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