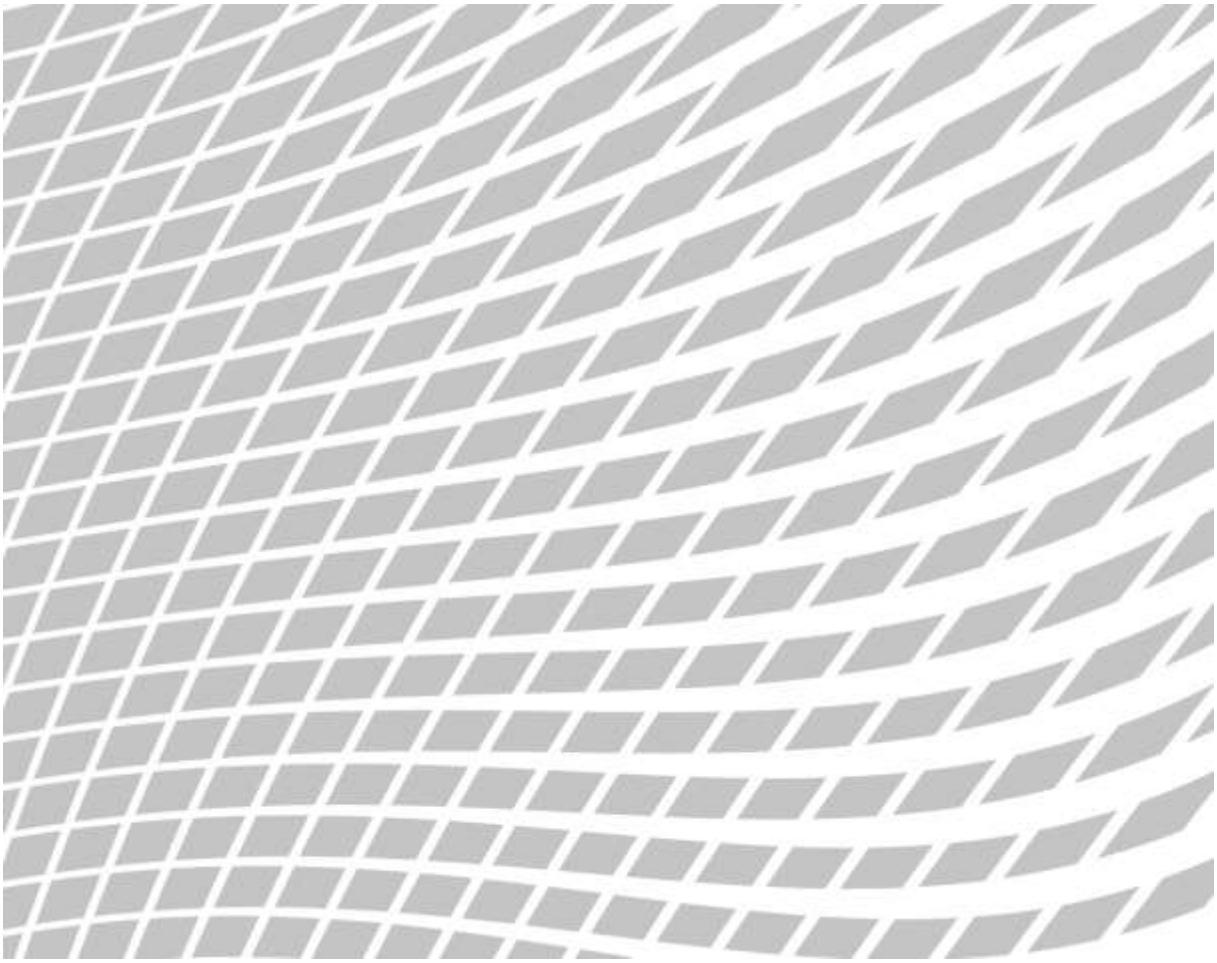
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

29. August 2013

Teilrevision FINMA-Rundschreiben 2008/21 "Operationelle Risiken Banken"

Bericht der FINMA über die Anhörung vom 23. Mai 2013 bis zum 1. Juli 2013 zum Entwurf zur Teilrevision des Rundschreibens „Operationelle Risiken Banken“



Einsteinstrasse 2, 3003 Bern
Tel. +41 (0)31 327 91 00, Fax +41 (0)31 327 91 01
www.finma.ch

A225834/00097/1046297

Inhaltsverzeichnis

Kernpunkte

1. Schwerwiegende Verluste für operationelle Risiken während der Finanzkrise sowie während der letzten Jahre haben weltweit zu einer neuen Beurteilung der Wichtigkeit dieses Risikogebiets geführt. Diese neue Beurteilung hat international zur Bearbeitung von qualitativen regulatorischen Anforderungen geführt, die durch den Basler Ausschuss für Bankenaufsicht als Standard im Papier „Principles for the Sound Management of Operational Risk“ im Juni 2011 ausgearbeitet wurden. Quantitative (Eigenmittel-) Anforderungen sind nicht Teil dieser Teilrevision des Rundschreibens und bleiben damit unverändert.

2. Die elf Prinzipien vorgenannter Regulierung werden im FINMA-Rundschreiben 2008/21 „Operationelle Risiken Banken“ in sechs Grundsätzen abgebildet. Diejenigen Grundsätze, die für das Risikomanagement von operationellen Risiken besonders relevant oder nicht bereits in anderen schweizerischen Regelwerken genügend umgesetzt sind, werden um ausgewählte Erläuterungen erweitert.

3. Das revidierte Rundschreiben sieht vor, dass die qualitativen Anforderungen abhängig von der Grösse der Bank umzusetzen sind. So werden kleine Banken und Effektenhändler der FINMA-Kategorie 5 und Banken der FINMA-Kategorie 4, welche über Geschäftsaktivitäten ohne bedeutende Komplexität verfügen, von der Anwendung gewisser Bestimmungen ausgenommen.

4. Neben der Anpassung der allgemeinen qualitativen Anforderungen im neuen IV. Kapitel des FINMA-RS 08/21 besteht neu die Möglichkeit, sehr konkrete Anforderungen für spezifische Risiken in einem Anhang zu regulieren. So wird der Umgang mit elektronischen Kundendaten in einem neuen Anhang 3 detailliert. Weitere Themen können in Zukunft entsprechend detailliert unter Berücksichtigung des zu diesem Zeitpunkt gültigen Regulierungsprozesses (Anhörung) eingeführt werden.

5. Der neue Anhang 3 enthält neun Grundsätze und zahlreiche Ausführungen betreffend das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Kundendaten von natürlichen Personen („Privatkunden“), deren Geschäftsbeziehungen in oder von der Schweiz ausgeführt werden. Die Grundsätze behandeln hauptsächlich das Risiko von Vorfällen in Bezug auf die Vertraulichkeit von Kundendaten aufgrund der Verwendung elektronischer Systeme. Sie gehen nur am Rande auf Sicherheitsüberlegungen für physische Daten sowie auf Fragen im Zusammenhang mit der Integrität und der Verfügbarkeit von Daten ein.

1 Einleitung

Vom 23. Mai 2013 bis zum 1. Juli 2013 hörte die FINMA die Beaufsichtigten und weitere interessierte Kreise zum Entwurf für die Teilrevision des FINMA-Rundschreibens 2008/21 „Operationelle Risiken Banken“ an. Die Einladung zu der Anhörung erfolgte auf der Webseite der FINMA; der Teilnehmerkreis war offen.

Der vorliegende Bericht fasst die Stellungnahmen der Anhörungsteilnehmer zum FINMA-Rundschreibenentwurf zusammen und nimmt eine diesbezügliche Beurteilung vor.

2 Eingegangene Stellungnahmen

Die FINMA hat von folgenden Verbänden und Instituten eine schriftliche Stellungnahme mit Einverständnis zur Publikation erhalten (in alphabetischer Reihenfolge):

- Credit Suisse
- HSBC
- PostFinance
- Raiffeisen
- Schweizerische Bankiervereinigung (SBVg)
- SIX Securities Services (SIX)
- Treuhandkammer
- UBS
- Verband der Auslandbanken in der Schweiz (AFBS)
- Verband Schweizerischer Kantonalbanken (VSKB)
- Vereinigung Schweizerischer Handels- und Verwaltungsbanken (VHV)
- Vereinigung Schweizerischer Privatbankiers (VSPB)
- Zürcher Kantonalbank (ZKB)

3 Ergebnisse der Anhörung und Beurteilung durch die FINMA

Die Teilrevision des Rundschreibens fokussiert auf zwei spezifische Themen: die qualitativen Grundanforderungen (Kapitel IV.B) und der Umgang mit elektronischen Kundendaten (Anhang 3).

3.1 Qualitative Grundanforderungen (Kapitel IV.B), inklusive Proportionalitätsprinzip (Kapitel IV.A) und Einführung spezifischer qualitativer Anforderungen (IV.C)

Generelle Kritik

Zu den qualitativen Grundanforderungen konnte die FINMA keine klare, fundamentale Kritik identifizieren. Als einziges übergeordnetes Element, das in mehreren Stellungnahmen erwähnt wurde, wurde der Wunsch nach Präzisierung von Terminologie und Begrifflichkeiten geäussert. Die FINMA hat diesen Wunsch punktuell aufgenommen; auf die Erstellung eines Glossars wurde hingegen verzichtet. Die FINMA empfiehlt den Instituten die Definition und Auslegung von Termen wie „Risikobeurteilung", „Klassifikation", „Risikolimite" und „Schwellenwert" – unter Berücksichtigung des allgemeinen Branchenverständnisses – auf Institutsebene festzulegen.

Weitere Kritik

Im Weiteren betrafen die eingegangenen Stellungnahmen im Wesentlichen die folgenden Punkte:

- Proportionalitätsprinzip (Rz 117[1], 118)
- Risikobereitschaft und Risikotoleranz (Rz 120)
- Rolle der Geschäftsführung zur Entwicklung des Rahmenkonzepts (Rz 121)
- Einheit für das Management von operationellen Risiken (Rz 122)
- Festsetzung von Schwellenwerten und Limiten (Rz 125)
- Instrumente und Methoden (Rz 127)
- Interne Berichterstattung / Externe Ereignisse (Rz 130)
- Offenlegungspolitik (Rz 131, 132)
- Technologieinfrastruktur (Rz 133)
- Risikospezifische qualitative Anforderungen (Rz 135, 136)

Weitere, kleinere Anpassungsvorschläge wurden aufgenommen, werden aber in diesem Bericht nicht einzeln kommentiert.

3.1.1 Proportionalitätsprinzip (Rz 117, 118, 119)

Stellungnahmen (summarisch)

- Rz 118 definiert, welche Institute als „kleine Banken" nach Rz 117 qualifizieren. Mehrere Stellungnahmen haben diesbezüglich einerseits das Grössenkriterium sowie anderseits die Formulierung „Geschäftsaktivitäten ohne bedeutende Komplexität" als zu beschränkt beurteilt und namentlich eine Annäherung an die Begriffe im FINMA-Rundschreiben 2013/6 „Liquidität Banken" vorgeschlagen.

[1] **Die Referenzen auf die Randziffern beziehen sich auf die Nummerierung der Randziffern in der Anhörungsversion.**

- Die Treuhandkammer sieht darüber hinaus Klärungsbedarf in folgenden zwei Punkten: 1. Welches Bankorgan der Kategorie 4 hat die Beurteilung und den Entscheid über das Vorliegen bzw. Fehlen einer „bedeutenden Komplexität" vorzunehmen und 2. Wann und wie eine Klassifikation einer Bank der Kategorie 4 als „ohne bedeutende Komplexität" mit der FINMA abzustimmen ist.

Würdigung

Die FINMA hat die Kriterien für die Klassierung von Banken der FINMA-Kategorie 4 erweitert; neu sind nebst der Komplexität auch die Art, der Umfang und der Risikogehalt der Geschäftsaktivitäten des Instituts in die Beurteilung einzubeziehen.

Bei der Anwendung des Proportionalitätsprinzips in Rz 117–118 verfolgt die FINMA dasselbe Vorgehen, wie es im FINMA-RS 13/6 „Liquidität Banken"[2] stipuliert wird. Die FINMA überlässt es in erster Linie der Bank und der Prüfgesellschaft die institutsspezifische Beurteilung der Erfüllung der Kriterien vorzunehmen. Nichtdestotrotz wird die FINMA die Implementierung des Proportionalitätsprinzips kritisch mitverfolgen. Als Grundanforderung erwartet die FINMA, dass die Beurteilung der Bank und der Prüfgesellschaft transparent und nachvollziehbar dokumentiert sind.

Die FINMA überlässt es den Banken das Organ für die Beurteilung und die Entscheidung in Sachen Komplexität und der weiteren Kriterien zu bestimmen. Dennoch empfiehlt sich – u.a. aus Konsistenzüberlegungen (vgl. Genehmigung der Risikobereitschaft und Risikotoleranz in Rz 120) – für diese Aufgabe den Verwaltungsrat zu bestimmen.

Die Rz 118 wurde dementsprechend überarbeitet.

Fazit

Die FINMA hat die Rz 117–119 sinngemäss überarbeitet. Obige Ausführungen dienen den Instituten und Prüfgesellschaften zudem als Richtschnur.

3.1.2 Risikobereitschaft und Risikotoleranz (Rz 120)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen haben das Bedürfnis zur Präzisierung der Begriffe „Art", „Typ" und „Ebene" geäussert.

- Mehrere Stellungnahmen haben Änderungen in den Verantwortlichkeiten u.a. für die Entwicklung und die Bewilligung des Rahmenkonzepts vorgeschlagen.

[2] Ein einheitlicher / ähnlicher Prozess muss nicht zwingend zu einer identischen Schlussfolgerung führen; eine unterschiedliche Qualifizierung in den beiden Rundschreiben ist möglich.

Würdigung

Der Erläuterungsbericht stellte Folgendes dar: „Eine wichtige Anforderung für die Ausgestaltung eines sinnvollen Konzepts für die Definition von Risikobereitschaft und -toleranz für operationelle Risiken besteht darin, dass diese individuell für jedes materielle Risiko zu definieren sind (beispielsweise Crossborder-Risiken, Risiken betreffend unautorisierte Handelstätigkeit, *Investment Suitability*, *Business Continuity Management*, Kundendatenvertraulichkeit usw.). Zusätzlich haben die Banken die Risikotoleranz dem eigenen Management und den eigenen Kontrollstrukturen anzupassen, damit diese effizient überwacht und gemessen werden kann."

Diejenigen Institute, die für wesentliche operationelle Risiken keine eigene Begrifflichkeit bestimmt haben und die über den Erläuterungsbericht hinausgehende Erklärungen benötigen, können sich für die Begriffe „Art" und „Typ" am Anhang 2 des Rundschreibens orientieren („Übersicht zur Klassifikation von Ereignistypen"), insbesondere an den Subkategorien der Stufen 2 und 3, und den Begriff „Ebene" als „Gruppe" oder „Konzern" interpretieren.

Es wurden im teilrevidierten FINMA-RS 08/21 geringfügige Anpassungen der Verantwortlichkeiten vorgenommen, indem sie für die Entwicklung des Rahmenkonzepts ein von einem Geschäftsführungsmitglied geführten Ausschuss als zulässig erachtet.

Fazit

Einerseits erfolgte eine geringfügige Anpassung im Bereich der Verantwortlichkeiten, anderseits wurden die im Rahmen der Anhörung eingegangenen Fragestellungen in diesem Anhörungsbericht kommentiert.

3.1.3 Rolle der Geschäftsführung zur Entwicklung des Rahmenkonzepts (Rz 121)

Stellungnahmen (summarisch)

- In Bezug auf die Entwicklung des Rahmenkonzepts hat sich die SBVg für eine Anlehnung der Formulierung zu den Verantwortlichkeiten der Geschäftsführung an das FINMA-RS 13/6 „Liquidität Banken" ausgesprochen.

Würdigung

Die FINMA begrüsst den Vorschlag einer Anpassung der Formulierungen.

Fazit

Die FINMA hat Rz 121 sinngemäss überarbeitet.

3.1.4 Funktion für das Management von operationellen Risiken (Rz 122)

Stellungnahmen (summarisch)

- Credit Suisse (und in Teilen andere Stellungnahmen auch) empfiehlt eine Präzisierung der Rolle der Geschäftsführung bei der Definition von Verantwortlichkeiten sowie die Zuweisung der in der Rz aufgeführten Zuständigkeiten an eine „Einheit" anstelle einer „Funktion".

- Die Treuhandkammer empfiehlt im Rundschreiben zu präzisieren, ob die „Funktion für das Management von operationellen Risiken" von der „Risikokontrolle" gemäss Rz 113–125 des FINMA-RS 08/24 „Überwachung und interne Kontrolle Banken" zwingend getrennt sein bzw. eine vollständige Funktionentrennung bestehen muss.

Würdigung

Die Frage der Treuhandkammer ist verständlich und von grosser Relevanz. Hinweis: Da in der Praxis eine unterschiedliche Verwendung der Begriffe „Risikokontrolle" und „Risiko Management" beobachtet wird, verzichten wir in nachfolgenden Ausführungen auf diese Begriffe.

Die FINMA erwartet, dass die in Rz 122 genannte Funktion (neu „Organisationseinheit") sowohl „vergangenheitsorientierte" Instrumente und Methoden verwendet (z.B. Projekte zur Minderung der Risiken, die sich in operationellen Vorfällen bereits verwirklicht haben; Durchführung der Kontrollen von bereits identifizierten Risiken), als auch neue und „vorausschauende" Elemente im Rahmenkonzept abdeckt (z.B. Überlegungen zur Cyberkriminalität, zunehmende Exposition in Rechtsfällen, umfassender Überblick zur Risikoexposition und Abschätzung des Verlustpotenzials). Diese unterschiedlichen „Perspektiven" und dementsprechend unterschiedlichen Methoden und Instrumente erfordern komplementäre Denkweisen, evtl. unterschiedliche Ausbildungen.

Anders als beim Management der Kredit- und Marktrisiken[3] sind sowohl die „Funktion für das Management von operationellen Risiken" als auch die Risikokontrolle organisatorisch in der „zweiten Verteidigungslinie" angesiedelt. Aus diesem Grund ist sowohl eine Zusammenführung der beiden „Organisationseinheiten" in einer einzigen Einheit als auch die Trennung in unterschiedliche Einheiten (gängigere Lösung für grössere Banken) möglich. Die Institute haben bei der Ausgestaltung Ihrer diesbezüglichen Organisation die Methoden, Instrumente, Ausbildungen usw. ihrer Wahl entsprechend auszurichten.

Fazit

Rz 122 wurde sinngemäss überarbeitet.

[3] Das Risk Management, im Sinne von Steuerung der Risiken/Positionen, ist oft eine Aufgabe der Linie.

3.1.5 Festsetzung von Schwellenwerten und Limiten (Rz 125)

Stellungnahmen (summarisch)

- Diverse Stellungnahmen fordern eine einheitlichere und/oder klarere Begrifflichkeit.

- Die SBVg hält zur Festlegung von Limiten/Schwellenwerten u.a. fest, 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."

Würdigung

Die Begrifflichkeiten wurden geprüft und punktuell angepasst. Zu den Änderungen gehören insbesondere der Verzicht auf die explizite Nennung der Definition der Instrumente für die „Messung" der operationellen Risiken (mehr dazu auch unter Rz 127) sowie eine Bündelung der Anforderungen an die Berichterstattung in einem Listenpunkt. Auf eine Berücksichtigung aller Anpassungsvorschläge wurde verzichtet, da unter Berücksichtigung des unterschiedlichen Kontexts der einzelnen Listenpunkte eine unterschiedliche Begrifflichkeit angebracht ist.

Die FINMA teilt die Einschätzung der SBVg bezüglich Limiten/Schwellenwerten. Die bestehende Formulierung des Rz 125 widerspricht dem unseres Erachtens nicht.

Fazit

Rz 125 wurde punktuell überarbeitet.

3.1.6 Instrumente und Methoden (Rz 127)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen haben Unklarheiten bezüglich der aus der Rz resultierenden Grundanforderungen geäussert. So sei bspw. die aus Rz 119 resultierende Ausnahmeregelung für kleine Banken nicht notwendig, da es sich bei der Auflistung in Rz 127 ohnehin um (nicht verbindliche) „Beispiele" handle.

- VHV und ZKB haben ihre Bedenken zur Wortwahl in Listenpunkt h) „Messung und Quantifizierung" bzw. zu generellen Anforderungen oder Erwartungen an die Quantifizierung der operationellen Risiken (bspw. mittels komplexen Modellen) geäussert.

Würdigung

Die Unklarheiten der aus Rz 127 resultierenden Grundanforderungen wurden mit der Trennung der Pflichtanforderungen in Rz 128^{neu} sowie (möglicher) weiterer, zu prüfender Faktoren für nicht kleine

Banken (gemäss Rz 118) in einer separaten, neuen Rz 129[neu] sowie weiteren Umformulierungen behoben.

Zur Anregung der VHV und der ZKB zu h) kann auf den Erläuterungsbericht hingewiesen werden: „Die Messung und Quantifizierung des Verlustpotenzials muss nicht zwingend mittels eines sophistizierten Ansatzes erfolgen. Die AMA-Anforderungen können allerdings als *Best Practice-Benchmark* dienen. Insbesondere soll die Komplexität des Quantifizierungsansatzes in einem angemessenen Verhältnis zu den getroffenen Annahmen[4] stehen."

Der Kommentar im Erläuterungsbericht hat u.U. den Eindruck erweckt, dass von den Instituten sophistizierte Ansätze erwartet werden. Diese Rz statuiert jedoch keine Quantifizierung des Verlustpotenzials für alle Banken mittels komplexen statistischen Verfahren. Expertenschätzungen (z.B. Szenarioanalysen) können bspw. ebenfalls eine ausreichende Quantifizierung des Verlustpotenzials ermöglichen. Ungeachtet davon gilt: Werden für die Bestimmung des gesamten Verlustpotentials Einzelfälle aggregiert, sollen entweder konservative, Experten-basierte Annahmen getroffen oder statistisch begründete alternative Verfahren benutzt werden.

Zum besseren Verständnis der im Titel des Grundsatzes genannten „Begrenzung" und „Überwachung" wurde in Rz 130[neu] auf das vom Institut zu erarbeitende Rahmenkonzept verwiesen. Zudem wurde das im Rundschreiben-Entwurf erwähnte Pricing sowie die Performance-Messung als mögliche indirekte Massnahmen für die Begrenzung der operationellen Risiken aufgeführt.

Fazit

Rz 127 wurde auf zwei Randziffern aufgeteilt und die Anwendbarkeit in Zusammenhang mit dem Proportionalitätsprinzip sowie die Formulierung des Listenpunkts h) überarbeitet.

3.1.7 Interne Berichterstattung / Externe Ereignisse (Rz 130)

Stellungnahmen (summarisch)

- Diverse Stellungnahmen fordern punktuelle Umformulierungen.
- Mehrere Stellungnahmen fordern eine Umformulierung und Abschwächung des Listenpunkts c).

Würdigung

Die Stossrichtung der Rz 130 zielt dahin, dass Institute für sie relevante sowie prominente Ereignisse (wie bspw. US-Cross-Border, BGE Retrozessionen sowie Verluste oder offene Rechtsfälle bei Peers) identifizieren, deren Konsequenzen für das eigene Institut abschätzen und daraus letztlich die notwendigen Massnahmen ableiten. Die Identifikation solcher Ereignisse kann unterschiedlich erfolgen: Vom Medien-Monitoring bis hin zur Sammlung von anonymisierten Ereignissen/Verlustdaten von

[4] V.a. der Konservativität der Annahmen.

Drittinstituten. Mit letzterer Aufgabe könnte beispielsweise ein Verband von seinen Mitgliedern beauftragt werden.

Fazit

Rz 130 wurde punktuell überarbeitet.

3.1.8 Offenlegungspolitik (Rz 131, 132)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen kritisieren den Vorschlag einer formellen Offenlegungspolitik.
- Die SBVg fordert eine Anpassung der offenzulegenden Informationen bzw. der Anforderungen an solche Informationen.

Würdigung

Die Anforderungen zur Offenlegung sind im Vergleich zu anderen Risikoarten tatsächlich erhöht. Sie sind Ausdruck einer internationalen Tendenz hin zu umfassenderen Offenlegungspflichten. Die FINMA geht davon aus, dass in Zukunft die Standards auch in Bezug auf andere Risikoarten erhöht werden.

Fazit

Rz 131 wurde gekürzt, um eine einfache und klare Formulierung der Anforderungen zu gewährleisten.

3.1.9 Technologieinfrastruktur (Rz 133)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen äussern sich kritisch zu Inhalt und Formulierung der Rz 133; diese wird u.a. als zu allgemein wahrgenommen.

Würdigung

Die Einschätzung zur Ambiguität dieser Rz scheint berechtigt. Die Rz soll die Bedeutung der IT für die Abdeckung der Geschäftsbedürfnisse und für die Minderung von operationellen Risiken betonen. Gleichzeitig unterstreicht Rz 133 die Verantwortung der Geschäftsführung indem es für Themen der Technologieinfrastruktur die notwendige Aufmerksamkeit fordert.

Fazit

Rz 133 wurde überarbeitet.

3.1.10 Risikospezifische qualitative Anforderungen (Rz 135, 136)

Stellungnahmen (summarisch)

- Rz 135: Mehrere Stellungnahmen kritisieren die mangelnde Konkretisierung der weitergehenden Anforderungen und fordern deren ersatzlose Streichung.

- Rz 136: Mehrere Stellungnahmen bemängeln, dass die aktuelle Formulierung die Einführung oder Konkretisierung weitergehender qualitativer Anforderungen der FINMA frei lässt. Sie fordern die ersatzlose Streichung der Rz bzw. die Einhaltung des regulären Anhörungsprozesses im Falle von weitergehenden Anforderungen.

Würdigung

In Rz 135 wurde präzisiert, dass es sich bei den genannten operationellen Risiken um Risiken mit weitreichender Tragweite handelt. Bezüglich Massnahmen wird die Verantwortung der Geschäftsführung zugewiesen und es werden hierzu neu detailliertere Angaben gemacht („ergänzende" Massnahmen oder eine „Verschärfung bestehender Massnahmen"). Auf eine Präzisierung der möglichen Massnahmen im Rundschreiben wurde verzichtet; aus Sicht der FINMA können dies bspw. kürzere Reportingfrequenzen, eine höhere Ansiedlung der Reportingempfänger, höhere Management Attention bzw. eine höhere hierarchische Ansiedelung von Themen, die Einsetzung einer Task Force/von Ausschüssen, das Beiziehen externer Spezialisten oder die Einholung externer Gutachten, die Bereitstellung grösserer oder separater Ressourcen usw. umfassen.

Rz 136 wurde unverändert belassen. Die Rz beabsichtigt nicht das ordentliche Anhörungsverfahren zu umgehen; für allfällige neue Anhänge oder Themen wird die FINMA den zu diesem Zeitpunkt gültigen Regulierungsprozess anwenden[5]. Sollten die instituts- bzw. branchenspezifischen Herausforderungen gemäss Rz 135 nicht befriedigt werden, würde das Rundschreiben i.S. von Rz 136 themenspezifisch angepasst.

Fazit

Rz 135 wurde überarbeitet. Auf eine Anpassung von Rz 136 wurde hingegen verzichtet.

3.2 Umgang mit elektronischen Kundendaten (Anhang 3)

3.2.1 Generelle Kritik

- Prinzipienbasierter Ansatz oder detaillierter Ansatz: Mehrere Stellungnahmen haben sich zum Detaillierungsgrad des Anhangs 3 geäussert und schlugen einen „prinzipienbasierten Ansatz" statt des in der Anhörung vorgesehenen „präzisen Ansatzes" vor. Insbesondere wurde bezweifelt, dass die Anforderungen gemäss Anhang 3 eine institutsspezifische Implementierung (z.B. in Bezug auf unterschiedliche IT-Systeme und organisatorische Gestaltung) ermöglichen. Auch wurde vorge-

[5] Aktuelle Regulierungsleitlinien: http://www.finma.ch/d/regulierung/seiten/regulierungsprozess.aspx

bracht, dass die Anforderungen möglicherweise kurzfristig durch technische Entwicklungen überholt sein könnten.

- Mehrere Stellungnahmen haben auch die Kostenfolgen der Implementation der Anforderungen kommentiert und diese als materiell bezeichnet.

Würdigung

Eine Regelung des Umgangs mit elektronischen Kundendaten wurde in einigen Stellungnahmen grundsätzlich begrüsst. Der Vertraulichkeit von Kundenangaben soll auf dem Schweizer Finanzplatz auch in Zukunft die notwendige Bedeutung zukommen. Entsprechende Regulierungen vergleichbarer Finanzplätze wurden publiziert (beispielsweise UK FSA „Data Security in Financial Services" [April 2008] oder Singapore MAS „Technology Risk Management Guidelines" [June 2013]). Zudem wurde die Selbstregulierung nur von wenigen Stellungnahmen als Alternative vorgebracht. Die SBVg hatte hierzu anlässlich des gemeinsamen Workshops im März 2013 folgendes festgehalten: „Das Papier der SBVg „Data Leakage Protection"[6] [ist] keine Empfehlung sondern ein Informationspapier, welches nicht geprüft wird." Das Papier umfasst somit eine Darstellung von *Best Practices*, die per Definition nicht als Selbstregulierung konzipiert wurden und auch nicht als solche dienen können.

Die verbleibende konstruktive Kritik äusserte sich zur Granularität der Anforderungen und ihre sogenannte „Flughöhe". Die FINMA ist der Auffassung, dass der gewählte Ansatz weitgehend prinzipien- und nicht regelbasiert ist. Die Anforderungen im Anhang 3 benützen nur marginal technische Begriffe (grundsätzlich Anonymisierung, Pseudonymisierung und Verschlüsselung) und schränken damit die institutsspezifische Umsetzung nicht ein. Der gewählte prinzipienbasierte Ansatz gewährleistet zeitliche Gültigkeit, denn technische Entwicklungen können bei den nicht technisch formulierten Prinzipien nur längerfristig eine Aktualisierung erfordern.

Die Anforderungen des Anhangs 3 sind im Vergleich zu den qualitativen Grundanforderungen im Kapitel IV.B mit einer risikospezifischeren Granularität gestaltet. Eine solche vertiefte „Flughöhe" wurde für den Umgang mit elektronischen Kundendaten absichtlich gewählt, damit Anhang 3 die qualitativen Grundanforderungen des Kapitels IV.B optimal ergänzt (vgl. Rz 135, 136) und sich entsprechend als wirksam erweist.

Die in den Stellungnahmen vorgebrachten Einwände zum Detaillierungsgrad der Anforderungen wurden entsprechend punktuell berücksichtigt und der Text des Anhangs 3 an einigen Stellen deutlich gekürzt.

Bezüglich der Kosten der Implementierung der Anforderungen ist es wichtig die Institute, die einen allgemeinen Rückstand ihrer IT-Infrastruktur aufweisen von denjenigen Instituten, die bereits Investitionen für eine robuste IT-Infrastruktur getätigt haben und für die Zukunft angemessene Ressourcen für die Einhaltung des bestehenden Niveaus einsetzen und planen, zu unterscheiden. Die FINMA – entweder direkt durch ihre Aufsichtstätigkeit oder gestützt auf die Arbeit der Revisionsstelle – wird die Implementierung der Anforderungen mit Interesse verfolgen und damit auch beobachten, welche Institute in der ersten bzw. zweiten der oben genannten Kategorien fallen werden.

[6] Marktpraktiken zu Sicherheitsszenarien und damit verbundenen Schlüsselkontrollen sind umfassend durch die SBVg unter dem Titel „Data Leakage Protection – Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association" behandelt (verabschiedet im Oktober 2012).

Fazit

Die drastische Reduktion des Detaillierungsgrades auf die Grundsätze wurde abgelehnt. Der Text des Anhangs 3 wurde dennoch stark gekürzt.

Weitere Kritik

Die eingegangenen Stellungnahmen betrafen im Wesentlichen die folgenden Punkte:

- Vorgaben, Prozesse und Systeme (Rz 6)
- Definition von CID, Klassifikation und Ausnahmen (Rz 9–12), sowie Kapitel III (Rz 67)
- Datenspeicherort und –zugriff im Ausland (Rz 20–23)
- „Need to know"-Grundsatz (Rz 24–26)
- Liste der Mitarbeitenden mit Zugriff auf CID und Liste der "Schlüsselmitarbeitenden" (Rz 28, 29, 41)
- Sorgfältige Auswahl der Mitarbeitenden (Rz 38)
- Produktionsumfeld, Aktivitäten in Verbindung mit Massen-CID (Rz 47)
- Meldung (Rz 51)

Weitere kleinere Einwände zur Anpassung wurden aufgenommen, werden aber in diesem Bericht nicht einzeln kommentiert.

3.2.2 Vorgaben, Prozesse und Systeme (Rz 6)

Stellungnahmen (summarisch)

- Die Treuhandkammer weist darauf hin, dass die geforderten Rahmenkonzepte und deren Einhaltung nur geprüft werden können, sofern die Institute ihre Konzepte (insbes. Massnahmen und dazugehörige Häufigkeiten) konkretisieren. Dafür empfiehlt die Treuhandkammer eine textliche Ergänzung.

Fazit

Die Anregung der Treuhandkammer wurde in einer neuen Rz 7 aufgenommen.

3.2.3 Definition von CID, Klassifikation und Ausnahmen (Rz 9–12) sowie Kapitel III (Rz 67)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen haben sich zur Definition von CID sowie zur Klassifikation, wie sie in Kapitel III illustrativ dargestellt wurde, geäussert. Zudem wurden Fragen – bspw. ob die Implementierung nach Segmenten unterschiedlich erfolgen könne und ob Meldungen an externe Instanzen (z.B. Inkasso) als Ausnahmen zur Vertraulichkeit an CID gelten können – gestellt.

Würdigung

Da es trotz Formulierung der Rz 10 und der spezifischen Erläuterungen im Erläuterungsbericht nicht genug klar war, dass Definition und Klassifikation von CID dem Institut obliegt, wurde das Beispiel in Kapitel III und die entsprechenden Verweise im Rundschreiben gelöscht.

Diese Massnahme kommt dem allgemeinen Wunsch nach nicht zu präzisen bzw. nicht zu granularen Anforderungen entgegen. Die Konzeption liegt damit in der Hand der Institute.

Fazit

Die Beispiele zur Definition von CID in Kapitel III sowie die entsprechenden Verweise im Rundschreiben wurden gelöscht.

3.2.4 Datenspeicherort und –zugriff im Ausland (Rz 20–23)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen äusserten sich zu den als unangemessen und zu detailliert wahrgenommenen Regelungen in Rz 20–23 sowie zu den potentiellen Inkonsistenzen mit dem Rundschreiben 2008/7 „Outsourcing Banken".

- Die SBVg präzisiert, dass «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.»

Würdigung

Rz 20–23 sollen beobachtete Inkonsistenzen zwischen Instituten bei der Implementation und widersprüchlichen Interpretationen zwischen Revisionsstellen von bestehenden Anforderungen (z.B. FINMA-RS 08/07 „Outsourcing Banken") beseitigen. Zum Beispiel wurde festgestellt, dass der Wegfall des Erfordernisses für ein besonderes Kundenschreiben bei einer Anonymisierung[7] von CID, die ausserhalb der Schweiz aufbewahrt werden oder auf welche vom Ausland zugegriffen wird, nicht von allen Instituten verstanden wurde.

Gestützt auf die schriftliche Stellungnahme des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragter EDÖB hat die FINMA im Erläuterungsbericht wie auch in vorliegendem Dokument erklärt, dass nur anonymisierte Daten (gemäss Definition im Glossar, das die Anonymisierung von der Pseudonymisierung und der Verschlüsselung abgrenzt) mit Sicherheit keine Rückschlüsse auf die Identität

[7] Gemäss Definition im Glossar, die dieses von Pseudonymisierung und Verschlüsselung ausgrenzt.

der betroffenen Kunden zulassen, und damit nur bei anonymisierten Daten die Pflicht eines besonderen Schreibens an die Kunden gemäss Rz 39 des RS 08/7 entfällt.

Nichtsdestotrotz wurde dem Wunsch nach weniger präzisen und nicht zu granularen Anforderungen aufgenommen und Rz 20–23 auf einen einzigen, prinzipienbasierten Paragraphen reduziert.

Fazit

Rz 20 wurde leicht geändert und Rz 21–23 ersatzlos gestrichen.

3.2.5 „Need to know"- Grundsatz (Rz 24–26)

Stellungnahmen (summarisch)

- Die SBVg hat sich zu Rz 24 wie folgt geäussert: «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.» Die gleiche Bemerkung wurde auch von der VHV vorgebracht.

- Mehrere Stellungnahmen haben sich über die Präzisierung der Erteilung der Zugriffsrechte in Rz 25 und 26 negativ geäussert.

Würdigung

Der „Need to Know"-Grundsatz wurde zu einem einzigen Satz reduziert und wird in der finalen Version ohne weitere Präzisierungen für alle Banken gelten. Rz 2 wurde entsprechend aktualisiert.

Fazit

Rz 2 und 24 wurden geändert und Rz 25–26 ersatzlos gestrichen.

3.2.6 Liste der Mitarbeitenden mit Zugriff auf CID und Liste der "Schlüsselmitarbeitenden" (Rz 28, 29, 41)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen haben sich über den Nutzen einer Liste der Mitarbeitenden mit Zugriff auf CID skeptisch geäussert. Zum Beispiel kommentierte die VHV: „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."

Würdigung

Rz 28 wurde entsprechend dem Kommentar der VHV geändert.

Fazit

Rz 28 wurde angepasst und der Inhalt von Rz 29 neu Rz 41 angefügt.

3.2.7 Sorgfältige Auswahl der Mitarbeitenden (Rz 38)

Stellungnahmen (summarisch)

- SIX Securities Services kommentierte, eine „Bank kann keine Prozesse von Dritten sicherstellen; sinnvollerweise kann und sollte eine Bank diese Pflichten entsprechend vertraglich festhalten und sich damit auch das Recht sichern, eine Einhalteprüfung bzgl. Erfüllung dieser Anforderungen durchführen zu dürfen."

Würdigung

Rz 38 wurde entsprechend dem Kommentar von SIX Security Services geändert.

Fazit

Rz 38 wurde angepasst.

3.2.8 Produktionsumfeld, Aktivitäten in Verbindung mit Massen-CID (Rz 47)

Stellungnahmen (summarisch)

- Mehrere Stellungnahmen haben sich zum Begriff „Aktivitäten" geäussert und eine Präzisierung gefordert.

Würdigung

In Rz 47 steht die Arbeit von IT Administratoren und Mitarbeitenden (inkl. Dritter) mit erhöhten Zugriffsrechten im Fokus. Typischerweise sind in diesem Bereich „Aktivitäten" als „Datenbearbeitung" auf Massen-CID zu verstehen. Da solche „Aktivitäten" zum Aufgabenprofil der oben genannten Mitarbeitenden gehören, können sie nicht beschränkt oder verhindert werden. Die möglichen Sicherheitsmassnahmen stützen sich auf zwei Aspekte:

- Die Benachrichtigung solcher Aktivitäten an die für die Datensicherheit zuständige Einheit, der solche zur Kenntnis gebracht werden müssen;
- Die Nachvollziehbarkeit der geleisteten Aktivitäten, entweder durch elektronische (z.B. mittels Log-Dateien) oder weitere Massnahmen (z.B. Vier-Augen-Prinzip).

Fazit

Rz 47 wurde dementsprechend angepasst.

3.2.9 Meldung (Rz 51)

Stellungnahmen (summarisch)

- Die VHV kommentiert: „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“. Sie schlägt eine alternative Formulierung vor.

- SIX Securities Services kommentiert: „Vertraulichkeit per se ist kein Risiko.“

Fazit

Rz 51 wurde dementsprechend angepasst.

3.3 Spezifische Fragen zur Anhörung und übrige Themen

Die eingegangenen Stellungnahmen betrafen im Wesentlichen die folgenden Punkte:

- Fragen zur Anhörung
- Mindesteigenmittel und Untergrenze (*Floor*, Rz 116)

3.3.1 Fragen zur Anhörung

Im Rahmen dieser Anhörung hat die FINMA folgende weitergehenden spezifischen Fragen gestellt:

> 1. Kapitel IV.B „Qualitative Grundanforderungen“:
>
> Das Inkrafttreten dieses Kapitels ist im Entwurf für den 1. Januar 2015 vorgesehen.
>
> Wie beurteilen Sie die Möglichkeit, das Inkrafttreten des Kapitels IV.B „Qualitative Grundanforderungen“ bereits auf den 1. Juli 2014 festzusetzen?
>
> (Der Anhang 3 „Umgang mit elektronischen Kundendaten“ würde wie vorgesehen am 1. Januar 2015 in Kraft treten.)
>
> 2. Anhang 3 „Umgang mit elektronischen Kundendaten“:
>
> Dieser Anhang ist gemäss Entwurf auf natürliche Personen („Privatkunden“), deren Geschäftsbeziehungen in oder von der Schweiz aus betreut oder geführt werden, begrenzt.
>
> Wie beurteilen Sie die Möglichkeit einer Ausweitung des Anwendungsbereichs

a) auf natürlichen Personen („Privatkunden“), deren Geschäftsbeziehungen im Ausland betreut oder geführt werden?

b) auf juristische Personen (z.B. „Firmenkunden“)?

Die eingegangenen Antworten betrafen im Wesentlichen die folgenden Punkte:

- Zu 1) haben sich alle Stellungnahmen negativ geäussert und die Möglichkeit eines frühzeitigen Inkrafttretens auf den 1.7.2014 abgelehnt.
- Zu 2a) haben sich viele Stellungnahmen negativ geäussert. Das AFBS betonte, dass aus Unterschieden in Datenschutzregelungen sowie weiteren spezifischen Anforderungen (z.B. diejenigen in U.K. und Singapur[8]) schwer administrierbare Widersprüche oder Doppelspurigkeiten entstehen könnten. Dazu kommentierte Credit Suisse, dass eine Ausweitung auf im Ausland betreute oder geführte Kundenbeziehungen die Komplexität in Bezug auf Zeitrahmen, Ressourcen und Kosten massiv erhöhen würde.
- Zu 2b) gab es wenig fundamentalen Widerstand. Einige Stellungnahmen erachteten die Möglichkeit einer Ausweitung des Anwendungsbereichs von Anhang 3 auf juristische Personen als machbar, da bereits heute in kleineren Instituten vergleichbare Systeme zum Einsatz kommen. Gleichzeitig wurde jedoch betont, dass juristische Personen nicht im Fokus des Anhangs 3 seien. In diesem Zusammenhang sei die Präzisierung der Treuhandkammer genannt: «Privatkunden, die ihre Geschäftsbeziehungen nicht direkt mit den Banken sondern mittels Sitzgesellschaften, Domizilgesellschaften, Stiftungen, Trusts oder anderen Rechtsformen unterhalten, welche nicht als „natürliche Personen“ gelten.»

Würdigung

Die FINMA hat die Anhörungsversion hinsichtlich der spezifischen Fragen 1) und 2a) nicht geändert, was der Mehrheit der eingegangenen Stellungnahmen entspricht.

Eine Ausweitung auf juristische Personen gemäss 2b) wäre möglich gewesen. Die FINMA hat sich unter Kosten-/Nutzen-Betrachtungen entschieden, eine solche Ausweitung des Anwendungsbereichs nicht in einer präskriptiven Weise durchzuführen. Die Anwendung der in Anhang 3 genannten Anforderungen bleibt damit auch für CIDs von juristischen Personen empfohlen, wird aber nicht als zwingend gesehen.

Die Einwände der Treuhandkammer wurden berücksichtigt durch eine Präzisierung von Rz 1.

Fazit

Das Rundschreiben tritt auch für die qualitativen Grundanforderungen am 1. Januar 2015 in Kraft. Der Anwendungsbereich des Anhangs 3 bleibt unverändert mit Ausnahme einer Präzisierung von Rz 1.

[8] UK FSA „Data Security in Financial Services“ (April 2008) oder Singapore MAS „Technology Risk Management Guidelines“ (June 2013)

3.3.2 Mindesteigenmittel und Untergrenze (*Floor*, Rz 116)

Stellungnahmen (summarisch)

- Credit Suisse, UBS und SBVg haben weitere Erläuterungen zu Rz 116 für AMA Banken – insbesondere welche Methode zum Einsatz kommen soll – verlangt.

Würdigung

Die neuen Bestimmungen zu den Mindesteigenmitteln und zur Untergrenze bringt das FINMA-RS 08/21 in Übereinstimmung mit den Rz 381–381.1 des FINMA-Rundschreibens 2008/19 „Kreditrisiken Banken". Sie sind nur relevant für Banken, die den AMA-Ansatz anwenden.

Die Berechnung der Mindesteigenmittel für operationelle Risiken orientiert sich am Standardansatz gemäss Art. 93 der Eigenmittelverordnung (ERV; SR 952.03). Diese Information wird Rz 116 beigefügt.

Die FINMA weist darauf hin, dass bei der Berechnung des *Floors* immer sämtliche Eigenmittelanforderungen zu berücksichtigen sind. Hierfür kommt ein internes Verfahren unter Anwendung des Standardansatzes zum Einsatz. Dies bedeutet, dass nie die Rede von einem segmentierten Vergleich ist, in dem der Standardansatz für operationelle Risiken allein im Verhältnis zum Eigenmittelerfordernis gemäss AMA gestellt wird.

Da in den meisten Fällen der Anteil erforderlicher Eigenmittel für operationelle Risiken im Verhältnis zum Gesamttotal der erforderlichen Eigenmittel gering ist (nur in einzelnen extremen Fällen erreicht dieses 40 %), bleibt die Wahrscheinlichkeit sehr gering durch Anwendung des AMA alleine eine Reduktion auf Gesamtbankstufe von 20 % zu erreichen. Auch für eine Bank, die stark überproportional in operationellen Risiken exponiert ist (als Beispiel wird die Annahme getroffen, dass dieser Anteil 40 % sei, berechnet mittels Standardansatz – SA – für operationelle Risiken), würde eine Reduktion von 20 % resultieren, so dass die Eigenmittelanforderungen für operationelle Risiken mit AMA 50 % tiefer wären als diejenigen, die mittels Anwendung des SA resultieren würden. Eine derartige Reduktion würde von der FINMA ohnehin als sehr kritisch beurteilt.

Fazit

Rz 116 wurde wie ausgeführt überarbeitet.

4 Weiteres Vorgehen

Die Teilrevision des Rundschreibens operationelle Risiken Banken stiess auf einen unterschiedlichen Grad an Zustimmung. Da die Hauptkritiken auf den Anhang 3 des Rundschreibens fokussiert waren, hat die FINMA insbesondere die Thematik des „Umgang mit elektronischen Kundendaten" überarbeitet und die Ergebnisse der Anhörung entsprechend weitgehend berücksichtigt.

Das teilrevidierte Rundschreiben tritt auf den 1. Januar 2015 in Kraft.