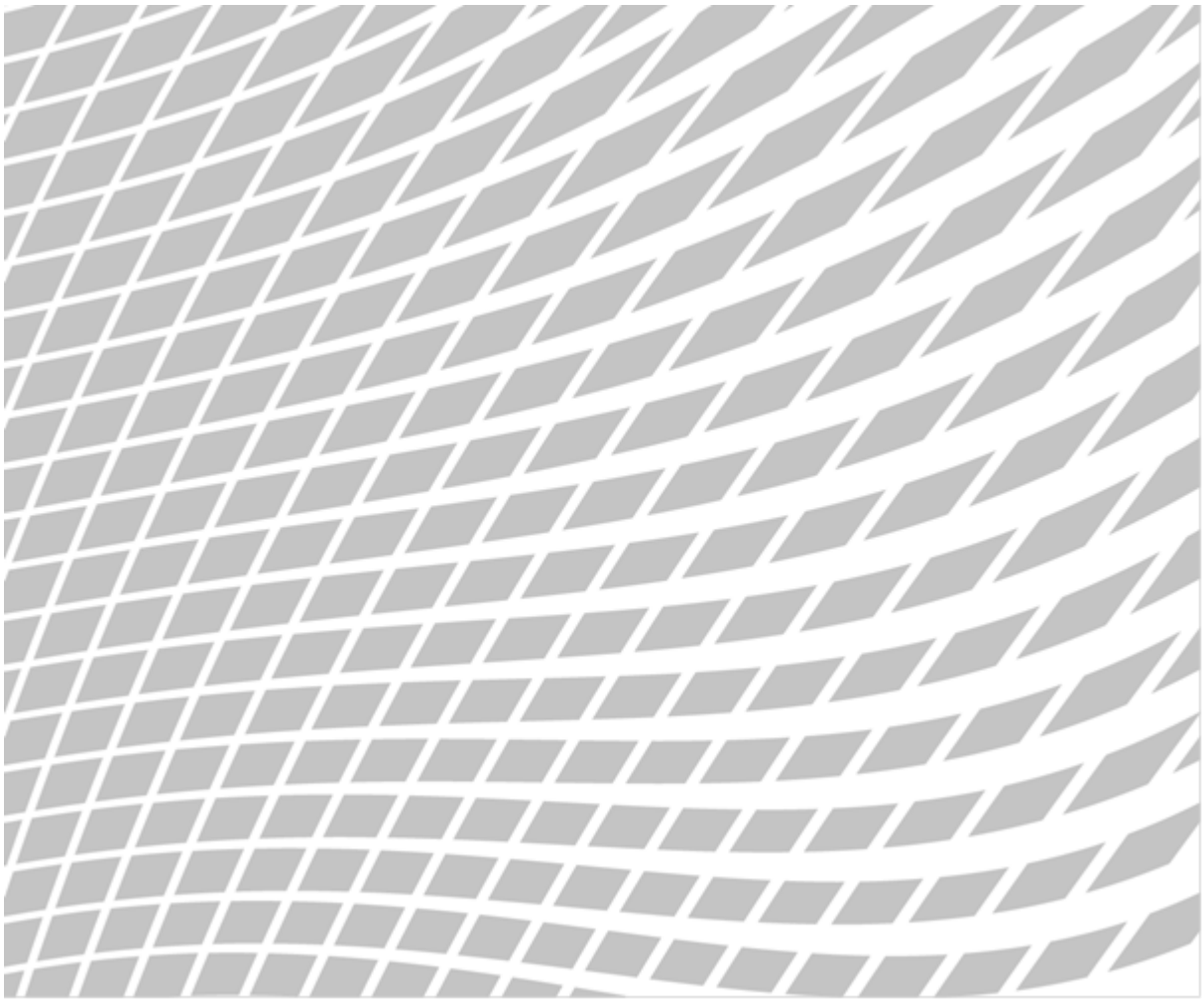
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

23. Mai 2013

# FINMA-Rundschreiben 2008/21: Operationelle Risiken Banken – Teilrevision

## Erläuterungsbericht



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

b102255-0000008

Referenz: b102255-0000008

# 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 als Standard im Papier „*Principles for the Sound Management of Operational Risk*“ in Juni 2011 ausgearbeitet wurden. Quantitative (Eigenmittel-) Anforderungen sind nicht Teil dieser Revision 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-Rundschreibens 2008/21 besteht neu die Möglichkeit, sehr konkrete Anforderungen für spezifische Risiken in einem Anhang zu regeln. So wird zusätzlich der Umgang mit elektronischen Kundendaten im neuen Anhang 3 geregelt. Weitere Themen werden unter Umständen in Zukunft ebenfalls mit höherem Detaillierungsgrad in ähnlicher Form eingeführt.

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 Hintergrund

## 1.1 Internationale Entwicklungen

Schwerwiegende operationelle Verluste während der Finanzkrise und der letzten Jahre führten weltweit zu einer Neubeurteilung der operationellen Risiken. In der Folge wurden auf internationaler Ebene sowohl die quantitativen als auch die qualitativen regulatorischen Anforderungen in Bezug auf das operationelle Risikomanagement bei Banken diskutiert. Die Standard Implementation Sub-Group for Operational Risk („SIGOR"), in der die FINMA vertreten ist, arbeitet unter dem Mandat des Basler Ausschusses für Bankenaufsicht (Basel Committee on Banking Supervision, „BCBS") seit 2010 an der Revision der Kapitalanforderungen für operationelle Risiken. In erster Linie wurden die bestehenden Kapitalanforderungen für operationelle Risiken in Frage gestellt und eine Neukalibrierung – die möglicherweise zu höheren Kapitalanforderungen führen wird, namentlich für grosse und mittelgrosse Banken – ins Auge gefasst. Ausserdem wurden konzeptionelle Schwächen in der Basel II-Definition des Basisindikatoren- und Standardansatzes für die Kapitalberechnung identifiziert. Die Diskussionen sind allerdings noch nicht soweit fortgeschritten, als dass ein konkreter Zeitplan für die Übernahme ins Basel Regelwerk bestünde. Vorderhand besteht deshalb kein Anlass das FINMA-Rundschreiben 2008/21 hinsichtlich der quantitativen Anforderungen anzupassen.

Die von der Arbeitsgruppe SIGOR erarbeiteten Grundsätze „*Principles for the Sound Management of Operational Risk*" („BCBS-Principles") gelten als neue Richtlinie für das Management von operationellen Risiken und wurden im Jahr 2011 durch das BCBS verabschiedet. Dieses Regelwerk ist der Nachfolger des BCBS-Regelwerks „*Sound Practices for the Management and Supervision of Operational Risk*" („BCBS-Practices 2003") aus dem Jahr 2003, welches die Grundlage für die qualitativen Anforderungen des aktuellen FINMA-Rundschreibens 2008/21 bildet. In vielen Mitgliedstaaten des BCBS wurde das Regelwerk zu den qualitativen Anforderungen direkt, als Bestandteil der lokalen Regulierung von operationellen Risiken, oder indirekt, in Form eines Self-Assessment-Templates, bereits implementiert.

Weitere Gründe für die Revision des FINMA-Rundschreibens 2008/21 sind die mangelnde Tiefe der bisherigen qualitativen Grundanforderungen sowie deren eingeschränkter Geltungsbereich. Als Konsequenz der Schwachpunkte hat sich die Berichterstattung der aufsichtsrechtlichen Prüfgesellschaften zu den operationellen Risiken als wenig effektiv erwiesen. So kann beispielsweise kaum zwischen Banken mit einem guten oder mangelhaften Risikomanagement für operationelle Risiken differenziert werden. Die zahlreichen Fälle von aufgetretenen operationellen Ereignissen der letzten Jahre zeigten zudem, dass differenziertere Anforderungen an das Management für operationelle Risiken nötig sind.

## 1.2 Übernahme der BCBS-Principles ins FINMA-Rundschreiben 2008/21

Die elf BCBS-Principles 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 genü-

gend umgesetzt sind, werden um ausgewählte Erläuterungen aus den BCBS-Principles erweitert. Redundanzen mit anderen Rundschreiben werden wo immer möglich gering gehalten.

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 der Randziffern 124, 125, 127 Bst. c bis i, 128, 130-131 ausgenommen.

Aufgrund der erhöhten Tiefe der allgemeinen qualitativen Anforderungen, welche zudem neu von einer grösseren Population von Banken zu erfüllen sind, befinden sich diese erweiterten Grundsätze im (neuen) IV. Kapitel des FINMA-Rundschreibens 2008/21. Zusätzlich besteht neu die Möglichkeit, sehr konkrete Anforderungen für spezifische Risiken in einem Anhang zu regeln. So wird der Umgang mit elektronischen Kundendaten im neuen Anhang 3 geregelt. Weitere Themen werden unter Umständen in Zukunft ebenfalls mit höherem Detaillierungsgrad in ähnlicher Form eingeführt.

## 1.3 Neuer Anhang 3 – Ergänzung des FINMA-Rundschreibens um Grundsätze für das sachgerechte Management von Risiken im Umgang mit elektronischen Kundendaten

Die Gewährleistung der Vertraulichkeit von Kundendaten stellt für Banken und Effektenhändler in der Schweiz ein wesentliches operationelles Risiko dar. Wie bei anderen operationellen Risiken mit einer Reputationskomponente besteht namentlich bei erheblichen Diskrepanzen gegenüber den Branchenstandards eine ernste Gefahr nicht nur für das betroffene Institut, sondern auch für den Ruf des Schweizer Finanzmarkts.

Der neue Anhang 3 enthält Grundsätze und 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. Die grundlegenden rechtlichen Bestimmungen finden sich nicht nur im Aufsichtsrecht[1], sondern auch im Datenschutzrecht[2] und Zivilrecht.

Der Anhang 3 umfasst insgesamt neun Grundsätze und neunundfünfzig Randziffern, die in Zusammenarbeit mit Vertretern aus der Industrie entwickelt wurden und deren relevante Erfahrungen im Umgang mit Kundendaten beschreiben. Er regelt detailliert die von der FINMA erwartete Vorgehensweise bei der Errichtung eines umfassenden Rahmens zur Sicherstellung der Vertraulichkeit von Kundendaten. Zunächst werden Governance-Aspekte und anschliessend die Definition von Kundenidenti-

[1] Insbesondere Art. 3 und 47 BankG sowie Art. 9 BankV; Art. 10 und 43 BEHG sowie Art. 19 f. BEHV.
[2] Insbesondere Art. 7 DSG sowie Art. 8 ff. VDSG (vgl. dazu auch die Leitfäden des EDÖB, abrufbar unter <www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=de>).

fikationsdaten (Client Identifying Data – „CID“) erläutert. Danach werden die Anforderungen an Systeme, Prozesse und Personen erörtert. Schliesslich richtet sich der Fokus auf Risikoidentifizierungs- und Überwachungsverfahren unter Berücksichtigung von CID-Vertraulichkeitsrisiken im Zusammenhang mit Outsourcing.

Abschliessend sei darauf hingewiesen, dass sich Vorfälle in Verbindung mit der Vertraulichkeit von Kundenmassendaten fahrlässig oder vorsätzlich ereignen können. Die FINMA erwartet daher, dass der Schaffung eines unternehmensweiten Bewusstseins für einen sorgfältigen Umgang mit den Kundendaten besondere Aufmerksamkeit geschenkt wird.

Im zweiten Kapitel findet sich ein Glossar mit den Definitionen der wichtigsten Begriffe, die im Anhang 3 des Rundschreibens verwendet werden.

### 1.4 Workshop zum vorliegenden Entwurf des FINMA-Rundschreibens 2008/21

Die Änderungen im FINMA-Rundschreiben 2008/21 „Operationelle Risiken Banken“ wurden am 8. März 2013 an einem Workshop vorgestellt und diskutiert. Beteiligt waren: FINMA (Vorsitz), Schweizerische Bankiervereinigung, Credit Suisse AG, Deloitte AG, Ernst & Young AG, KPMG AG, PricewaterhouseCoopers AG, Raiffeisen Schweiz Genossenschaft, RBA Holding AG, Treuhand-Kammer, UBS AG, Verband der Auslandsbanken in der Schweiz, Verband Schweizerischer Kantonalbanken, Vereinigung Schweizer Privatbanquiers. Die von den anwesenden Teilnehmern aufgebrachten Punkte wurden durch die FINMA in einem Protokoll festgehalten, welches bei Bedarf noch angepasst wurde. Sämtliche protokollierte Themen wurden nachfolgend durch die FINMA geprüft.

## 2 Ausblick auf zukünftige Anpassungen des FINMA-Rundschreibens 2008/21

Die quantitativen Regeln zu den operationellen Risiken wurden im Rahmen von Basel III nicht revidiert. Die Berechnung der Eigenmittel-Anforderungen für operationelle Risiken erfolgt unverändert. Für andere Risikotypen gelten inzwischen höhere Eigenmittel-Anforderungen und/oder erhöhte qualitative Anforderungen (beispielsweise Liquidität). Inzwischen hat das BCBS zwar erkannt, dass die einfachen Ansätze (Basisindikatoransatz, Standardansatz) für die Berechnung des Eigenmittel-Erfordernisses für operationelle Risiken gewisse Schwächen aufweisen (beispielsweise mangelnde Risikosensitivität des Ertragsindikators). Die Überarbeitung der quantitativen Anforderungen wurde durch das BCBS in Angriff genommen. Die Arbeiten sind jedoch noch nicht ausreichend fortgeschritten, dass eine Planung aufgesetzt werden kann. Die FINMA wird die entsprechenden Anpassungen zu gegebener Zeit unter Wahrung der üblichen Prozesse in die nationale Regulierung einpflegen.

## 3 Die wesentlichsten Änderungen und Auswirkungen im Überblick

Der bisherige Anhang 1 „Qualitative Anforderungen“ wurde komplett überarbeitet und aufgrund seiner Bedeutung als neues IV. Kapitel ins Rundschreiben integriert. Gleichzeitig wurde die Struktur des Rundschreibens wie in der untenstehenden Tabelle 1 abgebildet angepasst. Dies führte auch dazu, dass der bisherige Anhang 2, der die Geschäftsfelder nach Art. 93 Abs. 2 ERV kategorisiert, zum neuen Anhang 1 wurde. Die Übersicht zur Klassifikation von Ereignistypen findet sich neu nicht mehr in Anhang 3 sondern in Anhang 2. Schliesslich wurde bei der vorliegenden Revision darauf verzichtet, den Vergleich zwischen den Bestimmungen im FINMA-Rundschreiben und den Basler Mindeststandards in Form einer Konkordanztabelle im dritten Anhang abzudrucken. Neuer Anhang 3 bilden folglich die neu geschaffenen Grundsätze zum Umgang mit elektronischen Kundendaten.

Die Revision und der Einbezug der qualitativen Anforderungen in den Haupttext des FINMA-Rundschreibens führte schliesslich dazu, dass die Bestimmung des Gegenstands des FINMA-Rundschreibens und der Begriff „Operationelle Risiken“ sowie die Bestimmungen zu den Eigenmittelanforderungen (neuer Abschnitt III) leichte Anpassungen erfahren haben.

| Bisherige Struktur des FINMA-Rundschreibens | Neue Struktur des FINMA-Rundschreibens |
|---|---|
| **I. Gegenstand** | **I. Gegenstand** |
| **II. Begriff (Art. 89 ERV)** | **II. Begriff** |
| | **III. Eigenmittelanforderungen** |
| **III. Der Basisindikatoransatz (BIA, Art. 92 ERV)** | A. Der Basisindikatoransatz (BIA, Art. 92 ERV) |
| **IV. Der Standardansatz (Art. 93 ERV)** | B. Der Standardansatz (SA, Art. 93 ERV) |
| A. Mechanismus | a) Mechanismus |
| B. Allgemeine Anforderungen (Art. 93 Abs. 3 ERV) | b) Allgemeine Anforderungen (Art. 93 Abs. 3 ERV) |
| C. Zusätzliche Anforderungen für im Ausland tätige Banken | - |
| **V. Institutsspezifische Ansätze (AMA, Art. 94 ERV)** | C. Institutsspezifische Ansätze (AMA, Art. 94 ERV) |
| A. Bewilligung | a) Bewilligung |
| B. Qualitative Anforderungen | b) Zusätzliche qualitative Anforderungen |
| C. Allgemeine quantitative Anforderungen | c) Allgemeine quantitative Anforderungen |
| D. Interne Verlustdaten (Art. 94 Abs. 2 ERV) | d) Interne Verlustdaten (Art. 94 Abs. 2 ERV) |
| E. Externe Verlustdaten (Art. 94 Abs. 2 ERV) | e) Externe Verlustdaten (Art. 94 Abs. 2 ERV) |
| F. Szenarioanalyse (Art. 94 Abs. 2 ERV) | f) Szenarioanalyse (Art. 94 Abs. 2 ERV) |
| G. Geschäftsfeld und internes Kontrollsystem (Art. 94 Abs. 2 ERV) | g) Geschäftsfeld und internes Kontrollsystem (Art. 94 Abs. 2 ERV) |
| H. Risikoverminderung durch Versicherungen | h) Risikoverminderung durch Versicherungen |
| **VI. Partielle Anwendung von Ansätzen** | D. Partielle Anwendung von Ansätzen |
| **VII. Anpassungen der Eigenmittelanforderungen (Art. 45 Abs. 3 ERV)** | E. Anpassungen der Eigenmittelanforderungen (Art. 45 Abs. 3 ERV) |
| | F. Mindesteigenmittel und Untergrenze (Floor) |
| **Anhang 1 – Qualitative Grundanforderungen** | **IV. Qualitative Anforderungen** |
| | A. Proportionalitätsprinzip |
| | B. Qualitative Grundanforderungen |
| | C. Risikospezifische Qualitative Anforderungen |
| | **V. Prüfung und Beurteilung durch die Prüfgesellschaften** |
| **Anhang 2 – Kategorisierung der Geschäftsfelder nach** | **Anhang 1 – Kategorisierung der Geschäftsfelder nach** |

| | |
|---|---|
| **Art. 93 Abs. 2 ERV** | **Art. 93 Abs. 2 ERV** |
| **Anhang 3 – Übersicht zur Klassifikation von Ereignistypen** | **Anhang 2 – Übersicht zur Klassifikation von Ereignistypen** |
| **Anhang 4 – Vergleich zwischen FINMA-RS und Basler Mindeststandards** | - |
| | **Anhang 3 – Umgang mit elektronischen Kundendaten** |

Tabelle 1

# 4 Erläuterungen zu den einzelnen Änderungen im Rundschreiben und in den Anhängen

## 4.1 Titel und rechtliche Grundlagen

Der Untertitel des FINMA-Rundschreibens 2008/21 „Operationelle Risiken Banken“ lautet neu „Eigenmittelanforderungen und Qualitative Anforderungen für Operationelle Risiken bei Banken“[3], womit die Bedeutung der qualitativen Anforderungen besser zum Ausdruck gebracht wird. Ausserdem wurde Art. 9 Abs. 2 BankV zu den rechtlichen Grundlagen hinzugefügt, um die Verbindung zu den Bestimmungen an das Risikomanagement sicherzustellen.

## 4.2 Gegenstand (Rz 1)

Der Gegenstand wurde ergänzt um die Definition der qualitativen Grundanforderungen an das Management der operationellen Risiken gestützt auf Art. 9 Abs. 2 BankV sowie um den Verweis, dass die qualitativen Grundanforderungen den BCBS-Principles entsprechen.

## 4.3 Begriff (Rz 2 und neue Rz 2.1)

Der Verweis auf Art. 89 ERV im Titel wurde gestrichen, da die Definition der operationellen Risiken um einen Absatz betreffend die Reputationsrisiken ergänzt worden ist.

## 4.4 Eigenmittelanforderungen (Rz 3 ff.)

### 4.4.1 Der Basisindikatoransatz (BIA, Art. 92 ERV)

***Rz 20-22***
Diese Bestimmungen wurden gestrichen, da sie durch das neue Proportionalitätsprinzip (vgl. Abschnitt IV. A des Rundschreibens) ersetzt werden.

[3] Bisher „Eigenmittelanforderungen für Operationelle Risiken bei Banken“.

### 4.4.2 Der Standardansatz (SA, Art. 93 ERV)

***Rz 28***
Diese Bestimmung wurde gestrichen, da sie durch das neue Proportionalitätsprinzip (vgl. Abschnitt IV. A des Rundschreibens) ersetzt werden.

***Rz 29***
Korrektur des Verweises auf den neuen Anhang 1 (bisher Anhang 2).

***Rz 30-44***
Aufgehoben. Die Randziffern 30-44 enthielten zusätzliche operative Anforderungen für im Ausland tätige Banken. Die Anforderungen der früheren Randziffern 30-44 sind in den neuen qualitativen Grundanforderungen (Rz 117 ff.) integral enthalten. Der Geltungsbereich der neuen qualitativen Anforderungen orientiert sich an der Grösse und Komplexität der einzelnen Institute (Rz 117-118). Tätigkeiten im Ausland tragen zur Komplexität des Instituts bei.

### 4.4.3 Institutsspezifische Ansätze (AMA, Art. 94 ERV)

***Rz 50***
Änderung der Überschrift und des Verweises, wonach Banken, die einen institutsspezifischen Ansatz verwenden, neu die qualitativen Grundanforderungen gemäss Kapitel IV.B statt dem bisherigen Anhang 1 erfüllen müssen.

***Rz 64***
Aufgehoben, (vgl. die Ausführungen zu den Rz 40-42 oben).

***Rz 71 und Rz 79***
Korrektur des Verweises auf den neuen Anhang 2 (bisher Anhang 3).

## 4.5 Mindesteigenmittel und Untergrenze (Floor; neue Rz 116)

Die neue Bestimmungen zu den Mindesteigenmittel und der Untergrenze bringt das FINMA-Rundschreiben 2008/21 in Übereinstimmung mit den Randziffern 381-381.1 des FINMA-Rundschreibens 2008/19 „Kreditrisiken Banken“ und ist nur relevant für Banken, die den AMA-Ansatz verwenden.

## 4.6 Qualitative Anforderungen (neue Rz 117 ff.)

### 4.6.1 Vorbemerkungen

In das im Jahr 2006 anlässlich der Umsetzung der damals neuen Basler Eigenkapitalvereinbarung (Basel II) gemeinsam mit den FINMA-Rundschreiben 2008/19 "Kreditrisiken Banken", 2008/20 "Marktrisiken Banken", 2008/22 "EM-Offenlegung Banken" und 2008/23 "Risikoverteilung Banken" als Ausführungsbestimmungen zur damals neuen Eigenmittelverordnung (ERV) geschaffene aktuelle FINMA-Rundschreiben 2008/21, wurden lediglich die sieben Grundsätze zu den qualitativen Anforderungen aus den BCBS-Practices 2003 übernommen und auf detailliertere Ausführungen – gestützt auf die erläuternden Paragraphen der BCBS-Practices 2003 – verzichtet. Heute zeigt sich, dass die Grundsätze zu wenig konkret ausformuliert sind und namentlich folgende Themen nicht oder nicht ausreichend abgedeckt werden:

- Analyse interner (oder externer) Verlustdaten in Bezug auf systematische Schwächen des internen Kontroll-Frameworks für operationelle Risiken;
- allgemeine Anforderungen für die Definition und laufende Weiterentwicklung von Risiko- und Performance-Indikatoren, den sogenannten Key Risk Indicators (KRI) und Key Performance Indicators (KPI) in Bezug auf die operationellen Risiken[4];
- Anforderung in Bezug auf Risikoszenarien betreffend operationelle Risiken, welche mittels Experten-Meinung definiert werden (beispielsweise Szenarien mit Fokus auf Kundendatensicherheit).

Da derzeit Banken, die den Basisindikatorenansatz verwenden und keines der in den aktuellen Randziffern 22 und 23 festgehaltenen Kriterien erfüllen, von der Einhaltung der qualitativen Anforderungen befreit sind, hat nur eine sehr kleine Anzahl der Banken und Effektenhändler (weniger als 10% der gesamten Aufsichtspopulation) die qualitativen Anforderungen einzuhalten.

Als Konsequenz dieser Schwachpunkte hat sich die Berichterstattung der aufsichtsrechtlichen Prüfgesellschaften bezüglich der operationellen Risiken als wenig effektiv erwiesen. Das Management von operationellen Risiken wird gestützt auf die aktuelle Regulierung nur auf allgemeiner Ebene durch die aufsichtsrechtlichen Prüfgesellschaften beurteilt.

Das revidierte Rundschreiben sieht vor, dass die qualitativen Anforderungen abhängig von der Grösse der Bank umzusetzen sind (vgl. unten 4.6.2 Proportionalitätsprinzip).

### 4.6.2 Proportionalitätsprinzip (Rz 117-118)

Sogenannte „Kleine Banken“ werden von der Umsetzung gewisser qualitativer Anforderungen ausgenommen, wobei die relevanten Bestimmungen in den Randziffern markiert sind. Als „Kleine Banken“ im Sinne des Rundschreibens qualifizieren Banken und Effektenhändler der Kategorie 5, alle Effek-

[4] Beispielsweise operationelle Risiko-Indikatoren im Bereich von nicht autorisierten Handelsaktivitäten gemäss den Anforderungen der FINMA-Mitteilung 31 (2011) „Nicht autorisierte Transaktionen im Handel“.

tenhändler der Kategorie 4 sowie Banken der Kategorie 4, die über Geschäftsaktivitäten von geringer Komplexität verfügen. Sie werden von der Anwendung der Randziffern 124, 125, 127 Bst. c bis i, 128, 130-131 ausgenommen.

Banken der FINMA-Kategorien 4 und 5 entsprechen ungefähr 90% der gesamten Aufsichtspopulation. Nichtsdestotrotz, erwartet die FINMA dass zahlreiche Banken der Kategorie 4, unter Anwendung des Proportionalitätsprinzips, alle qualitative Grundanforderungen werden erfüllen müssen.

### 4.6.3 Qualitative Grundanforderungen (Rz 119 ff.)

Die elf BCBS-Principles werden im revidierten FINMA-Rundschreiben 2008/21 neu im Hauptteil und in sechs Grundsätzen abgebildet. Das vorliegende Rundschreiben fokussiert auf diejenige Elemente, die der FINMA für das Management von operationellen Risiken als wichtig erachtet. Die nicht ins Rundschreiben übernommenen Erläuterungen wurden teilweise bereits in anderen Regulierungen (Gesetzen, Verordnungen und Rundschreiben) umgesetzt und deshalb im Rundschreiben nicht wiederholt. Einige Erläuterungen in den BCBS-Principles sind trivial, so dass auf eine explizierte Regelung im Rundschreiben bewusst verzichtet worden ist.

***Grundsatz 1: Verantwortlichkeiten (Rz 120-123)***
Die Risikobereitschaft (*Risk Appetite*) bezieht sich auf die inhärenten Risiken, die eine Bank *a priori* einzugehen bereit ist. Die Massnahmen einer Bank, solche Risiken zu beschränken (beispielsweise durch Risikolimiten und -reduktionen sowie Absicherungen) und Residualrisiken zu tolerieren, bestimmen deren Risikotoleranz (*Risk Tolerance*).

Beispielsweise kann eine Bank die operationellen Risiken im Crossborder-Geschäft mit Kunden eines bestimmten Landes derart hoch einschätzen, dass sie darauf verzichtet. Ein solcher Entscheid kann mit finanziellen oder reputationellen Argumenten begründet werden und aufzeigen, dass die Bank diesbezüglich über keine Risikobereitschaft verfügt.

Hingegen kann eine Bank auch entscheiden, dass sie die inhärenten operationellen Risiken im Crossborder-Geschäft mit Kunden eines bestimmten Landes bis zu einem gewisseren Grad zu tragen bereit ist. Diesfalls formuliert sie interne Vorgaben um die Geschäftstätigkeit zu regeln (beispielsweise mittels interner Weisung zum Crossborder-Geschäft mit Kunden des betroffenen Landes). Die Vorgaben können unterschiedlich detailliert und entweder deskriptiv oder präskriptiv sein. Sie müssen aber in Abstimmung mit der Definition der Risikotoleranz gebracht werden. Da eine Bank immer mit Ausnahmen und Fehlern konfrontiert wird (beispielsweise als Folge unzureichender Schulung oder Ressourcen oder durch mangelhafte Kontrollen), wird sie bestimmen müssen, bis zu welchem Grad solche Ausnahmen oder Fehler toleriert werden, beispielsweise durch Setzen eines Schwellenwerts bei sog. „Exceptions to Policy“. Diese sind dann regelmässig zu erheben, zu kontrollieren und zu rapportieren. Wird die entsprechende Risikotoleranz verletzt, muss die GL informiert werden und allenfalls intervenieren.

Die Definitionen von Risikobereitschaft und Risikotoleranz können zeitlich unterschiedlich aufgesetzt sein. Da die Risikobereitschaft eher strategischer Natur ist, gilt sie in der Regel als vorausschauende

Komponente der Risikoanalyse einer Bank. Die Risikobereitschaft wird folglich für mehrere Jahre (beispielsweise über einen Zweijahreshorizont) festgelegt. Im Gegensatz dazu, zielt die Risikotoleranz auf einen kürzeren Zeitraum ab und wird dementsprechend mit höherer Frequenz überprüft und falls notwendig angepasst (beispielsweise durch die Überwachung von Limiten auf monatlicher oder Quartalsbasis).

Beim obigen Beispiel ist es ausserdem möglich, dass sich die Bank aufgrund eines strategischen Entscheids des Verwaltungsrats vom Crossborder-Geschäft mit Kunden eines bestimmten Landes verabschiedet, weil die operationelle Risiken unter Wirtschaftlichkeitsaspekten nicht mehr zu tragen sind. Konsequenterweise wird die Bank keine neuen Kunden dieses Landes aufnehmen, wird aber mit den bestehenden Kunden und Infrastrukturen während einer bestimmten Periode weiterarbeiten müssen. Die Bank hat aber ihre diesbezüglich definierte Risikotoleranz weiterhin einzuhalten und zu überwachen bis zum Abschluss des Exit-Verfahrens des besagten Geschäfts, beispielsweise durch Kündigung aller betroffenen Crossborder-Kundenbeziehungen oder durch Verkauf der zuständigen Einheit an eine Drittbank.

Schliesslich gehören Aussagen, dass keine Toleranz für operationelle Risiken bestehen, der Vergangenheit an und erfüllen nicht mehr die Anforderungen betreffend Risikobereitschaft und -toleranz. Wenn ein neues Geschäft aufgenommen oder ein bestehendes Geschäftsfeld weiterbetrieben wird, ent- resp. bestehen operationelle Risiken, die solange als kein gegenteiliger Entscheid vorliegt, bis zu einem festgelegten Grad toleriert werden.

Eine wichtige Anforderung für die Ausgestaltung von sinnvollen Konzepten 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 etc.). Zusätzlich haben die Banken die Risikotoleranz dem eigenen Management und den eigenen Kontrollstrukturen anzupassen, damit diese effizient überwacht und gemessen werden kann.

***Grundsatz 2: Rahmenkonzept und Kontrollumfeld (Rz 124-126)***

Als inhärente operationelle Risiken werden operationelle Risiken vor der Berücksichtigung von Kontrollen bezeichnet. Sie können auch als „zugrundeliegende“ oder „ursprüngliche“ Risiken bezeichnet werden und sich über die Zeit ändern.

Beispielsweise können sich operationelle Risiken im IT-Bereich durch neue Technologien und Angriffsmethoden (Cyberangriffe) rasch verschärfen. Interne Betrugsfälle können zahlenmässig und in der Schadenhöhe beispielweise in Zeiten tiefer Margen und volatiler Märkte stark zunehmen.

Residualrisiken sind die Risiken nach Berücksichtigung von Kontrollen. Sie ergeben sich aus der Differenz des inhärenten Risikos im Vergleich zum Kontrollsystem. Folglich können sich Residualrisiken unabhängig von der Entwicklung des inhärenten Risikos ändern, beispielsweise durch Kürzungen von Ressourcen in Kontrollfunktionen oder laschere Kontrollen.

Regelmässig und vor allem bei für die Bank bedeutsamen Geschäften und Produkten können aber externe Faktoren nicht unmittelbar durch Verbesserungen des internen Kontrollsystems kompensiert werden. Die separate Betrachtung von inhärenten und Residualrisiken ist auch deswegen wichtig, um rechtzeitig über die Notwendigkeit von ausserordentlichen Massnahmen befinden zu können.

Die Anforderung der einheitlichen Klassifizierung von materiellen operationellen Risiken wird in der Regel durch eine Bewertungsskala der Risiken erfüllt, welche die Frequenz und potentielle Schadenhöhe von Ereignistypen einstuft. Die Einstufung kann mittels Expertenschätzungen sowie durch Datenanalyse erfolgen. Die Auswirkungen bei einem Risikoeintritt können finanzieller und/oder reputationeller Art sein. Eine einheitliche Klassifizierung ermöglicht eine konsistente Berichterstattung an die Risikogremien über sämtliche materiellen operationellen Risiken. Ausserdem können Entscheidungen zur Ressourcenallokation, zur Priorisierung und betreffend Risikominderungsmassnahmen durch eine konsistente Einstufung der operationellen Risiken gestützt werden.

Beispielsweise vermeidet eine einheitliche Klassifizierung, dass Rechts- und Compliance-Risiken inkonsistent zu den übrigen operationellen Risiken beurteilt werden.

***Grundsatz 3: Identifizierung, Begrenzung und Überwachung (Rz 127-128)***
Die Risikoidentifikation soll in- und externe Faktoren berücksichtigen, weil diese in der Regel komplementär sind. Die Erkenntnisse aus der Analyse interner Verluste sind primär vergangenheitsbezogen und können durch vorausschauende Elemente ergänzt werden, beispielsweise Sammlungen und Analysen von Ereignissen, die bei anderen, vergleichbaren Banken stattgefunden haben (sog. *„externe Ereignisse“*) sowie Analysen schwerwiegender Ereignisse, die mit einem hohen Verlustpotenzial verbunden sind (sog. *„Szenarioanalysen“*).

Um zielführende Risiko- und Kontrollbeurteilungen durchzuführen, wird typischerweise mit der Erstellung eines Risikokatalogs der inhärenten Risiken angefangen, der anschliessend mit Eischätzungen und Bewertungen der Risiken ergänzt wird. Zusätzlich werden die Effizienz der Kontrollen beurteilt und die Residualrisiken geschätzt (sog. „RCSA – Risk Control Self Assessments“).

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. Diesbezüglich empfiehlt sich beispielsweise die Lektüre des SIGOR-BCBS-Papiers vom Juni 2011 *„Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches“*, wo im Kapitel „Data“ die Thematik der Verlustdaten gut erläutert wird. Für externe Daten kann man sich zusätzlich auf die Randziffern 86-88 des vorliegenden Rundschreibens stützen.

Szenarioanalysen können für alle Banken sehr nützlich sein, insbesondere für Banken, die nur über wenige Verlustdaten verfügen. Es ist wichtig, dass die Anwendung von Szenarioanalysen konsistent zur Bestimmung der OpRisk-Szenarien bei der Kapitalplanung erfolgt.

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[5] stehen. Das Verhältnis des quantifizierten Verlustpotenzials zu den Eigenmittelanforderungen bedingt einen Ansatz des 99.9%-Quantils der einjährigen Verlustverteilung neben weiteren Kennzahlen einhält.

Unter den Anforderungen zur Preisfestsetzung und Performancemessung sind in der Regel die Verfahren zur Allokation der Eigenmittelanforderungen für operationelle Risiken auf Geschäftsbereiche oder -einheiten sowie die Performancebeurteilung von spezifischen Einheiten oder Mitarbeitern zu verstehen. Beispielsweise darf die jährliche Performancebeurteilung des Leiters einer Handelseinheit nicht losgelöst von der Anzahl Verstösse seiner Einheit gegen die internen Richtlinien zur Minderung der Risiken in Zusammenhang mit unautorisierten Transaktionen erfolgen.

***Grundsatz 4: Interne und Externe Berichterstattung (Rz 129-132)***
Wie bei der Risikoidentifikation im dritten Grundsatz, soll die in- und externe Berichterstattung vergangenheitsbezogene sowie vorausschauende Elemente (beispielsweise externe Ereignisse und potentielle neue Risiken) abdecken.

***Grundsatz 5: Technologieinfrastruktur (Rz 133)***
Operationelle Risiken im IT-Bereich sind in den letzten Jahren exponentiell gewachsen und für jede Bank als materielles Risiko einzustufen.

***Grundsatz 6: Kontinuität bei Geschäftsunterbrechung (Rz 134)***
Schwerwiegende Geschäftsunterbrechungen werden von Retailbanken oft als das höchste operationelle Risiko beurteilt.

### 4.6.4 Risikospezifische Qualitative Anforderungen (Rz 135-136)

Hier schafft die FINMA die Grundlage, um weitergehende Konkretisierungen und Ausführungen an das Management von operationellen Risiken thematisch gegliedert in Anhängen zu veröffentlichen.

## 4.7 Prüfung und Beurteilung durch die Prüfgesellschaften (Rz 137)

Die Prüfung zur Einhaltung der Eigenmittelanforderungen und der qualitativen Anforderungen für operationelle Risiken erfolgt nach Massgabe des FINMA-Rundschreibens 2013/3 „Prüfwesen“.

## 4.8 Anhang 1 – Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV

Der bisherige Anhang 2, der die Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV enthält, wurde durch die vorgenommene Integration der qualitativen Anforderungen ins Rundschreiben zum Anhang 1.

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

Inhaltlich wurden keine Änderungen vorgenommen.

## 4.9 Anhang 2 – Klassifizierung von Ereignistypen

Der bisherige Anhang 3, der die Übersicht zur Klassifizierung von Ereignistypen enthält, wurde durch die vorgenommene Integration der qualitativen Anforderungen ins Rundschreiben zum Anhang 2.

Inhaltlich wurden keine Änderungen vorgenommen.

## 4.10 Neuer Anhang 3 – Umgang mit elektronischen Kundendaten (Rz 1-69)

### 4.10.1 Vorbemerkungen

Der bisherige Anhang 4, der eine Vergleichstabelle zwischen den Bestimmungen des FINMA-Rundschreibens und den Basler Mindeststandards enthielt, wurde im revidierten FINMA-Rundschreiben 2008/21 ersatzlos gestrichen.

Der neue Anhang 3 enthält neun Grundsätze sowie die dazugehörigen Ausführungen in Bezug auf das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Kundendaten natürlicher Personen mit Buchungszentrum Schweiz, die einen Vertrag nach schweizerischem Recht und schweizerischen Vorschriften unterzeichnet haben. Im Fokus steht dabei das Risiko von Vorfällen in Bezug auf die Vertraulichkeit von Kundendaten durch die Verwendung elektronischer Systeme. Sicherheitsüberlegungen für physische Daten sowie Bestimmungen über die Integrität und Verfügbarkeit von Daten werden nur am Rande ausgeführt.

### 4.10.2 Geltungsbereich und Proportionalitätsprinzip (Rz 1-2)

Kleine[6] 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.

[6] Vgl. Rz 118 des Kapitels IV. A.

### 4.10.3 Grundsätze für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten (Rz 3-59)

***Grundsatz 1: Governance (Rz 3-7)***

Die Schaffung einer unabhängigen Kontrollfunktion, welche die Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten zu schaffen und aufrechtzuerhalten hat, ist von zentraler Bedeutung. Typischerweise wird die Verarbeitung von Kundendaten zum grossen Teil durch interne IT-Fachspezialisten oder Dritte sichergestellt. Diese müssen für die Einhaltung der Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten entsprechend von einer unabhängigen Einheit (beispielsweise Teil der Risikokontrollorganisation) überwacht werden. Die Unabhängigkeit der Kontrollfunktion dient auch der Sicherstellung effektiver Eskalationsstrukturen und der laufenden Identifizierung von Verbesserungsmöglichkeiten des Rahmenkonzepts zur Sicherstellung der Vertraulichkeit von Kundendaten.

Eine klare Aufteilung der Verantwortlichkeiten ermöglicht es, jederzeit und an allen Standorten auf allfällige Vorfälle zeitnah reagieren zu können. Dies ist für eine wirksame Bewirtschaftung der Risiken im Umgang mit Kundedaten von zentraler Bedeutung. Um Klarheit betreffend den Verantwortlichkeiten schaffen und konsistent umzusetzen zu können, wird ein formales und umfassendes Rahmenkonzept zu den Aktivitäten, Prozessen und Systemen benötigt.

***Grundsatz 2: Kundenidentifikationsdaten (Client Identifying Data, CID; Rz 8-14)***

Die Anzahl und Vielfalt der Kundendaten, die ein Institut zu bearbeiten hat, kann sehr umfassend sein. Die Grundanforderung, aus der grossen Menge an Kundendaten jene zur Identifikation der Kunden bestimmen zu können, ist Bestandteil eines soliden Rahmenkonzepts und muss durch jedes Institut erfüllt werden.

Die Definition der Kundenidentifikationsdaten und deren Kategorisierung ist eine institutsspezifische Aufgabe, weil den Banken aufgrund unterschiedlicher Geschäftsmodelle, Produkte, Dienstleistungen und Standorte unterschiedliche Informationen zur Verfügung stehen. Beispielsweise wird ein Institut, welches sich auf die Abwicklung des Zahlungsverkehrs spezialisiert hat, Transaktionsdaten in grösserer Zahl abwickeln als ein Hypothekarinstitut, welches wiederum andere Kundendaten verarbeitet wie ein Vermögensverwaltungsinstitut. Bei der institutsspezifischen Definition von CID sind zudem institutsspezifische Vorfälle (beispielsweise Daten-Lecks) zu berücksichtigen.

Die Identifizierung der für die CIDs verantwortlichen Einheiten („Data Owners“) – typischerweise Business Einheiten, die mit den spezifischen Kunden und Kundendaten vertraut sind – hilft zu vermeiden, dass Dienstleistungsfunktionen (beispielsweise IT) alleine für die Vollständigkeit und Konsistenz der Klassifizierung verantwortlich sind.

***Grundsatz 3: Datenspeicherort und -zugriff (Rz 15-29) und Grundsatz 4: Sicherheitsstandards für die Infrastruktur und die Technologie (Rz 30-36)***

Nach der Einstiegsfrage, über welche Kundendaten eine Bank verfügt, widmet sich der dritte Grundsatz den Anschlussfragen, wo überall Kundendaten lokalisiert sind und wie diese geschützt werden sollen.

Erfahrungen aus diversen Vorfällen zeigen, dass sich die Ermittlungen bei Verlusten von CID durch illegale Handlungen zuerst mit der Identifizierung der Datenquelle befassen. Die Identifizierung der Datenquelle in nützlicher Zeit ist nur möglich, wenn aktuelle Inventare von Applikationen und Mitarbeitern (inkl. Dritten), die auf CID Zugriff haben, bestehen. Werden aufgrund der Ermittlungen interne Quellen ausgeschlossen, müssen externe Quellen (beispielsweise ein Cyberangriff) in Betracht gezogen werden.

Die Speicherung und der Zugriff auf CIDs im Ausland sind nur dann problematisch, wenn die damit verbundenen erhöhten Risiken nicht durch angemessen erhöhte Schutz- und Transparenzvorkehrungen kompensiert werden. Beobachtungen aus der Praxis und der Industrie gegenüber den unterschiedlichen Methoden zum Schutz der Daten im Ausland (Anonymisierung, Pseudonymisierung, Verschlüsselung etc.) zeigen, dass die Verfahren unterschiedlich bewertet werden. Zum Beispiel, wird für pseudonymisierte Daten, die Aufbewahrung der Konkordanztabellen in einer sicheren Umgebung innerhalb der Schweiz als angemessene Vorkehrung angesehen. Bezüglich der Pflicht „Kunden mittels besonderem Schreiben über die Auslagerung im Ausland zu informieren“, hat die Konsultation mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gezeigt, dass nur „anonymisierte Daten“ vollumfänglich „keine Rückschlüsse auf die Identität der betroffenen Kunden (Irreversibilität) im Sinne von Rz. 23 zulässt.

Der „Need to Know“-Grundsatz ist eine wichtige Anforderung im Hinblick auf die Förderung eines unternehmensweiten Bewusstseins im Umgang mit Kundendaten und hinsichtlich Anerkennung von CID als „Asset“.

Die technischen Anforderungen zu den Sicherheitsstandards im vierten Grundsatz sind bewusst sehr generisch formuliert, um einerseits institutsspezifische Lösungen zu ermöglichen und andererseits die zeitlichen Abhängigkeiten so weit als möglich zu reduzieren. Nichtsdestotrotz besteht die Anforderung (wie allgemein für IT-Lösungen üblich), regelmässig die eigenen Sicherheitsstandards mit der Marktpraxis zu vergleichen (im Sinne von „gegenwärtigen Stands der Technik“, VDSG RS 235.11, Art. 8 Abs. 2 lit. d). Um solche Vergleiche sicherstellen zu können, ist in erster Linie das Know-how der internen Fachspezialisten gefordert, die in der Lage sein müssen zu erkennen, ob externe Inputs notwendig sind.

***Grundsatz 5: Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben (Rz 37-42)***

Die ersten vier Grundsätze decken die organisatorischen und infrastrukturellen Anforderungen ab, damit nur berechtigte Mitarbeiter und Dritte Zugang zu den CIDs haben. Zusätzlich muss ein Institut

sicherstellen, dass die berechtigten Mitarbeiter, die Massen-CID bearbeiten dürfen, sorgfältig ausgewählt, geschult und überwacht werden. Es wird von den Banken erwartet, dass sie zumindest gleichwertige Schutzvorkehrungen bezüglich den „Human Factor", der im Zentrum des fünften Grundsatzes steht, zu denjenigen technischer Art treffen. Dabei ist die FINMA bewusst wenig konkret.

***Grundsatz 6: Risikoidentifizierung und -kontrolle in Bezug auf die CID-Vertraulichkeit (Rz 43-45) und Grundsatz 7: Risikominderung in Bezug auf die CID-Vertraulichkeit (Rz 46-48)***

Die Thematik der „Vertraulichkeit von Kundendaten", die im Fokus des Anhangs 3 des revidierten Rundschreibens 2008/21 steht, kann grundsätzlich aus zwei Perspektiven angegangen werden:

- Die organisatorische Perspektive: Erarbeitung der minimalen Anforderungen zur Ausgestaltung eines angemessenen Rahmenkonzeptes zur Gewährleistung der Vertraulichkeit von Kundendaten. Diesen Ansatz hat die FINMA für die Entwicklung des Anhangs 3 verfolgt.
- Die Risiko- und Kontrollperspektive – Erarbeitung von konkreten Szenarien, die zu einer Verletzung der CID-Vertraulichkeit führen können, sowie Kontrollen, welche diese Risiken mindern. Dieser Ansatz führt zu einen spezifischeren und vertieften Detaillierungsgrad und wurde von der Schweizerische Bankiervereinigung für die Entwicklung des Dokumentes „Data Leakage Protection"[7] von Oktober 2012 verfolgt.

Beide Ansätze sind gleichwertig und als komplementär zu betrachten. Der sechste Grundsatz bildet das Bindeglied zwischen diesen Ansätzen.

Der siebte Grundsatz formuliert die Erwartung der FINMA, wonach Aktivitäten, bei denen grosse Mengen von CID verändert oder migriert werden (beispielsweise infolge von Technologie-Upgrades oder organisatorischen Restrukturierungen) Bestandteil der oben erwähnten Risikoszenarien bilden.

***Grundsatz 8: Vorfälle im Zusammenhang mit der CID-Vertraulichkeit, interne und externe Kommunikation (Rz 49-51)***

Die FINMA, die Strafverfolgungsbehörden und die betroffenen Kunden können die Bank in der Abklärungsphase eines Vorfalls oder nach Abschluss preliminärer Untersuchungen, unterstützen um die finanziellen und reputationellen Auswirkungen zu begrenzen. In diesem Zusammenhang hat die Bank über eine klare Kommunikationsstrategie zu verfügen.

[7] Marktpraktiken zu Sicherheitsszenarien und damit verbundenen Schlüsselkontrollen sind umfassend durch die Schweizerische Bankiervereinigung 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).

***Grundsatz 9: Outsourcing-Dienstleistungen und Grossaufträge in Verbindung mit CID (Rz 54-59)***

Insbesondere bei kleinen Banken ist die Risikoexposition im Umgang mit Kundendaten oft stark abhängig von den Vertraulichkeitsstandards ihrer Outsourcing-Dienstleister. Da nicht alle Dienstleiter über dieselben Standards verfügen, muss die Bank die Vertraulichkeit von CID im Auswahl- und Erneuerungsprozess eines Outsourcing-Dienstleiters angemessen berücksichtigen.

### 4.10.4 Glossar (Rz 60-67) und Beispiel zu Kundenidentifikationsdaten (Rz 68)

Kundenidentifikationsdaten (Client Identifying Data, CID) sind sämtliche Datenelemente im Sinne von Personendaten nach Art. 3 Bst. a DSG, die dazu verwendet werden können, einen Kunden direkt zu bestimmen bzw. zu identifizieren oder die verwendet werden können, um durch Kombination mehrerer Datenelemente oder Informationsquellen oder durch die Beobachtung von Datenelementen über eine bestimmte Zeit, Rückschlüsse auf die Identität eines Kunden zu ziehen (für Beispiele siehe III. Kapitel des Anhangs 3, Rz 69).

## 5 Auswirkungen der Teilrevision

Diese Teilrevision des Rundschreibens hat keine Auswirkungen auf die Eigenmittelanforderungen[8] für operationelle Risiken bei Banken und Effektenhändlern.

Allerdings sind aufgrund der erhöhten qualitativen Anforderungen an das Management von operationellen Risiken, die mit dieser Teilrevision in Kraft treten werden, folgende Auswirkungen zu erwarten:

- **Qualitative Grundanforderungen (Kapitel IV.B)**: Die organisatorischen sowie finanziellen Auswirkungen der aktualisierten qualitativen Grundanforderungen sind für die Banken minim. Bei Banken der FINMA-Kategorien 1 bis 3, die ohne Ausnahme alle Anforderungen erfüllen müssen, ist materieller Handlungsbedarf nur bei diejenigen Banken zu erwarten, die dem Management von operationellen Risiken in den vergangenen Jahren nicht ausreichend Aufmerksamkeit geschenkt haben.

  Die Anpassungen der Grundanforderungen, welche auf den BCBS-Principles basieren, bringen die Regulierung von operationellen Risiken in der Schweiz auf den Stand anderer Länder. Diese Revision der qualitativen Grundanforderungen wird zudem der Notwendigkeit an eine verbesserte Regulierung gerecht, als Konsequenz eines negativen Trends von vermehrt auftretenden Fällen mit höheren operationellen Verlusten. Neben diesen qualitativen Verbesserungen hat das überar-

[8] Die neue Randziffer 116 zum „Floor-Regimes“ bringt das FINMA-Rundschreiben 2008/21 in Abstimmung mit den Randziffern 381-381.1 des FINMA-Rundschreibens 2008/19 „Kreditrisiken Banken“ und ist nur für AMA-Banken relevant. Zurzeit hat aber diese Bestimmung keinen quantitativen Effekt auf AMA-Banken.

beitete Rundschreiben eine Signalwirkung im Hinblick auf die Gestaltung angemessener Führungsstrukturen und spezifischer Kontrollmechanismen für operationelle Risiken.

- **Umgang mit elektronische Kundendaten (Anhang 3)**: Organisatorische sowie finanzielle Auswirkungen der neuen qualitativen Anforderungen im Zusammenhang mit dem Umgang mit Kundendaten sind für die Banken als materiell zu betrachten. Marginale Auswirkungen sind nur bei jenen Banken zu erwarten, die bereits institutsspezifische Massnahmen pro-aktiv oder aufgrund konkreter Vorfälle zur Erfüllung der Anforderungen des Anhangs 3 weitgehend eingeleitet haben. Banken, welche jedoch unterdurchschnittlich in Know-how und Infrastruktur zum Schutz der Kundendatenvertraulichkeit investiert haben, werden vermehrt Lücken schliessen müssen.

  Die Implementierung der Anforderungen wird im allgemeinen das Ausmass der Risiken im Umgang mit Kundendaten in der Schweiz reduzieren und die aufsichtsrechtlichen Anforderungen näher an diejenigen anderer Länder[9] rücken lassen, welche auf vergleichbare Werte des Finanzplatzes (beispielsweise Best-in-Class Vermögensverwaltung) setzen.

## 6 Weiteres Vorgehen

Das Inkrafttreten des revidierten FINMA-Rundschreibens 2008/21 ist nach erfolgter Anhörung auf den 1. Januar 2015 vorgesehen. Die Bestimmungen zum Floor (vgl. Rz 116) sind unmittelbar anwendbar.

[9] Beispielsweise: UK FSA „Data Security in Financial Services“ (April 2008) oder Singapore MAS „Technology Risk Management Guidelines“ (June 2012).