ist. Ausserdem ist klar zu unterscheiden zwischen der Anforderung, etwas offenzulegen und der Anforderung, dass sich jemand ein Urteil über etwas bilden kann. Unserer Meinung nach bedarf die Formulierung dieser Randziffer einer Überarbeitung im Sinne der Klarheit.

Der Anspruch, dass die Offenlegungen den Anspruchsgruppen eine „Beurteilung der Wirksamkeit“ ermöglichen sollen, ist völlig unrealistisch. Auch geht dies weit über die Anforderungen an Risikooffenlegungen gemäss FINMA-RS 2008/2 und 2008/22 hinaus, welche keine Vorgaben zur notwendigen Wirkung der Offenlegung machen. Wir beantragen daher eine Streichung dieses Satzes oder aber zumindest eine Anpassung, beispielsweise wie folgt: „Die offen gelegten Informationen sollen den Investoren, Gläubigern, Einlegern und der interessierten Öffentlichkeit einen Einblick in das Management von operationellen Risiken erlauben.“ Zudem ist im letzten Satz dieser Randziffer unklar, worauf sich das Wort „dieses“ bezieht: Auf das Konzept? In diesem Zusammenhang sind wir der Ansicht, dass die Details des (Rahmen-) Konzeptes nicht Bestandteil der Offenlegung bilden.

1.4.5 Grundsatz 5: Technologieinfrastruktur

Die **Randziffer 133*** betreffend Technologieinfrastruktur scheint uns sowohl hinsichtlich Inhalt als auch Formulierung unbefriedigend. Zum einen sind wir der Ansicht, dass die ersten beiden Sätze der Randziffer für eine Bank allgemein und in jeder Situation bzw. betreffend alle Risiken Gültigkeit haben und daher hier nicht explizit wiederholt werden müssen. Ausserdem sind wir der Meinung, dass es zur Unterstützung des Managements von operationellen Risiken keine eigene Technologieinfrastruktur braucht. Der erste Satz dieser Randziffer ist diesbezüglich irreführend.

Zum anderen ist uns der Sinn und Zweck des letzten Satzes dieser Randziffer nicht klar. Darin wird verlangt, dass die Geschäftsleitung ein „integriertes und umfassendes Risikomanagement“ implementiert, ohne dass erläutert wird, was darunter zu verstehen ist. Besonders unklar ist der Begriff des „integrierten“ Risikomanagements. Die Vorgaben zu Aufbau und Art des Managements von operationellen Risiken sind zudem bereits in den Grundsätzen 1 bis 4 erläutert und sollten daher hier nicht nochmals aufgenommen werden. Wir bitten Sie, den letzten Teil dieser Randziffer zu streichen („sowie ein integriertes […]“).

1.4.6 Grundsatz 6: Kontinuität bei Geschäftsunterbrechung

Wie bereits am Workshop vom 8. März 2013 erwähnt, erwarten wir, dass der Grundsatz 6 betreffend Kontinuität bei Geschäftsunterbrechung eng an die in wesentlichen Punkten als Mindeststandard anerkannten Empfehlungen der SBVg zum Business Continuity Management (BCM) angelehnt ist. Wir begrüssen daher den Verweis in Fussnote 13, würden aber in **Randziffer 134*** eine leicht angepasste Formulierung und zum Teil andere Begriffe vorschlagen, welche den Bezug zu den SBVg Empfehlungen deutlicher machen:

„Die Geschäftsleitung ist zuständig für die Konkretisierung der Business Continuity Management Strategie (Strategie für das betriebliche Kontinuitätsmanagement), welche die Kontinuität des Geschäftsbetriebes und die Wiederherstellung der kritischen Geschäftsprozesse im Falle eines schweren Unterbruches sicherstellen soll.“

Gerne weisen wir Sie zudem darauf hin, dass unsere Empfehlungen derzeit in Überarbeitung sind. Die Referenz in der Fussnote müsste daher zu gegebener Zeit nochmals angepasst werden.

1.5 Risikospezifische Qualitative Anforderungen (Kapitel IV.C)

In **Randziffer 135*** wird impliziert, dass gewisse Banken in ihren Anstrengungen zum Management der operationellen Risiken über die Anforderungen von Kapitel IV.B hinausgehen müssen, ohne dass jedoch ausgeführt wird, welche zusätzlichen Massnahmen zu ergreifen bzw. Anforderungen zu erfüllen wären.

Diese offene Formulierung führt zu massiver Rechtsunsicherheit für die Banken, insbesondere da die Kriterien, welche eine „umfassendere und intensivere“ Steuerung und Kontrolle der operationellen Risiken begründen würden, völlig unklar sind. Als einziges Kriterium werden „spezifische operationelle Risiken“ genannt, welche beispielsweise dem Geschäftsmodell der Bank geschuldet sein könnten. In diesem Zusammenhang werden als Beispiele die „operationellen Risiken im Umgang mit Kundendaten“ und „grenzüberschreitende Tätigkeiten“ genannt.

Diese beiden Beispiele sind jedoch eher verwirrend als klärend, da sie zwei grundsätzlich verschiedene Dimensionen betreffen: Das eine ist ein Risiko und das andere eine Art der Geschäftstätigkeit. Des Weiteren kann davon ausgegangen werden, dass grundsätzlich allen Banken gewisse Risiken im Umgang mit Kundendaten erwachsen, weshalb gemäss der Formulierung von Rz 135 alle Banken

unspezifizierte zusätzliche Massnahmen einführen müssten, die über die Grundanforderungen von Kapitel IV.B hinausgehen. Wir gehen davon aus, dass eine solche weitreichende Ausdehnung der Anforderungen auch nicht im Sinne der FINMA ist, weshalb die Randziffer u.E. ganz gestrichen oder aber zumindest umformuliert werden sollte.

Auch die **Randziffer 136*** muss unseres Erachtens vollständig gestrichen werden, da eine "Eigen-Ermächtigung" der FINMA weder rechtlich möglich noch nötig ist. Falls es Themen gibt, die nach Ansicht der FINMA weiter konkretisiert werden müssen, so kann sie dies jederzeit via ein ordentliches Regulierungs- und Anhörungsverfahren tun. Auch ist sie frei, dies im Rundschreiben oder aber in einem Anhang, der ja integrierender Bestandteil des Rundschreibens ist, vorzunehmen.

Falls die FINMA jedoch beabsichtigt, aufgrund von Rz 136* „weitergehende Konkretisierungen" oder „weitergehende qualitative Anforderungen" ohne ordentliches Verfahren anzuordnen, so könnten wir dies nicht unterstützen.

1.6 Fragenliste zur Anhörung

Eine Inkraftsetzung des Kapitels IV.B „Qualitative Grundanforderungen" auf den 1. Juli 2014 lehnen wir ab. Es besteht kein nachvollziehbarer Grund, weshalb das Kapitel IV.B frühzeitig in Kraft treten sollte. Des Weiteren gilt es zu bedenken, dass die Banken aktuell sowie in absehbarer Zukunft eine Reihe weiterer regulatorischer Themen zu bearbeiten haben, welche erhebliche Ressourcen absorbieren.

Zudem wäre eine Inkraftsetzung von Kapitel IV.B auf den 1. Juli 2014 ohne die dazugehörigen Kapitel IV.A und IV.C wenig sinnvoll. Insbesondere das Proportionalitätsprinzip (Kapitel IV.A) ist unseres Erachtens ein zentraler Bestandteil für die Umsetzung der Grundanforderungen, weshalb die Inkraftsetzung der verschiedenen Kapitel zeitgleich und frühestens am 1. Januar 2015 erfolgen sollte.

2. Anhang 3: Umgang mit elektronischen Kundendaten

2.1 Grundsätzliches

Wir begrüssen Bemühungen, die darauf abzielen, einen besseren Schutz im Umgang mit elektronischen Kundendaten zu erlangen. Was den revidierten Anhang 3 des Rundschreibens 2008/21 „Operationelle Risiken Banken" (Anhang 3) betrifft, wird die vorgesehene Struktur grundsätzlich befürwortet. Aus unserer Sicht ist es hingegen notwendig, die einzelnen Grundsätze prinzipien-basiert zu formulieren und auf Detailregelungen zu verzichten.

Konkret schlagen wir vor, jeweils nur die ersten Randziffern der Grundsätze 1 bis 9 beizubehalten („Grundsätze") und die restlichen Vorgaben („Detailregelungen") zu streichen. Der vorliegend hohe Detaillierungsgrad der Anforderungen greift zu tief in die operationellen Abläufe und Systeme der Banken ein, die je nach Institut sehr unterschiedlich ausgestaltet sind. Die praktische Umsetzung solch detaillierter

Vorgaben wäre aus unserer Sicht zum Teil gar nicht oder nur mit erheblichen technischen Schwierigkeiten und Kostenfolgen möglich. Dies würde am Ziel der Regulierung, einen erhöhten Schutz im Umgang mit elektronischen Kundendaten zu erreichen, vorbeiführen.

Stattdessen würden wir der FINMA vorschlagen, nebst den Grundsätzen auf unser Informationspapier vom Oktober 2012 betreffend „Data Leakage Protection“ (vgl. SBVg-Zirkular 7752) zu verweisen. Dieses wurde von den entsprechenden Experten der Banken entwickelt und schlägt mögliche, aber nicht zwingende Lösungen für den Umgang mit vertraulichen Kundendaten vor. Diese „Best Practices“ sind unseres Erachtens klar besser geeignet als die vorgeschlagenen Detailregelungen, da sie den unterschiedlichen Geschäftstätigkeiten und IT-Lösungen der Banken besser Rechnung tragen und daher wirkungsvoller umsetzbar sind.

2.2 Gesetzliche Grundlagen und Eignung der Vorgaben

2.2.1 Gesetzliche Grundlage

Im Grossen und Ganzen basieren die von der FINMA im Anhang 3 formulierten Grundsätze auf den bereits durch die Praxis zum Bankkundengeheimnis (Art. 47 BankG) und zur schweizerischen Datenschutzgesetzgebung aufgestellten Vorschriften (insbesondere Art. 8 ff. VDSG). Diese werden nun aber in den Detailregelungen in hohem Masse konkretisiert, sodass der grosse Ermessensspielraum, welchen die schweizerische Datenschutzgesetzgebung mit Begriffen wie „Erkennbarkeit“ oder „Verhältnismässigkeit“ bewusst zur Verfügung stellt, um dem jeweiligen Kontext im Einzelfall gerecht zu werden, weitgehend aufgehoben wird.

Bei manchen Detailregelungen geht die FINMA gar über die datenschutzrechtlichen Pflichten hinaus und nimmt mit der Anordnung von gesetzlich nicht vorgesehenen Organisationspflichten eine „kalte Gesetzesrevision“ vor. Folgende Beispiele können dazu genannt werden:

- Randziffer 23*: Über das FINMA-RS 2008/7 „Outsourcing Banken“ hinaus werden zusätzliche Anforderungen an Outsourcing-Transaktionen aufgestellt. Die bisherigen, im Rahmen des RS 2008/7 festgelegten Bestimmungen zum Outsourcing dürfen durch die Vorgaben des neuen Anhang 3 nicht eingeschränkt oder mit unverhältnismässigem Zusatzaufwand belastet werden.
- Randziffer 53*: Eine solche allgemeine Pflicht zur Information der Öffentlichkeit besteht nach Schweizer Recht nicht.

2.2.2 Schnittstelle zu Kapitel IV (Qualitative Anforderungen)

Der Grundsatz 1 betreffend Governance ist unseres Erachtens bereits ausreichend durch die Bestimmungen des Rundschreibens zu den qualitativen Anforderungen an das Management von operationellen Risiken (vgl. oben, Kapitel 1.4) abgedeckt und daher vollständig zu streichen oder aber durch einen Verweis auf Kapitel IV.B zu ersetzen. Eine zusätzliche Governance-Regelung nur für Anhang 3 wäre unverhältnis-

mässig und würde in Bezug auf die Sicherheit von vertraulichen Kundendaten keinerlei Mehrwert bringen.

2.2.3 Eignung der Vorgaben

Neben der Gesetzeskonformität stellt sich die Frage nach der Eignung der vorgeschlagenen Vorgaben zur Erreichung eines erhöhten Schutzes im Umgang mit Kundendaten. In der vorgesehenen Form stellen die vorgeschlagenen Detailregelungen unseres Erachtens kein geeignetes Mittel zur Erreichung der gesetzten Ziele dar. Der hohe Detaillierungsgrad vermittelt eine Scheinsicherheit und -vollkommenheit, da unweigerlich der Eindruck entsteht, dass neben der Einhaltung der aufgeführten Vorgaben keine weiteren, je nach Sachlage gegebenenfalls notwendigen zusätzlichen Massnahmen rechtlicher, technischer oder organisatorischer Natur ergriffen werden müssen. Um eine kunden- und institutsgerechte Umsetzung zu gewährleisten, muss unseres Erachtens vielmehr ein prinzipien-basierter Ansatz mit entsprechendem Ausgestaltungsfreiraum auf Einzelfallbasis gewählt werden (vgl. dazu die Ausführungen unter Kapitel 2.3).
Manche der im Entwurf vorgeschlagenen Regelungen sind aus unserer Sicht ungeeignet zur Zielerreichung:

- Kundendaten sind ein wesentliches Asset jedes Finanzdienstleisters und entsprechend vor unberechtigtem Zugriff von oder Abfluss nach extern zu schützen. Innerhalb des Instituts müssen Kundendaten aber umfassend bearbeitet werden können. Damit sind auf allen Stufen viele Mitarbeitende befasst, und zwar aus sehr unterschiedlichen Blickwinkeln (z.B. zur Kundenberatung an der Vertriebsfront, zur Abwicklung, zwecks Risikomanagement). Eine umfassende „Pseudonymisierung“ der Kundendaten, wie die Vorgaben dies vorsehen, würde deshalb zahlreiche im Interesse der Kunden notwendige Tätigkeiten eines Finanzdienstleisters erschweren. Soweit der Kunde beispielsweise seine vorherige informierte Einwilligung erteilt, muss es – gerade auf Wunsch und im Interesse des Kunden – nach wie vor möglich sein, von den geforderten rechtlichen, technischen und organisatorischen Sicherheitsmassnahmen im Einzelfall abzusehen.
- Vor diesem Hintergrund erscheint es fragwürdig, losgelöst von der gezielten Kontrolle bestimmter Applikationen oder Datenbanken, ein allgemeines Verzeichnis sämtlicher Mitarbeitenden zu fordern, welche Zugriff auf Kundenidentifikationsdaten (CID) haben (vgl. Rz 28*), da diese Liste gerade bei kleineren Bankinstituten weitgehend deckungsgleich mit der Liste sämtlicher Mitarbeitenden wäre. Eine Pflicht zur Listenführung ist in diesem Fall nicht zielführend. Darüber hinaus ist die Vergabe von Zugriffsrechten in den Bankinstituten unterschiedlich geregelt; von einer einschränkenden Regelung, wie sie die Rz 25* bis 27* treffen, sollte daher abgesehen werden.
- Die Vorgaben lassen auch kaum Differenzierungen zwischen den Daten unterschiedlicher Kundensegmente zu. Beispielsweise ist das Risiko des Diebstahls von Daten bei Private Banking Kunden mit Domizil Ausland um ein Vielfaches grösser als bei Retailkunden mit Domizil Schweiz. Die wesentlichen Pflichten gemäss FINMA würden sämtliche CID in gleicher Weise treffen. Damit kann der im Risikomanagement anerkannte und bewährte Grundsatz des risiko-basierten Ansatzes kaum zum Tragen kommen. Dies generiert massive Mehraufwendungen und -kosten, denen kein klar erkennbarer Zusatznutzen gegenübersteht.

2.3 Prinzipien-basierter Ansatz

2.3.1 Prinzipien-basierter Ansatz als Leitmotiv

Der vorgelegte Rundschreiben-Entwurf geht von der Prämisse aus, dass sich der Umgang mit elektronischen Kundendaten systemtechnisch durch Schaffung detaillierter Vorschriften regeln lässt. Diese Prämisse kollidiert unseres Erachtens mit weit verbreiteter Praxis. Die Bearbeitung von und der Umgang mit Kundendaten ist im täglichen Bankgeschäft so vielfältig, dass ein starres und bis ins letzte Detail geregeltes System unweigerlich an seine Grenzen stossen wird. Jedes Finanzinstitut ist im Einzelnen unterschiedlich strukturiert und organisiert (z.B. mit Bezug auf Kundensegmente, Märkte, IT-Systeme, Datenhaltung, Verantwortlichkeiten).

Innerhalb des an sich klaren gesetzlichen Rahmens und damit unter Anwendung von Grundsätzen wie „Need to know“ oder „Schutz der Daten entsprechend ihrem Sensitivitätsgrad“ ist deshalb jedes Finanzinstitut berechtigt, die Anforderungen adaptiert auf seine eigenen konkreten Verhältnisse umzusetzen. Zur Einhaltung der entsprechenden Grundsätze ist jedes Finanzinstitut aufgrund der schweizerischen Datenschutz- und Bankengesetzgebung bereits heute schon verpflichtet. Um die notwendige Flexibilität bei der Umsetzung auf Institutsebene zu gewährleisten, verwendet die schweizerische Datenschutzgesetzgebung bewusst offene Begriffe (z.B. „überwiegendes Interesse der bearbeitenden Person“).

Derart detaillierte Vorgaben wie im vorgeschlagenen Entwurf vorgesehen, sind weder erforderlich, verhältnismässig noch zielführend. Detailregelungen können zudem den institutsspezifischen Ermessensspielraum bei der Umsetzung der datenschutz- und bankenrechtlichen Vorgaben in unerwünschter Weise einschränken. Als Beispiel kann hier der in Randziffer 24* aufgeführte „Need to know“-Grundsatz genannt werden. Die Nennung des Grundsatzes genügt; weiterer Ausführungen bedarf es nicht. Unnötige Detailregelungen beinhalten das Risiko, dass bereits bestehende Lösungen, welche sogar besser und für die Zielerreichung geeigneter sind als die vorgeschlagenen Ansätze, mit viel Aufwand umgebaut werden müssten, was geradezu kontraproduktiv wäre. Ausserdem muss berücksichtigt werden, dass verschiedene Banken (v.a. Auslandbanken) nur begrenzt Einfluss auf die technischen Systeme bzw. die Systemumgebung nehmen können, da diese auf Konzernstufe festgelegt und betrieben werden. Es ist deshalb notwendig, dass sich die Vorgaben am Resultat und nicht am Mittel orientieren.

Mit der Wahl eines prinzipien-basierten Ansatzes ist insbesondere auch gewährleistet, dass bei der Umsetzung der Grundsätze künftige technische und rechtliche Entwicklungen angemessen berücksichtigt werden können. Einer Detailregelung fehlt es gerade in dieser Hinsicht an Flexibilität. Die Regelung des Umgangs mit elektronischen Kundendaten sollte sich dabei an anderen FINMA Rundschreiben orientieren, die wesentlich generischer gehalten sind und von Detailregelungen absehen. Ein gutes Beispiel einer prinzipien-basierten Regulierung liefert das RS 2008/7 „Outsourcing Banken“.

2.3.2 Kategorisierung von Kundenidentifikationsdaten

Die in Randziffer 67* vorgenommene Auflistung von CID-Kategorien (direkt / indirekt / potentiell indirekt) ist nicht klar und die Abgrenzung teilweise schwierig (insbesondere

zwischen den Kategorien B und C). Auch ist nicht ersichtlich, ob es nach diesem Ansatz überhaupt noch Angaben zu Kunden geben kann, welche nicht als CID zu klassifizieren sind. Der Grund der Zuordnung der einzelnen Daten zu den jeweiligen Kategorien ist zudem nicht immer nachvollziehbar. So können z.B. gewisse der Kategorie C zugeordnete Daten von hoher persönlichkeitsrechtlicher Relevanz sein und damit einen höheren Schutzgehalt rechtfertigen. Darüber hinaus macht eine Kategorisierung von CID nur Sinn, wenn auch der Verwendungszweck der einzelnen Kategorien bzw. die daraus resultierenden Schlussfolgerungen klar definiert sind. Zu bedenken ist hier auch, dass eine derartige Kategorisierung zu massiven Eingriffen in die bestehenden IT-Strukturen und Systeme der betroffenen Institute und gegebenenfalls sogar zu einem Rückbau bewährter Sicherheitsarchitekturen führen kann.

Wir sind daher der Ansicht, dass es jedem Institut selbst überlassen sein muss, die Anzahl und Art von Kategorien, die Frage nach der Aufnahme von CID in die Kategorisierung und die eigentliche Kategorisierung der CID festzulegen und zu beantworten. Wir bitten Sie daher, in Randziffer 67* klarzustellen, dass es sich bei der aufgeführten Liste lediglich um unverbindliche Beispiele handelt. Hierzu müsste zumindest der Satzteil „zu berücksichtigen sind“ gestrichen wird. Ebenso wäre Randziffer 12* entsprechend anzupassen.

2.3.3 Geltungsbereich

Die für kleinere Banken vorgesehenen Ausnahmeregelungen (Rz 2*) sind nicht schlüssig. So ist beispielsweise nicht nachvollziehbar, weshalb ein kleineres Institut vom „Need to know“-Grundsatz (Rz 24*) ausgenommen werden sollte, zumal es sich hier um ein vom Datenschutz gefordertes Grundprinzip handelt. Mit der Errichtung eines prinzipien-basierten Grundsatzkatalogs würde auch für dieses Problem Abhilfe geschaffen werden, da damit die Umsetzung der Grundsätze institutsspezifisch und der Grösse und Struktur des Instituts angepasst erfolgen kann.

2.3.4 Aufwand und Kosten

Müssen die Grundsätze in dieser Form tatsächlich umgesetzt werden, wird der zeitliche und kostenseitige Aufwand sowohl auf technischer wie auch auf personeller Seite massiv sein. Zahlreiche bewährte Prozesse müssten umgebaut werden, was mit Blick auf die weiteren aktuellen Regulierungsvorhaben zu einer erheblichen Zusatzbelastung der Ressourcen der Banken führen würde.

2.4 Formelles und Begrifflichkeiten

Die Grundsätze sollten keine abweichenden Definitionen von Begriffen vornehmen, die bereits in anderen Rechtstexten enthalten sind (beispielsweise in Rz 54* in Bezug auf das RS 2008/7 „Outsourcing Banken). Besser wäre es, wenn in solchen Fällen auf die bestehenden Definitionen in den entsprechenden Regulierungen verwiesen würde.

Im Glossar (Rz 60* ff.) fehlen aussagekräftige Definitionen zu den verwendeten Begriffen (wie z.B. der Begriff „Massen-CID“). Dadurch ergeben sich aus den Vorgaben Auslegungsfragen. 16

Im Sinne einer einfacheren Lesbarkeit und Abgrenzung von Rundschreiben und Anhängen würden wir vorschlagen, die Anhänge zusätzlich zur Nummerierung mittels dem Buchstaben A zu kennzeichnen und die Randziffern in den drei Anhängen damit in Verbindung zu bringen. Randziffer 8* von Anhang 3 betreffend CID würde dann künftig “A3.8“ heissen.

2.5 Umsetzbarkeit der technischen Vorgaben

In Ergänzung zu unserem Hauptstandpunkt, wonach auf die Detailregelungen verzichtet werden sollte, möchten wir betreffend die Umsetzbarkeit der in Anhang 3 formulierten Anforderungen auf systemtechnischer Ebene folgende Bemerkungen zu einzelnen Vorgaben anbringen:

- Randziffer 24* ff., „Need to know“-Grundsatz:
  Mit gängigen IT-Lösungen für Schweizer Banken könnten die Anforderungen, wie sie z.B. in Rz 25* aufgeführt sind, heute nicht umgesetzt werden. Die IT-Lösungen müssten die Applikation erweitern und dabei sicherstellen, dass diese Logik auch bei den Umsystemen bzw. der restlichen Systemumgebung umgesetzt wird. Die Art und Weise, wie Zugriffsrechte vergeben werden, ist sehr unterschiedlich in den diversen Instituten, weshalb von einer Detailregelung abzusehen ist.
- Randziffer 30*, Schutz auf dem Endgerät:
  Diese Anforderung würde zwangsläufig dazu führen, dass jede Bank eine „Data Leakage Protection“ (DLP) - Lösung einführen muss, die sehr teuer ist.
- Randziffer 43*, Risikoidentifizierung und -kontrolle in Bezug auf CID-Vertraulichkeit:
  Der Grundsatz sollte dahingehend ergänzt werden, dass die Risikoidentifizierung und -kontrolle abhängig vom Tätigkeitsprofil und der Risikosituation des jeweiligen Finanzinstituts erfolgen sollte.
- Randziffer 47*, Produktionsumfeld, Aktivitäten in Verbindung mit Massen-CID:
  Hier wäre der Begriff „Aktivitäten“ zu präzisieren, da in dieser Form nicht klar ist, welche Tätigkeiten darunter fallen.
- Randziffer 48*, Tests für die Entwicklung, Veränderungen und Migration von Systemen:
  Auch hier ist nicht klar, was genau gemeint ist. So können beispielsweise die Daten bei einer Migration nicht anonymisiert oder verschlüsselt werden. Darüber hinaus wäre auszuführen, was unter „strikter Vieraugenkontrolle“ zu verstehen ist.
- Randziffer 59*, Ausgestaltung der Kontrollen und Wirksamkeitstests:
  Für die Überwachung der externen Dienstleister müssten Log-Protokolle (“Log-Files“) erzeugt und gesammelt werden. Es müssten Hilfsmittel für die automatischen Log-Auswertungen / Alerts eingeführt werden. Dafür würden auch personelle Ressourcen für die fortlaufende Überwachung benötigt, was wiederum hohe Kosten zur Folge hätte.

Zum Anhang 3 haben Sie die Frage nach einer Ausweitung des Anwendungsbereiches des Rundschreibens auf natürliche Personen, deren Geschäftsbeziehungen im Ausland betreut oder geführt werden, bzw. auf juristische Personen gestellt. Diese Fragen können wir folgendermassen beantworten:

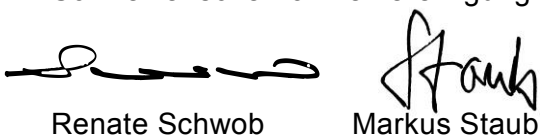
- Eine Ausweitung auf natürliche Personen, deren Geschäftsbeziehungen im Ausland betreut werden, erachten wir nicht als notwendig, da die lokalen Datenschutzbestimmungen grundsätzlich genügend sind. Zudem geht das vor Ort geltende zwingende Recht ohnehin einer allfälligen schweizerischen Regelung vor.
- Juristische Personen sind bereits heute ausreichend durch die einschlägigen Bestimmungen der Datenschutzgesetzgebung geschützt. Eine Ausweitung des Anwendungsbereichs von Anhang 3 ist daher weder notwendig noch sinnvoll.

* * *

Da unsere Stellungnahme sowohl zu den qualitativen Anforderungen als auch zum Umgang mit vertraulichen Kundendaten viele und zum Teil grundlegende Kommentare und Anpassungsvorschläge enthält, würden wir es sehr begrüssen, wenn die FINMA die betroffenen Kreise nach der Auswertung der Anhörung und der Überarbeitung ihres Rundschreiben-Entwurfes zumindest mündlich nochmals informieren und über die wichtigsten Anpassungen anhören würde.

Wir bedanken uns für die wohlwollende Prüfung unserer Kommentare und Anliegen. Für allfällige Rückfragen oder eine vertiefte Erörterung unserer Stellungnahme stehen wir Ihnen selbstverständlich jederzeit gerne zur Verfügung.

Freundliche Grüsse
Schweizerische Bankiervereinigung



Renate Schwob Markus Staub

Securities Services

Eidgenössische Finanzmarktaufsicht FINMA
Alessandro Lana
Einsteinstrasse 2
CH-3003 Bern

SIX Securities Services AG
Brandschenkestrasse 47
CH-8002 Zurich

Mailing address:
P.O. Box 1758
CH-8021 Zurich

T +41 58 399 4311
F +41 58 499 4311
www.six-securities-services.com

Contact person:
Marcel Schühle
T +41 58 399 4828
marcel.schuehle@six-group.com

Zurich, 1. Juli 2013

Anhörung betreffend FINMA-RS 2008/21 “Operationelle Risiken Banken“ - Teilrevision

Sehr geehrter Herr Lana

Wir danken Ihnen für die Möglichkeit, uns im Rahmen der Anhörung betreffend dem Rundschreiben zu den operationellen Risiken bei Banken einbringen zu können. Dieser Einladung kommt SIX Securities Services AG gerne nach.
Unsere Anmerkungen beziehen sich in diesem Schreiben auf den neuen Anhang 3.

Anhang 3, Grundsatz 2, Abs. c, Ziffer 13/14
Die Definition der CID (client identifying data) Verantwortung über den gesamten Lebenszyklus als Forderung an einer Stelle anzusiedeln ist unseres Erachtens zu weitreichend.
Es ist nachvollziehbar, dass die Verantwortlichkeiten für alle Aktivitäten definiert werden müssen. Ob diese an einer Stelle zu zentralisieren sind oder nicht, ist jedoch weitgehend abhängig von der Organisation und stellt unseres Erachtens keine inhärente Notwendigkeit dar.

Anhang 3, Grundsatz 3, Abs. a, Ziffer 16
Die Forderung nach Inventarisierung resp. Zuordnung von Backups zu CID ist vielfach nicht möglich, da Backupsysteme teilweise mit chaotischer Verteilung der Daten auf andere Medien arbeiten und es somit nicht mehr inventarisierbar ist, wo genau die Backups von welchen Daten sind.

Anhang 3, Grundsatz 3, Abs. c, Ziffer 25/26
Die Forderung nach "Need to know" sowie Definition der Verantwortlichkeit bzgl. der Erteilung der Rechte ist sinnvoll, allerdings sollte die Definition der Umsetzung den Banken überlassen sein. Zudem eröffnen sich in Zukunft vielleicht noch weitere Möglichkeiten der Kategorisierung resp. Zuordnung von Zugriffsrechten. Dadurch könnte die vorgesehene Regelung auf Umsetzungsbasis allenfalls sehr schnell veralten. Deshalb sollten Anforderungen grundsätzlich das Ziel definieren, nicht aber den konkreten Umsetzungsweg.

Anhang 3, Grundsatz 4, Abs. c, Ziffer 36
Die mit der Verschlüsselung auf Backup Medien verbundenen Probleme sollten hier berücksichtigt werden (z.B. Key Management, Software Lifecycle).

Anhang 3, Grundsatz 5, Abs. a, Ziffer 38

Eine Bank kann keine Prozesse von Dritten sicherstellen; sinnvollerweise kann und sollte eine Bank diese Pflichten entsprechen vertraglich festhalten und sich damit auch das Recht sichern, eine Einhalteprüfung bzgl. Erfüllung dieser Anforderungen durchführen zu dürfen.

Anhang 3, Grundsatz 5, Abs. c, Ziffer 39
Analog dem Kommentar zu Ziffer 38 erscheint uns auch hier eine vertragliche Regelung sinnvoll. Eine Schulung externer Dienstleister ist als eher unrealistisch einzustufen. Insbesondere wenn Dienstleister für mehrere Banken tätig sind, würde dies bedeuten, dass die entsprechenden Mitarbeiter bei jeder Bank eine Schulung besuchen müssten.

Anhang 3, Grundsatz 6 Ziffer 43
Die Forderung nach einer rollierenden CID beinhaltenden Risikoanalyse ist sicher sinnvoll. Es sollte aber jeder Organisation überlassen sein, welches die verantwortliche Stelle für deren Durchführung sein soll.

Anhang 3, Grundsatz 7, Abs. a, Ziffer 47
Das Vieraugenprinzip erscheint in diesem Zusammenhang als nicht anwendbar. Müsste es sich bei der Rechtevergabe nicht ausschliesslich um Leseberechtigungen handeln? Das Vieraugenprinzip wird im Normalfall zur Sicherstellung einer Gewaltentrennung eingeführt.
Eine Einführung des Vieraugenprinzips würde es ermöglichen resp. sogar erforderlich machen, dass mehr Personen als wirklich nötig auf die Daten zugreifen können, was im Widerspruch zur „Need-to-Know“- Forderung stünde.

Anhang 3, Grundsatz 7, Abs. b, Ziffer 48
Analog dem Kommentar zu Ziffer 47 stellt sich auch hier die Frage nach dem verfolgten Ziel einer Vieraugenkontrolle resp. es stellt sich die Frage, welches konkrete Risiko sich mit dieser Massnahme eindämmen liesse.

Anhang 3, Grundsatz 8, Abs. b, Ziffer 51
Vertraulichkeit per se ist kein Risiko. Das damit zusammenhängende Szenario wäre vielmehr "Verlust der Vertraulichkeit".

Anhang 3, Grundsatz 9, Abs. a, Ziffer 55
Es kann nicht zielführend sein, das oberste Management bzgl. jeder relevanten Änderung in Vertraulichkeitsstandards oder gar Lösungen zu informieren. Die Verantwortlichkeiten bzgl. CID sind festzulegen und diese regelmässig auf ihre Richtigkeit zu Prüfen. Sofern nicht grundlegende Veränderungen der e Anforderungen an CID erfolgen, ist die Verantwortung gem. vorangegangener Grundsätze definiert und es sollte der Organisation überlassen sein, auf welcher Stufe und mit welchen Prozessen sie diese wahrnehmen möchte. Zudem ist es sinnvoll, CID relevante Kriterien festzulegen und diese in die Evaluation von Dritten einzubeziehen, jedoch ist die Prüfung der entsprechenden Compliance eher als unrealistisch einzustufen. Wirkungsvoller wäre eine klare Anforderungen an den Umgang bezüglich Sicherheit von CID in die Verträge einzubeziehen - inklusive allfälligen Haftungsklauseln wie dies in Ziffer 57 beschrieben ist.

Anhang 3, Grundsatz 9, Abs. c, Ziffer 58
Gemäss Grundsatz 2 Ziffer 13&14 sind hierfür Data Owner zu bestimmen. Ob der Bereich ausgelagert ist oder nicht. ist bzgl. der Definition der Verantwortung unserer Ansicht nach irrelevant und daher teilweise (bzgl. der Definition der Verantwortlichkeiten) redundant zu den beiden genannten Ziffern unter Grundsatz 2.

Wir ersuchen das Eidgenössische Finanzdepartement höflich, unsere in dieser Stellungnahme aufgeführten Anliegen zu berücksichtigen. Für eine Besprechung oder bei allfälligen Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.
SIX Securities Services AG

Dr. Hansjörg Schief
Head DSS Risk Management

Marcel Schühle
Head IT Architecture & Security

TREUHAND KAMMER
Wirtschaftsprüfer · Steuerexperten

Eidgenössische Finanzmarktaufsicht FINMA
Alessandro Lana
Einsteinstrasse 2
3003 Bern

Zürich, 1. Juli 2013

Anhörung Teilrevision FINMA-RS 2008/21 „Operationelle Risiken Banken“

Sehr geehrter Herr Lana

Für die Zustellung der Anhörungsunterlagen danken wir Ihnen bestens. Gerne lassen wir Ihnen in der Beilage die von der Fachkommission Bankenprüfung der Treuhand-Kammer erarbeitete Stellungnahme zugehen.

Für Fragen stehen Ihnen die Herren Rolf Walker und Pascal Portmann gerne zur Verfügung.

Freundliche Grüsse
TREUHAND-KAMMER

Thorsten Kleibold
Mitglied der Geschäftsleitung

Rolf Walker
Präsident Fachkommission Bankenprüfung

Beilage

TREUHAND-KAMMER Schweizerische Kammer der Wirtschaftsprüfer und Steuerexperten
Limmatquai 120, Postfach 1477, CH-8021 Zürich, Tel. +41 44 267 75 75, Fax +41 44 267 75 85
info@treuhand-kammer.ch, www.treuhand-kammer.ch

(geänderte Rz des Rundschreibens: vorgeschlagene Änderungen in blauer Schrift)

Rz	Neuer Wortlaut	Bemerkungen
29	Jede Bank muss nach Massgabe von Anhang 1 spezifische Grundsätze zur Allokation von Geschäftsaktivitäten in die standardisierten Geschäftsfelder nach Rz 23 festlegen und dafür über dokumentierte Kriterien verfügen. Die Kriterien sind regelmässig zu überprüfen und müssen den jeweils aktuellen Veränderungen der Aktivitäten der Bank angepasst werden.	Wir empfehlen folgende Präzisierung im zweiten Satz: „Die Kriterien sind *durch das Institut* regelmässig zu überprüfen...“. Damit soll klargestellt werden, dass diese Tätigkeit in erster Linie durch die Bank zu erfolgen hat. Weiter empfehlen wir verbindlicher zu regeln, in welchen Zeitabständen die Überprüfung mindestens zu erfolgen hat. Vorschlag (Beispiel): „Die Kriterien sind *durch das Institut mindestens [jährlich / alle drei Jahre] sowie bei massgeblichen* Veränderungen *(Strategie, Geschäftsaktivitäten, Risikosituation usw.)* zu *überprüfen und an die aktuellen* Aktivitäten der Bank anzupassen.“
	IV. Qualitative Anforderungen	
	A. Proportionalitätsprinzip	
118	Kleine Banken im Sinne der Rz 117 sind: • Banken der FINMA-Kategorie[6] 5 • Effektenhändler der FINMA-Kategorie 4 und 5 • sowie in Einzelfällen Banken der FINMA-Kategorie 4, welche über Geschäftsaktivitäten ohne bedeutende Komplexität verfügen.	Wir begrüssen die Regelung des Proportionalitätsprinzips auf der Ebene des Rundschreibens. Zur Erhöhung der Rechtssicherheit und zur Gewährleistung der Gleichbehandlung der Institute ist im Rundschreiben noch zu klären, 1. wie eine „bedeutende Komplexität“ bei Banken der FINMA-Kategorie 4 zu definieren ist (einziges im Erläuterungsbericht genanntes Merkmal, welches zur Komplexität beiträgt, sind „Tätigkeiten im Ausland“); 2. welches Organ einer Bank der FINMA-Kategorie 4 die Beurteilung und den Entscheid über das Vorliegen bzw. Fehlen einer „bedeutenden Komplexität“ vorzunehmen hat; und 3. wann und wie die Klassifikation als „Bank der FINMA-Kategorie 4 ohne bedeutende Komplexität“ mit der FINMA abzustimmen ist.
	B. Qualitative Grundanforderungen	
	a) Grundsatz 1: Verantwortlichkeiten	
120	Das Organ für die Oberleitung, Aufsicht und Kontrolle (nachfolgend „Verwaltungsrat“) hat ein Rahmenkonzept für das Management von operationellen Risiken, insbesondere	Wir empfehlen ebenfalls verbindlicher zu regeln, in welchen Zeitabständen die Überprüfung mindestens zu erfolgen hat.

Rz	Neuer Wortlaut	Bemerkungen
	Festlegung von Risikobereitschaft und Risikotoleranz, zu genehmigen und regelmässig zu überprüfen. Dabei sind Art, Typ und Ebene der operationellen Risiken festzuhalten, welchen die Bank ausgesetzt ist und welche sie einzugehen bereit ist.	Die Erwartung betreffend der Dokumentation der operationellen Risiken nach „Art, Typ und Ebene“ ist nicht vollständig klar. Wir empfehlen die Anwendung von klar definierten Begriffen bzw. eine Erläuterung von nicht entsprechenden Begriffen in einem Anhang zum Rundschreiben.
121	Die Geschäftsführung hat dieses Rahmenkonzept zu entwickeln, in konkrete Vorgaben und Prozesse zu übertragen und anschliessend in den Geschäftseinheiten überprüfbar in den Risikomanagement-prozessen umzusetzen. Dabei sind Massnahmen vorzusehen, um Verletzungen der Risikobereitschaft und Risikotoleranz rechtzeitig zu erkennen und zu beheben.	Wir empfehlen, den Begriff „kontrollierbar“ anstelle von „überprüfbar“ zu verwenden.
122	Die Geschäftsführung definiert eine eindeutige, wirksame und solide Führungsstruktur, welche die Verantwortung zum Management der operationellen Risiken übernimmt. Diese Funktion ist für die Aufrechterhaltung und die laufende Weiterentwicklung des Rahmenkonzepts für das Management von operationellen Risiken zuständig. Sie muss zudem über genügend qualifiziertes Personal verfügen, um ihre zahlreichen Verantwortlichkeiten wirkungsvoll wahrnehmen zu können. Konsistent zu weiteren Risikomanagementfunktionen soll die Funktion des Management von operationellen Risiken adäquat in relevanten Gremien vertreten sein.	Rz 126 des FINMA-RS 08/24 „Überwachung und interne Kontrolle bei Banken“ weist das „Risikomanagement“ den „jeweils geeigneten organisatorischen Ebenen“ zu. Im Widerspruch dazu weist Rz 122 des FINMA-RS 08/21neu „die Verantwortung zum Management der operationellen Risiken“ einer „Funktion“ der Bank zu. Rz 122 RS 08/21neu spricht von „zahlreichen Verantwortlichkeiten“ der Funktion mit der Verantwortung zum Management der operationellen Risiken, was die Vermutung zulässt, dass auch jene in Rz 126 des FINMA-RS 08/24 damit gemeint sind. Wir empfehlen, in den RS eindeutiger zu klären, welche Verantwortlichkeiten für das Management der operationellen Risiken einer „Funktion“ und welche Verantwortlichkeiten für das Management der operationellen Risiken den „jeweils geeigneten organisatorischen Ebenen“ zuzuordnen sind.
		Nach unserem Verständnis des Aufgabenkatalogs in Rz 122 des FINMA-RS 08/21neu und des Aufgabenkataloges für die Risikokontrolle im bestehenden FINMA-RS 08/24 „Überwachung und interne Kontrolle bei Banken“ sind zwei voneinander getrennte Funktionen gefordert: a) Funktion für das Management der operationellen Risiken (Rz 122 RS 08/21neu)

Rz	Neuer Wortlaut	Bemerkungen
		b) Risikokontrolle (Rz 113-125 RS 08/24). Dies ist für grosse Banken (z.B. FINMA Kat. 2) durchaus sinnvoll, wichtig und umsetzbar. Wir empfehlen zu erwägen und im RS zu präzisieren, ob für kleinere Banken eine vollständige Funktionentrennung zwischen dem Management der operationellen Risiken und der Risikokontrolle erforderlich ist.
		Textliche Präzisierung: „Konsistent zu weiteren Risikomanagementfunktionen soll die Funktion des Management von operationellen Risiken adäquat in relevanten Gremien *der Bank* vertreten sein.“
	b) Grundsatz 2: Rahmenkonzept und Kontrollsystem	
125	Das Rahmenkonzept hat mindestens folgende Aspekte abzudecken: a. Strukturen für das Management der operationellen Risiken, einschliesslich Kompetenzen, Rechenschaftspflichten und Berichtslinien; b. Definition der Instrumente für die Identifikation, Messung, Beurteilung, Steuerung und Berichterstattung und ihrer Verwendung; c. Bestimmung der Risikobereitschaft und der Risikotoleranz in Bezug auf die relevanten Arten von operationellen Risiken; Festsetzung von Schwellenwerten und/oder Limiten; Definition von Risikominderungsstrategien und -instrumenten; d. Ansatz der Bank zur Identifikation von inhärenten Risiken (die Risiken vor Berücksichtigung der Kontrollen) sowie zur Festlegung und Überwachung von Schwellenwerten und/oder Limiten für Residualrisiken (die Risiken nach Berücksichtigung der Kontrollen); e. Etablierung von Risikoberichterstattungs- und Management-informationssystemen (MIS) für operationelle Risiken; f. Festlegung einer einheitlichen Klassifizierung von materiellen operationellen Risiken zur Gewährleistung der Konsistenz im Rahmen der Risikoidentifikation, der Risikobewertung und Zielsetzung im operativen Risikomanagement;[8]	Wir empfehlen folgende textliche Anpassungen: b. Definition der Instrumente für die Identifikation, Messung, Beurteilung, Steuerung und Berichterstattung *von operationellen Risiken und* ihrer Verwendung; f. Festlegung einer einheitlichen Klassifizierung von materiellen operationellen Risiken zur Gewährleistung der Konsistenz im Rahmen der Risikoidentifikation, der Risikobewertung und ~~*Zielsetzung*~~ *der Berichterstattung* im operativen Risikomanagement;[8] *h.* Pflicht zur…

Rz	Neuer Wortlaut	Bemerkungen
	g. Sicherstellung einer angemessenen unabhängigen Überprüfung und Beurteilung der operationellen Risiken; Pflicht zur zeitnahen Überprüfung und Anpassung des Rahmenkonzepts im Falle einer wesentlichen Veränderung der Risikosituation.	
	d) Grundsatz 4: Interne und Externe Berichterstattung	
130	Die interne Berichterstattung über operationelle Risiken kann Finanz-, Betriebs- und Compliance-Daten, aber auch risikorelevante externe Informationen über Ereignisse und Bedingungen umfassen, die für die Entscheidungsfindung wesentlich sind. Die Berichterstattung über operationelle Risiken muss dabei mindestens folgende Punkte abdecken und deren mögliche Auswirkungen auf die Bank und das für die operationellen Risiken erforderliche Eigenkapital darstellen: a. Verstösse gegen die definierte Risikobereitschaft und die Risikotoleranz der Bank sowie Überschreitungen von diesbezüglich festgesetzten Schwellenwerten und/oder Limiten bei relevanten Arten von operationellen Risiken; b. Einzelheiten zu signifikanten internen operationellen Risikoereignissen und/oder Verlusten; c. Informationen zu relevanten externen Ereignissen und potentiellen Risiken sowie deren mögliche Auswirkungen auf die Bank.	Wir empfehlen folgende textliche Anpassung: Die interne Berichterstattung über operationelle Risiken ~~*kann*~~ *sollte* Finanz-, Betriebs- und Compliance-Daten, aber auch risikorelevante externe Informationen über Ereignisse und Bedingungen umfassen, die….
131	Eine Bank muss über eine formelle, vom Verwaltungsrat genehmigte Offenlegungspolitik verfügen. Aus dieser muss hervorgehen, welchen Ansatz die Bank im Rahmen der Offenlegung der operationellen Risiken verfolgt und welche Kontrollprozesse bezüglich der Offenlegung anzuwenden sind. Zudem ist ein Prozess zu implementieren, der die Angemessenheit bezüglich Inhalt und Frequenz der Offenlegungen sicherstellt und deren regelmässige Überprüfung regelt.	Wir empfehlen erneut verbindlicher zu regeln, in welchen Zeitabständen die Überprüfung mindestens zu erfolgen hat.
	e) Grundsatz 5: Technologieinfrastruktur	
133	Zur Unterstützung des Management operationeller Risiken hat	In der Informatik-Fachliteratur wird der Begriff „Sicherheit“ als

Rz	Neuer Wortlaut	Bemerkungen
	die Geschäftsführung insbesondere für eine angemessene Technologieinfrastruktur[12] zu sorgen, die den aktuellen und längerfristigen Geschäftsbedürfnissen Rechnung trägt. Zu diesem Zweck hat sie ausreichende Kapazitäten bereitzustellen, die sowohl den üblichen Geschäftsbetrieb als auch Stressphasen abdecken. Überdies hat sie die Sicherheit, Integrität und Verfügbarkeit der Daten und Systeme zu gewährleisten sowie ein integriertes und umfassendes Risikomanagement zu implementieren.	Oberbegriff für „Vertraulichkeit, Verfügbarkeit und Integrität“ verwendet (vgl. z.B. http://security.practitioner.com/introduction/infosec_2.htm). Wir empfehlen den letzten Satz daher wie folgt zu formulieren: „Überdies hat sie die Sicherheit *(Vertraulichkeit, Integrität und Verfügbarkeit)* der Daten und Systeme zu gewährleisten sowie ein integriertes und umfassendes Risikomanagement zu implementieren.“
	V. Prüfung und Beurteilung durch die Prüfgesellschaften	
137	Die Prüfgesellschaften prüfen die Einhaltung dieses Rundschreibens nach Massgabe des FINMA-RS 13/3 „Prüfwesen“ und halten das Ergebnis ihrer Prüfungshandlungen im Prüfbericht fest.	In den Anhängen 1 und 2 des FINMA-RS 13/3 „Standardprüfstrategie – Banken / Effektenhändler“ ist das RS 08/21 lediglich im Prüffeld „Eigenmittelanforderungen und -Planung“ erwähnt. Die Prüfung der qualitativen Anforderungen an das Management der operationellen Risiken (Rz 117-136 FINMA-RS 08/21neu) sowie die Prüfung des Umgangs mit elektronischen Kundendaten (Anhang 4 des FINMA-RS 08/21neu) passen thematisch nicht zu jenem Prüffeld. Wir regen an, die Prüfung der qualitativen Anforderungen an das operationelle Risikomanagement im Prüffeld „Zentrale Funktionen zur Risikokontrolle und Risikominderung“ vorzusehen, damit eine Prüfung im Kontext des in diesem Prüffeld ebenfalls genannten FINMA-RS 08/24 gewährleistet ist. Weiter regen wir an, die Prüfung des Umgangs mit elektronischen Kundendaten im Prüffeld „Interne Organisation, internes Kontrollsystem, Informatik (IT)“ vorzusehen, da ein enger Zusammenhang zur Informatik besteht.
	Anhang 3: Umgang mit elektronischen Kundendaten	
1	In diesem Anhang werden Grundsätze und die dazugehörigen Ausführungen für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten natürlicher Personen („Privatkunden“), deren	Einige Privatkunden unterhalten ihre Geschäftsbeziehungen nicht direkt mit den Banken sondern mittels Sitzgesellschaften, Domizilgesellschaften, Stiftungen, Trusts oder anderer Rechtsformen, welche nicht als „natürliche Personen“ gelten. Es ist

Rz	Neuer Wortlaut	Bemerkungen
	Geschäftsbeziehungen in oder von der Schweiz aus betreut oder geführt werden („Kundendaten“), formuliert. 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. Die einschlägigen rechtlichen Bestimmungen finden sich nicht nur im Aufsichtsrecht, sondern auch im Datenschutzrecht und Zivilrecht.	nicht eindeutig klar, ob diese Kunden vom Anhang 3 „Umgang mit elektronischen Kundendaten“ erfasst werden. Wir empfehlen eine entsprechende Präzisierung.
5	Für alle beteiligten Funktionen und Standorte müssen die Verantwortlichkeiten geregelt sein und klare Eskalationsstrukturen geschaffen werden. Insbesondere die Festlegung der Verantwortlichkeiten und ihre Zuteilung an Front-Office-, IT- und Kontrollfunktionen sind von der Geschäftsführung zu definieren und vom Verwaltungsrat zu genehmigen. Die Geschäftsführung informiert den Verwaltungsrat regelmässig über die Wirksamkeit der eingeführten Kontrollen.	Wir empfehlen erneut verbindlicher zu regeln, in welchen Zeitabständen die Information mindestens zu erfolgen hat.
6	Es wird erwartet, dass ein formales und umfassendes Rahmenkonzept von Aktivitäten, Prozessen und Systemen zur Datenvertraulichkeit besteht, dessen Struktur der Grösse und Komplexität der Bank Rechnung trägt. Dieses Rahmenkonzept muss in allen Funktionsbereichen und Einheiten, die auf Kundendaten zugreifen oder diese bearbeiten, konsistent umgesetzt werden.	Wir nehmen zur Kenntnis, dass im Anhang 3 bewusst zugunsten allgemeiner Grundsätze auf eine explizite Regelung der konkret zu treffenden Massnahmen und deren Häufigkeit verzichtet wurde, um den Banken die Definition von risikoorientierten und situationsgerechten Lösungen zu ermöglichen. Wir weisen darauf hin, dass die in Rz 6 des Anhangs 3 geforderten Rahmenkonzepte und deren Einhaltung nur geprüft werden können, sofern die Institute ihre Konzepte (insbes. Massnahmen und dazugehörige Häufigkeiten) konkretisieren. Wir empfehlen folgende textliche Ergänzung: *„Die Massnahmen und die Periodizität deren Durchführung sind aufgrund der Risikoeinschätzung und der Risikotoleranz der Banken schriftlich, nachvollziehbar und verbindlich festzulegen.“*

Rz	Neuer Wortlaut	Bemerkungen
7	Die Implementierung und Einhaltung des Rahmenkonzepts zur Vertraulichkeit von Kundendaten ist durch den Verwaltungsrat zu überwachen und muss durch regelmässige Kontrollen der für Datensicherheit und -vertraulichkeit zuständigen Einheit sichergestellt werden.	Wir empfehlen, die Mindestintervalle dieser Kontrollen klarer zu regeln. Konsequenterweise sollte ferner von „*der für Datenvertraulichkeit zuständigen Einheit*“ anstelle von „der für Datensicherheit und -vertraulichkeit zuständigen Einheit“ gesprochen werden, da im Anhang zu diesem RS der Fokus auf der Datenvertraulichkeit und nicht auf der Datensicherheit insgesamt gelegt wird.
15	Die Bank muss wissen, wo CID gespeichert werden, von welchen Anwendungen und IT Systemen CID verarbeitet werden und wo elektronisch auf sie zugegriffen werden kann. Mittels angemessenen Kontrollen ist sicherzustellen, dass die Daten nach Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz bearbeitet werden. Für physische Bereiche (z.B. Serverräume) oder Netzwerkzonen, in denen grosse Mengen an CID gespeichert oder zugänglich gemacht werden, sind spezielle Kontrollen erforderlich. Der Datenzugriff muss klar geregelt werden und darf nur auf einer strikten „Need to know“-Basis erfolgen.	Die Feststellung „sind spezielle Kontrollen erforderlich“ sollte klarer als Anforderung formuliert und mittels Kriterien versehen werden, worauf die Kontrollen auszurichten sind, z.B. „Für physische Bereiche (z.B. Serverräume) oder Netzwerkzonen, in denen grosse Mengen an CID gespeichert oder zugänglich gemacht werden, sind spezielle *risikoadäquate* Kontrollen *umzusetzen*.“
17	Es wird erwartet, dass die Granularität des Inventars es der Bank erlaubt, zu ermitteln:	Wir empfehlen die Rz 17, 18 und 19 vorzugsweise in einer gemeinsamen Rz zu erfassen.
20	Falls CID ausserhalb der Schweiz gespeichert werden oder vom Ausland aus auf sie zugegriffen wird (z.B. aufgrund einer Auslagerung spezifischer Aktivitäten innerhalb der Unternehmensgruppe oder an externe Dritte), sind die damit verbundenen erhöhten Risiken in Bezug auf den Kundendatenschutz angemessen zu begrenzen.[20] CID müssen angemessen geschützt (anonymisiert, verschlüsselt oder pseudonymisiert) werden. Es sind die folgenden Massnahmen zu ergreifen:	*Generelle Bemerkungen zu Rz 20-23* Die Prüfung der Einhaltung der Vorgaben ist sehr anspruchsvoll, insbesondere ob die Daten im Ausland keine Rückschlüsse auf die Identität des Kunden zulassen. Die vom Anhang 3 erfassten Geschäftsbeziehungen mit Auslandsbezug sind vom ausdrücklichen Nachweis der Prüfmöglichkeiten im Ausland abhängig zu machen. Die Bank muss nachweisen können, dass sowohl sie selber wie auch ihre banken- oder börsengesetzliche Prüfgesellschaft sowie die FINMA ihre Prüfaufgaben im Ausland wahrnehmen und rechtlich auch durchsetzen können. Dieser Nachweis kann z.B. mittels Rechtsgutachten oder Bestätigungen einer entsprechenden Aufsichtsbehörde erbracht werden. Mit dem Verweis auf das FINMA-RS 08/7 „Outsourcing Banken“ wird
21	- Schutzvorkehrungen, ihre Implementierung und Anwendung müssen sachgerecht erfolgen;	
22	- Die Anwendung von Schutzvorkehrungen ist durch die Festlegung von Schlüsselkontrollen, die regelmässig überprüft werden, zu überwachen;	

Rz	Neuer Wortlaut	Bemerkungen
23	- Die Kunden sind detailliert mittels besonderem Schreiben über die Auslagerung spezifischer Aktivitäten innerhalb der Gruppe oder an externe Dritte, die im Ausland durchgeführt werden, zu informieren und auf die getroffenen Vorkehrungen zum Schutz der Vertraulichkeithinzuweisen. Lassen die ausserhalb der Schweiz verfügbaren Daten keine Rückschlüsse auf die Identität der betroffenen Kunden zu, so entfällt diese Pflicht. In diesem Fall sind die allgemeinen Anforderungen zur Information über ausgelagerte Aktivitäten im Sinne der Grundsätze 5 und 6 des FINMA-RS 08/7 „Outsourcing Banken“ ausreichend.	leider nach wie vor keine Rechtssicherheit bezüglich des Einsatzes von Verschlüsselung gegeben. Es ist nach wie vor unklar, ob Verschlüsselung als Sicherheitsmassnahme akzeptiert wird, um die Kunden über das Outsourcing ins Ausland nicht informieren zu müssen. Diese fehlende Klarheit führt in der Praxis zu unterschiedlichsten Lösungen, ohne Gewähr, dass die gewählten Lösungen aus regulatorischer Sicht als angemessen erachtet werden. Wir empfehlen, diesen Sachverhalt im Rundschreiben zu regeln. Weiter empfehlen wir, die Rz 20 - 23 vorzugsweise in einer gemeinsamen Rz zu erfassen.
20	Falls CID ausserhalb der Schweiz gespeichert werden oder vom Ausland aus auf sie zugegriffen wird (z.B. aufgrund einer Auslagerung spezifischer Aktivitäten innerhalb der Unternehmensgruppe oder an externe Dritte), sind die damit verbundenen erhöhten Risiken in Bezug auf den Kundendatenschutz angemessen zu begrenzen.20 CID müssen angemessen geschützt (anonymisiert, verschlüsselt oder pseudonymisiert) werden. Es sind die folgenden Massnahmen zu ergreifen:	Die Formulierung „müssen angemessen geschützt (anonymisiert, verschlüsselt oder pseudonymisiert) werden“ begrenzt die Mittel des angemessenen Schutzes auf die drei abschliessend aufgezählten Schutzvorkehrungen Anonymisierung, Verschlüsselung oder Pseudonymisierung, obwohl weitere Massnahmen für dieses Risiko denkbar sind. Die gewählte Formulierung begründet die Frage, ob die Banken eine der drei Schutzvorkehrungen zwingend umzusetzen haben. Wir bitten um eine klarere Formulierung, allenfalls durch Ergänzung von „z.B.“ am Anfang dieser Klammer.
22	- Die Anwendung von Schutzvorkehrungen ist durch die Festlegung von Schlüsselkontrollen, die regelmässig überprüft werden, zu überwachen;	Die gleichzeitige Verwendung der Begriffe „Schutzvorkehrung“, „Schlüsselkontrollen“, „überprüft“ sowie „überwachen“ im gleichen Satz kann zu Verwirrung bezüglich der Bedeutung dieses Satzkonstrukts führen. Der Begriff „regelmässig“ ist unpräzise. Vorschlag für eine textliche Anpassung: *„Die Anwendung von Schutzvorkehrungen ist durch die Festlegung von Schlüsselkontrollen zu kontrollieren. Die Angemessenheit der Schlüsselkontrollen ist von der Geschäftsführung oder einer von ihr bezeichneten Stelle mindestens alle [jährlich / alle 3 Jahre oder bei massgeblichen Anpassungen der Prozesse] zu kontrollieren.“*
24	Personen dürfen nur auf diejenigen Informationen oder Funktionalitäten Zugriff haben, die für die Wahrnehmung ihrer Aufgaben erforderlich sind. Der Zugriff auf CID darf nur	Wir empfehlen, die Rz 24 - 26 vorzugsweise in einer gemeinsamen Rz zu erfassen.

Rz	Neuer Wortlaut	Bemerkungen
	erfolgen, wenn die CID verantwortlichen Einheiten (*„Data Owners“)* die Zugriffsrechte genehmigt haben. Die Erteilung von Zugriffsrechten hat wie folgt zu erfolgen*:*	
27	Die Erteilung von Zugriffsrechten muss regelmässig überprüft werden.	Wir empfehlen, den Begriff „kontrolliert“ anstelle von „überprüft“ zu verwenden. Weiter empfehlen wir, die Mindestanforderung an die Periodizität der Kontrolle klarer zu regeln.
28	Die Bank muss ein Verzeichnis der Mitarbeitenden und Dritten, die Zugriffsberechtigungen auf CID haben, führen. Im Verzeichnis müssen auch privilegierte IT-Benutzer und Anwender aufgeführt sein (siehe Rz 41 dieses Anhangs). Nur Personen welche im Verzeichnis aufgeführt sind, dürfen auf CID zugreifen.	Die Formulierung der Anforderung dürfte dazu führen, dass letztlich beinahe alle oder zumindest eine Vielzahl der Mitarbeitenden einer Bank in einem solchen Verzeichnis geführt werden müssen. Der konkrete Nutzen dieser Massnahme kann sicher in Frage gestellt werden.
29	Vorkehrungen, wie z.B. das Führen von Log-Dateien, müssen eingeführt werden, um die Identifizierung von Benutzern, die auf Massen-CID zugegriffen haben, zu ermöglichen.	Die Umsetzung dieser Anforderung dürfte für viele Institute eine Herausforderung aus technischer Sicht darstellen, da gemäss Formulierung auch alle Lese-Zugriffe auf (Massen-)Kundendaten aufgezeichnet werden müssen.
30	Die zum Schutz der CID-Vertraulichkeit verwendeten Sicherheitsstandards für die Infrastruktur und Technologie müssen in Bezug auf die Komplexität der Bank sowie seiner Risikoexposition angemessen sein und den Schutz von CID auf dem Endgerät (am Endpoint), von übertragenen und gespeicherten CID sicherstellen. Da die Informationstechnologien schnellen Änderungen unterliegen, ist die Entwicklung von Datensicherheitslösungen aufmerksam zu verfolgen. Lücken zwischen dem bestehenden internen Rahmenkonzept zur Sicherstellung der Vertraulichkeit von Kundendaten und der Marktpraxis sind regelmässig zu beurteilen.	Wir empfehlen, die Mindestanforderung an die Periodizität der Beurteilung klarer zu regeln.
32	Die Sicherheitsstandards bilden einen festen Bestandteil des Rahmenkonzept zur Sicherstellung der Vertraulichkeit von Kundendaten. Es wird erwartet, dass sie regelmässig mit der Marktpraxis verglichen werden, um potenzielle	Wir empfehlen, die Mindestanforderung an die Periodizität des Abgleichs verbindlicher zu regeln. Den letzten Satz empfehlen wir wie folgt zu präzisieren *„Auch Erkenntnisse aus unabhängigen Kontrolltätigkeiten sowie*

Rz	Neuer Wortlaut	Bemerkungen
	Sicherheitslücken zu ermitteln. Auch externe Inputs in Form von unabhängigen Überprüfungen und Prüfberichte müssen berücksichtigt werden.	*Prüfberichten z.B. der internen Revision und der Prüfgesellschaft* müssen berücksichtigt werden.“
33	Um die Vertraulichkeit von CID sicherzustellen, muss die Bank Schutzmassnahmen (z.B. Verschlüsselung) prüfen und diese soweit erforderlich auf den folgenden Ebenen umsetzen:	Wir empfehlen, den Begriff „prüfen“ durch „abwägen“ zu ersetzen. Die Formulierung „soweit erforderlich“ erlaubt, nach eingehender Abwägung zum Schluss zu kommen, dass keine Schutzmassnahmen erforderlich sind – ist dies so beabsichtigt? Wir empfehlen die Rz 33 - 36 vorzugsweise in einer gemeinsamen Rz zu erfassen.
40	Die Bank muss über klare Sicherheitsanforderungen für Mitarbeiter, 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. Ihnen ist besondere Aufmerksamkeit zu schenken.	Wir empfehlen, die Mindestanforderung an die Periodizität der Kontrolltätigkeit verbindlicher zu regeln.
41	Als Ergänzung zu den allgemeinen Anforderungen in Bezug auf Mitarbeitende mit Zugriff auf CID (siehe Rz 28) wird von der Bank die Führung und laufende Aktualisierung einer Liste mit den Namen aller internen und externen privilegierten IT-Benutzer und Anwender (Schlüsselmitarbeitenden) erwartet, die Zugriff auf Massen-CID haben und/oder denen Verantwortlichkeiten hinsichtlich der Kontrolle und Überwachung der Vertraulichkeit von Kundendaten übertragen wurden. Die Identität von privilegierten IT-Benutzern und Anwendern muss dem lokal oder gesamthaft verantwortlichen obersten Management bekannt sein.	Wir empfehlen den Begriff „oberstes Management“ zu präzisieren, z.B. „Geschäftsführung“ oder „Geschäftsleitung“.
43	Die für die Datensicherheit und -vertraulichkeit zuständige Einheit identifiziert und bewertet die inhärenten Risiken und die Residualrisiken betreffend die Vertraulichkeit von CID mithilfe eines strukturierten Prozesses. Dieser Prozess muss die Risikoszenarien in Bezug auf die CID-Vertraulichkeit	Erneut sollte von „der für Datenvertraulichkeit zuständigen Einheit“ anstelle von „der für Datensicherheit und -vertraulichkeit zuständigen Einheit“ gesprochen werden, da der der Fokus dieses RS auf der Datenvertraulichkeit und nicht auf der Datensicherheit insgesamt gelegt wird.

Rz	Neuer Wortlaut	Bemerkungen
	umfassen, die für die Bank und die Definition der entsprechenden Schlüsselkontrollen relevant sind. Der Katalog der Schlüsselkontrollen in Bezug auf die Datenvertraulichkeit zur Gewährleistung des CID-Schutzes muss laufend um neue und verbesserte Kontrollen aktualisiert werden	
45	Die Definition von Risikoszenarien und entsprechenden Schlüsselkontrollen in Bezug auf die Vertraulichkeit von CID muss der Risikoexposition sowie der Komplexität der Bank angemessen sein und regelmässig überarbeitet werden.	Wir empfehlen, die Mindestanforderung an die Periodizität der Kontrolltätigkeit verbindlicher zu regeln.
47	Aktivitäten, die im Produktionsumfeld mit nicht anonymisierten, nicht verschlüsselten und nicht pseudonymisierten Massen-CID durchgeführt werden, müssen geeigneten Verfahren unterliegen (z.B. Vieraugenprinzip und Log-Dateien), einschliesslich der Benachrichtigung der für die Datensicherheit und -vertraulichkeit zuständigen Einheit. Es wird erwartet, dass dies die Arbeit von IT-Administratoren, Mitarbeitenden mit erhöhten Zugriffsrechten und Mitarbeitenden Dritter miteinschliesst. Umfangreiche Anfragen zu CID – die nicht anonymisiert, pseudonymisiert oder verschlüsselt sind – und die nicht bewilligt wurden, oder Anfragen, die auf ein verdächtiges Verhalten hinweisen könnten, müssen sofort dem obersten Management gemeldet werden.	Wir empfehlen den Begriff „oberstes Management“ zu präzisieren, z.B. „Geschäftsführung“ oder „Geschäftsleitung“. Administrative Tätigkeiten einem konsequenten 4-Augen-Prinzip zu unterstellen erscheint unrealistisch. Demzufolge wäre ein Klammerausdruck „(z.B. Vieraugenprinzip *oder* Log-Dateien)“ zu bevorzugen (anstelle von Vieraugenprinzip *und* Log-Dateien). Auch die Benachrichtigung der für die Datensicherheit und -vertraulichkeit zuständigen Einheiten bei allen administrativen Tätigkeiten erscheint nicht praktikabel. Weiter empfehlen wir den Begriff „Anfragen“ näher zu beschreiben (z.B. auch in einem Glossar). Konsequenterweise sollte erneut von „der für Datenvertraulichkeit zuständigen Einheit“ anstelle von „der für Datensicherheit und -vertraulichkeit zuständigen Einheit“ gesprochen werden, da der Fokus des RS auf der Datenvertraulichkeit und nicht auf der Datensicherheit insgesamt gelegt wird.
49	Von den Banken wird erwartet, dass sie vordefinierte Prozesse einführen, um rasch auf Vorfälle in Verbindung mit der Vertraulichkeit zu reagieren, einschliesslich einer klaren Strategie zur Kommunikation schwerwiegender Vorfälle. Zudem müssen Ausnahmen, Vorfälle und Prüfergebnisse überwacht, analysiert und in geeigneter Form dem obersten Management gemeldet werden. Dies muss zur laufenden	Wir empfehlen, in der Aufzählung neben Ausnahmen, Vorfällen und Prüfergebnissen auch die Überwachung von *„Kontrollergebnissen“* zu erfassen. Wir empfehlen den Begriff „oberstes Management“ zu präzisieren, z.B. „Geschäftsführung“ oder „Geschäftsleitung“.

Rz	Neuer Wortlaut	Bemerkungen
	Verfeinerung der Massnahmen zur Sicherstellung der Vertraulichkeit von CID beitragen.	
52	Das Rahmenkonzept zur Sicherstellung der Vertraulichkeit von CID (Rz 6 und 7) und die Sicherheitsstandards (Rz 31) müssen regelmässig überprüft werden. Vorfälle, Ausnahmen und Prüfergebnisse müssen zur laufenden Verfeinerung dieses Rahmenkonzeptes beitragen.	Wir empfehlen die Begriffe „überprüft“ und „Prüfergebnisse“ vorzugsweise durch „kontrolliert“ und „Kontrollergebnisse“ zu ersetzen. Weiter empfehlen wir, die Mindestanforderung an die Periodizität der Kontrolltätigkeit verbindlicher zu regeln.
55	Die Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID muss Teil des Prozesses für die Auswahl von Outsourcing-Dienstleistern und Anbietern von Grossaufträge sein. Es muss klare Kriterien für die Beurteilung der Sicherheits- und Vertraulichkeitsstandards solcher Dritter definiert werden. Die Prüfung in Bezug auf die CID- Sicherheits- und –Vertraulichkeitsstandards muss vor der Vertragsvereinbarung erfolgen und regelmässig wiederholt werden. Zudem muss das oberste Management über relevante Änderungen der Vertraulichkeitsstandards und -lösungen, die intern und/oder von Dritten angewandt werden, orientiert werden.	Wir empfehlen, den Begriff „Prüfung“ durch „Kontrolle“ zu ersetzen. Weiter empfehlen wir, die Mindestanforderung an die Periodizität der Kontrolltätigkeit verbindlicher zu regeln und den Begriff „oberstes Management“ zu präzisieren, z.B. mit „Geschäftsführung“ oder „Geschäftsleitung“.
61	Grossaufträge: Alle durch Dritte erbrachten Dienstleistungen, die Zugriff auf Massen-CID erfordern oder potenziell zum Zugriff auf Massen-CID führen (z.B. bei der Implementierung von Zugriffsrechtsprofilen durch Mitarbeitende eines Dritten). Ein CID-Risiko kann beispielsweise auftreten bei der Installation von Anwendungen oder der Implementierung von lokalen Einstellungen (z.B. Zugriffsrechten), der Datenspeicherung oder dem laufenden Systemunterhalt (z.B. Drittanbieter von IT-Services, extern entwickelte IT-Plattformen). Dies umfasst auch interne Prüfarbeiten und externe Prüfungen. Gewöhnlich sind solche Grossaufträge langfristiger Natur.	Wir empfehlen folgende textliche Anpassung im letzten Satz: „Dies umfasst auch interne *Kontroll*arbeiten, *interne Revisionsarbeiten* und externe Prüfungen.“
63	Schlüsselmitarbeitende: Alle internen und externen im IT-Bereich sowie in weiteren Unternehmensbereichen tätigen Mitarbeitenden, die aufgrund ihres Tätigkeitsprofils und ihrer	Wir empfehlen den Begriff „oberstes Management“ zu präzisieren, z.B. „Geschäftsführung“ oder „Geschäftsleitung“.

Rz	Neuer Wortlaut	Bemerkungen
	Aufgaben privilegierten Zugriff auf CID im grossen Umfang haben (z.B. Datenbankadministratoren, Mitglieder des obersten Managements).	
65	Reversible Datenverarbeitungstechniken: • Pseudonymisierte Daten (Pseudonymisierung): Unter Pseudonymisierung versteht man den Vorgang der Trennung der identifizierenden (z.B. Name, Foto, E-Mail Adresse, Telefonnummer) von anderen Daten (z.B. Kontostand, Kreditwürdigkeit). Das Bindeglied zwischen den beiden Datenbereichen bilden sogenannte Pseudonyme und eine Zuordnungsregel (Konkordanztabelle). Beispielsweise können Pseudonyme durch einen Zufallszahlengenerator erzeugt und mittels einer Konkordanztabelle den identifizierenden Personendaten bei Bedarf zugeordnet werden. • Verschlüsselte Daten: In der Praxis wird die Pseudonymisierung auch mittels Verschlüsselungsverfahren umgesetzt. Das Pseudonym wird in diesem Fall durch Verschlüsselung von identifizierenden Personendaten mit einem kryptographischen Schlüssel erzeugt. Die Reidentifikation erfolgt aufgrund der Entschlüsselung mit Hilfe des geheimen Schlüssels.	Sowohl die Pseudonymisierung als auch die Verschlüsselung stellen zwar reversible Datenverarbeitungstechniken dar, wir würden jedoch davon absehen, die Verschlüsselung von Daten als Sonderform der Pseudonymisierung zu definieren. Die Pseudonymisierung und die Verschlüsselung basieren grundsätzlich auf unterschiedlichen Methoden und Techniken und sollten demzufolge nicht miteinander vermischt werden.
	Fragenliste zur Anhörung	
	1. Kapitel IV.B „Qualitative Grundanforderungen“: Das Inkrafttreten dieses Kapitels ist im Entwurf für den 1. Januar 2015 vorgesehen. Wie beurteilen Sie die Möglichkeit, das Inkrafttreten des Kapitels IV.B „Qualitative Grundanforderungen“ bereits auf den 1. Juli 2014 festzusetzen? (Der Anhang 3 „Umgang mit elektronischen Kundendaten“ würde wie vorgesehen am 1. Januar 2015 in Kraft treten.)	Gemäss Rz 62 FINMA-RS 13/3 entspricht die Aufsichtsprüfperiode in der Regel der Rechnungsprüfperiode. Bei den meisten Banken entspricht die Rechnungsprüfperiode dem Kalenderjahr. Aus wirtschaftlichen Gründen empfehlen wir, aufsichtsrechtliche Normen, welche einen erheblichen Anpassungsbedarf mit sich bringen, nach Möglichkeit auf den 1. Januar in Kraft zu setzen. Auch denkbar wäre eine Koordination des Inkrafttretens mit dem Beginn der Rechnungslegungsperiode, z.B. „Das Inkrafttreten des Kapitels IV.B „Qualitative Grundanforderungen“ wird auf den ersten Tag nach dem

Rz	Neuer Wortlaut	Bemerkungen
		Abschlussstichtag der Bank festgelegt, welcher dem 1. Juli 2014 folgt.“
	2. Anhang 3 „Umgang mit elektronischen Kundendaten“: Dieser Anhang ist gemäss Entwurf auf natürliche Personen („Privatkunden“), deren Geschäftsbeziehungen in oder von der Schweiz aus betreut oder geführt werden, begrenzt. Wie beurteilen Sie die Möglichkeit einer Ausweitung des Anwendungsbereichs a) auf natürlichen Personen („Privatkunden“), deren Geschäftsbeziehungen im Ausland betreut oder geführt werden? b) auf juristische Personen (z.B. „Firmenkunden“)?	Wir verweisen auf unsere Ausführung zu Rz 1 des Anhangs 3.

UBS Investment Bank

UBS AG
100 Liverpool Street
London EC2M 2RH
Tel. +44-20-7567 8000
Fax +44-20-7568 4800

www.ubs.com/investmentbank

Colin Bell
Global Head of
Operational Risk Control
Colin.Bell@ubs.com
www.ubs.com

Mr Alessandro Lana
Eidgenössische Finanzmarktaufsicht FINMA
Einsteinstrasse 2
3003 Bern
Switzerland

8 July 2013

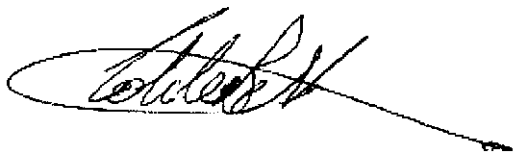
Dear Mr Lana,

Thank you for the opportunity to comment on the amendments to the Operational Risk Circular and overall we welcome the additional detail provided in the document. As you are aware we have participated in round table events and engaged extensively with the SBA, providing feedback through both mechanisms. Therefore rather than rehearse those conversations again I would only highlight the following two points where further clarification would be helpful:

- Capital floor (AMA banks): it is proposed that AMA banks are only allowed to reduce their capital position to 80% of a referenced methodology – it would be helpful to better understand 'the floor methodology' given that the Standard Approach under Basel II is undergoing an overhaul by the BIS.

- 'Inventory of people accessing CID' and 'Inventory of CID': whilst we fully understand the intent of these requirements, the practical application – particularly with respect to unstructured data – will be extremely challenging to implement. Therefore it would be helpful to have additional clarity on the expectations, or move to more principle based guidance given other potentially more efficient risk mitigations solutions such as encryption and access control to individual files containing CID (unstructured data).

Yours sincerely



Colin Bell
Global Head of Operational Risk Control

Association of Foreign Banks in Switzerland
Verband der Auslandsbanken in der Schweiz
Association des banques étrangères en Suisse
Associazione delle banche estere in Svizzera

foreign banks . in switzerland .

Eidgenössische Finanzmarktaufsicht FINMA
Herrn Alessandro Lana
3003 Bern
alessandro.lana@finma.ch

Zürich, 30. Juni 2013

AFBS Comments Revision FINMA 2008/21 Rundschreiben Operationelle Risiken

Sehr geehrter Herr Lana

Wir nehmen Bezug auf die Vernehmlassung zur Revision des FINMA Rundschreibens Operationelle Risiken und übermitteln Ihnen anbei gerne die Stellungnahme unseres Verbandes.

Zu den spezifischen Fragen nehmen wir wie folgt Stellung:

1. Die Anwendung der **Qualitativen Grundanforderungen bereits ab 1. Juli 2014** erachten wir als verfrüht. Dieses Kapitel enthält die zentralen Neuerungen welche Grundlegende Anpassungen der internen Abläufe und Organisation verlangen. Es ist unsicher, ob weniger als zwölf Monate ausreichen, um diese Anpassungen vorzunehmen und die notwendigen Tests vorzunehmen, bevor die Systeme dem Tagesgebrauch übergeben werden.
Weiter ist zu bedenken, dass sich die Anforderungen ändern, sollte die Schweiz eine Form des Informationsaustauschs übernehmen. Gewisse Risiken werden sich nicht mehr stellen und andere auf eine andere Weise. Um eine massvolle und kosteneffiziente Umsetzung zu gewährleisten sollte dies im Rundschreiben berücksichtigt werden, kann es aber nicht, wenn dieses schon im Juli 2014 angewandt werden soll.

2. Die extraterritoriale **Anwendung der schweizerischen Regulierung** ist fragwürdig, insbesondere da ja die meisten anderen Länder auch eine ihrem regulatorischen und gesetzlichen Rahmen angepasste Datenschutzregelung kennen. Es besteht Gefahr, dass schwer administrierbare Widersprüche oder Doppelspurigkeiten entstehen, weshalb auf die extraterritoriale Anwendung zu verzichten ist. Die Anwendung auf Daten natürlicher und juristischer Personen sollte, im Ausmass des technisch sinnvollen und möglichen, zulässig sein.

Wir haben die Stellungnahme in Zusammenarbeit mit Vertretern von Auslandsbanken ausgearbeitet. Die Herausforderungen, die sich durch die grenzüberschreitende Tätigkeit dieser Institute stellen, standen im Zentrum der Überlegungen.

Wir danken für die Aufmerksamkeit, die Sie unserer Stellungnahme entgegenbringen. Gerne stehen wir für eine vertiefte Diskussion einzelner Punkte zur Verfügung.

Freundliche Grüsse

VERBAND DER AUSLANDSBANKEN IN DER SCHWEIZ

Dr. Martin Maurer
Geschäftsführer

Raoul Wuergler
stv Geschäftsführer

Usteristrasse 23 · Postfach 1211 · CH-8021 Zürich
T +41 44 224 4070 · F +41 44 221 0029
www.foreignbanks.ch · info@foreignbanks.ch

Revisionsentwurf
FINMA Rundschreiben 2008/21 Operationelle Risiken

Stellungnahme des Verbands der Auslandsbanken in der Schweiz VAS

Allgemeine Bemerkungen

Wir unterstützen die Stellungnahme der Schweiz. Bankiervereinigung, an deren Ausarbeitung unser Verband über die Vertretung in den zuständigen Gremien beteiligt war. Insbesondere unterstreichen wir die zwingende Notwendigkeit, Begriffe und Konzepte klar und eindeutig zu formulieren.
Die Vorgaben des Rundschreibens sollen die internationale Entwicklung einbeziehen. Dazu gehört die Unterscheidung der Schutzpflichten in verschiedene Kategorien je nachdem, ob das traditionell verstandene Bankkundengeheimnis in der Schweiz bestehen bleibt oder ob sich der Datenschutz auf die Standards der beruflichen Geheimhaltungspflicht und des Datenschutzgesetzes beschränkt.
Ebenso hat die Umsetzung Grösse und Risikoexposition der jeweiligen Institute und deren allfällige Einbettung in eine internationale Organisation zu berücksichtigen. Diesem Grundsatz der Proportionalität kann nur Rechnung getragen werden, wenn die spezifische Umsetzung – wie zum Beispiel die Kategorisierung der Kundenidentifikationsdaten – den einzelnen Instituten überlassen wird.

B. Qualitative Grundanforderungen

Grundsatz 1: Verantwortlichkeiten

In Grundsatz 1 ist neben Rahmenkonzept mit Vorgaben und Prozessen sinnvollerweise auch das Eignerschaft von und Verantwortung für Systeme zu erläutern. Verantwortung kann nur definiert und wahrgenommen werden, wenn sie auch zugeordnet werden kann.

Der VAS schlägt vor, Rz 122 wie folgt zu ergänzen:

Rz 122 Die Geschäftsführung … von operationellen Risiken zuständig. Sie definiert die Eignerschaft von und damit einhergehende Verantwortung für die jeweiligen Daten und Systeme eindeutig. Sie muss zudem …

Grundsatz 2: Rahmenkonzept und Kontrollsystem

Der VAS versteht, dass das Rahmenkonzept auch die Verpflichtung umfasst, Zugriffsrechte und die Erteilung derselben zu definieren. Sinnvollerweise ist diese Verpflichtung in Rz 125 Bst a zu präzisieren:

a. Strukturen für das Management der operationellen Risiken, einschliesslich Definition und Zuteilung von Kompetenzen (inklusive Zugriffsrechte) sowie, Rechenschaftspflichten und Berichtslinien.

Grundsatz 4: Interne und Externe Berichterstattung

Rz 130 Bst c verlangt von der Bank, relevante interne und externe Ereignisse und potentielle Risiken in die Berichterstattung über operationelle Risiken einzubeziehen. Diese Anforderung ist zu präzisieren und die betroffenen Ereignisse sind einzugrenzen. Es kann nicht sein, dass Ereignisse, die ausserhalb der Kontrolle der Bank sind, auf dieselbe Weise einzubeziehen sind wie kontrollierbare interne Ereignisse. Es erscheint sinnvoll, dass sich die Bank bei der Identifizierung der betroffenen Ereignisse an die Definition anlehne, die sie aufgrund der Empfehlungen für das Business Continuity Management der Schweiz. Bankiervereinigung anwendet. Dies gilt sowohl für die internen wie auch für die externen Ereignisse. Daher schlägt der VAS vor, Rz 130 Bst c wie folgt zu ergänzen:

Rz 130

c. Informationen zu relevanten Ereignissen und potentiellen Risiken sowie deren mögliche Auswirkungen auf die Bank.

Bei der Definition der relevanten internen und externen Ereignisse lehnt sich die Bank an die Standards aus den Empfehlungen der Schweiz. Bankiervereinigung für das Business Continuity Management.

Die in Rz 132 angesprochenen Anspruchsgruppen für externe Information sind zu umschreiben; die vorliegende Definition ist unklar und führt zu Missverständnis und Widersprüchen. Der VAS schlägt vor, den Kreis der externen Anspruchgruppen gleich zu fassen wie in Grundsatz 8 des Anhangs. Sinnvollerweise gehören neben Revision und FINMA, falls angebracht, die Strafverfolgungsbehörden, Geschäftspartner, Kunden dazu. Dies ist im Rundschreiben klar festzuhalten.

Rz 132 Von den Banken extern offen zu legende Informationen müssen es den Anspruchgruppen erlauben, sich ein Urteil über den Ansatz zum Management von operationellen Risiken zu bilden. Hierzu gehört u.a. das Konzept für das Management operationeller Risiken. Dieses soll den Anspruchgruppen eine Beurteilung der Wirksamkeit der Identifikation, Begrenzung und Überwachung der operationellen Risiken ermöglichen. Zur Anspruchgruppe gehören der Revisor, die FINMA sowie gegebenenfalls Strafverfolgungsbehörden, Geschäftspartner und Kunden. Falls angebracht ordnet die Bank weitere Kunden oder Geschäftspartner der Anspruchgruppe zu.

Grundsätze 5 und 6: Technologieinfrastruktur und Kontinuität bei Geschäftsunterbrechung

Fragen der technischen Infrastruktur und der Geschäftsfortführung sind eng miteinander verbunden und abhängig voneinander, weshalb die beiden Grundsätze sinnvollerweise in einem zusammenzufassen sind.
Es ist auf die Tatsache Rücksicht zu nehmen, dass nicht alle Banken die gesamte Risk Management Funktion in der Schweiz ausüben. Zahlreiche international strukturierte Institute verfügen über eine matrizielle Organisation, in der gewisse Kompetenzen und Verantwortlichkeiten grenzüberschreitend zusammengefasst sind. Die Vorgaben sollen diese Situation berücksichtigen, indem sie Bedingungen vorgeben, unter welchen die Risk Management Funktion aus dem Konzern im Ausland ausgeübt werden kann. Die Luxemburgische CSSF sieht diese Situation explizit vor, wie im Rundschreiben 13/554 vom 7. Januar 2013. Ähnliche Regeln können in vorliegendem Rundschreiben definiert werden.
Weiter geht es nicht nur darum, die Sicherheit der Daten sondern auch die Verwendung derselben, also auch den Zugriff auf die Daten zu kontrollieren. Aus diesem Grunde ist der Grundsatz 5 anzupassen.

Rz 133 Überdies hat sie die Sicherheit, Integrität und Verfügbarkeit der Daten und Systeme sowie die Kontrolle über den Zugriff auf dieselben zu gewährleisten~~sowie ein integriertes und umfassendes Risikomanagement zu implementieren~~.

C. Risikospezifische Qualitative Anforderungen

Der VAS unterstützt die Delegation an die Geschäftsführung der Verantwortung für die adäquate Überwachung geschäftsspezifischer Risiken. Die Geschäftsführung, mit Unterstützung der zuständigen internen Stellen, ist am besten geeignet, die relevanten Risiken zu identifizieren und passende Massnahmen zu deren Minimierung zu treffen.
Vor diesem Hintergrund schlägt der VAS vor, Rz 136 anzupassen und die Konkretisierung weiterer Vorgaben zu spezifischen Aspekten im Rahmen einer durch die betroffenen Institute erarbeitete und von der FINMA anerkannten Selbstregulierung festzulegen.

Rz 136 Falls die FINMA es als notwendig erachtet, kann sie die betroffenen Institute dazu auffordern, für spezifische Themen weitergehende Konkretisierungen an das Management von operationellen Risiken im Rahmen der anerkannten Selbstregulierung zu definieren.

Anhang 3

Der Anhang 3 präzisiert die Vorgaben zur Anwendung der jeweiligen im Rundschreiben festgehaltenen Grundsätze. Einleitend sollte der Anhang festhalten, ob seine Vorgaben sich auf strukturierte, unstrukturierte oder beide Kategorien von Daten anwenden. Es besteht ein massgeblicher Unterschied bei der Verwaltung von zentral und nach einheitlichen Standards verwalteten Daten (die zB auf einem zentralen Server/Host gelagert werden) und Daten, die in einzelnen Abteilungen oder Teams für die spezifischen Bedürfnisse erstellt, verarbeitet und aufbewahrt werden. Beide Formen der Daten treten auf und müssen nebeneinander bestehen können. Mitarbeiterschulung kann dazu beitragen, die Sicherheit der Daten zu erhöhen. Es ist jedoch nicht möglich, auf beide Datenkategorien dieselben Schutz- und Risikomanagementstandards anzuwenden.

Grundsatz 1: Governance

Wie schon unter Punkt B Grundsatz 1: Verantwortlichkeiten erwähnt, geht es nicht nur darum, Verantwortung für die Prozesse vorzusehen, sondern ebenfalls klar die Dateneigner und die Zugriffsberechtigung zu identifizieren. Daher ist der erste Satz wie folgt anzupassen:

Rz 3 Kundendaten werden eindeutig Dateneignern (Data Owners) zugeordnet. Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten werden systematisch identifiziert, begrenzt und überwacht. …

Grundsatz 2: Kundenidentifikationsdaten

Es gilt festzuhalten, dass nicht alle Datensätze unter allen Umständen einer der drei im Entwurf vorgeschlagenen Kategorien von Client Identifying Data CID zugeordnet werden können. In relationalen Datenbanken, wie sie häufig verwendet werden, erhalten individuelle Datensätze oft erst durch ihre Relation untereinander Sinn und können erst aufgrund der bestehenden Relationen als direkte, indirekte oder potentiell indirekte CID erkannt werden. Da Institute meist ihre eigenen spezifischen relationalen Datenbanken verfügen ist es sinnvoll, die Kategorien nicht zwingend für alle Institute im Rundschreiben festzusetzen, sondern den Instituten selbst diese Aufgabe aufzuerlegen. Der VAS schlägt vor, die Institute dazu zu verpflichten, eine auf ihre spezifische Situation passende Kategorisierung der CID vorzunehmen und festzuhalten. Diese kann mit dem Revisor besprochen werden, bevor sie verabschiedet wird.

Rz 9 Eine klare und transparente Liste der Kundenkategorien, einschliesslich der unternehmensspezifischen Festlegung von CID, muss in der Bank vorliegen und formell dokumentiert werden. Die Kategorisierung und Definition von Kundendaten hat direkte Kundenidentifikationsdaten (z.B. Vorname, zweiter Name, Nachname), indirekte Kundenidentifikationsdaten (z.B. Passnummer) und potentiell indirekte Kundenidentifikationsdaten (z.B. Kombinationen aus Geburtsdatum, Beruf, Staatsangehörigkeit usw.) zu umfassen.
Kapitel III "Beispiel zu Kundenidentifikationsdaten" enthält Beispiele, wie Kundenidentifikationsdaten den drei Kategorien zugeordnet werden können. Jedes Institut hat aufgrund seiner Organisation eine passende Zuordnung vorzunehmen.

Grundsatz 3: Datenspeicherort und -zugriff

Es versteht sich von selbst, dass Verzeichnis (Rz 28) und Kontrolle sowohl über die Zugriffsberechtigung wie auch über die effektiven Zugriffe zu führen ist. Diese Vorgabe ist jedoch präzise zu formulieren, damit keine Widersprüche und Missverständnisse entstehen. Die Logs haben Zugriffe zu erfassen (Mitarbeiter, Zeitpunkt, Dauer, Art der zugegriffenen Daten, nicht jedoch die Aktivität). Der VAS schlägt vor, die Rz 28 und 29 zusammenzuführen. Dieser Grundsatz ist mit Grundsätzen 5 und 6 im Rundschreiben zu koordinieren; neben dem effektiven Zugriff ist auch die Berechtigung zur Zugriffserteilung und zum Zugriff selbst zu dokumentieren.

Rz 28 Die Bank muss ein Verzeichnis der Mitarbeitenden und Dritten, die Zugriffsberechtigungen auf CID haben, deren Zugriffsberechtigung sowie der effektiv erfolgten Zugriffe führen. …

Rz 29 *streichen*

Grundsatz 4: Sicherheitsstandards für Infrastruktur

Logs der effektiv erfolgten Zugriffe (Grundsatz 3) und Mitarbeiterschulung und -sensibilisierung (Grundsatz 5) werden dazu beitragen, den Datenschutz auch auf den Endgeräten zu erhöhen. Die Sicherheit von Daten auf Endgeräten kann nur auf diese Weise gewährleistet werden. Egal wie sophistiziert die technische Infrastruktur ist, unachtsame Nutzer stellen immer eine Gefahr dar, weshalb der Schulung und Sensibilisierung der Mitarbeiter spezielle Aufmerksamkeit zu schenken ist.

Grundsatz 5: Auswahl und Schulung von Mitarbeitern

Es gilt nicht nur, die Auswahl der Mitarbeiter, sondern auch deren Verhalten einer regelmässigen Prüfung zu unterziehen. Aus diesen und den unter Grundsatz 4 erwähnen Gründen ist Rz 38 zu ergänzen; neben der Prüfung bei Auswahl der Mitarbeiter auch eine regelmässige Prüfung im Laufe des Anstellungsverhältnisses stattfindet.

Rz 38 … Diese Abklärungen sind während dem Anstellungsverhältnis zu wiederholen und gegebenenfalls den neuen Aufgaben des jeweiligen Mitarbeiters anzupassen.

Grundsatz 7: Risikominderung in Bezug auf CID Vertraulichkeit

Der VAS unterstützt die Forderung nach Angemessenheit beim Schutz der CID im Entwicklungsprozess. Es versteht sich von selbst, dass in der Entwicklungsphase kein Zugriff auf CID notwendig ist. In der Testphase ist dieser jedoch zwingend, damit die Mitarbeiter in einem ihnen bekannten Umfeld die neuen Applikationen testen können. Die Tests durch IT Entwickler können von Tests durch Kundenberater getrennt werden, was den Schutz der CID erleichtert.

Grundsatz 9: Outsourcing

Die in Rz 54-59 definierten Anforderungen an die Kontrolle der Bank über ihren Outsourcing Dienstleister sind sehr umfassend und zum Teil komplex. Es ist fraglich, ob speziell kleine und mittelgrosse Institute in dieser Situation weiterhin effizient operieren können. Die sorgfältige Auswahl des Outsourcing Dienstleisters ist im Rundschreiben Outsourcing als Pflicht definiert. Outsourcing hat zum Ziel, gewisse Kompetenzen, Aufgaben und Kontrollfunktionen an Dritte zu delegieren. Dieses Konzept soll weitehrin Bestand haben. Während es logisch scheint und daher annehmbar ist, dass die Bank adäquate Due Diligence Prüfung ihres Outsourcing Dienstleisters vornimmt sowie Zuständigkeiten und verantwortliche Personen definiert gehen die Forderungen nach der Zuordnung einzelner Mitarbeiter zu jeder ausgelagerten Aktivität sowie nach der fortlaufenden Überwachung des Outsourcers eindeutig zu weit. Die Zuordnung der Verantwortung für die ausgelagerten Aktivitäten sowie eine "regelmässige" Kontrolle derselben ist ausreichend.

Rz 59 Die Bank muss ~~für jede~~ die Verantwortung für ausgelagerte Aktivitäten, die Zugriff auf CID beinhalten, ~~einen oder mehreren Mitarbeitende(n) bestimmen~~ zuordnen, damit sichergestellt ist, ~~der/die dafür verantwortlich ist/sind~~ dass die Sicherheits- und Vertraulichkeitsstandards in Bezug auf die Vertraulichkeit von CID eingehalten werden. … Alle Dienstleistungen, die von externen Anbietern erbracht werden und Risiken in Bezug auf die Vertraulichkeit von CID bergen, sind ~~fortlaufend~~ in regelmässigen Intervallen zu überwachen.

Abschliessend legt der VAS Wert darauf, dass die in diesem Rundschreiben enthaltenen Vorgaben sehr umfassende und weitgehende Anpassungen an interne Organisation, Prozesse und Abläufe der betroffenen Institute stellen. Aus diesem Grund ist für die Umsetzung eine ausreichende Übergangsfrist von 18 bis 24 Monaten zu gewähren.

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
z. H. Herr Alessandro Lana
Einsteinstrasse 2
CH-3003 Bern

Datum 1. Juli 2013
Kontaktperson Jacopo Buss
Direktwahl 061 206 66 26
E-Mail j.buss@vskb.ch

Stellungnahme der Kantonalbanken zur Teilrevision des FINMA-Rundschreibens 2008/21 „Operationelle Risiken Banken“

Sehr geehrte Damen und Herren

Am 23. Mai 2013 hat die Eidgenössische Finanzmarktaufsicht (FINMA) die öffentliche Anhörung zur Teilrevision des FINMA-Rundschreibens 2008/21 „Operationelle Risiken Banken“ eröffnet und interessierte Kreise eingeladen, zum Revisionsentwurf Stellung zu nehmen. Wir danken Ihnen für die uns gebotene Gelegenheit, uns einbringen zu können. Ebenso danken wir der FINMA für die Durchführung des Workshops vom 8. März 2013; dieser bot eine gute Gelegenheit um sich im Vorfeld der Vernehmlassung direkt zu diesem wichtigen Thema auszutauschen.

Wir stellen jedoch auch fest, dass der Workshop nicht genügend Raum zur fundierten Diskussion der fragwürdigen Punkte der Revision gegeben hat. Dies trug dazu bei, dass im Vernehmlassungsentwurf einige kontroverse Punkte in ähnlicher oder unveränderter Form wie in der Workshop-Fassung beibehalten wurden.

Es ist unbestritten, dass die operationellen Risiken – nicht zuletzt vor dem Hintergrund diverser Verlustfälle in den letzten Jahren – als Risikokategorie an Bedeutung gewonnen haben. Es ist deshalb nachvollziehbar, dass die FINMA die Mitigation dieser Risiken durch geeignete Auflagen und Massnahmen herbeiführen will. Ebenso anerkennen wir, dass die Konformität nationaler Regelungen mit internationalen Standards herbeizuführen ist. Wir begrüssen somit grundsätzlich die Revision des Rundschreibens „Operationelle Risiken Banken“.

Jedoch sind wir der Auffassung, dass der hier vorliegende Entwurf zur Teilrevision in verschiedenen Teilen, insbesondere aber im neuen Anhang 3, deutlich übers Ziel hinaus schiesst und unbedingt grundlegend überdacht werden muss, vor allem hinsichtlich der

nachfolgenden Kommentare. Weiter weisen wir darauf hin, dass einzelne der neu enthaltenen qualitativen Vorgaben bereits heute angemessen und hinreichend in bestehenden FINMA-Rundschreiben (im Folgenden „RS“) geregelt sind. Eine weitere (zum Teil widersprüchliche) Konkretisierung dieser Vorgaben ist weder notwendig noch förderlich.

1 Generelle Bemerkungen

Wir begrüssen grundsätzlich die Anlehnung an die Empfehlungen des Basler Ausschuss. Wir erinnern aber an dieser Stelle, dass diese für international tätige Banken definiert wurden, welche den Modellansatz für operationelle Risiken (AMA) verwenden. Die Grundlagen hierfür (Messung des Verlustpotentials) sind aber nach heutigem Wissensstand gerade für Inlandbanken kleiner und mittlerer Grösse nicht gegeben. Zwar wird im vorliegenden RS von einem Proportionalitätsprinzip gesprochen, welches diesem Umstand eigentlich Rechnung tragen sollte, doch profitieren de facto nur ein kleiner Teil der zahlenmässig bedeutenden Kategorie-4-Banken und die Kategorie-5-Banken von Erleichterungen. Das Proportionalitätsprinzip ist deshalb zu überarbeiten und hinsichtlich Differenzierungskriterien und Angemessenheit im Sinne der Kosten/Nutzen-Abwägungen nachvollziehbarer zu gestalten.

Wir bezweifeln grundsätzlich die Quantifizierbarkeit der operationellen Risiken bei Nicht-AMA-Banken. Bei den qualitativen Anforderungen wird aber implizit immer wieder davon ausgegangen, dass die operationellen Risiken messbar und quantifizierbar sind (z.B. Grundsatz 3: Identifizierung, Begrenzung und Überwachung, insbesondere Randziffer 128). Dies ist unserer Meinung nach ein zentrales Problem des Entwurfs und wir empfehlen dringendst, diese Betrachtungsweise zu überdenken bzw zu korrigieren. Weitere Bemerkungen dazu finden Sie im Abschnitt 2 A.

Mit dem IKS-Rundschreiben (FINMA-RS 08/24 „Überwachung und interne Kontrolle Banken“) sind die wichtigsten Grundsätze und qualitativen Anforderungen ans Kontrollumfeld und die Prozesse bereits geregelt (Rollen von VR-, GL-, interner Revision und Prüfgesellschaft). Der in den Anforderungen des RS „Operationelle Risiken Banken“ definierte Detaillierungsgrad für Kontrollumfeld und Prozesse liegt viel höher als z.B. in den FINMA-RS Marktrisiken, Kreditrisiken oder Liquidität. Er ist unseres Erachtens viel zu hoch und scheint keinen Bezug zur heutigen Praxis in der Schweiz zu haben. Es fällt insbesondere auf, dass die Rolle des VR sehr operativ definiert werden soll.

Der VSKB lehnt die Neuregulierung im Bereich KID in Form eines FINMA-Rundschreibens grundsätzlich ab. Anhang 3 enthält Vorgaben, welche in der heutigen politischen Diskussion zum automatischen Informationsaustausch nur mit Bedacht und im Austausch mit den betroffenen Verbänden sowie im parlamentarischen Prozess auf dem ordentlichen Rechtsweg beschlossen werden sollten.

Die im Anhang 3 beschriebenen Anforderungen hätten eine vollständige Überarbeitung der IT-Systeme der Banken und ein fragwürdiges Resultat zur Folge. Der sichere Umgang mit elektronischen Kundendaten ist eine Grundanforderung an das Bankengeschäft und wird

sowohl im Bankengesetz wie im Datenschutzgesetz geregelt. Es handelt sich nicht um ein spezifisches operationelles Risiko im Zusammenhang mit dem Geschäftsmodell der Banken, sondern es betrifft alle Organisationen, welche mit elektronischen Personendaten arbeiten. Dazu ist keine spezifische FINMA-Regulierung notwendig, sondern es sind geeignete IT- und Bankenstandards erforderlich. Diese sind von den betroffenen Organisationen und Verbänden laufend zu entwickeln und umzusetzen. Im Übrigen sollte die allgemeine Formulierung der qualitativen Anforderungen dieses Thema auch abdecken können. Dies würde einen Ansatz zur Verhältnismässigkeit liefern und damit verbunden die Möglichkeit, die Vorgaben für unterschiedliche Institute spezifisch auszugestalten. Ein allfälliger Miteinbezug der Kundendaten (unabhängig davon ob elektronisch oder physisch) sollte sich auf kurze und prägnante Grundsätze zum Risikomanagement beschränken. Die Massnahmen und deren Tiefe sollte jede Bank im Rahmen der festgestellten Risiken und ihrer strategischen Ausrichtung selber festlegen können, wobei die aufsichtsrechtlichen Prüfgesellschaften deren Wirksamkeit überprüfen sollen (analog heute). Muss-Formulierungen sind zu vermeiden.

Wir sind grundsätzlich der Meinung, dass ein komplexes und detailliertes Regulierungsnetz **nicht** das richtige Instrument ist, um an den äusserst vielschichtigen und mit einem hohen Mass an „Softfaktoren“ behafteten Bereich des operationellen Risikos heranzugehen. Auch möchten wir eine schleichende Einführung des AMA verhindern, einerseits aufgrund der Komplexität, andererseits, da die Konzepte zum Basisindikatoransatz und Standardansatz auf dem Prüfstand sind und auch dort Änderungen zu erwarten sind. Risikomanagement, insbesondere das von operationellen Risiken, hat viel mit menschlichem Verhalten zu tun. Menschliches Verhalten zu kontrollieren und risikomindernd zu beeinflussen, ist nach unserer Überzeugung denn auch vielmehr eine Frage der Unternehmens- bzw. Risikokultur. Hier spielen Aspekte wie Vertrauen, Loyalität, (Eigen-)Verantwortung, individuelles Risikobewusstsein und Wertschätzung entscheidende Rollen. Diese sind aus Sicht des Regulators zwar zweifellos deutlich schwieriger definier-, mess- und auditierbar, haben aber im Sinne der Risikomitigation einen ungleich höheren Hebel als die meisten noch so ausgeklügelten Limiten-, Weisungs- und Kontrollsysteme. Die mit diesem RS stipulierten, sehr umfangreichen und detaillierten Anforderungen werden unserer Ansicht nach in ihrer Wirkung überschätzt und liegen jenseits eines ausgewogenen Aufwand-/Nutzenverhältnisses. Dies umso mehr, als es ein erklärtes Ziel der Behörden ist, die Komplexität der Banken zu reduzieren.

Es ist verständlich, dass die FINMA das RS nicht mit dem Fokus auf eine kostengünstige Umsetzung der Regulierung entworfen hat, sondern mit dem Fokus auf eine stabilisierende Wirkung für den Finanzplatz Schweiz, indem ein relevanter Bestandteil der Bankrisiken besser kontrolliert wird. Wir erinnern aber an dieser Stelle klar daran, dass es sich dabei hauptsächlich um finanzielle Risiken der Institute handelt (zugegebenermassen mit negativen Externalitäten). Eine Regulierung zur Einschränkung von operationellen Risiken kann daher (auch aus Sicht des Finanzplatzes Schweiz) nur Sinn machen, wenn die Kosten der Umsetzung der Regulierung kleiner sind als ein erwarteter Verlust im Zusammenhang mit den operationellen Risiken. Die Frage nach der Kosteneffizienz des RS und vor allem von Anhang 3 lässt sich daher nicht umgehen. Bankinternen Schätzungen zufolge dürften sich die

Kosten der Implementierung von Anhang 3 pro Bank im Millionenbereich bewegen. Dazu kommen jährliche Betriebs- bzw. Prozesskosten in sechsstelliger Höhe. Wir sind klar der Meinung, dass dieser Aufwand insbesondere bei kleineren Banken in keinem Verhältnis zum erzielten Nutzen bzw. zum Gefahrenpotential steht. Die vorgeschlagene Regulierung (als Teil des Gesamtkonzepts von Basel III, welches primär auf die Stärkung der Resilienz der Banken abzielt) erschwert den Banken somit insgesamt die Geschäftstätigkeit und wirkt sich letztlich negativ auf die Eigenmittelunterlegung aus. Das kann nicht Ziel des Verfassers sein.

2 A Spezifische Bemerkungen zu den Randziffern der qualitativen Anforderungen

Rz 1
Die Bezeichnung «Qualitative Grundanforderungen» impliziert etwas anderes als die in der Rz 1 genannten «Sound Principles». Die „Sound Principles“ haben Empfehlungscharakter und sind unter Berücksichtigung der Grösse, des Geschäftsumfangs und des Risikoprofils eines Instituts anzuwenden (Sie beschreiben das Anspruchsniveau von grossen internationalen Banken). Die qualitativen Anforderungen im Rundschreiben sind zu detailliert, bzw. engen den nötigen Spielraum der Banken für ein dem Risikoprofil der Bank angemessenes Risikomanagement zu stark ein. Eine bessere Grundlage für die Regulierung unter dem Titel „Anforderungen“ sind die im Grundsatz 25 der „Grundsätze für eine wirksame Bankenaufsicht (The Basel Core Principles)“ explizit erwähnten „Zentralen Kriterien (8)“.

Rz 2
Es ist nicht klar, was diese Randziffer regeln soll: Die Definition gemäss Rz 2 schliesst die Reputationsrisiken aus. Der Grund für den Ausschluss der Reputationsrisiken liegt nicht in deren fehlenden Quantifizierbarkeit (was auch für die operationellen Risiken in den meisten Fällen gilt) sondern darin, dass Reputationsrisiken allen anderen Risikokategorien nachgelagert sind oder die Folge von enttäuschten Erwartungen sind, welche nicht zwingend mit einem operationellen Verlust in Verbindung stehen. Wir empfehlen daher auf diese Randziffer zu verzichten.

Rz 50-68
Eine Abstimmung zwischen den zusätzlichen qualitativen Anforderungen und den qualitativen Grundanforderungen scheint nicht erfolgt zu sein. Ein Grossteil der „zusätzlichen Anforderungen“ ist bereits in den Grundanforderungen enthalten, zum Teil gehen die Grundanforderungen sogar weiter als die „Zusatzanforderungen“.

Rz 117/118/119
Das Proportionalitätsprinzip wird zu eng ausgelegt: Hauptausschlusskriterium ist die FINMA-Kategorisierung, welche in dieser Beziehung nicht adäquat ist. Vor allem der Unterschied zwischen AMA- und Nicht-AMA-Banken wird viel zu wenig berücksichtigt (Aufzeigen der Auswirkungen auf die Eigenmittelanforderungen, Abnahme der Risikobereitschaft und -toleranz durch den VR). Die FINMA-Kategorie 4 „ohne bedeutende Komplexität“ lässt zu viel

Interpretationsspielraum zu. Eine bessere Lösung für das Proportionalitätsprinzip wurde im Rundschreiben 2013/6 „Liquidität Banken“ gefunden (Rz 10):
„*Die Anforderungen des Dritten Kapitels dieses Rundschreibens sind abhängig von der Grösse der Bank sowie Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten umzusetzen. Öffnungsklauseln in den Randziffern des Kapitels III weisen auf die verhältnismässige Anwendung hin, indem kleine Banken von deren Umsetzung ausgenommen sind.“*

Grundsatz 1 (Verantwortlichkeiten)
Im Gegensatz zu anderen Risikoquellen werden die operationellen Risiken nicht aktiv von einer Bank verfolgt, sondern resultieren sozusagen als Nebenprodukt aus ihrer Geschäftstätigkeit. Ein gutes Management operationeller Risiken basiert daher viel mehr auf einer qualitätsorientierten Haltung, als auf quantitativen Limiten. Auch ergeben die Begriffe Risikobereitschaft und Risikotoleranz sowie die Festsetzung von Limiten im Zusammenhang mit den operationellen Risiken keinen Sinn, da sie nicht (oder nur schlecht) direkt quantifizierbar sind. Vielmehr besteht die Gefahr bei einer Quantifizierung, dass man sich in einer Scheinsicherheit fühlt. Die Einschätzung und Kategorisierung der operationellen Risiken sollte nach qualitativen Vorgaben erfolgen. Risikobereitschaft und Risikotoleranz für operationelle Risiken lassen sich nicht wie bei den anderen Risikokategorien Markt- und Ausfallrisiken auf oberster Stufe anhand eines Rahmenkonzepts definieren. Operationelle Risiken sind inhärent verbunden mit der Geschäftstätigkeit des Bankengeschäfts und die Folge der gewählten strategischen Stossrichtungen und Geschäftstätigkeit. Der Verwaltungsrat könnte jedoch periodisch die qualitative Haltung im Zusammenhang mit den operationellen Risiken evaluieren. Auf die Begriffe Risikobereitschaft und -toleranz sollte dabei verzichtet werden.

Rz 120
Die Beurteilung ob operationelle Risiken von der Bank vermieden, eingegangen oder mittels risikomindernden Massnahmen (u.a. Kontrollen, Zielvorgaben) reduziert werden sollen, ist ein Entscheid des Verwaltungsrats. Dieser Grundsatz der regelmässigen Identifikation, Beurteilung, Begrenzung und Überwachung der operationellen Risiken wird implizit aber auch bereits im FINMA-Rundschreiben 2008/24 „Überwachung und interne Kontrolle Banken“ (Rz 9 – 14 bzw. 80 – 96) gefordert. Insbesondere ist die Anforderung aus Rz 120 des vorliegenden Rundschreibens bereits auch in Rz 10 des FINMA-RS 2008/24 enthalten. Die Rz 120 wäre somit auf das „Wording“ des FINMA-RS 2008/24 abzustimmen und könnte entsprechend gekürzt oder ganz weggelassen werden.

Rz 122
Die Verantwortung für das Management der operationellen Risiken ist einer Funktion zuzuweisen, welche u.a. für die Aufrechterhaltung und die laufende Weiterentwicklung des Rahmenkonzepts des Managements der operationellen Risiken zuständig sein soll. Wie bereits oben bemerkt, ergeben sich die operationellen Risiken aus der Geschäftstätigkeit und damit aus der spezifisch gewählten Aufbau- und Ablauforganisation. Das Management der sich daraus ergebenden operationellen Risiken erfolgt durch jeden einzelnen Mitarbeitenden

im Rahmen der definierten Prozesse und ihm zugewiesenen Aufgaben, Verantwortungen und Kompetenzen. Deshalb kann das Management der operationellen Risiken nicht von einer einzelnen Funktion innerhalb der Bank wahrgenommen werden. Vom eigentlichen Management der operationellen Risiken sollte jedoch die unabhängige Funktion der Risikokontrolle (u.a. auch in Rz 125 Ziff. g angedeutet) getrennt sein. Die Funktion der Risikokontrolle ist bereits in Rz 133 ff. des FINMA-RS 2008/24 „Überwachung und interne Kontrolle Banken“ angemessen festgehalten. Die dort beschriebene Risikokontrolle ist umfassend und beinhaltet auch die operationellen Risiken (vgl. Rz 116 FINMA-RS 2008/24). Die Rz 122 des vorliegenden Rundschreibens wäre somit auf das „Wording“ des FINMA-RS 2008/24 abzustimmen und könnte entsprechend gekürzt respektive gänzlich gestrichen werden.

Bei der Neubearbeitung ist folgender für uns unklar formulierter Satz zu prüfen:
„*Die Geschäftsführung definiert eine eindeutige, wirksame und solide **Führungsstruktur**, welche die Verantwortung zum Management der operationellen Risiken übernimmt. **Diese Funktion** ist für…“*

Grundsatz 2 (Rahmenkonzept und Kontrollsystem)
Rz 125
Die Mindestanforderungen für das Rahmenkonzept sind zu detailliert und wurden für grosse internationale Banken mit einem AMA-Ansatz definiert. Generell sind Begriffe, welche ein Messkonzept für operationelle Risiken voraussetzen, zu vermeiden. Folgende Punkte sind insbesondere als Mindestanforderung für alle Banken zu überdenken:

- **lit. b:** *„Definition der Instrumente für die […] Messung […]“*:
  Instrumente für die Messung der operationellen Risiken stellen gemäss heutigem Stand der Praxis für nicht AMA-Banken keine angemessene Grundanforderung dar.
- **lit. c/d:** In der Praxis zeigt sich, dass die operationellen Risiken **nach** der Berücksichtigung von Kontrollen einzuschätzen sind (Nettorisiken). Die im Rundschreiben festgehaltenen "inhärenten Risiken" sind nicht zielführend, da die Einschätzung derselben abstrakt ist. Neue Risiken oder sich verschärfende Risiken führen zwingendermassen zu neuen/zusätzlichen Massnahmen/Kontrollen, da ansonsten die Risikotoleranz überschritten werden könnte. Das Rundschreiben ist dahingehend anzupassen, dass der Risikomanagementkreislauf die operationellen Risiken **nach** Massnahmen/Kontrollen berücksichtigt. Dabei ist zu beachten, dass „die Risikobereitschaft und -toleranz in Bezug auf die relevanten Risiken“ sich nicht in aggregierter Form durch ein Rahmenkonzept generell festlegen lassen. Desgleichen sind eine Festlegung und insbesondere eine Überwachung von Schwellenwerten und/oder Limiten für Residualrisiken nicht sinnvoll, da für die operationellen Risiken in der Praxis von Nicht-AMA-Banken keine Messkonzepte vorliegen.

In der deutschen Version fehlt der Buchstabe h). Ausserdem wurde dabei „zeitnah“ mit „en temps réel“ übersetzt, was nicht korrekt ist. Wir schlagen folgende französische Übersetzung vor:

«Obligation de vérifier et d'adapter, lors de l'analyse d'un évènement de risque avéré, dans les meilleurs délais le concept-cadre en cas de modification essentielle de la situation de risque»

Rz 126
Diese Randziffer ist mit dem IKS-Rundschreiben 08/24 bereits abgedeckt bzw. redundant.

Grundsatz 3 (Identifizierung, Begrenzung und Überwachung)
Rz 127 lit. h
Siehe Bemerkung zu Rz 125 oben bezüglich Messung der operationellen Risiken. Auch hier wird dem Proportionalitätsprinzip zu wenig Beachtung geschenkt.

Rz 128
Aus den Anforderungen lässt sich die Notwendigkeit zur Einführung bzw. zur Anpassung eines Transferpreissystems für operationelle Risiken, analog den Liquiditätsrisiken (Rz 17ff. des FINMA-RS 2013/6 „Liquidität Banken“), ableiten. Diese Vorgabe geht, hauptsächlich für Banken mit übersichtlichen und nicht komplexen Geschäftsaktivitäten der FINMA-Kategorie 3, zu weit. Das Proportionalitätsprinzip greift hier zu wenig und die Anforderung würde für diese Banken einen unnötigen und nicht zielführenden zusätzlichen Administrationsaufwand bedeuten. Zudem ist eine Quantifizierung sowie entsprechend auch die Performance der operationellen Risiken schwierig objektiv zu messen und zu beurteilen. Die zur Reduzierung von operationellen Risiken eingesetzten Kontrollen und Zielvorgaben sollten anstatt in ein Transferpreissystem eingebunden, vielmehr Bestandteil eines umfassenden IKS- sowie MBO-Prozesses sein. Die Anforderung sollte entweder praxisnaher formuliert oder gestrichen werden.

Grundsatz 4 (Interne und Externe Berichterstattung)
Rz 129
Der Begriff „proaktives Management“ sollte mit „Management“ ersetzt werden, sonst wäre zu definieren, was unter diesem Titel von Verwaltungsrat und Geschäftsleitung konkret erwartet wird. Die Ausgestaltung des Management-Information-Systems bedarf keiner detaillierten Vorschrift.

Wie soll die laufende Überwachung des operationellen Risikoprofils und der wesentlichen Verlustrisiken konkret umgesetzt werden? Muss nun jeder Mitarbeitende von (unabhängigen!) Risk Managern permanent überwacht werden? Die Formulierung ist anzupassen (z.B. regelmässige Überwachung oder zeitnahe Überwachung).

Rz 130
Diese Rz ist offensichtlich auf Banken ausgerichtet, welche fortschrittliche Messverfahren verwenden und kann nicht als Grundanforderung für alle Banken gelten. Die Offenlegungsvorschriften sind an anderer Stelle geregelt und gehören nicht ins Rundschreiben „Operationelle Risiken Banken“.

- **lit. a:** Dieser Passus im RS lässt sich nach unserem Verständnis in der internen Berichterstattung nicht oder zumindest nicht vernünftig umsetzen. Operationelle Risiken erwachsen einer Bank (wie bereits erwähnt) aus ihrer Geschäftstätigkeit, sie werden von einer Bank nicht aktiv „gesucht" oder bewusst eingegangen. Im Zusammenhang mit operationellen Risiken sind gerade grosse Verluste sehr selten und unerwartet. Entsprechend können solche „Verstösse" nicht nach dem Konzept des Rundschreibens gemessen oder festgestellt werden und es kann keine Aussage gemacht werden, ob die Risikobereitschaft/-toleranz bzw. definierte Schwellenwerte oder Limiten eingehalten wurden.
- **lit. c:** Wie werden „relevante“ externe Ereignisse definiert?

Rz 131/132
Wir sind überzeugt, dass die Vorgaben einer formellen, vom Verwaltungsrat genehmigten Offenlegungspolitik, insbesondere für die Offenlegung operationeller Risiken, keine zusätzliche Transparenz schaffen, sondern für zusätzliches Unverständnis sorgen. Entsprechende Offenlegungsvorschriften der Risikopolitik (Strategie, Prozesse und Organisation) sind bereits angemessen im FINMA-RS 2008/22 „EM-Offenlegung Banken“ vorgegeben. Diese umfassen auch die operationellen Risiken. Eine zusätzliche bzw. explizite Offenlegungspolitik für operationelle Risiken ist nicht sinnvoll und könnte zudem zu Abstimmungs- und Auslegungsschwierigkeiten führen. Die Rz 131 und 132 sind deshalb ersatzlos zu streichen.

Grundsatz 5 (Technologieinfrastruktur)
Rz 133
Dieser Abschnitt ist so generisch formuliert, dass er weder nützliche Hinweise zur Umsetzung noch wirklich praktische Relevanz enthält. Zum einen werden genügend IT-Investitionen für den heutigen und zukünftigen Bedarf einer geregelten Geschäftstätigkeit gefordert. Zum anderen werden spezifische Anforderungen an Daten und Systeme erwähnt. Schliesslich wird ein integriertes und umfassendes Risikomanagement gefordert. Die Liste der Anforderungen an Daten und Systeme ist zum Teil unvollständig, bei den Daten fehlt z.B. die Anforderung bezüglich der Vertraulichkeit. Was integriertes und umfassendes Risikomanagement der Technologieinfrastruktur bedeutet, bleibt offen. Es ist insbesondere auch zu prüfen, ob die Einhaltung der Grundsätze 1 bis 4 des vorliegenden Rundschreibens dies nicht bereits gewährleistet. Für ein effektives Management der operationellen Risiken ist nicht nur eine angemessene Technologieinfrastruktur erforderlich, sondern es sind auch genügend Personal und sonstige Ressourcen notwendig. Der Abschnitt ist nicht nützlich, schafft dagegen Unsicherheit und ist daher zu streichen.

Grundsatz 6 (Kontinuität bei Geschäftsunterbrechung)
Rz 134
Da die Empfehlungen der SBVg für das Business Continuity Management (BCM) vom 14. November 2007 gemäss FINMA-Rundschreiben 2008/10 als Mindeststandard anerkannt sind, erübrigt sich dieser Grundsatz bzw. die Rz 134.

Rz 135
Diese Regelung ergibt sich bereits implizit aus den Vorgaben der Rz 120 – 128. U.a. hat das Rahmenkonzept unternehmensspezifische Präzisierungen (Rz 124) zu enthalten und die Risikoidentifikation hat sowohl interne als auch externe Faktoren zu berücksichtigen (Rz 127). Die Notwendigkeit, in Rz 135 noch einmal auf spezifische operationelle Risiken einzugehen, ist damit nicht gegeben. Rz 135 kann somit ersatzlos gestrichen werden.

Rz 136
Falls Änderungen am Rundschreiben und an den Anhängen vorgenommen werden, erwarten wir, dass dies unter Einhaltung des üblichen Vernehmlassungsprozesses und der Untersuchung der Regulierungsfolgen erfolgt. Nach diesem Verständnis kann die Rz 136 ersatzlos gestrichen werden.

2 B Spezifische Bemerkungen bzw. Fragen zu den Randziffern von Anhang 3

Wie bereits in den einleitenden Bemerkungen ausgeführt, sind wir klar der Ansicht, dass Anhang 3 grundsätzlich nicht und vor allem nicht in dieser detaillierten Form als Anhang eines Rundschreibens erlassen werden soll. Im weiteren weisen wir nachstehend auf mehrere Punkte hin, die durch den Anhang trotz der umfassenden Formulierung nicht geklärt werden konnten. Sollte der Anhang tatsächlich in dieser oder ähnlicher Form in Kraft treten, müsste in mehreren Punkten Klarheit geschaffen werden, wodurch der Anhang noch gewichtiger werden würde. Wir beantragen daher den Umgang mit elektronischen Kundendaten lediglich auf der Basis von Prinzipien zu regeln. Damit erhielten die Banken die nötige Freiheit, um eine für sie vernünftige und individuelle Strategie zu verfolgen und Unsicherheiten, die sich aus dem Regulierungstext ergeben, würden vermieden.

Grundsatz 1 (Governance)
In Bezug auf Daten sind im Bankengeschäft mehrere Schutzziele zu definieren. Die Datenvertraulichkeit stellt eins davon. Im Grundsatz 1 ist es nicht begreiflich, warum für die Datenvertraulichkeit und insbesondere für natürliche Personen spezifisch eine Governance und ein Rahmenkonzept definiert werden sollten. Die Governance und das Rahmenkonzept sollten die IT-Systeme, -Prozesse und die elektronischen Daten als Ganzes abdecken.

Rz 2
Die FINMA-Banken-Klassifizierung ist nicht geeignet, im vorliegenden Zusammenhang das Proportionalitätsprinzip zu definieren. Der Ausschluss der genannten Rz für kleine Banken erscheint deshalb nicht stichhaltig. Wir empfehlen, das Proportionalitätsprinzip offener zu formulieren (siehe Anmerkungen zu den „Qualitativen Anforderungen“).

Rz 6
Die essentiellen Elemente (Struktur, Inhalt) des erwähnten Rahmenkonzepts sind unklar.

Grundsatz 2 (Kundenidentifikation)
Rz 8
Die Datenownership ist bei kleineren Instituten schwierig umzusetzen, da sich die verlangte Governance (komplette Neutralität) kaum einhalten lässt.

Rz 9
Müssen die Kategorien der Kundendaten in der Bank uniform betrachtet werden oder müssen sie nach Segmenten differenziert werden?

Rz 11
CID-Daten: Die vorliegende Liste schiesst v.a. im Bereich der (potentiell) indirekten Daten übers Ziel hinaus. Autokennzeichen oder Grundbuch Nr. können z. B. in jedem öffentlichen Register eingesehen werden. Kleinere Banken sollten hier selbst entscheiden können, welche Daten sie als schützenswert erachten.

Grundsatz 3 (Datenspeicherort und -zugriff)
Rz 16
Bei einem so hohen Detaillierungsgrad muss auch geklärt werden, was genau Inhalt des erwähnten Inventars sein muss.

Rz 23
Bei einer Behandlung der Kundendaten von geringer Relevanz im Ausland (z.B. Versand eines Communiqués an verschiedene Kunden), müssten die Kunden gleichermassen spezifisch und getrennt informiert werden. Dieser Aufwand erscheint uns nicht verhältnismässig. Ausserdem gibt es Überschneidungen zwischen dem vorliegenden RS und dem FINMA-RS 2008/7 „Outsourcing Banken“ (insbesondere Grundsatz 4 „Sicherheit“). Die bisherigen Vorgaben sollten respektiert werden.

Rz 24-26
Wir weisen darauf hin, dass Universalbanken eher eine offenere Konsultation der Kundendaten erlauben, wobei lediglich sensible Daten codiert werden. Das vorgeschlagene System wird bei vielen Instituten zu hohen Kosten bei der Umsetzung und dem Betrieb sowie zu einem negativen Einfluss auf den Kundenservice führen, mit einem zumindest fragwürdigen Nutzen.

Grundsatz 4 (Sicherheitsstandards für die Infrastruktur und die Technologie)
Rz 30
Wie soll die regelmässige Beurteilung der Lücken zwischen bestehendem internen Konzept und der Sicherstellung der Vertraulichkeit der Kundendaten und der Marktpraxis ablaufen? Mit den übrigen Rz gibt es genügend Vorgaben; der letzte Satz von Rz 30 sollte gestrichen werden.

Rz 31
Es ist nicht nachvollziehbar, welcher Sicherheitsstandard durch den jeweiligen Komplexitätsgrad der IT-Architektur nach der Meinung der FINMA angemessen wäre. Dies sollte in der Verantwortung der Banken liegen.

Rz 32
Wenn die Institute sich regelmässig mit der Marktpraxis vergleichen müssen, dann sollte die FINMA mit Hinblick auf die Vertraulichkeit der Daten selber einen Fragebogen erstellen, mit dem sie die Praxis der Banken ermitteln und sie miteinander vergleichen kann. Somit kann die FINMA jedem Institut eine Rückmeldung mit Vergleich zum Benchmark geben.

Grundsatz 5 (Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben)
Rz 37
Strebt die FINMA eine Zertifizierung des Kundendatenschutzes an? Wir verstehen diese Rz so, dass jedes Institut frei in der Wahl der Schutzmittel und des Schutzniveaus ist, wenn es von der Ausbildung des Mitarbeitenden überzeugt ist.

Rz 38
Welche Kriterien und Analysen sollten beim Rekrutierungsprozess von Mitarbeitenden, die mit Kundendaten arbeiten sollen, verwendet werden? Wie wird sichergestellt, dass die Mitarbeiterauswahl durch Dritte den CID-Vorgaben entspricht?

Rz 40
Welches sind die „Anforderungen für einen angemessenen Umgang mit CID“ falls eine Bank eine offenere Datenpolitik verfolgt, wodurch die Need-to-know-Personen nicht auf eine kleine Anzahl Mitarbeitende reduziert werden können?

Rz 41
In der Praxis wird die Führung einer Liste sämtlicher externen Mitarbeitenden mit Zugriff auf Massen-CID kaum möglich sein. Aus diesem Grunde sollten für das Outsourcing andere Bestimmungen gelten.

Grundsatz 6 (Risikoidentifizierung und –kontrolle in Bezug auf die CID-Vertraulichkeit)
Rz 44
Die Definition der Frequenz und Tiefe der Selbsteinschätzung fehlt.

Rz 45
Was erwartet die FINMA von den Risikoszenarien im Zusammenhang mit Kundendaten, wo doch der Risikobeurteilungsprozess in Ziffer 44 geregelt ist?

Grundsatz 7 (Risikominderung in Bezug auf die CID-Vertraulichkeit
Rz 47
Dieser Grundsatz würde bedeuten, dass als Beispiel jeder Report bei der Ausführung dem 4-Augenprinzip sowie einer Benachrichtigung an die Dateneigner unterliegt. Diese Daten- und Meldeflut ist nicht handhabbar. Zudem wird es kaum möglich sein, verdächtige Verhaltensweisen, insbesondere von Schüsselmitarbeitenden, zu identifizieren.

Rz 48
Nach Rz 48 sind Kundendaten für Tests für die Entwicklungen, Veränderung und Migration von Systemen mittels Techniken (Anonymisierung, Pseudonymisierung und Verschlüsselung) angemessen zu schützen. Dieser Forderung im IT-System nachzukommen, liesse sich nur mit hohen Aufwendungen realisieren. Zudem würde wegen der Anonymisierung die Qualität der Tests beeinträchtigt und das Betriebsrisiko aufgrund der höheren Komplexität gesteigert.

Rz 49ff
Diese Randziffern sind artfremd. Warum ist ein Kommunikationskonzept bei CID-Vertraulichkeit zu erarbeiten und in anderen Bereichen nicht?

Grundsatz 8 (Vorfälle im Zusammenhang mit der CID-Vertraulichkeit, interne und externe Kommunikation)
Rz 50
Wie sollte das Monitoring (und Reporting) dieser Vorfälle gestaltet werden und was sollte es enthalten? Was ist bei einem Institut, welches eine offenere Konsultation der Kundendaten erlaubt, unter einem Vorfall zu verstehen?

Es müssen insbesondere auch sämtliche Standorte, welche auf CID zugreifen, über Ressourcen verfügen, welche auf Vorfälle reagieren können. Der Begriff Standort meint in der Praxis eine Filiale der Bank. Da die entsprechenden Prozesse grundsätzlich zentralisiert sind, hat ein Standort bewusst nicht die nötigen Ressourcen um zu reagieren. Der Begriff Standort ist im Rundschreiben anzupassen.

Rz 51
Wie wird differenziert zwischen Vorfällen, die in der Berichterstattung abgebildet werden müssen, und solchen, die das nicht müssen; und wie muss das mit der Funktionsstufe des Empfängers abgestimmt werden?

Rz 53
Was ist unter einem schwerwiegenden Vorfall in Bezug auf die Vertraulichkeit von CID zu verstehen? Wann ist eine externe Kommunikation angezeigt und lässt sich eine solche tatsächlich auf Basis eines FINMA-RS vorschreiben?

Grundsatz 9 (Outsourcing-Dienstleistungen und Grossaufträge in Verbindung mit CID)
Diese Anforderungen gehören thematisch zum RS 2008/7 „Outsourcing Banken“.

Rz 55/56
An welche Kriterien denkt die FINMA bei der Einstufung der Sicherheits- und

Vertraulichkeitsstandards von Dritten (Dienstleistern)? Wie soll diese Abstützung auf unabhängige Informationen funktionieren?

Rz 59
Wie sollen die erwähnten Schlüsselkontrollen dokumentiert werden? Nach welchen Kriterien soll die Wirksamkeit der Schlüsselkontrollen beurteilt werden?

Rz 60ff
Wir empfehlen den Begriff „Schlüsselkontrollen“ im Glossar zu definieren.

3 Fragen der FINMA an die Banken

Frage 1
Eine Einführung per 1.1.2015 ist insbesondere mit Blick auf die Anforderungen aus Anhang 3 unrealistisch. Vor allem auf der technischen Seite sind fundamentale Systemanpassungen bei den verschiedenen Systemzulieferern notwendig. Dazu werden umfangreiche Analysen, Entwicklungen, Konfigurationen und Testzyklen notwendig sein. Da sowohl Banken als auch Softwarehersteller derzeit schon mit vielen weiteren regulatorischen Themen stark absorbiert sind, halten wir eine vollständige Einführung auf Beginn 2015 für illusorisch. Dementsprechend lehnen wir auch eine frühere Einführung der qualitativen Grundanforderungen ab.

Frage 2a
Die Kantonalbanken sind in dieser Thematik nur am Rande betroffen.

Frage 2b
Dies ist nicht das Kernproblem von Anhang 3.

Wir bedanken uns für die wohlwollende Prüfung unserer Kommentare und Anliegen. Für allfällige Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Thomas Hodel
Vizedirektor

VHV BCG

Vereinigung
Schweizerischer Handels-
und Verwaltungsbanken

Association
de Banques Suisses
Commerciales et de Gestion

Associazione
di Banche Svizzere
Commerciali e di Gestione

Per E-Mail
Eidgenössische Finanzmarktaufsicht FINMA
Herrn Alessandro Lana
Einsteinstrasse 2
3003 Bern

alessandro.lana@finma.ch

6300 Zug, 28. Juni 2013 Dg/jf
Baarerstrasse 12
Tel. 041 729 15 35 Fax 041 729 15 36
benno.degrandi@vhv-bcg.ch
www.vhv-bcg.ch

Anhörung zur Teilrevision des FINMA-Rundschreiben 2008/21:
Operationelle Risiken Banken

Sehr geehrte Damen und Herren
Sehr geehrter Herr Lana

Ich beziehe mich auf die eröffnete Anhörung zum FINMA-RS 2008/21 „Operationelle Risiken Banken"-Teilrevision. Die Vereinigung Schweizerischer Handels- und Verwaltungsbanken VHV dankt Ihnen für die Möglichkeit zur Stellungnahme und machen davon gerne Gebrauch.

Unsere Stellungnahme ist wie folgt gegliedert:

1. Allgemeine Bemerkungen
   1.1. Revision der „qualitativen Anforderungen gemäss Abschnitt IV
   1.2 Neuer Anhang 3: Umgang mit elektronischen Kundendaten

2. Detailkommentare zu einzelnen Randziffern
   2.1 Rundschreiben
   2.2 Anhang 3: Umgang mit elektronischen Kundendaten

3. Fragenliste zur Anhörung

4. Weiteres

1. Allgemeine Bemerkungen

1.1 Revision der „qualitativen Anforderungen“ gemäss Abschnitt IV

Eine stärkere Würdigung der operationellen Risiken sowie eine vermehrte Anlehnung an internationale Standards (z.B. Principles for the Sound Management of Operational Risk“) wird grundsätzlich begrüsst. **Dabei muss das Ziel darin bestehen, im Sinne von „Sound Practices“ Prinzipien zu definieren, welche abhängig vom Risikoprofil jedes einzelnen Instituts mehr oder weniger relevant und damit anwendbar sind. Der vorliegende Entwurf des FINMA RS 2008/21 (Teilrevision) erreicht jedoch unseres Erachtens die Zielsetzung nicht, und ist deshalb in** verschiedenen Punkten zu überarbeiten.

Insgesamt besteht die grosse Gefahr, dass mit Berücksichtigung von zu vielen Details und direkten/indirekten Vorgaben zu starre Leitplanken gesetzt werden, was die wirtschaftliche Freiheit einzelner Unternehmungen in einem zu hohen Masse einschränkt. Da der Entwurf nicht Prinzipien-basiert ist, sondern vielmehr zahlreiche formelle Detailregelungen für sämtliche Institute festschreibt, verstärkt er die bestehende Tendenz der sehr starken Formalisierung des Risikomanagements und erschwert damit eine effektive und effiziente Fokussierung der Risikomanagement-Ressourcen der kleineren und mittleren Institute auf die im spezifischen Fall wirklich relevanten Aspekte. Die mit dem Rundschreiben avisierte, sehr hohe Regulierungsdichte bezogen auf die Operationellen Risiken verhält sich relativ zur Regulierung und den qualitativen Anforderungen für Marktrisiken und Kreditrisiken inkonsistent: **Für viele Bereiche (Governance, Eigenmittelallokation, Festlegung des Risikoappetits, Offenlegung etc.) gehen die detaillierten qualitativen Anforderungen im vorliegenden Rundschreiben für Operationelle Risiken weit über jene für andere, ebenso relevante Risikokategorien hinaus.**

Mit Bezug auf die Vorgaben für andere Risikokategorien ist auch zu berücksichtigen, dass **operationelle Risiken nicht direkt vergleichbar mit anderen Risikokategorien (z.B. Markt- und Kreditrisiken) sind, was deren Identifizierung, Messung und Überwachung betrifft.** Vielfach muss mit Experteneinschätzungen und Annahmen gearbeitet werden, da nicht sämtliche Ereignisse und Tätigkeiten in direkt quantifizierbare Kosten umgewandelt werden können. **Damit sind auch Festlegungen von Limiten und Schwellenwerten nur bedingt anwendbar bzw. teilweise gar kontraproduktiv**, weil so eine Berechenbarkeit der Risiken vorgetäuscht wird, die nicht vorhanden ist.

Der Versuch, mittels einem **„Proportionalitätsprinzip“** (Abschnitt IV.A.) die Grösse der Bank zu berücksichtigen, ist sinnvoll. Unseres Erachtens wird die Anwendung dieses im Risikomanagement zentralen Prinzips jedoch zu stark eingeschränkt durch das Rundschreiben, indem es nicht als Grundsatz für alle Bestimmungen Gültigkeit hat, sondern darauf reduziert wird, dass kleine Banken (gemäss FINMA-Kategorien) einige wenige Bestimmungen nicht direkt umsetzen müssen, Es wäre wünschenswert, weitere Kriterien zu berücksichtigen und das Proportionalitätsprinzip umfassender einfliessen zu lassen, so dass für die Bewirtschaftung und Kontrolle Operationeller Risiken – wie auch für die anderen Risikokategorien – eine fokussierte Umsetzung abhängig vom Risikoprofil jedes einzelnen Instituts weiterhin möglich ist, unabhängig von der FINMA-Instituts-Kategorisierung. Zu beachten ist dabei, dass einzelne Ausführungen grosse Kostenfolgen mit sich bringen, die durch den Entwurf zu wenig bedacht wurden (Ertrag/Nutzen-Verhältnis nicht überall gegeben).

Weiter möchten wir anfügen, dass der **Zeitplan für eine allfällige Umsetzung der qualitativen Anforderungen bereits per Juli 2013 als zu knapp erachtet wird**. Es wird grundsätzlich empfohlen, den Zeitplan entsprechend zu verlängern. Es gilt zu berücksichtigen,

dass derzeit eine Reihe von regulatorischen Anforderungen zur Umsetzung im Raum stehen, die bereits einen beachtlichen Ressourceneinsatz erfordern (FATCA, Liquidität,…).

1.2 Allgemeine Bemerkung zum neuen Anhang 3: Umgang mit elektronischen Kundendaten

Der sorgfältige Umgang mit elektronischen Kundendaten ist im grössten Interesse jedes einzelnen Instituts. Die gesetzliche Vorgabe dafür ist in Art. 47 BankG definiert. **Sinn und Zweck sowie die Notwendigkeit des neuen, sehr detaillierten Anhanges sind u.E. nicht klar ersichtlich.** Die zusätzlichen Spezifizierungen bzw. Erweiterungen gehen zudem teilweise über die gesetzlichen Anforderungen hinaus (vgl. z.B. Rz 23/53) und führen zu Fragen bezüglich der Verhältnismässigkeit.

Falls der Anhang jedoch beibehalten werden soll, empfehlen wir, die einzelnen Grundsätze prinzipien-basiert zu formulieren und auf Detailregelungen zu verzichten. Konkret schlagen wir vor, jeweils nur die ersten Randziffern der Grundsätze 1 bis 9 beizubehalten („Grundsätze“) und die restlichen Vorgaben („Detailregelungen“) zu streichen. Der vorliegend hohe Detaillierungsgrad der Anforderungen greift zu tief in die operationellen Abläufe und Systeme der Banken ein, die je nach Institut sehr unterschiedlich ausgestaltet sind. Die praktische Umsetzung solch detaillierter Vorgaben wäre aus unserer Sicht zum Teil gar nicht oder nur mit erheblichen technischen Schwierigkeiten und Kostenfolgen möglich. Dies würde am Ziel der Regulierung, einen erhöhten Schutz im Umgang mit Kundendaten zu erreichen, vorbeiführen.

Stattdessen schlagen wir der FINMA vor, nebst den Grundsätzen **auf das SBVg Informationspapier vom Oktober 2012 betreffend „Data Leakage Protection“ (vgl. SBVg-Zirkular 7752) zu verweisen**. Dieses wurde von den entsprechenden Experten der Banken entwickelt und schlägt mögliche, aber nicht zwingende Lösungen für den Umgang mit vertraulichen Kundendaten vor. Diese „Best Practices“ sind unseres Erachtens besser geeignet als die vorgeschlagenen Detailregelungen, da sie den unterschiedlichen Geschäftstätigkeiten und IT-Lösungen der Banken besser Rechnung tragen und daher wirkungsvoller umsetzbar sind.

2. Detailkommentare zu einzelnen Randziffern

2.1 Rundschreiben

III. Eigenmittelanforderungen

F. Mindesteigenmittel und Untergrenze (Floor)

Rz 116/117/118: Es wird auf die Stellungnahme der SBVg verwiesen.

B. Qualitative Grundanforderungen

Rz 119: Es wird auf die Stellungnahme der SBVg verwiesen.

a) Grundsatz 1: Verantwortlichkeiten

Rz 120: Es wird auf die Stellungnahme der SBVg verwiesen.

Rz 121

Die Geschäftsführung hat dieses Rahmenkonzept zu entwickeln, in konkrete Vorgaben und Prozesse zu übertragen und anschliessend in den Geschäftseinheiten überprüfbar in den Risikomanagementprozessen umzusetzen. Dabei sind Massnahmen vorzusehen, um Verletzungen der Risikobereitschaft und Risikotoleranz rechtzeitig zu erkennen und zu beheben.

Bemerkung

Gegenüber den Konzepten der „Risikobereitschaft“ („Risk Appetite“ gemäss Erläuterungsbericht, p. 11) und der „Risikotoleranz“ im Zusammenhang mit operationellen Risiken sind grundsätzliche Vorbehalte anzubringen. Insbesondere die Vorstellung, dass eine Bank bereit ist, inhärente Risiken (d.h. ohne jegliche Kontrollen) einzugehen, erachten wir als konzeptionell falsch bzw. unrealistisch. Eine Bank sucht die operationellen Risiken im Vergleich zu anderen Risiken nicht aktiv, sondern sie erwachsen ihr aus ihrer Geschäftstätigkeit. Diesen Unterschied in der Art der Risiken gilt es zu berücksichtigen.

Empfehlung

Gänzliche Streichung der Konzepte der „Risikobereitschaft“ und der „inhärenten Risiken“ aus dem Rundschreiben.

Es wird empfohlen in Anlehnung an FINMA-RS 2013/6 „Liquidität Banken“ folgende Formulierung zu verwenden:

„Die Geschäftsleitung oder ein ihr direkt unterstellter Ausschuss entwickelt und setzt das Rahmenkonzept zur Bewirtschaftung des operationellen Risikos um.

Rz 122

Die Geschäftsführung definiert eine eindeutige, wirksame und solide Führungsstruktur, welche die Verantwortung zum Management der operationellen Risiken übernimmt. Diese Funktion ist für die Aufrechterhaltung und die laufende Weiterentwicklung des Rahmenkonzepts für das Management von operationellen Risiken zuständig. Sie muss zudem über genügend qualifiziertes Personal verfügen, um ihre zahlreichen Verantwortlichkeiten wirkungsvoll wahrnehmen zu können. Konsistent zu weiteren Risikomanagementfunktionen soll die Funktion des Management von operationellen Risiken adäquat in relevanten Gremien vertreten sein.

Bemerkung

Der Verweis auf „genügend qualifiziertes Personal“ ist wenig aussagekräftig, insbesondere, wenn kein Hinweis darauf besteht, was als adäquat erachtet oder als Minimum erwartet wird.

Empfehlung

Es wird empfohlen in Anlehnung an FINMA-RS 2013/6 „Liquidität Banken“ folgende Formulierung zu verwenden:

„Die Geschäftsleitung definiert eindeutige und wirksame Verantwortlichkeiten für das Management von operationellen Risiken. Des Weiteren ist eine klar bezeichnete Einheit für die Aufrechterhaltung und die laufende Weiterentwicklung des Rahmenkonzeptes für das Management von operationellen Risiken verantwortlich. Konsistent zu analogen Risikoeinheiten soll die Einheit für operationelle Risiken adäquat in relevanten bankinternen Gremien vertreten sein.

Rz 123: Es wird auf die Stellungnahme der SBVg verwiesen.

b) Grundsatz 2: Rahmenkonzept und Kontrollsystem

Rz 125

Das Rahmenkonzept hat mindestens folgende Aspekte abzudecken:

a. *Strukturen für das Management der operationellen Risiken, einschliesslich Kompetenzen, Rechenschaftspflichten und Berichtslinien;*
b. *Definition der Instrumente für die Identifikation, Messung, Beurteilung, Steuerung und Berichterstattung und ihrer Verwendung;*
c. *Bestimmung der Risikobereitschaft und der Risikotoleranz in Bezug auf die relevanten Arten von operationellen Risiken; Festsetzung von Schwellenwerten und/oder Limiten; Definition von Risikominderungsstrategien und -instrumenten;*
d. *Ansatz der Bank zur Identifikation von inhärenten Risiken (die Risiken vor Berücksichtigung der Kontrollen) sowie zur Festlegung und Überwachung von Schwellenwerten und/oder Limiten für Residualrisiken (die Risiken nach Berücksichtigung der Kontrollen);*
e. *Etablierung von Risikoberichterstattungs- und Managementinformationssystemen (MIS) für operationelle Risiken;*
f. *Festlegung einer einheitlichen Klassifizierung von materiellen operationellen Risiken zur Gewährleistung der Konsistenz im Rahmen der Risikoidentifikation, der Risikobewertung und Zielsetzung im operativen Risikomanagement;*
g. *Sicherstellung einer angemessenen unabhängigen Überprüfung und Beurteilung der operationellen Risiken;*

Pflicht zur zeitnahen Überprüfung und Anpassung des Rahmenkonzepts im Falle einer wesentlichen Veränderung der Risikosituation.

Bemerkung

Zu b: Nicht einheitliche Verwendung der Begrifflichkeiten.

Zu c/d: Operationelle Risiken sind nicht von der gleichen Art wie Markt- oder Kreditrisiken. Operationelle Risiken lassen sich nur sehr beschränkt mit "Limiten" oder Schwellenwerten steuern (am ehesten ist das möglich bei quantifizierbaren Risiken wie Anzahl Fehlbuchungen, Anzahl offener Posten, etc.). Nicht möglich ist dies jedoch bezogen auf Betrugsrisiken, Information Security, Legal- und Compliance- Risiken, welche als signifikanter als die quantifi-

zierbaren operationellen Risiken betrachtet werden. Grundsätzlich wird auch der Nutzen von Limiten bei operationellen Risiken stark angezweifelt.

Weiter ist unklar, ob eine Festlegung von Schwellenwerten und Limiten auf oberster Unternehmensebene als ausreichend erachtet wird oder ein Herunterbrechen auf zusätzlichen Ebenen erforderlich ist.

Zu h: Der Buchstabe „h)“ fehlt derzeit in der deutschen Version der Anhörungsunterlagen als Aufzählungspunkt noch. In der französischen Version wurde „zeitnah“ mit „en temps réel“ übersetzt, was jedoch „in Echtzeit“ bedeutet und ein deutlicher Unterschied zu „zeitnah“ darstellt.

Empfehlung

Zu b: Umformulierung der Begrifflichkeiten in „Identifizierung, Begrenzung und Überwachung“ (Vereinheitlichung; siehe dazu auch Bemerkungen zu den Begriffen unter „Weiteres“).
Die Komponente „Berichterstattung“ kann entfernt werden, da diese bereits unter e) aufgeführt wird.

Zu c/d: Entsprechend würden wir ganz davon absehen, den Begriff „Limiten“ zu verwenden. Falls Limiten trotzdem zur Anwendung gelangen sollen, schlagen wir eine Formulierung sinngemäss wie folgt vor: „(...) Bestimmung der Risikobereitschaft und der Risikotoleranz in Bezug auf die relevanten Arten von operationellen Risiken; Festsetzung von Schwellenwerten und/oder Limiten wo dies möglich und sinnvoll ist; Definition von Risikominderungsstrategien und -instrumenten“

Zu h: Eine französische Übersetzung „dans les meilleurs délais“ ist zu bevorzugen.

Hinweis: Bei Anpassungen zu dieser Rz sind allfällige Auswirkungen auf Rz 130 zu überprüfen.

Rz 126

Die Banken haben über ein adäquates, dokumentiertes Kontrollsystem, das auf Vorgaben, Prozessen und Systemen aufbaut, zu verfügen. Weiter haben sie interne Kontrollen sowie angemessene Risikominderungs- und/oder Risikotransferstrategien zu implementieren.

Bemerkung

Der Einschub ", das auf Vorgaben, Prozessen und Systemen aufbaut," ist u. E. nicht erforderlich. Massgebend ist, dass das Kontrollsystem adäquat und dokumentiert ist. Eine Definition, worauf dieses basieren muss, erachten wir als unnötige Einschränkung bzw. dies führt u. U. zu einem ungebührlichen Bürokratieaufwand. Das Kontrollsystem muss dem Geschäft und der Grössenordnung der jeweiligen Bank Rechnung tragen. Des Weiteren verstehen wir den Unterschied zwischen "über ein Kontrollsystem verfügen" und "interne Kontrollen zu implementieren" nicht. Insofern wird im 2. Satz nur wiederholt, was im ersten erwähnt ist. Entsprechend kann man diesen Passus im 2. Satz ersatzlos streichen.

Empfehlung

Die Banken haben über ein adäquates, dokumentiertes Kontrollsystem~~, das auf Vorgaben, Prozessen und Systemen aufbaut,~~ zu verfügen. Weiter haben sie angemessene Risikominderungs- und/oder Risikotransferstrategien zu implementieren.

Es sollte zudem auf das FINMA-RS 2008/24 „Überwachung und interne Kontrolle Banken“ verwiesen werden, damit klar wird, dass das Kontrollsystem bezüglich operationeller Risiken auf das allgemeine Kontrollsystem der Bank aufbauen und nicht als davon losgelöst betrachtet werden soll.

c) Grundsatz 3: Identifizierung, Begrenzung und Überwachung

Rz 127

Die Identifizierung, Begrenzung und Überwachung von Risiken bilden die Grundlage eines wirksamen Risikomanagementsystems. Eine wirksame Risikoidentifikation berücksichtigt sowohl interne als auch externe Faktoren. Beispiele von Instrumenten und Methoden, die zur Identifikation und Beurteilung der operationellen Risiken eingesetzt werden können, sind:

a. *Risiko- und Kontrollbeurteilungen;*
b. *Revisionsergebnisse;*
c. *Erhebung und Analyse interner Verlustdaten;*
d. *Erhebung und Analyse externer Ereignisse mit operationellen Risiken;*
e. *Analyse der Zusammenhänge zwischen Risiken, Prozessen und Kontrollen;*
f. *Risiko- und Performance-Indikatoren für die Überwachung von operationellen Risiken und die Wirksamkeit des internen Kontrollsystems;*
g. *Szenarioanalysen;*
h. *Messung und Quantifizierung des Verlustpotenzials;*
i. *Vergleichende Analysen.*

Bemerkung

Die Quantifizierung des Verlustpotentials ist bei seltenen, aber gravierenden Ereignissen eine äusserst ungenaue und nicht zielführende Angelegenheit. Wir warnen vor einer Zahlen- und Modellgläubigkeit und vor einer zu starken Ressourcenallokation auf diese Themen, mit der Folge, dass diese Ressourcen im effektiven Risikomanagement dann fehlen.

Es wird zudem zuerst von der „Identifizierung, Begrenzung und Überwachung“ von Risiken als Grundlage des Risikomanagements gesprochen, während danach aber nur von „Identifizierung und Beurteilung“ die Rede ist und zu Begrenzung und Überwachung keine weiteren Hinweise gegeben werden.

Bei den Beispielen von Instrumenten und Methoden (Bst. a bis i) stellen sich uns folgende Fragen:

Zu a) Was ist unter „Risiko-und Kontrollbeurteilungen“ zu verstehen? Diese sollten doch gerade das Resultat dieser Instrumente und Methoden sein und sollten daher u.E. nicht in dieser Liste aufgeführt werden.

Zu d) Im Erläuterungsbericht (4.6.3 p. 13) wird folgende Ergänzung angebracht: *„Die Sammlung und Analyse der in- und externen Verlustdaten muss durch ein transparentes Verfahren erfolgen und dokumentiert werden. Diesbezüglich kann von den Erfahrungen der AMA-Banken profitiert werden. […] Für externe Daten kann man sich zusätzlich auf die Randziffern 86-88 des vorliegenden Rundschreibens stützen."*

Die Anbindung an eine externe Datenbank oder gar ein systematischer Aufbau einer eigenen Lösung ist für kleine und mittlere Banken nur bedingt eine Option, da dies zu erheblichen administrativen Mehr-Aufwand und damit zu deutlich höherem Ressourcenbedarf (Mitarbeiter, Finanziell,…) führt, ohne einen entsprechenden Nutzen zu generieren. Der Verweis auf AMA-Banken ist somit auch eine indirekte Anweisung, sich nach diesen „Best-Practice"-Modellen auszurichten und quasi eine Einführung eines neuen „Standard-Modells".

Zu i) Wird hier vorgeschlagen, mehrere Methoden parallel anzuwenden und diese gegeneinander abzuwägen bzw. mehrere unterschiedliche Ergebnisse zu berücksichtigen?

Empfehlung

Überprüfung der Begrifflichkeiten und gegebenenfalls Anpassungen (beispielsweise Streichung von „Beurteilung").

Streichung der Verweise auf die institutsspezifischen Ansätze „AMA" (Erläuterungsbericht). Ein Verweis auf AMA ist ungeeignet für Institute, welche einer der beiden anderen Ansätze anwenden. Denn durch einen solchen Verweis werden neue Vorgaben geschaffen, die für diese einfacheren Standards explizit nicht vorgesehen waren.

Rz 128: Es wird auf die Stellungnahme der SBVg verwiesen und zudem auf unsere Bemerkung nachstehend unter „4. Weiteres", Punkt „Pricing".

d) Grundsatz 4: Interne und Externe Berichterstattung

Rz 129: Es wird auf die Stellungnahme der SBVg verwiesen.

Rz 130

Die interne Berichterstattung über operationelle Risiken kann Finanz-, Betriebs- und Compliance-Daten, aber auch risikorelevante externe Informationen über Ereignisse und Bedingungen umfassen, die für die Entscheidungsfindung wesentlich sind. Die Berichterstattung über operationelle Risiken muss dabei mindestens folgende Punkte abdecken und deren mögliche Auswirkungen auf die Bank und das für die operationellen Risiken erforderliche Eigenkapital darstellen:

a. *Verstösse gegen die definierte Risikobereitschaft und die Risikotoleranz der Bank sowie Überschreitungen von diesbezüglich festgesetzten Schwellenwerten und/oder Limiten bei relevanten Arten von operationellen Risiken;*
b. *Einzelheiten zu signifikanten internen operationellen Risikoereignissen und/oder Verlusten;*

c. Informationen zu relevanten externen Ereignissen und potentiellen Risiken sowie deren mögliche Auswirkungen auf die Bank.

Bemerkung

Formulierung als "…mindestens folgende Punkte abdecken…" für Punkt c. erachten wir als sehr problematisch in der Umsetzung. Das Universum relevanter externer Ereignisse ist riesig, und dem entsprechend ist eine vollumfängliche Berücksichtigung unmöglich.

Empfehlung

Zu a) Wir verweisen auf unseren Kommentar zu Grundsatz 1 und schlagen vor, den Begriff „Risikobereitschaft“ zu streichen

Zu c) Umformulierung von c. in:

„Im Weiteren können auch Informationen zu relevanten externen Ereignissen und potentiellen Risiken sowie deren mögliche Auswirkungen auf die Bank in die Berichterstattung miteinbezogen werden.“

„Entscheidungsfindung“ durch „Identifizierung, Begrenzung und Überwachung“ zu ersetzen, damit klar wird, welchem Zweck die Berichterstattung dient.

Rz 131

Eine Bank muss über eine formelle, vom Verwaltungsrat genehmigte Offenlegungspolitik verfügen. Aus dieser muss hervorgehen, welchen Ansatz die Bank im Rahmen der Offenlegung

der operationellen Risiken verfolgt und welche Kontrollprozesse bezüglich der Offenlegung anzuwenden sind. Zudem ist ein Prozess zu implementieren, der die Angemessenheit bezüglich

Inhalt und Frequenz der Offenlegungen sicherstellt und deren regelmässige Überprüfung regelt.

Bemerkung

Unklarheit bezüglich der Bedeutung der „Offenlegung“? Offenlegung (z.B. via Geschäftsbericht) gegenüber Aufsichtsbehörden, Aktionären, Kunden, Mitarbeiter, Medien,…?

Die Offenlegung von Risikoinformationen jeglicher Art wird in der Regel nicht von der Unternehmung selbst bestimmt, sondern wird im Rahmen des Rechnungslegungsstandards (z.B. FINMA-RS 2008/2 „Rechnungslegung Banken“, Rz 149) oder aufgrund von aufsichtsrechtlichen Anforderungen (z.B. FINMA-RS 2008/22 „EM-Offenlegung Banken“) verlangt. Dabei sind jeweils auch Inhalt, Frequenz und Überprüfung der Offenlegungen geregelt.

Eine über die bestehenden aufsichtsrechtlichen und rechnungslegungstechnischen Anforderungen hinausgehende, separate Offenlegung zum Management von operationellen Risiken würden wir klar ablehnen. Eine solche wäre, insbesondere im Ver-

gleich zu anderen Risiken (z.B. Kredit-oder Liquiditätsrisiken), unverhältnismässig und würde zu Redundanzen mit anderen Offenlegungen führen.

Zudem wäre es unverhältnismässig und unsachgemäss, den Erlass einer solchen Offenlegungspolitik für operationelle Risiken auf Stufe des Verwaltungsrates anzusiedeln, zumal dies im Falle von Markt- und Kreditrisiken nicht verlangt ist. Falls eine Bank einen Prozess betreffend ihre Risikooffenlegungen festhalten möchte, so ist es ihr selbst zu überlassen, wie und auf welcher Stufe sie dies regelt.

Empfehlung

Streichung der Rz, falls die Offenlegung nach Aussen (Extern) gemeint ist, andernfalls Ersetzen des Begriffs „Offenlegung" durch „Rapportierung" oder „internes Berichtswesen". Hierbei sollte es primär um eine stufengerechte und situationsadäquate Informationspolitik gehen, welche innerhalb der Bank wie auch (in grösseren Fällen) nach aussen gegenüber Audit und/oder der FINMA stattfindet.

Rz 132: Es wird auf die Stellungnahme der SBVg verwiesen.

e) Grundsatz 5: Technologieinfrastruktur

Rz 133

Zur Unterstützung des Management operationeller Risiken hat die Geschäftsführung insbesondere für eine angemessene Technologieinfrastruktur zu sorgen, die den aktuellen und längerfristigen Geschäftsbedürfnissen Rechnung trägt. Zu diesem Zweck hat sie ausreichende Kapazitäten bereitzustellen, die sowohl den üblichen Geschäftsbetrieb als auch Stressphasen abdecken. Überdies hat sie die Sicherheit, Integrität und Verfügbarkeit der Daten und Systeme zu gewährleisten sowie ein integriertes und umfassendes Risikomanagement zu implementieren.

Bemerkung

Die Randziffer scheint uns sowohl hinsichtlich Inhalt als auch Formulierung problematisch. Zum einen sind wir der Ansicht, dass die ersten beiden Sätze der Randziffer für eine Bank allgemein und in jeder Situation bzw. betreffend alle möglichen Risiken Gültigkeit haben und daher hier nicht explizit wiederholt werden müssten. Es liegt unseres Erachtens ein grundsätzliches Interesse der Banken daran, dass die IT einem adäquaten Zustand entspricht. Unklar ist auch inwieweit die Technologieinfrastruktur für die längerfristigen Geschäftsbedürfnissen angemessen ausgerichtet werden muss? Weswegen wird dennoch auf diesen Punkt hingewiesen (→ Geschäftsrisiko)? Wird auf die operationellen Risiken aufgrund von inadäquaten Systemen explizit hingewiesen, müssten demnach auch z.B. die Mitarbeiter oder interne Verfahren aufgeführt werden.

Weiter ist der Sinn und Zweck des letzten Satzes dieser Randziffer nicht klar. Darin wird verlangt, dass die Geschäftsleitung ein „integriertes und umfassendes Risikomanagement" implementiert, ohne dass erläutert wird, was darunter zu verstehen ist. Besonders unklar ist auch der Begriff des „integrierten" Risiko-managements. Die Vorgaben zu Aufbau und Art des Managements von operationellen Risiken sind zudem bereits in den Grundsätzen 1 bis 4 erläutert und sollten daher hier nicht nochmals aufgenommen werden.

Empfehlung

Streichung der gesamten Rz oder zumindest des letzten Teiles dieser Randziffer („sowie ein integriertes […]“).

f) Grundsatz 6: Kontinuität bei Geschäftsunterbrechung

Rz 134

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.

Bemerkung

Was ist die Begründung, dass dieser bereits abgedeckte Punkt (SBVg-Empfehlung zum Business Continuity Management) aufgeführt wird? Eine derzeitige Beurteilung für eine bestimmte Bankengruppe als besonders relevant (gemäss Erläuterungsbericht), kann nicht einziger Gradmesser sein, da diese eine dynamische ist und bereits nächstes Jahr überholt sein könnte.

Von Seiten SBVg wird zudem darauf hingewiesen, dass die Empfehlungen derzeit in Überarbeitung sind. Die Referenz in der Fussnote müsste daher zu gegebener Zeit nochmals angepasst werden. Unten stehender Formulierungsvorschlag (Empfehlung) ist mit den überarbeiteten Empfehlungen abgeglichen und kompatibel.

Empfehlung

Streichung der Rz oder folgende Anpassung (in Anlehnung an SBVg):

„Die Geschäftsleitung ist zuständig für die Konkretisierung der Business Continuity Management Strategie (Strategie für das betriebliche Kontinuitätsmanagement), welche die Kontinuität des Geschäftsbetriebes und die Wiederherstellung der kritischen Geschäftsprozesse im Falle eines schweren Unterbruches sicherstellen soll.“

C. Risikospezifische Qualitative Anforderungen

Rz 135

Spezifische operationelle Risiken, u.a. beruhend auf dem Geschäftsmodell (z.B. operationelle Risiken im Umgang mit Kundendaten oder grenzüberschreitenden Tätigkeiten), verlangen eine umfassendere und intensivere Steuerung sowie Kontrolle der operationellen Risiken als dies in den qualitativen Grundanforderungen vorgegeben ist. Die Geschäftsführung ist generell verpflichtet, die nötigen weitergehenden Massnahmen zu implementieren, um eine adäquate Überwachung solcher Risiken sicherzustellen.

Bemerkung

Die Zielsetzung dieser Bestimmung ist u.E. unklar. Die qualitativen Grundanforderungen geben wenig bzw. keine Anhaltspunkte bzgl. Umfang der Steuerung und Kontrolle. Weswegen wird dennoch darauf hingewiesen, dass diese für besonders relevante operationelle Risiken aufgrund des Geschäftsmodells weitergehen sollen?

Es wird impliziert, dass gewisse Banken in ihren Anstrengungen zum Management der operationellen Risiken über die Anforderungen von Kapitel IV.B hinausgehen müssen, ohne dass jedoch ausgeführt wird, welche zusätzlichen Massnahmen zu ergreifen bzw. Anforderungen zu erfüllen wären. Diese offene Formulierung führt zu massiver Rechtsunsicherheit für die Banken, insbesondere da die Kriterien, welche eine „umfassendere und intensivere“ Steuerung und Kontrolle der operationellen Risiken begründen würden, völlig unklar sind. Als einziges Kriterium werden „spezifische operationelle Risiken“ genannt, welche beispielsweise dem Geschäftsmodell der Bank geschuldet sein könnten. In diesem Zusammenhang werden als Beispiele die „operationellen Risiken im Umgang mit Kundendaten“ und „grenzüberschreitende Tätigkeiten“ genannt.

Diese beiden Beispiele sind jedoch eher verwirrend als klärend, da sie zwei grundsätzlich verschiedene Dimensionen betreffen: Das eine ist ein Risiko und das andere eine Art der Geschäftstätigkeit. Des Weiteren kann davon ausgegangen werden, dass grundsätzlich allen Banken gewisse Risiken im Umgang mit Kundendaten erwachsen, weshalb gemäss der Formulierung von Rz 135 alle Banken nicht näher spezifizierte, zusätzliche Massnahmen einführen müssten, die über die Grundanforderungen von Kapitel IV.B hinausgehen. Wir gehen davon aus, dass eine solche weitreichende Ausdehnung der Anforderungen auch nicht im Sinne der FINMA ist.

Empfehlung

Streichung der Rz oder aber zumindest nochmals überarbeiten und entsprechend umformulieren.

Rz 136

Falls die FINMA es als notwendig erachtet, kann sie für spezifische Themen weitergehende Konkretisierungen an das Management von operationellen Risiken definieren. Dies geschieht zurückhaltend und unter Anwendung des Proportionalitätsprinzips. Weitergehende qualitative Anforderungen werden thematisch sortiert im Anhang zum Rundschreiben veröffentlicht.

Bemerkung

Inwieweit wird damit die Grundlage geschaffen um weitergehende Konkretisierungen und Ausführungen an das OpRisk Mgmt diese Themen in Anhängen zu gliedern?

Auch diese Rz muss unseres Erachtens vollständig gestrichen werden, da eine “Eigen-Ermächtigung“ der FINMA weder rechtlich möglich noch nötig ist. Falls es Themen gibt, die nach Ansicht der FINMA weiter konkretisiert werden müssen, so kann sie dies jederzeit via ein ordentliches Regulierungs- und Anhörungsverfahren tun. Auch ist sie frei, dies im Rundschreiben oder aber in einem Anhang, der ja ein integrierender Bestandteil des Rundschreibens darstellt, zu tun.

Falls jedoch die FINMA beabsichtigt, aufgrund von Rz 136* „weitergehende Konkretisierungen“ oder „weitergehende qualitative Anforderungen“ ohne ordentliches Verfahren anzuordnen, so würden wir dies vehement ablehnen.

Empfehlung

Streichung der Rz.

2.2 Anhang 3: Umgang mit elektronischen Kundendaten

Rz 2

Kleine Banken sind von der Erfüllung folgender Randziffern ausgenommen:

- *Randziffern 15 bis 19, sowie 24 bis 29 des Grundsatzes 3;*
- *Alle Randziffern der Grundsätze 4 bis 6;*
- *Randziffer 48 des Grundsatzes 7.*

Bemerkung

Die für kleinere Banken vorgesehenen Ausnahmeregelungen sind nicht schlüssig. So ist beispielsweise nicht nachvollziehbar, weshalb ein kleineres Institut vom „Need to know"-Grundsatz (Rz 24*) ausgenommen werden sollte, zumal es sich hier um ein vom Datenschutz gefordertes Grundprinzip handelt.

Empfehlung

Mit der Errichtung eines prinzipien-basierten Grundsatzkatalogs würde auch für dieses Problem Abhilfe geschaffen werden, da damit die Umsetzung der Grundsätze institutsspezifisch und der Grösse und Struktur des Instituts angepasst erfolgen kann.

I. Grundsätze für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten

A. Grundsatz 1: Governance

Rz 3: Es wird auf die Stellungnahme der SBVg verwiesen.

C. Grundsatz 3: Datenspeicherort und -zugriff

Rz 15

Die Bank muss wissen, wo CID gespeichert werden, von welchen Anwendungen und IT-Systemen CID verarbeitet werden und wo elektronisch auf sie zugegriffen werden kann. Mittels angemessenen Kontrollen ist sicherzustellen, dass die Daten nach Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz bearbeitet werden. Für physische Bereiche (z.B. Serverräume) oder Netzwerkzonen, in denen grosse Mengen an CID gespeichert oder zugänglich gemacht werden, sind spezielle Kontrollen erforderlich. Der Datenzugriff muss klar geregelt werden und darf nur auf einer strikten „Need to know"-Basis erfolgen.

Bemerkung

Wir sind einverstanden, dass der Datenzugriff auf der Basis von "need to know" erfolgt. Dies ist typischerweise für alle normalen Userzugriffe implementiert. Für spezielle Benutzergruppen wie Administratoren hingegen kann dieses Prinzip nicht eingehalten werden. Um dennoch Datensicherheit zu gewähren, müssen solche Gruppen speziell behandelt werden.

Empfehlung

Anpassung des Abschnitts wie folgt:

~~Der Datenzugriff muss klar geregelt werden und darf nur auf einer strikten „Need to know"-Basis erfolgen~~. → „Für Applikationsbenutzer muss der Datenzugriff klar geregelt werden und darf nur auf einer strikten „Need to know"-Basis erfolgen. Für Benutzer mit erweiterten Rechten (bspw. Datenbankadministratoren) muss deren Zugriff auf die Daten mittels Logging und Monitoring überwacht werden, dass diese jederzeit zur Verantwortung gezogen werden können (accountability)."

c) „Need to know"-Grundsatz

Rz 24

Personen dürfen nur auf diejenigen Informationen oder Funktionalitäten Zugriff haben, die für die Wahrnehmung ihrer Aufgaben erforderlich sind. Der Zugriff auf CID darf nur erfolgen, wenn die CID verantwortlichen Einheiten („Data Owners") die Zugriffsrechte genehmigt haben. Die Erteilung von Zugriffsrechten hat wie folgt zu erfolgen:

Bemerkung / **Empfehlung**

Die Nennung des Grundsatzes genügt; weitere Ausführungen bedarf es nicht.

Rz 26

- *Funktional: Die Zugriffsberechtigung ist nach der Funktion (Art der Aufgaben), die der Mitarbeitende im Zusammenhang mit CID ausübt, zu erteilen. Wenn die Ausübung der Aufgabe keine Bearbeitung von CID erfordert (z.B. Erstellung von Berichten, Datenanalyse, Beratung), so ist die Zugriffsberechtigung zu beschränken (z.B. durch die Erteilung von Read-only-Rechten).*

Bemerkung

Read-only Zugriff schützt nicht gegen den Verlust der Vertraulichkeit.

Empfehlung

Hinweis ersatzlos streichen.

Rz 27

Die Erteilung von Zugriffsrechten muss regelmässig überprüft werden.

Bemerkung

Siehe Empfehlung für Anpassung: Dieser Unterschied mag auf den ersten Blick unbedeutend erscheinen, hat aber eine andere Bedeutung. Ersteres hat den Fokus auf den Prozess der Zuteilung und zweites auf das Resultat. Vielleicht müssten sogar beide Aspekte berücksichtigt werden.

Empfehlung

Die Gültigkeit der erteilten Zugriffsrechte ~~Erteilung von Zugriffsrechten~~ muss regelmässig überprüft werden.

d) Zugriffs-Verzeichnis

Rz 28

Die Bank muss ein Verzeichnis der Mitarbeitenden und Dritten, die Zugriffsberechtigungen auf CID haben, führen. Im Verzeichnis müssen auch privilegierte IT-Benutzer und Anwender aufgeführt sein (siehe Rz 41 dieses Anhangs). Nur Personen, welche im Verzeichnis aufgeführt sind, dürfen auf CID zugreifen.

Bemerkung

Wir sind der Meinung, dass dieser Punkt Ursache und Folge vermischt. Wir glauben, dass durch ein Autorisierungssystem, welches ggf. rollenbasiert ist, Zugriffsrechte erteilt werden sollen. Das Verzeichnis aller Zugriffsrechte ist dann ein Ausfluss (Report) dieses Systems. Ein Vorgehen, wie in Rz 28 stipuliert ist in einer mittleren oder grossen Bank nicht implementierbar (Liste als Grundlage der Autorisierungsvergabe)

Empfehlung

Streichung der Rz oder zumindest eine Umformulierung erwägen.

D. Grundsatz 4: Sicherheitsstandards für die Infrastruktur und die Technologie

Rz 30

Die zum Schutz der CID-Vertraulichkeit verwendeten Sicherheitsstandards für die Infrastruktur und Technologie müssen in Bezug auf die Komplexität der Bank sowie seiner Risikoexposition angemessen sein und den Schutz von CID auf dem Endgerät (am Endpoint), von übertragenen und gespeicherten CID sicherstellen. Da die Informationstechnologien schnellen Änderungen unterliegen, ist die Entwicklung von Datensicherheitslösungen aufmerksam zu verfolgen. Lücken zwischen dem bestehenden internen Rahmenkonzept zur Sicherstellung der Vertraulichkeit von Kundendaten und der Marktpraxis sind regelmässig zu beurteilen.

Bemerkung

Diese Anforderung würde zwangsläufig dazu führen, dass jede Bank eine „Data Leakage Protection“ (DLP) - Lösung einführen muss, die sehr teuer ist.

Empfehlung

Dieser Satz enthält keine massgeblichen zusätzlichen Informationen und kann ersatzlos gestrichen werden: „Da die Informationstechnologien schnellen Änderungen unterliegen, ist die Entwicklung von Datensicherheitslösungen aufmerksam zu verfolgen.“

E. Grundsatz 5: Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben

a) Sorgfältig[e] Auswahl der Mitarbeitenden

b) Gezielte Schulungen der Mitarbeitenden

c) Sicherheitsanforderungen

Rz 38-40

Bemerkung

Wir sind an sich mit dem Inhalt der RZ 38-40 einverstanden, sehen aber bei der Umsetzung (und deren Evidenzerbringung) grosse Probleme. Die allermeisten Mitarbeiter einer Bank haben auf die eine oder andere Art Zugriff auf CID Daten. Uns sind keine Methoden bekannt, mit Hilfe derer verlässlich im Vorfeld einer Anstellung (Rz 38) oder danach im laufenden Betrieb (Rz 40) der "angemessene Umgang" überprüft werden kann.

Empfehlung

Wir schlagen vor, diese Sätze zu streichen oder ggf. nur auf Mitarbeiter mit Massen-CID Zugriff zu beschränken.

F. Grundsatz 6: Risikoidentifizierung und -kontrolle in Bezug auf die CID-Vertraulichkeit

Rz 43

Die für die Datensicherheit und -vertraulichkeit zuständige Einheit identifiziert und bewertet die inhärenten Risiken und die Residualrisiken betreffend die Vertraulichkeit von CID mithilfe eines strukturierten Prozesses. Dieser Prozess muss die Risikoszenarien in Bezug auf die CID-Vertraulichkeit umfassen, die für die Bank und die Definition der entsprechenden Schlüsselkontrollen relevant sind. Der Katalog der Schlüsselkontrollen in Bezug auf die Datenvertraulichkeit zur Gewährleistung des CID-Schutzes muss laufend um neue und verbesserte Kontrollen aktualisiert werden.

Bemerkung

Die Forderung nach "immer mehr und neuen Kontrollen" ist nicht zielführend. Es muss vielmehr die Adäquanz garantiert werden.

Randziffer 43*, Risikoidentifizierung und -kontrolle in Bezug auf CID-Vertraulichkeit: Der Grundsatz sollte dahingehend ergänzt werden, dass die Risikoidentifizierung und -kontrolle abhängig vom Tätigkeitsprofil und der Risikosituation des jeweiligen Finanzinstituts erfolgen sollte.

Empfehlung

Anpassung des Satzes wie folgt:

„[…] muss laufend ~~um neue und Verbesserte Kontrollen aktualisiert werden.~~ auf Adäquanz überprüft werden und gegebenenfalls angepasst werden."

G. Grundsatz 7: Risikominderung in Bezug auf die CID-Vertraulichkeit

a) Produktionsumfeld, Aktivitäten in Verbindung mit Massen-CID

Rz 47

Aktivitäten, die im Produktionsumfeld mit nicht anonymisierten, nicht verschlüsselten und nicht pseudonymisierten Massen-CID durchgeführt werden, müssen geeigneten Verfahren unterliegen (z.B. Vieraugenprinzip und Log-Dateien), einschliesslich der Benachrichtigung der für die Datensicherheit und -vertraulichkeit zuständigen Einheit. Es wird erwartet, dass dies die Arbeit von IT-Administratoren, Mitarbeitenden mit erhöhten Zugriffsrechten und Mitarbeitenden Dritter miteinschliesst. Umfangreiche Anfragen zu CID – die nicht anonymisiert, pseudonymisiert oder verschlüsselt sind – und die nicht bewilligt wurden, oder Anfragen, die auf ein verdächtiges Verhalten hinweisen könnten, müssen sofort dem obersten Management gemeldet werden.

Bemerkung

Im ersten Satz der Rz ist die Rede von Aktivitäten. Dies ist ein sehr weiter Begriff, der hier nicht weiter präzisiert wird und somit offen lässt, was die FINMA alles darunter versteht. Dieser Interpretationsspielraum ist zu gross und wird unweigerlich zu Diskussionen zwischen der FINMA, den Revisionsgesellschaften und den Banken führen. Produktionsumfeld, Aktivitäten in Verbindung mit Massen-CID:

Empfehlung
Der Begriff „Aktivitäten" ist zu präzisieren, da in dieser Form nicht klar ist, welche Tätigkeiten darunter fallen.

b) Tests für die Entwicklung, Veränderung und Migration von Systemen

Rz 48

Während der Entwicklung, Veränderung und Migration von Systemen müssen die CID angemessen vor dem Zugriff und der Nutzung durch Unberechtigte geschützt werden. Techniken zur Anonymisierung, Pseudonymisierung und Verschlüsselung (ob intern oder extern entwickelt) müssen umfassend getestet sowie periodisch überprüft werden und haben einer strikten Vieraugenkontrolle zu unterliegen. Vor ihrer Anwendung auf grosse Datensätze müssen Tests auf eine Reihe von kleinen CID-Sätzen beschränkt werden.

Bemerkung

Der Hinweis auf die „strikte Vieraugenkontrolle" ist unklar. Soll mit dem Prinzip die Anonymisierung sichergestellt werden bzw. festgestellt werden, ob diese korrekt durchgeführt wurde oder die Techniken selbst adäquat sind?

Empfehlung

Weitere Erläuterungen zur Bedeutung des „strikten Vieraugenkontrolle".

H. Grundsatz 8: Vorfälle im Zusammenhang mit der CID-Vertraulichkeit, interne und externe Kommunikation

b) Meldung

Rz 51

Es wird erwartet, dass das Risiko der Vertraulichkeit von CID und diesbezügliche Compliance-Meldungen in den internen Berichterstattungen angemessen abgebildet sind.

Bemerkung

Wir sind der Meinung, dass Events im Bereich CID von höchster Geheimhaltungsstufe sind, und weder im "normalen Berichtswesen" noch breitgestreut in einem speziellen Berichtswesen erfolgen soll. Es ist im Interesse der Bank, aus Fehlern zu lernen, nicht jedoch jedermann die Mechanismen zu erklären, welche den Event erlaubt (bzw. nicht verhindert) haben.

Empfehlung

Umformulierung der Rz wie folg:

„Es wird erwartet, dass das Risiko der Vertraulichkeit von CID und diesbezügliche Compliance-Meldungen in den internen Berichterstattungen angemessen abgebildet sind oder alternativ sichergestellt ist, dass eine systematische Erfassung und Eskalierung an geeignete Stellen erfolgt, falls dies die Geheimhaltung solcher Vorkommnisse erfordert.“

I. Grundsatz 9: Outsourcing-Dienstleistungen und Grossaufträge in Verbindung mit CID

d) Ausgestaltung der Kontrollen und Wirksamkeitstests

Rz 59

Die Bank muss wissen und verstehen, welche Schlüsselkontrollen in Verbindung mit der Vertraulichkeit von CID der Outsourcing-Dienstleister durchzuführen hat. Mit dem externen Anbieter sind sämtliche Themen im Zusammenhang mit der Ausgestaltung solcher Kontrollen zu ermitteln und zu besprechen. Alle Dienstleistungen, die von externen Anbietern erbracht werden und Risiken in Bezug auf die Vertraulichkeit von CID bergen, sind fortlaufend zu überwachen. Die Einhaltung interner Anforderungen sowie die Wirksamkeit der Schlüsselkontrollen sind dabei zu prüfen und zu beurteilen.

Bemerkung

Für die Überwachung der externen Dienstleister müssten Log-Protokolle (“Log-Files“) erzeugt und gesammelt werden. Es müssten Hilfsmittel für die automatischen Log-Auswertungen/Alerts eingeführt werden. Dafür würden auch personelle Ressourcen für die fortlaufende Überwachung benötigt, was wiederum hohe Kosten zur Folge hätte.

Empfehlung

Auch in diesem Fall sind u.E. Detailbestimmungen in diesem Rundschreiben nicht sinnvoll, da bereits ein anderes Rundschreiben besteht, das genau diese Punkte regelt. Daher empfehlen wir, die Rz 59 in dieser Form zu streichen und durch einen Verweis auf das RS 2008/07 Outsourcing Banken zu ersetzen.

3. Fragenliste zur Anhörung

Es wird auf die Stellungnahme der SBVg verwiesen.

4. Weiteres

- Begrifflichkeiten / Bestimmungen

Bemerkung

Diverse Begriffe werden nicht einheitlich verwendet oder sind nur ungenau, was zu zusätzlichen Unklarheiten führt. Folgende nicht abschliessende Begriffe bedürfen einer Klärung bzw. Anpassung:

- Geschäftsführung vs. Geschäftsleitung
- Identifikation, Messung, Beurteilung und Steuerung vs. Risikobewertung vs. Identifizierung, Begrenzung und Überwachung
- Verallgemeinernde Begriffe: angemessen, adäquat,… (Diese Wortwahl wird in der Praxis wohl immer wieder zu Auseinandersetzungen betreffend deren Definition zwischen den Revisionsgesellschaften, Aufsichtsbehörden sowie involvierten Banken führen. Entsprechend kann es auch zu unterschiedlichen Handhabungen in der Praxis führen.
- Unverhältnismässige oder ungenaue und unklar formulierte Bestimmungen

- Definitionen/Grundsätze

Bemerkung

Die Grundsätze sollten keine abweichenden Definitionen von Begriffen vornehmen, die bereits in anderen Rundschreiben, Empfehlungen, etc. enthalten sind (z.B. in Rz 54 in Bezug auf das RS 2008/7 „Outsourcing Banken). Besser wäre es, wenn in solchen Fällen auf die bestehenden Definitionen in den entsprechenden Regulierungen verwiesen würde.

Der Fokus sollte zudem mehr auf Prinzipien und weniger auf detaillierte Regelung gelegt werden.

- Glossar

Bemerkung

Im Glossar (Rz 60 ff.) fehlen aussagekräftige Definitionen zu den verwendeten Begriffen (z.B. „Massen-CID“). Dadurch ergeben sich aus den Vorgaben zum Teil mehr Auslegungsfragen als Klärung.

- Anhang

  Bemerkung

  Im Sinne einer einfacheren Lesbarkeit und Abgrenzung von Rundschreiben und Anhängen würden wir vorschlagen, die Anhänge mittels Buchstaben (A, B, C) zu kennzeichnen und die Randziffern in den drei Anhängen mit dem jeweiligen Buchstaben in Verbindung zu bringen (z.B. Rz 8 von Anhang 3 betreffend CID würde dann künftig „C.8“ heissen.)

- Fussnoten

  Bemerkung

  Ebenfalls zu einer verbesserten Lesbarkeit würde der Verzicht auf diverse Fussnoten haben. Im vorliegenden RS hat es etliche davon, was die Frage der Wesentlichkeit von diesen aufbringt.

- Pricing

  Bemerkung

  Die explizite Berücksichtigung von operationellen Risiken im Pricing ist abzulehnen

- Kundendaten

  Bemerkung

  Qualitative Anforderung / Umgang mit vertraulichen Kundendaten im Anhörungsentwurf inhaltlich und formell noch ungenügend.

- Kostenfolgen

  Bemerkung

  Teilweise wird eine angemessenere Berücksichtigung allfälliger Kosten vermisst. Diverse Bestimmungen führen zu unverhältnismässigen Kosten (Ertrag/Nutzen-Verhältnis). Eine differenziertere Analyse bzgl. organisatorischen, technischen und finanziellen Auswirkungen für die verschiedenen Bankengruppen wäre wünschenswert

- Datenschutzbestimmungen

  Bemerkung

  Inwieweit wurden bestehende Datenschutzbestimmungen berücksichtigt? Gibt es eine Notwendigkeit zur Abweichung von dieser?

Unsere Vereinigung dankt Ihnen im Voraus für die Prüfung und Berücksichtigung dieser Kommentare und Vorschläge. Für Rückfragen steht Ihnen Frau Dr. Susanne Brandenberger (susanne.brandenberger@vontobel.ch) gerne zur Verfügung.

Mit freundlichen Grüssen

Dr. Benno Degrandi
Sekretär

Geschäftsleitung

FINMA
D 0151395

Zürcher Kantonalbank

Kontakt Beatrice Zanella
Telefon 044 292 84 46
E-Mail beatrice.zanella.fux.@zkb.ch
Adresse Josefstrasse 222, 8010 Zürich

Briefadresse: Postfach, 8010 Zürich

A-Post
Eidgenössische Finanzmarktaufsicht FINMA
Herr Alessandro Lana
Einsteinstrasse 2
CH-3003 Bern

FINMA
ORG BA | 28. JUNI 2013 | SB
Bemerkung: FLY

Zürich, 28. Juni 2013

Stellungnahme in Sachen Anhörung zur Teilrevision „FINMA-RS 2008/21 Operationelle Risiken Banken"

Sehr geehrter Herr Lana

Wir nehmen die Möglichkeit gerne wahr, zum vorliegenden Anhörungspapier Stellung zu nehmen.

Einleitend möchten wir festhalten, dass wir die Stellungnahmen von „SwissBanking" (SBVg) und des „Verbandes Schweizerischer Kantonalbanken" (VSKB) unterstützen. Die nachfolgenden Ausführungen sind entsprechend ergänzend und fokussieren auf die spezifischen Gegebenheiten der Zürcher Kantonalbank.

Zur generellen Stossrichtung

Wie bereits an der Sitzung vom 30. Mai 2013 ausgeführt, begrüssen wir es, dass Sie im Rahmen der Überarbeitung des Rundschreibens (RS) 08/21 den Ansatz verfolgen, die Themen „Operationelles Risikomanagement", „Informationssicherheit" und „Interne Kontrolle" integral zu betrachten.

Nachfolgend sind unsere Kommentare und Anliegen zu einzelnen Kapiteln/Ziffern beschrieben:

Abgrenzung von operationellen und reputationellen Risiken

In Kapitel II. Ziffer 2 wird formuliert, dass bei der Bewertung der Verluste aufgrund von operationellen Risiken, die potentiellen zusätzlichen Folgen bzw. Verluste aufgrund von Reputationsschäden nicht zu berücksichtigen sind.

In Ziffer 2.1 wird zudem erläutert, dass die Reputationsrisiken aus der Definition der operationellen Risiken ausgeschlossen sind, da sie in der Regel kaum oder gar nicht quantifizierbar sind. Der letzte Satz lautet wie

folgt: *„Nichtdestotrotz ist festzuhalten, dass die Realisierung von operationellen Risiken indirekte und potentiell schwerwiegende Auswirkungen auf die Reputation einer Bank haben kann."*

Wir verstehen die konkreten Anforderungen aufgrund der neuen Ziffer 2.1 nicht. Sind die Reputationsrisiken bei der Festlegung der Risikobereitschaft und -toleranz z.B. gemäss Ziffer 125 auf Ebene Verwaltungsrat zu berücksichtigen oder nicht?

1. Wir erachten es als erforderlich, dass explizit definiert wird, welche Arten von Verlustkategorien bei AMA- und Nicht-AMA-Banken für die Bewertung, Beurteilung, Steuerung und Messung der operationellen Risiken bis auf Ebene Verwaltungsrat zu berücksichtigen bzw. nicht zu berücksichtigen sind.

Abgrenzung von operationellen Risiken und Compliancerisiken

Im FINMA-RS 08/24 „Überwachung und interne Kontrolle Banken" werden in Ziffer 98 Compliancerisiken definiert als *„das Risiko von Verstössen gegen Vorschriften, Standards und Standesregeln und entsprechenden rechtlichen und regulatorischen Sanktionen, finanziellen Verlusten oder Reputationsschäden"*.

Im vorliegenden RS 08/21 werden Rechtsrisiken als Teil der operationellen Risiken definiert. Bei den operationellen Risiken sind Reputationsschäden nicht zu berücksichtigen (vgl. vorhergehender Punkt).

Wir schliessen daraus, dass Rechtsrisiken nicht Teil der Compliancerisiken sind. Ist dieses Verständnis korrekt?

2. Wir erachten es als erforderlich, die Abgrenzung zwischen operationellen Risiken und Compliancerisiken einerseits und zwischen Compliancerisiken und Rechtsrisiken andererseits zu präzisieren.

OpRisk Quantifizierung - ab Ziffer 120

Als Nicht-AMA-Bank, d.h. eine Bank, die ihre Eigenmittelunterlegung nicht mittels einer Methode zur Quantifizierung der operationellen Risiken berechnet, haben wir es sehr geschätzt, dass die „Qualitativen Grundanforderungen" frei von fachlich vorbelasteten Begriffen von quantifizierbaren Risikokategorien wie Kredit oder Markt waren wie z.B. Schwellenwerte, Limiten, Risikobereitschaft, Risikotoleranz (Ziffern 120, 121, 125, 130), Messung und Quantifizierung des Verlustpotenzials (Ziffer 127).

3. Wir bitten die FINMA bei den qualitativen Grundanforderungen auf Begrifflichkeiten zu verzichten, welche als Anforderung zur Quantifizierung der operationellen Risiken interpretierbar sind.

Grundsatz 5 Technologieinfrastruktur - Ziffer 133

Bei der Aufzählung „Sicherheit, Integrität und Verfügbarkeit" gehen wir davon aus, dass „Vertraulichkeit, Integrität und Verfügbarkeit" gemeint war.

Wir schätzen im Thema Informationssicherheit die inhärenten Risiken der laufend professionalisierten Cyberkriminalität (d.h. Datenintegrität und -verfügbarkeit) für die Banken und den Finanzplatz Schweiz als weit höher ein als das inhärente Risiko der Verletzung der Vertraulichkeit von Kundendaten.

4. Wir empfehlen, auf die detaillierten Ausführungen im Anhang 3 zu verzichten und stattdessen bei den qualitativen Grundanforderungen die Etablierung eines angemessenen und wirksamen ISMS (Informations-Sicherheits-Management-System) in Anlehnung an einen internationalen Standard wie z.B. ISO 27001 zu fordern.

Anhang 3 - Ziffer 16

Kundendaten (CID) sind eine Teilmenge von Personendaten gemäss Datenschutzgesetz (DSG). Das DSG führt bereits zwei Klassen von Personendaten mit der Unterscheidung „Personendaten" und „besonders schützenswerte Personendaten" (oder -Profile). Bezüglich Datensammlungen verlangt der Gesetzgeber ebenfalls eine Inventarisierung. Weitere Überschneidungen oder Abgrenzungsfragen drängen sich auf, wie zum Beispiel: Sind „CID" für sich genommen „besonders schützenswerten Personendaten" gemäss DSG? Sind es die CID erst dann, wenn auch Informationen zum Vermögen vorhanden sind? Oder erst, wenn auch eine „Profilerstellung" möglich ist? Im DSG ist die „finanzielle Situation" einer Person nicht unter den Beispielen für „besonders schützenswerte Personendaten" aufgeführt.

Mit Gegenüberstellung der Klassen gemäss DSG stellt sich die Frage, wie die CID-Thematik zu positionieren ist. Ist es eine neue Klasse „unterhalb" der besonders schützenswerten Personendaten? Dann fehlt uns das Verständnis, wie die übergeordnet positionierten (kritischeren) Daten zu behandeln sind. Wenn CID mit „besonders schützenswerten Personendaten" gleichgesetzt werden, drängt sich die Frage auf, ob aus Sicht DSG für alle „besonders schützenswerten Daten" Massnahmen aus Anhang 3 umzusetzen sind.

5. Wir bitten die FINMA um eine Gegenüberstellung von CIDs gemäss diesem RS 08/21 und „besonders schützenswerte Personendaten" gemäss DSG.

Anhang 3 - Ziffern 20 bis 23 und 54 bis 59

Aus unserer Sicht ist es zielführender, die Anforderungen der Ziffern 20-23 und 54-59 im RS 08/07 „Outsourcing Banken" aufzunehmen und an dieser Stelle darauf zu verweisen.

Wenn Outsourcing zur Anwendung kommt, liegen alle zugehörigen Anforderungen in zwei FINMA-RS vor, nämlich 08/07 und 08/24 „Überwachung und interne Kontrolle Banken". Davon abgesehen gelten auch hier die Vorgaben aus dem DSG und zugehöriger Verordnung.

6. Die Zürcher Kantonalbank empfiehlt, die Anforderungen der Ziffern 20-23 und 54-49 im RS 08/07 aufzunehmen und im vorliegenden RS 08/21 darauf zu verweisen.

Generell Begriffe

Die Zürcher Kantonalbank verwendet im operationellen Risikomanagement und der internen Kontrolle ähnliche Begriffe wie im vorliegenden RS 08/21 aufgeführt. Wir vermuten aber, dass für die FINMA die gleichen Begriffe eine andere Bedeutung haben.

7. Wir erachten es als erforderlich, folgende Begriffe im Glossar zu definieren und wenn möglich mit Beispielen zu illustrieren: Inhärentes Risiko, Risikoszenario, Risikobewertung, Risikobeurteilung, (Schlüssel-)Kontrolle, Klassifikation, Risikolimite, Risikoakzeptanz und Schwellenwert.

Wir danken Ihnen für die Prüfung unserer Kommentare und Anliegen. Für allfällige Rückfragen oder eine vertiefte Erörterung unserer Stellungnahme steht Ihnen Frau Beatrice Zanella gerne zur Verfügung.

Freundliche Grüsse

Zürcher Kantonalbank

Roger Müller
Stv. CRO

Rudolf Sigg
CFO