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:

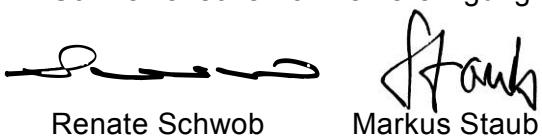
- Eine Ausweitung auf natürliche Personen, deren Geschäftsbeziehungen im Ausland betreut werden, erachten wir nicht als notwendig, da die lokalen Datenschutzbestimmungen grundsätzlich genügend sind. Zudem geht das vor Ort geltende zwingende Recht ohnehin einer allfälligen schweizerischen Regelung vor.
- 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