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

Rundschreiben 2008/21
Operationelle Risiken Banken

Eigenmittelanforderungen und Qualitative Anforderungen für Operationelle Risiken bei Banken

Referenz:	FINMA-RS 08/21 „Operationelle Risiken Banken“
Erlass:	20. November 2008
Inkraftsetzung:	1. Januar 2009
Letzte Änderung:	~~1. Juni 2012~~ XXX [Änderungen sind mit * gekennzeichnet und am Schluss des Dokuments aufgeführt]
Konkordanz:	vormals EBK-RS 06/3 „Operationelle Risiken“ vom 29. September 2006
Rechtliche Grundlagen:	FINMAG Art. 7 Abs. 1 Bst. b
	BankG Art. 3 Abs. 2 Bst. a und b, 3g, 4 Abs. 2 und 4, 4bis Abs. 2
	BankV Art. 9 Abs. 2 und 4
	BEHG Art. 10 Abs. 2 Bst. a
	BEHV Art. 19 Abs. 3, 20 Abs. 1, 29
	ERV Art. 2, 89–94
	FINMA-GebV Art. 5 ff.
~~Anhang 1:~~	~~Qualitative Grundanforderungen~~
Anhang ~~2~~1:	Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV
Anhang ~~3~~2:	Übersicht zur Klassifikation von Ereignistypen
Anhang ~~4~~3:	~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

Einsteinstrasse 2, 3003 Bern
Tel. +41 (0)31 327 9100, Fax +41 (0)31 327 9101
www.finma.ch

Adressaten																														
BankG			VAG			BEHG		KAG										GwG			Andere									
Banken	Finanzgruppen und -kongl.	Andere Intermediäre	Versicherer	Vers.-Gruppen und -Kongl.	Vermittler	Börsen und Teilnehmer	Effektenhändler	Fondsleitungen	SICAV	KG für KKA	SICAF	Depotbanken	Vermögensverwalter KKA	Vertriebsträger	Vertreter ausl. KKA	Andere Intermediäre		SRO	DUFI	SRO-Beaufsichtigte		Prüfgesellschaften	Ratingagenturen							
X	X						X																							

Inhaltsverzeichnis

Inhaltsverzeichnis

I. Gegenstand

Dieses Rundschreiben konkretisiert die Art. 89–94 der Eigenmittelverordnung (ERV; RS 952.03) und definiert die qualitativen Grundanforderungen an das Management der operationellen Risiken beruhend auf Art. 9 BankV sowie Art. 19 f. BEHV. Es regelt im quantitativen Bereich die Bestimmung der Eigenmittelanforderungen für operationelle Risiken nach den drei zur Auswahl stehenden Ansätzen sowie die damit einhergehenden Verpflichtungen. Die qualitativen Grundanforderungen entsprechen den Basler Empfehlungen zum einwandfreien Management der operationellen Risiken. 1*

II. Begriff ~~(Art. 89 ERV)~~

Operationelle Risiken sind gemäss Artikel 89 ERV definiert als die „Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen oder Systemen oder in Folge von externen Ereignissen eintreten." Die Definition umfasst sämtliche rechtlichen Risiken, inklusive Bussen durch Aufsichtsbehörden und Vergleiche. Sie schliesst aber strategische Risiken und Reputationsrisiken aus. 2

Reputationelle Risiken sind gemäss Art. 89 ERV aus der Definition der operationellen Risiken ausgeschlossen, da sie in der Regel kaum oder gar nicht quantifizierbar sind. Nichtsdestotrotz ist festzuhalten, dass die Realisierung von operationellen Risiken indirekte und potentiell schwerwiegende Auswirkungen auf die Reputation einer Bank haben kann. 2.1*

III. Eigenmittelanforderungen

A. Der Basisindikatoransatz (BIA, Art. 92 ERV)

Für Banken, die ihre Eigenmittelanforderungen für operationelle Risiken nach dem Basisindikatoransatz bestimmen, ergeben sich diese als Produkt des Multiplikators α und dem aus den vorangegangenen drei Jahren bestimmten Durchschnitt der jährlichen Ertragsindikatoren GI[1]. Für die Durchschnittsbildung sind jedoch nur diejenigen Jahre zu berücksichtigen, in denen GI einen positiven Wert aufweist. 3

Die drei vorangegangenen Jahre nach Rz 3 (bzw. Rz 24) entsprechen den drei unmittelbar dem Stichtag der letzten publizierten Erfolgsrechnung vorangegangenen Einjahresperioden. Wurde beispielsweise die letzte publizierte Erfolgsrechnung per Stichtag 30. Juni 2008 erstellt, so entsprechen die zu berücksichtigenden drei Jahre den Perioden 1. Juli 2005 bis 30. 4

[1] In den revidierten Mindeststandards des Basler Ausschusses für Bankenaufsicht („*International Convergence of Capital Measurement and Capital Standards – A Revised Framework / Comprehensive Version*") vom Juni 2006 wird der Ertragsindikator als „*Gross Income*" bezeichnet.

Juni 2006, 1. Juli 2006 bis 30. Juni 2007 und 1. Juli 2007 bis 30. Juni 2008.

Damit ergeben sich die Eigenmittelanforderungen K_{BIA} als 5

$$K_{BIA} = \alpha \cdot \sum_{j=1}^{3} \frac{\max[0, GI_j]}{\max[1, n]}$$

wobei

- α einheitlich als 15% festgelegt ist; 6
- GI_j dem Ertragsindikator für das jeweils relevante Jahr j entspricht; und 7
- n für die Anzahl jener der drei vorangegangenen Jahre steht, in denen jeweils ein positiver Ertragsindikator GI registriert wurde. 8

Der Ertragsindikator GI berechnet sich als Summe aus den folgenden Positionen der Erfolgsrechnung gemäss Rz 103 ff. FINMA-RS 08/2 „Rechnungslegung Banken“: 9

- Erfolg aus dem Zinsengeschäft (Rz 105–109 FINMA-RS 08/2 „Rechnungslegung Banken“); 10
- Erfolg aus dem Kommissions- und Dienstleistungsgeschäft[2] (Rz 110–116 FINMA-RS 08/2 „Rechnungslegung Banken“); 11
- Erfolg aus dem Handelsgeschäft (Rz 117 FINMA-RS 08/2 „Rechnungslegung Banken“); 12
- Beteiligungsertrag (Rz 119 f. FINMA-RS 08/2 „Rechnungslegung Banken“) aus nicht zu konsolidierenden Beteiligungen; und 13
- Liegenschaftenerfolg (Rz 121 f. FINMA-RS 08/2 „Rechnungslegung Banken“). 14

Die Grundlage zur Bestimmung des Ertragsindikators GI auf konsolidierter Ebene entspricht dem Konsolidierungskreis für die Bestimmung der Eigenmittelanforderungen. 15

Erweitern sich die Struktur oder die Aktivitäten einer Bank (z.B. infolge Übernahme einer neuen Geschäftseinheit) sind die historischen Werte des Ertragsindikators GI entsprechend nach oben anzupassen. Reduktionen des Ertragsindikators GI (z.B. nach der Veräusserung eines Geschäftsbereichs) erfordern eine Bewilligung der FINMA. 16

Zur Bestimmung des Ertragsindikators GI nach Art. 91 Abs. 1 ERV können Banken anstelle 17

[2] Die Berücksichtigung des Kommissionsaufwandes nach Rz 114 FINMA-RS 08/2 „Rechnungslegung Banken“ unterliegt den Restriktionen von Rz 18.

der schweizerischen Rechnungslegungsvorschriften international anerkannte Rechnungslegungsstandards verwenden, sofern die FINMA dafür die Bewilligung erteilt (vgl. Art. 91 Abs. 4 ERV).

Sämtliche Erträge aus Auslagerungsvereinbarungen (Outsourcing), bei denen die Bank selbst als Dienstleisterin auftritt, sind als Bestandteile des Ertragsindikators GI zu berücksichtigen (vgl. Art. 91 Abs. 2 ERV). 18

Tritt die Bank als Auftraggeberin einer ausgelagerten Dienstleistung auf, dürfen entsprechende Aufwendungen vom Ertragsindikator GI nur dann abgezogen werden, wenn die Auslagerung innerhalb derselben Finanzgruppe erfolgt und konsolidiert erfasst wird (vgl. Art. 91 Abs. 3 ERV). 19

~~Banken, die den Basisindikatoransatz verwenden, müssen die qualitativen Grundanforderungen gemäss Anhang 1 erfüllen, falls~~Aufgehoben 20*

- ~~ihre Eigenmittelanforderungen K_{BIA} innerhalb der vorangegangenen drei Jahre den Betrag von 100 Mio. CHF mindestens einmal übertroffen haben; oder~~Aufgehoben 21*

- ~~sie im Ausland durch Zweigniederlassungen oder nach den Eigenmittelvorschriften zu konsolidierende Gruppengesellschaften vertreten sind, die aggregiert mehr als 5% zu den gesamten erforderlichen Eigenmittel für operationelle Risiken beitragen.~~Aufgehoben 22*

B. Der Standardansatz (SA, Art. 93 ERV)

a) Mechanismus

Zur Bestimmung der Eigenmittelanforderungen haben Banken ihre gesamten Tätigkeiten den folgenden Geschäftsfeldern zuzuordnen: 23

i	Geschäftsfeld	β_i
1	Unternehmensfinanzierung/-beratung	18%
2	Handel	18%
3	Privatkundengeschäft	12%
4	Firmenkundengeschäft	15%
5	Zahlungsverkehr/Wertschriftenabwicklung	18%
6	Depot- und Treuhandgeschäfte	15%
7	Institutionelle Vermögensverwaltung	12%
8	Wertschriftenprovisionsgeschäft	12%

Tabelle 1

Für jedes Geschäftsfeld i und für jedes der drei vorangegangenen Jahre nach Rz 4 ist ein Ertragsindikator nach Rz 9–18 zu ermitteln und mit dem jeweiligen Faktor β_i gemäss Tabelle 1 zu multiplizieren. Die resultierenden Zahlenwerte sind für jedes Jahr zu addieren, wobei negative Zahlenwerte aus einzelnen Geschäftsfeldern mit positiven Zahlenwerten anderer Geschäftsfelder verrechnet werden können. Die Eigenmittelanforderungen entsprechen dem Betrag des Dreijahresdurchschnitts, wobei für die Durchschnittsbildung allfällige negative Sum- 24

manden gleich null gesetzt werden müssen (vgl. Art. 93 Abs. 1 ERV).

Die Eigenmittelanforderungen im Standardansatz K_{SA} ergeben sich als 25

$$K_{SA} = \frac{1}{3} \cdot \sum_{j=1}^{3} \max\left[0, \sum_{i=1}^{8} GI_{i,j} \cdot \beta_i\right]$$

Dabei entspricht

- GIi,j dem Ertragsindikator GI für das i-te Geschäftsfeld im jeweils relevanten Jahr j; und 26
- βi einem als fixer Prozentsatz für das i-te Geschäftsfeld vorgegebenen, für alle Banken identischen, Multiplikator. 27

b) Allgemeine Anforderungen (Art. 93 Abs. 3 ERV)

~~Sämtliche Banken, die den Standardansatz verwenden, müssen die qualitativen Grundanforderungen gemäss Anhang 1 erfüllen.~~Aufgehoben 28*

Jede Bank muss nach Massgabe von Anhang ~~2~~ 1 spezifische Grundsätze zur Allokation von Geschäftsaktivitäten in die standardisierten Geschäftsfelder nach Rz 23 festlegen und dafür über dokumentierte Kriterien verfügen. Die Kriterien sind regelmässig zu überprüfen und müssen den jeweils aktuellen Veränderungen der Aktivitäten der Bank angepasst werden. 29*

c) ~~Zusätzliche Anforderungen für im Ausland tätige Banken~~Aufgehoben

~~Eine Bank, die im Ausland über Zweigniederlassungen oder nach den Eigenmittelvorschriften zu konsolidierende Gruppengesellschaften verfügt, muss zusätzlich die Anforderungen nach Rz 31–44 erfüllen.~~Aufgehoben 30*

~~Die Bank muss über eine für das Management operationeller Risiken zuständige Stelle verfügen, welche dafür verantwortlich ist, dass~~Aufgehoben 31*

- ~~Strategien zur Identifikation, Beurteilung, Überwachung, Kontrolle und Verminderung operationeller Risiken entwickelt werden;~~Aufgehoben 32*
- ~~für die gesamte Bank geltende Grundsätze und Verfahren für das Management und die Kontrolle der operationellen Risiken etabliert werden;~~Aufgehoben 33*
- ~~eine Methodik zur Beurteilung der operationellen Risiken entwickelt und implementiert wird; und~~Aufgehoben 34*
- ~~ein Meldesystem für operationelle Risiken entwickelt und implementiert~~ 35*

wird.Aufgehoben

~~Als Teil des institutsinternen Systems zur Beurteilung operationeller Risiken muss die Bank systematisch die für ihr Geschäft relevanten Daten aus dem Bereich der operationellen Risiken sammeln, einschliesslich bedeutender Verluste aus den einzelnen Geschäftsfeldern.~~Aufgehoben 36*

~~Das Beurteilungssystem muss eng in die Risikomanagementprozesse der Bank integriert sein.~~Aufgehoben 37*

~~Die daraus gewonnenen Erkenntnisse müssen integraler Bestandteil der Prozesse zur Überwachung und Kontrolle des institutsspezifischen operationellen Risikoprofils sein. Beispielsweise müssen diese Informationen in der Berichterstattung an das Management und in der Risikoanalyse eine prominente Rolle spielen.~~Aufgehoben 38*

~~Die Bank muss über Anreizsysteme verfügen, welche zur Verbesserung des Managements operationeller Risiken beitragen können.~~Aufgehoben 39*

~~Die Leiter der einzelnen Geschäftsfelder, die Geschäftsleitung sowie das Organ für die Oberleitung, Aufsicht und Kontrolle sind regelmässig über die operationelle Risikoexposition sowie über bedeutende operationelle Verlustereignisse zu orientieren. Die Bank muss über Verfahren verfügen, um auf entsprechende Informationen adäquat reagieren zu können.~~Aufgehoben 40*

~~Das System für das Management operationeller Risiken in der Bank muss gut dokumentiert sein.~~Aufgehoben 41*

~~Die Bank muss über Verfahren verfügen, um die Einhaltung dokumentierter interner Grundsätze, Kontrollen und Verfahren betreffend das Managementsystem für operationelle Risiken sicherzustellen. Dazu gehören auch Grundsätze zum Umgang mit entsprechenden internen Verstössen.~~Aufgehoben 42*

~~Die Prozesse für das Management operationeller Risiken in der Bank und das entsprechende Beurteilungssystem müssen Gegenstand regelmässiger unabhängiger Validierung und Überprüfung sein. Diese Prüfungen müssen sowohl die Aktivitäten der einzelnen Geschäftsfelder als auch der Funktion für das Management operationeller Risiken abdecken.~~Aufgehoben 43*

~~Das System zur Beurteilung operationeller Risiken in der Bank (inklusive interner Validierungsprozesse) muss Gegenstand regelmässiger Überprüfungen durch die Prüfgesellschaft sein.~~Aufgehoben 44*

C. Institutsspezifische Ansätze (AMA, Art. 94 ERV)

a) Bewilligung

Institutsspezifische Ansätze („Advanced Measurement Approaches“, AMA) erlauben es den Banken, ihre Eigenmittelanforderungen für operationelle Risiken unter Einhaltung bestimmter Anforderungen nach einem individuellen Verfahren selbst zu quantifizieren. 45

Die Anwendung eines institutsspezifischen Ansatzes erfordert eine Bewilligung durch die FINMA. 46

Die FINMA kann von Banken vor einer Bewilligung für die Anwendung eines institutsspezifischen Ansatzes verlangen, dass über eine Zeitperiode von maximal zwei Jahren Berechnungen gestützt auf den entsprechenden Ansatz zu Test- und Vergleichszwecken durchgeführt werden müssen. 47

Verwendet eine Bank einen institutsspezifischen Ansatz, so kann ein allfälliger vollständiger oder partieller Wechsel zum Basisindikator- oder zum Standardansatz nur auf Anordnung oder mit Bewilligung der FINMA erfolgen. 48

Der Aufwand der FINMA im Zusammenhang mit dem Bewilligungsverfahren sowie mit notwendigen Prüfarbeiten nach Erteilung der Bewilligung wird den betreffenden Banken in Rechnung gestellt. 49

b) Zusätzliche Qqualitative Anforderungen

Banken, die einen institutsspezifischen Ansatz verwenden, müssen die qualitativen Grundanforderungen gemäss ~~Anhang 1~~Kapitel IV.B erfüllen. 50*

Die Verwendung eines institutsspezifischen Ansatzes zur Bestimmung der Eigenmittelanforderungen für operationelle Risiken setzt zusätzlich die Erfüllung folgender weiterer qualitativer Anforderungen voraus. 51

Das Organ für die Oberleitung, Aufsicht und Kontrolle muss aktiv in die Überwachung des Ansatzes involviert sein. 52

Die ~~Geschäftsleitung~~ Geschäftsführung muss mit dem Grundkonzept des Ansatzes vertraut sein und ihre entsprechenden Überwachungsfunktionen wahrnehmen können. 53*

Die Bank verfügt in Bezug auf ihr Management der operationellen Risiken über ein konzeptionell solides, zuverlässiges und integer implementiertes System. 54

Auf allen Ebenen der Bank stehen ausreichende Ressourcen für das Management, die Kontrolle und die interne Revision im Zusammenhang mit dem institutsspezifischen Ansatz zur Verfügung. 55

Die Bank muss über eine unabhängige zentrale Einheit für das Management der operationellen Risiken verfügen, die für die Ausarbeitung und Implementierung von Grundsätzen des operationellen Risikomanagements verantwortlich ist. Diese Einheit ist zuständig für: 56

- die Erstellung bankweiter Grundsätze und Verfahren für das Management und die Kontrolle operationeller Risiken; 57
- die Ausarbeitung und Anwendung der institutsspezifischen Quantifizierungsmethodik für operationelle Risiken; 58

- die Ausarbeitung und die Umsetzung eines Meldesystems für operationelle Risiken; und 59

- die Entwicklung von Strategien zur Identifikation, Messung, Überwachung sowie der Kontrolle bzw. Verminderung operationeller Risiken. 60

Das institutsspezifische Quantifizierungssystem muss eng in die täglichen Risikomanagementprozesse der Bank integriert sein. 61

Die Ergebnisse des institutsspezifischen Quantifizierungssystems sollen einen integralen Bestandteil der Risikoprofilüberwachung und -kontrolle darstellen. Beispielsweise müssen diese Informationen eine prominente Rolle in der Berichterstattung an das Management, bei der internen Eigenmittelallokation und bei der Risikoanalyse spielen. 62

Die Bank muss über Methoden zur Allokation von Eigenmitteln für operationelle Risiken auf die bedeutenden Geschäftsfelder und zur Schaffung von Anreizen zur Verbesserung des operationellen Risikomanagements in der gesamten Bank verfügen. 63

~~Zur Sicherstellung der institutsinternen Information und der Dokumentation sind die Anforderungen nach Rz 40–42 zu erfüllen:~~Aufgehoben 64*

Die interne Revision und die Prüfgesellschaft müssen die Prozesse für das Management operationeller Risiken und die Umsetzung des institutsspezifischen Ansatzes regelmässig überprüfen. Diese Prüfungen sollen sowohl die Aktivitäten der einzelnen Geschäftseinheiten als auch jene der zentralen Einheit für das Management operationeller Risiken umfassen. 65

Die Validierung des Quantifizierungssystems durch die Prüfgesellschaft muss insbesondere Folgendes beinhalten: 66

- Verifikation eines zufrieden stellenden Funktionierens der bankinternen Validierungsprozesse; und 67

- Sicherstellung der Transparenz und Zugänglichkeit der Datenflüsse und Prozesse des institutsspezifischen Ansatzes. Insbesondere muss sichergestellt sein, dass die interne Revision, die Prüfgesellschaft und die FINMA auf die Spezifikationen und Parameter des Ansatzes zugreifen können. 68

c) Allgemeine quantitative Anforderungen

In Übereinstimmung mit den Basler Mindeststandards[3] spezifiziert die FINMA keinen bestimmten Ansatz, sondern lässt den Banken diesbezüglich grosse Freiräume. Dieses Rundschreiben beschränkt sich daher auf die Darstellung zentraler Anforderungen, welche zur Anwendung eines solchen Ansatzes zwingend vorausgesetzt werden. Die Prüfung der detaillierten Spezifikationen eines institutsspezifischen Ansatzes ist Gegenstand des individuellen Be- 69

[3] Vgl. Fussnote 1.

willigungsprozesses. Dieser findet unter Leitung der FINMA und unter Einbezug der Prüfgesellschaft statt.

Unabhängig von der konkreten Ausgestaltung ihres Ansatzes muss eine Bank nachweisen können, dass dieser auch quantitativ bedeutungsvolle, mit kleiner Wahrscheinlichkeit auftretende Verlustereignisse berücksichtigt. Die aus dem Ansatz resultierende Eigenmittelanforderung soll etwa dem 99.9%-Quantil der Verteilungsfunktion der jeweils über ein Jahr aggregierten operationellen Verluste entsprechen. 70

Jeder institutsspezifische Ansatz muss von einem Begriff des operationellen Risikos ausgehen, der mit dem Begriff gemäss Art. 89 ERV sowie Rz 2 kompatibel ist. Er muss zusätzlich eine Kategorisierung von Verlustereignissen gemäss Anhang ~~3~~ 2 ermöglichen. 71*

Erforderliche Eigenmittel werden sowohl für die erwarteten als auch für die unerwarteten Verluste erhoben. Die FINMA kann jedoch einer Bank diesbezüglich Erleichterungen gewähren, wenn diese für zukünftige erwartete Verluste angemessene Rückstellungen gebildet hat. 72

Sämtliche expliziten und impliziten Annahmen betreffend Abhängigkeiten zwischen operationellen Verlustereignissen sowie zwischen verwendeten Schätzfunktionen müssen plausibel sein und begründet werden können. 73

Jeder Ansatz muss über bestimmte Grundeigenschaften verfügen. Dazu gehört insbesondere die Erfüllung der Anforderung zur Integration von: 74

- internen Verlustdaten (Rz 76–85);
- relevanten externen Verlustdaten (Rz 86–88);
- Szenarioanalyseverfahren (Rz 89–91); und
- Faktoren des Geschäftsumfelds und des internen Kontrollsystems (Rz 92–97).

Eine Bank benötigt ein zuverlässiges, transparentes, gut dokumentiertes und verifizierbares Konzept für den Einbezug und die Bestimmung der relativen Bedeutung all dieser vier Input-Faktoren in ihren Ansatz. Der Ansatz muss intern konsistent sein und insbesondere die mehrfache Berücksichtigung risikomindernder Elemente (z.B. Faktoren des Geschäftsumfelds und des internen Kontrollsystems oder Versicherungskontrakte) vermeiden. 75

d) Interne Verlustdaten (Art. 94 Abs. 2 ERV)

Eine Bank muss über dokumentierte Verfahren zur Beurteilung der fortlaufenden Relevanz historischer Verlustdaten verfügen. Dazu gehören insbesondere klare interne Regeln, wie die Berücksichtigung von Verlustdaten verändert werden kann (z.B. vollständige Nichtberücksichtigung auf Grund fehlender aktueller Relevanz, Skalierung auf Grund von veränderten Grössenverhältnissen oder Adjustierung in irgendeiner anderen Form). Dabei ist auch zu definieren, wer zu solchen Veränderungen bis zu welcher Dimension autorisiert ist. 76

Eine Bank muss eine Datenbank mit internen Verlustdaten verwenden. Diese muss bei der erstmaligen Verwendung des Ansatzes zu regulatorischen Zwecken einen Beobachtungszeit- 77

raum von mindestens drei Jahren umfassen. Spätestens zwei Jahre nach erstmaliger Verwendung des Ansatzes muss sich der Beobachtungszeitraum dauerhaft über mindestens fünf Jahre erstrecken.

Der Prozess zur Schaffung einer bankinternen Datenbank für operationelle Verluste muss die folgenden Anforderungen erfüllen: 78

- Zur Unterstützung der regulatorischen Validierung muss eine Bank sämtliche erfassten internen Verlustdaten den Geschäftsfeldern gemäss Rz 23 und den Ereignistypen gemäss Anhang ~~3~~ 2 zuordnen können. Sie muss über dokumentierte und objektive Kriterien für diese Kategorisierung verfügen. 79*

- Die internen Verlustdaten einer Bank müssen gestützt auf einen integeren und soliden Prozess umfassend gesammelt werden. Sie müssen alle materiellen Aktivitäten und Expositionen, inklusive aller relevanten Subsysteme und geographischen Lokalitäten abdecken. Bei der Verlustdatensammlung darf auf die systematische Erfassung von Verlusten unter einem bestimmten durch die FINMA festgelegten Brutto-Mindestbetrag verzichtet werden. 80

- Zu jedem Verlustereignis hat eine Bank die folgenden Informationen zu sammeln: Brutto-Verlustbetrag, Datum des Verlustereignisses und allfällige Verlustminderungen (z.B. auf Grund von Versicherungskontrakten). Für Verlustereignisse mit einem Brutto-Verlustbetrag von mindestens 1 Mio. CHF sind zudem Erläuterungen zu den Ursachen des Verlustes festzuhalten. 81

- Eine Bank muss Grundsätze für die Erfassung von Verlustereignissen definieren. Dazu gehören auch Kriterien für die Kategorisierung von Verlustereignissen aus zentralen Funktionen (zum Beispiel der EDV-Abteilung) oder von Verlustereignissen, die mehr als ein Geschäftsfeld betreffen. Im Weiteren muss geregelt sein, wie mit Serien von untereinander nicht unabhängigen Verlustereignissen umzugehen ist. 82

Verluste auf Grund operationeller Risiken, die im Kontext mit Kreditrisiken entstanden sind, und von einer Bank historisch als Kreditrisiko erfasst wurden, dürfen für die Bestimmung der erforderlichen Eigenmittel weiterhin ausschliesslich als Kreditrisikoereignis betrachtet werden. Sie müssen jedoch ab einem bestimmten durch die FINMA festgelegten Brutto-Mindestverlustbetrag trotzdem in die interne Verlustdatenbank für operationelle Risiken aufgenommen und für das Management operationeller Risiken berücksichtigt werden. Solche Verlustereignisse sind analog den übrigen internen Verlustdaten zu erfassen, jedoch als in Bezug auf operationelle Risiken nicht eigenmittelrelevant zu kennzeichnen. 83

Äussert sich ein Verlust auf Grund eines operationellen Risikos auch in Form eines Marktrisikoverlustes, so ist das entsprechende Ereignis ebenfalls analog den übrigen Verlustereignissen zu erfassen und in den institutsspezifischen Ansatz zu integrieren. Verwendet eine Bank zur Bestimmung ihrer erforderlichen Eigenmittel für Marktrisiken ein Risikoaggregationsmodell gemäss Rz 228–365 des FINMA-RS 08/20 „Marktrisiken Banken“, so dürfen durch Ereignisse infolge operationeller Risiken entstandene Positionen weder aus der Berechnung des Value-at-Risk, des Stress-basierten Value-at-Risk, der Incremental Risk Charge, der Comprehensive 84*

Risk Measure noch aus dem Backtesting ausgeschlossen werden.

Allfällige *„negative Verluste“* (z.B. Gewinne auf Grund einer irrtümlich erworbenen Aktienposition) dürfen im institutsspezifischen Ansatz keine die erforderlichen Eigenmittel reduzierende Wirkung entfalten. 85

e) Externe Verlustdaten (Art. 94 Abs. 2 ERV)

Banken müssen in ihren institutsspezifischen Ansatz relevante externe Verlustdaten einfliessen lassen. Dadurch soll die Berücksichtigung seltener aber potenziell schwerwiegender Verlustereignisse sichergestellt werden. Als Quelle der relevanten Informationen können sowohl öffentlich verfügbare als auch zwischen bestimmten Banken ausgetauschte externe Verlustdaten dienen. 86

Für diese externe Verlustdaten sind die effektive Verlusthöhe, Informationen zum Umfang der Aktivitäten im durch den Verlust betroffenen Geschäftsbereich, Informationen über die Ursachen und Umstände des Verlustes sowie Informationen zur Beurteilung der Relevanz des Verlustereignisses für die eigene Bank zu berücksichtigen. 87

Banken müssen die Verwendung externer Verlustdaten durch einen systematischen Prozess festlegen und dokumentieren. Dazu gehört insbesondere eine klare Methodik betreffend die Integration dieser Daten in den institutsspezifischen Ansatz (z.B. Skalierung, qualitative Anpassungen oder Einfluss auf die Szenarioanalyse). Die Rahmenbedingungen und die Verfahren zur Verwendung externer Verlustdaten sind regelmässig zu überprüfen, sowohl intern als auch durch die Prüfgesellschaft. 88

f) Szenarioanalyse (Art. 94 Abs. 2 ERV)

Institutsspezifische Ansätze müssen die Ergebnisse von Szenarioanalyseverfahren berücksichtigen. 89

Für Szenarioanalysen ist auf der Grundlage von Expertenmeinungen und externen Daten die Bedrohung der Bank durch potenziell schwerwiegende Verlustereignisse zu beurteilen. 90

Die für die Szenarioanalyse verwendeten Szenarien und die ihnen zugeordneten Parameter sind bei wesentlichen Veränderungen der Risikolage, mindestens aber jährlich, auf ihre Aktualität und Relevanz hin zu überprüfen und allenfalls anzupassen. Bei wesentlichen Veränderungen der Risikolage sind Anpassungen unmittelbar vorzunehmen. 91

g) Geschäftsumfeld und internes Kontrollsystem (Art. 94 Abs. 2 ERV)

Als vorausschauendes Element muss eine Bank prädiktive Faktoren aus dem Umfeld ihrer Geschäftsaktivitäten und aus ihrem internen Kontrollsystem im institutsspezifischen Ansatz berücksichtigen. Diese dienen dem Ziel, aktuellen Charakteristiken im Risikoprofil der Bank (z.B. neue Aktivitäten, neue Informatiklösungen, veränderte Prozessabläufe) oder Veränderungen in ihrem Umfeld (z.B. sicherheitspolitische Lage, veränderte Gerichtspraxis, Bedrohung durch Computerviren) spezifisch Rechnung tragen zu können. 92

Um im Rahmen eines institutsspezifischen Ansatzes verwendet werden zu dürfen, müssen für die Faktoren des Geschäftsumfelds und des internen Kontrollsystems die folgenden Anforderungen erfüllt sein: 93

- Jeder Faktor muss gemäss Erfahrungen und der Beurteilung aus dem betroffenen Geschäftsbereich ein relevanter Risikotreiber sein. Idealerweise sollte der Faktor quantifizier- und verifizierbar sein. 94

- Die Sensitivität der Risikoschätzungen einer Bank in Bezug auf Veränderungen der Faktoren und ihrer relativen Bedeutung muss begründet werden können und nachvollziehbar sein. Neben möglichen Veränderungen des Risikoprofils durch Verbesserungen der Kontrollumgebung muss das Konzept insbesondere auch potenzielle Erhöhungen der Risiken durch wachsende Komplexität oder durch Wachstum der Geschäftsaktivitäten erfassen. 95

- Das Konzept an sich sowie die Auswahl und Anwendung der einzelnen Faktoren, inklusive der Grundprinzipen zu Anpassungen der empirischen Schätzungen, müssen dokumentiert sein. Die Dokumentation soll auch innerhalb der Bank Gegenstand unabhängiger Überprüfung sein. 96

- Die Prozesse, deren Ergebnisse und vorgenommene Anpassungen sind in regelmässigen Zeitabständen mit den effektiven internen und externen Verlusterfahrungen zu vergleichen. 97

h) Risikoverminderung durch Versicherungen

Bei Verwendung eines institutsspezifischen Ansatzes dürfen Banken die Risiko vermindernde Wirkung von Versicherungskontrakten bei der Bestimmung ihrer Eigenmittelanforderungen für operationelle Risiken berücksichtigen. Die Anerkennung solcher Absicherungswirkungen ist jedoch auf eine Reduktion von maximal 20% der mittels eines institutsspezifischen Ansatzes berechneten Eigenmittelanforderungen beschränkt. 98

Die Möglichkeiten zur Reduktion der Eigenmittelanforderungen ist an die Erfüllung der folgenden Bedingungen geknüpft: 99

- Der Versicherungsgeber verfügt über ein langfristiges Kreditrating der Ratingklasse 3 oder besser. Das Kreditrating muss von einer durch die FINMA anerkannten Ratingagentur stammen. 100

- Der Versicherungskontrakt muss über eine Ursprungslaufzeit von mindestens einem Jahr verfügen. Sinkt seine Restlaufzeit auf unter ein Jahr, ist die Anerkennung seiner Absicherungswirkung linear von 100% (bei mindestens 365 Tagen Restlaufzeit) auf 0% (bei 90 Tagen Restlaufzeit) zu reduzieren. Absicherungswirkungen aus Versicherungskontrakten mit einer Restlaufzeit von 90 Tagen oder weniger werden für die Bestimmung der Eigenmittelanforderungen nicht anerkannt. 101

- Der Versicherungskontrakt verfügt über eine Kündigungsfrist von mindestens 90 Tagen. 102

Die Anerkennung der Absicherungswirkung nimmt bei Kündigungsfristen von unter einem Jahr linear ab; von 100% (bei einer Kündigungsfrist von mindestens 365 Tagen) bis zu 0% (bei einer Kündigungsfrist von 90 Tagen). Die Sätze sind auf die allenfalls bereits durch Rz 101 reduzierten Absicherungswirkungen anzuwenden.

- Der Versicherungskontrakt darf keine Ausschlussklauseln oder Einschränkungen für den Fall einer regulatorischen Intervention oder einer Zahlungsunfähigkeit der betreffenden Bank beinhalten, welche die Bank, ihren allfälligen Käufer, den Sanierungsbeauftragten oder den Liquidator von Versicherungsleistungen ausschliessen könnten. Zulässig wären entsprechende Ausschlussklauseln oder Einschränkungen jedoch, falls sie sich ausschliesslich auf Ereignisse nach Eröffnung des Konkursverfahrens oder nach der Liquidation beschränken. 103

- Die Berechnung der Absicherungswirkung aus Versicherungskontrakten muss transparent sein. Sie muss konsistent sein mit der im institutsspezifischen Ansatz verwendeten Wahrscheinlichkeit und der Grösse eines potenziellen Verlustereignisses. 104

- Der Versicherungsgeber muss eine externe Partei sein und darf nicht zur gleichen Gruppe wie die Bank gehören. Sollte er dies tun, so sind die Absicherungswirkungen aus den Versicherungskontrakten nur dann anerkennungsfähig, wenn der Versicherungsgeber die Risiken seinerseits an eine unabhängige dritte Partei (z.B. eine Rückversicherungsgesellschaft) weitergibt. Für eine Anerkennung der Absicherungswirkung muss diese unabhängige dritte Partei ihrerseits sämtliche entsprechenden Anforderungen an einen Versicherungsgeber erfüllen. 105

- Das bankinterne Konzept zur Berücksichtigung von Versicherungslösungen muss sich am effektiven Risikotransfer orientieren. Es muss gut dokumentiert sein. 106

- Die Bank hat Informationen zur Verwendung von Versicherungslösungen mit dem Ziel einer Verminderung operationeller Risiken zu publizieren. 107

D. Partielle Anwendung von Ansätzen

Es ist grundsätzlich zulässig, die Anwendung eines institutsspezifischen Ansatzes auf einzelne Aktivitätsbereiche zu beschränken und die übrigen entweder durch den Basisindikator- oder den Standardansatz abzudecken. Voraussetzung dazu ist die Erfüllung der folgenden Bedingungen: 108

- Sämtliche operationellen Risiken einer Bank werden durch einen in diesem Rundschreiben aufgeführten Ansatz erfasst. Dabei sind die jeweiligen Anforderungen für diese Ansätze in den entsprechenden Aktivitätsbereichen zu erfüllen. 109

- Zum Zeitpunkt der Anwendung eines institutsspezifischen Ansatzes hat dieser einen wesentlichen Teil der operationellen Risiken der Bank zu erfassen. 110

- Die Bank muss über einen Zeitplan verfügen, aus dem sich der zeitliche Ablauf der Ausdehnung des institutsspezifischen Ansatzes auf all ihre materiellen rechtlichen Ein- 111

heiten und Geschäftsfelder ergibt.

- Es ist nicht zulässig, den Basisindikator- oder den Standardansatz in einzelnen materiellen Aktivitätsbereichen aus Gründen der Minimierung von Eigenmittelanforderungen beizubehalten. 112

Die Abgrenzung zwischen dem institutsspezifischen Ansatz und dem Basisindikator- bzw. dem Standardansatz kann sich an Geschäftsfeldern, rechtlichen Strukturen, geographischen Abgrenzungen oder anderen intern klar definierten Abgrenzungskriterien orientieren. 113

Abgesehen von den in Rz 108–113 genannten Fällen ist es nicht zulässig, die Eigenmittelanforderungen für operationelle Risiken in einer Bank unter Verwendung unterschiedlicher Ansätze zu bestimmen. 114

E. Anpassungen der Eigenmittelanforderungen (Art. 45 Abs. 3 ERV)

Im Rahmen ihrer Überwachungsfunktionen betreffend zusätzliche Eigenmittel (Art. 45 ERV) kann die FINMA die Eigenmittelanforderungen für einzelne Banken individuell erhöhen. Solche individuellen Erhöhungen der Eigenmittelanforderungen drängen sich insbesondere dann auf, wenn eine ausschliesslich auf den Basisindikator- oder den Standardansatz gestützte Bestimmung der Eigenmittelanforderungen auf Grund tiefer Ertragsindikatoren GI zu unangemessen geringen Eigenmittelanforderungen führen würde. 115

F. Mindesteigenmittel und Untergrenze (Floor)

In Anwendung der vom Basler Ausschuss publizierten Fortführung des „Floor-Regimes“ gilt:[4] Für Banken, die operationelle Risiken nach dem AMA unterlegen, dürfen auf Gesamtbankstufe die Mindesteigenmittelanforderungen, unter zusätzlicher Berücksichtigung von Abzügen von den anrechenbaren Eigenmitteln, nicht tiefer als 80% jener Anforderungen und Abzüge betragen, welche die Bank theoretisch unter dem Mindeststandard von Basel I gehabt hätte.[5] In Anwendung von Art. 47 ERV regelt die FINMA im institutsspezifischen Einzelfall, wie eine angemessene approximative Berechnung der theoretischen Basel-I-Anforderungen vorgenommen werden kann. 116*

IV. Qualitative Anforderungen

A. Proportionalitätsprinzip

Die Anforderungen des vierten Kapitels dieses Rundschreibens sind abhängig von der Grösse der Bank umzusetzen. Rz 119 listet die entsprechenden Randziffern auf, von welchen kleine 117*

[4] Vgl. Pressemitteilung des Basler Ausschusses vom 13. Juli 2009: http://www.bis.org/press/p090713.htm

[5] Dies entspräche der Berechnung der Eigenmittelanforderungen nach der bis 31.12.2006 gültigen Bankenverordnung vom 17. Mai 1972 (AS 1995 253, 1998 16).

Banken in deren Umsetzung ausgenommen sind.

Kleine Banken im Sinne der Rz 117 sind: 118*

- Banken der FINMA-Kategorie[6] 5
- Effektenhändler der FINMA-Kategorie 4 und 5
- sowie in Einzelfällen Banken der FINMA-Kategorie 4, welche über Geschäftsaktivitäten ohne bedeutende Komplexität verfügen.

B. Qualitative Grundanforderungen

Kleine Banken gemäss Rz 117 und 118 sind von der Erfüllung von Rz 124, 125, 127 Bst. c bis Bst. i, 128, 130, 131 und 132 ausgenommen. 119*

Die qualitativen Grundanforderungen basieren auf den „Principles for the Sound Management of Operational Risk" des Basel Committee on Banking Supervision (Juni 2011).

a) Grundsatz 1: Verantwortlichkeiten

Das Organ für die Oberleitung, Aufsicht und Kontrolle (nachfolgend „Verwaltungsrat") hat ein Rahmenkonzept für das Management von operationellen Risiken, insbesondere Festlegung von Risikobereitschaft und Risikotoleranz, zu genehmigen und regelmässig zu überprüfen. Dabei sind Art, Typ und Ebene der operationellen Risiken festzuhalten, welchen die Bank ausgesetzt ist und welche sie einzugehen bereit ist. 120*

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. 121*

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. 122*

Die Geschäftsführung ist dafür verantwortlich, dass das Rahmenkonzept bezogen auf alle neuen und wesentlichen bestehenden Produkte, Aktivitäten, Prozesse und Systeme unternehmensweit konsistent angewendet und unterhalten wird. 123*

b) Grundsatz 2: Rahmenkonzept und Kontrollsystem

Das Rahmenkonzept ist in den vom Verwaltungsrat genehmigten internen Vorschriften umfas- 124*

[6] Vgl. den Anhang im FINMA-RS 11/2 „Eigenmittelpuffer und Kapitalplanung Banken".

send und angemessen festzuhalten und hat unternehmensspezifische Präzisierungen in Anlehnung an die aufsichtsrechtlichen Definitionen des operationellen Risikos und des operationellen Verlusts[7] zu enthalten.

Das Rahmenkonzept hat mindestens folgende Aspekte abzudecken: 125*

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;[8]

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.

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. 126*

c) Grundsatz 3: Identifizierung, Begrenzung und Überwachung

Die Identifizierung, Begrenzung und Überwachung von Risiken bilden die Grundlage eines wirksamen Risikomanagementsystems. Eine wirksame Risikoidentifikation berücksichtigt sowohl interne[9] als auch externe[10] Faktoren. Beispiele von Instrumenten und Methoden, die zur Identifikation und Beurteilung der operationellen Risiken eingesetzt werden können, sind: 127*

---

[7] Als operationelle Verluste werden Verluste bezeichnet, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen oder Systemen oder in Folge von externen Ereignissen eintreten. Eingeschlossen sind Rechtsrisiken, nicht aber strategische Risiken und Reputationsrisiken (Art. 89 ERV).

[8] Besteht keine einheitliche Klassifizierung der operationellen Risiken, kann dies die Wahrscheinlichkeit erhöhen, dass Risiken nicht identifiziert und kategorisiert werden oder keine Verantwortlichkeiten für die Beurteilung, Überwachung, Kontrolle und Minderung der Risiken zugeordnet wird.

[9] Beispielsweise Unternehmensstruktur, Art der Aktivitäten, Qualifikationen der Mitarbeiter, organisatorische Veränderungen und Personalfluktuation einer Bank.

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[11].

Die Bank muss sicherstellen, dass die Mechanismen bezüglich interner Preisfestsetzung (Pricing) und Performance-Messung den operationellen Risiken angemessen Rechnung tragen. 128*

d) Grundsatz 4: Interne und Externe Berichterstattung

Die Geschäftsführung hat einen Prozess zur laufenden Überwachung des operationellen Risikoprofils und der wesentlichen Verlustrisiken zu implementieren. Auf Ebene des Verwaltungsrates, der Geschäftsführung und der Geschäftsbereiche müssen geeignete Berichterstattungsmechanismen bestehen, die ein proaktives Management der operationellen Risiken unterstützen. 129*

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: 130*

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.

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 131*

[10] Beispielsweise Veränderungen des weiteren Umfelds und der Branche sowie technologische Fortschritte.

[11] Bei einer vergleichenden Analyse werden die Resultate der verschiedenen Beurteilungsinstrumente verglichen, um sich ein umfassenderes Bild der operationellen Risiken der Bank zu verschaffen.

anzuwenden sind. Zudem ist ein Prozess zu implementieren, der die Angemessenheit bezüglich Inhalt und Frequenz der Offenlegungen sicherstellt und deren regelmässige Überprüfung regelt.

Von den Banken extern offen zu legende Informationen müssen es den Anspruchsgruppen erlauben, sich ein Urteil über den Ansatz zum Management von operationellen Risiken zu bilden. Hierzu gehört u.a. das Konzept für das Management operationeller Risiken. Dieses soll den Anspruchsgruppen eine Beurteilung der Wirksamkeit der Identifikation, Begrenzung und Überwachung der operationellen Risiken ermöglichen. 132*

e) Grundsatz 5: Technologieinfrastruktur

Zur Unterstützung des Management operationeller Risiken hat die Geschäftsführung insbesondere für eine angemessene Technologieinfrastruktur[12] zu sorgen, die den aktuellen und längerfristigen Geschäftsbedürfnissen Rechnung trägt. Zu diesem Zweck hat sie ausreichende Kapazitäten bereitzustellen, die sowohl den üblichen Geschäftsbetrieb als auch Stressphasen abdecken. Überdies hat sie die Sicherheit, Integrität und Verfügbarkeit der Daten und Systeme zu gewährleisten sowie ein integriertes und umfassendes Risikomanagement zu implementieren. 133*

f) Grundsatz 6: Kontinuität bei Geschäftsunterbrechung

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.[13] 134*

C. Risikospezifische Qualitative Anforderungen

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 ädaquate Überwachung solcher Risiken sicherzustellen. 135*

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. 136*

---

[12] Technologieinfrastruktur bezeichnet den physischen und logischen (elektronischen) Aufbau von IT- und Kommunikationssystemen, die einzelnen Hard- und Softwarekomponenten, die Daten und die Betriebsumgebung.

[13] Ziffer 5.4.1 Business Impact Analyse und Ziffer 5.4.2 Business Continuity Strategie der SBVg-Empfehlungen für das Business Continuity Management (BCM) vom 14. November 2007 sind gemäss FINMA-Rundschreiben 2008/10 „Selbstregulierung als Mindeststandard“ als Mindeststandard anerkannt.

V. Prüfung und Beurteilung durch die Prüfgesellschaften

Die Prüfgesellschaften prüfen die Einhaltung dieses Rundschreibens nach Massgabe des FINMA-RS 13/3 „Prüfwesen“ und halten das Ergebnis ihrer Prüfungshandlungen im Prüfbericht fest. 137*

~~Anhang 1~~

~~Qualitative Grundanforderungen~~

~~Die nachstehenden Anforderungen gelten spätestens ab dem 1. Januar 2008 für alle Banken mit Ausnahme jener, die den Basisindikatoransatz verwenden und keines der beiden in Rz 21 und 22 festgehaltenen Kriterien erfüllen. Sie entsprechen der konkretisierten schweizerischen Umsetzung des durch den Basler Ausschuss für Bankenaufsicht im Februar 2003 publizierten Dokuments „Sound Practices for the Management and Supervision of Operational Risk".~~ 1

1. ~~Das Organ für die Oberleitung, Aufsicht und Kontrolle muss sich der wesentlichen operationellen Risiken seiner Bank bewusst sein. Es muss – direkt oder über einen Ausschuss – schriftliche Grundsätze für den Umgang mit operationellen Risiken bewilligen und diese periodisch überprüfen. Gegenstand dieser Grundsätze sind die Identifikation, Beurteilung, Überwachung und Kontrolle operationeller Risiken sowie Massnahmen zur Reduktion der operationellen Risikoexposition.~~ 2

2. ~~Das Organ für die Oberleitung, Aufsicht und Kontrolle stellt sicher, dass die Grundsätze für den Umgang mit operationellen Risiken durch die interne Revision überprüft werden. Die Funktionen für das Management operationeller Risiken dürfen nicht direkt durch die interne Revision wahrgenommen werden.~~ 3

3. ~~Die Verantwortung zur Umsetzung der Grundsätze für den Umgang mit operationellen Risiken in der Bank obliegt der Geschäftsleitung. Diese hat auf eine konsistente Umsetzung der Grundsätze in der ganzen Organisationsstruktur zu achten und sicherzustellen, dass sich alle Mitarbeiter ihrer Verantwortung im Umgang mit operationellen Risiken bewusst sind. Die Geschäftsleitung ist ferner verantwortlich für die Ausarbeitung von Massnahmen zum Management operationeller Risiken aus allen Aktivitäten der Bank.~~ 4

4. ~~Banken müssen die operationellen Risiken aus all ihren Aktivitäten, Produkten, Prozessen und Systemen identifizieren und beurteilen können. Vor einer Veränderung der Struktur von Aktivitäten, Produkten, Prozessen und Systemen sind diese mit Blick auf ihre operationellen Risiken adäquat zu beurteilen.~~ 5

5. ~~Banken müssen ihr operationelles Risikoprofil und ihre materiellen operationellen Risiken systematisch überwachen. Die Geschäftsleitung und das Organ für die Oberleitung, Aufsicht und Kontrolle sind über die entsprechenden Resultate auf dem Laufenden zu halten, um daraus allenfalls proaktiv Massnahmen ableiten zu können.~~ 6

6. ~~Banken müssen über Konzepte und konkrete Massnahmen zur Überwachung und/oder Verminderung materieller operationeller Risiken verfügen. Diese müssen auf die jeweils aktuelle Situation der Bank abgestimmt sein.~~ 7

7. ~~Banken müssen über Notfalllösungen verfügen, die ihnen auch unter aussergewöhnlichen Umständen die Weiterführung ihrer Aktivitäten ermöglichen und damit die Folgen schwerwiegender Beeinträchtigungen der normalen Geschäftstätigkeit begrenzen könnten.~~ 8

Anhang ~~21~~ 21*

finma

Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV

I. Übersicht

1

1. Ebene	2. Ebene	Aktivitäten
Unternehmens-finanzierung/-beratung	Unternehmensfinanzierung/-beratung	Fusionen und Übernahmen, Emissions- und Platzierungsgeschäfte, Privatisierungen, Verbriefungen, Research, Kredite (öffentliche Haushalte, High-Yield), Beteiligungen, Syndizierungen, Börsengänge (Initial Public Offerings), Privatplatzierungen im Sekundärhandel
	Öffentliche Haushalte	
	Handelsfinanzierungen	
	Beratungsdienstleistungen	
Handel	Kundenhandel	Anleihen, Aktien, Devisengeschäfte, Rohstoffgeschäfte, Kredite, Derivate, Funding, Eigenhandel, Wertpapierleihe und Repos, Brokerage (für Nicht-Retail-Investoren), Prime Brokerage
	Market Making	
	Eigenhandel	
	Treasury	
Privatkundengeschäft	Retail Banking	Anlage- und Kreditgeschäft, Serviceleistungen, Treuhandgeschäfte und Anlageberatung
	Private Banking	Anlage- und Kreditgeschäft, Serviceleistungen, Treuhandgeschäfte, Anlageberatung und andere Private-Banking-Dienstleistungen
	Karten-Dienstleistungen	Karten für Firmen und Privatpersonen
Firmenkundengeschäft	Firmenkundengeschäft	Projektfinanzierung, Immobilienfinanzierung, Exportfinanzierung, Handelsfinanzierung, Factoring, Leasing, Kreditgewährungen, Garantien und Bürgschaften, Wechselgeschäft
Zahlungsverkehr/Wertschriftenabwicklung[14]	Externe Kunden	Zahlungsverkehr, Clearing und Wertpapierabwicklung für Drittparteien
Depot- und Treuhandgeschäfte	Custody	Treuhandverwahrung, Depotgeschäft, Custody, Wertpapierleihe für Kunden; ähnliche Dienstleistungen für Firmen
	Treuhandgeschäft	Emissions- und Zahlstellenfunktionen
	Unternehmensstiftungen	
Institutionelle Vermögensverwaltung	Freie Vermögensverwaltung	Im Pool, segmentiert, Retail-bezogen, institutionell, geschlossen, offen, Private Equity
	Gebundene Vermögensverwaltung	Im Pool, segmentiert, Retail-bezogen, individuell, privat, institutionell, geschlossen, offen
Wertpapierprovisionsgeschäft	Ausführung von Wertschriftenaufträgen	Ausführung, inkl. sämtlicher damit verbundenen Dienstleistungen

[14] Verluste aus dem Bereich Zahlungsverkehr und Wertpapierabwicklung, die eigene Aktivitäten eines Institutes betreffen, sind jeweils dem entsprechenden Geschäftsfeld zuzuordnen.

Anhang ~~2~~1*

finma

Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV

II. Grundsätze für die Allokation

1.	Sämtliche Aktivitäten einer Bank müssen vollständig einem der acht Geschäftsfelder (1. Ebene in Tabelle 2) zugeordnet werden. Die Zuordnung darf nicht zu Überschneidungen führen.	2
2.	Auch jene Tätigkeiten, die nicht direkt mit dem eigentlichen Geschäft einer Bank zusammenhängen, sondern unterstützenden Charakter haben, sind einem Geschäftsfeld zuzuordnen. Falls die Unterstützung ein Geschäftsfeld betrifft, erfolgt auch die Zuordnung zu diesem Geschäftsfeld. Sind mehrere Geschäftsfelder durch eine unterstützende Aktivität betroffen, hat die Zuordnung gestützt auf objektive Kriterien zu erfolgen.	3
3.	Kann eine Aktivität nicht auf Grund objektiver Kriterien in ein bestimmtes Geschäftsfeld kategorisiert werden, so ist sie innerhalb der relevanten Geschäftsfelder jenem mit dem höchsten β-Faktor zuzuordnen. Dies gilt auch für die Aktivitäten mit Unterstützungscharakter.	4
4.	Banken dürfen für die Allokation ihres Ertragsindikators GI interne Verrechnungsmethoden anwenden. In jedem Fall muss jedoch die Summe der Ertragsindikatoren aus den acht Geschäftsfeldern dem Ertragsindikator für die gesamte Bank – wie er im Basisindikatoransatz verwendet wird – entsprechen.	5
5.	Die Kategorisierung von Aktivitäten in die verschiedenen Geschäftsfelder für die Bestimmung der Eigenmittelanforderungen für operationelle Risiken muss grundsätzlich mit den für Kredit- und Marktrisiken verwendeten Abgrenzungskriterien kompatibel sein. Allfällige Abweichungen von diesem Prinzip sind klar zu begründen und müssen dokumentiert sein.	6
6.	Der gesamte Kategorisierungsprozess muss klar dokumentiert sein. Insbesondere haben die schriftlichen Definitionen der Geschäftsfelder ausreichend klar und detailliert genug sein, um auch von nicht mit der Bank vertrauten Personen nachvollzogen werden zu können. Wo Ausnahmen von den Grundsätzen der Kategorisierung möglich sind, müssen auch diese klar begründet und dokumentiert sein.	7
7.	Die Bank muss über Verfahren verfügen, die ihr die Kategorisierung neuer Aktivitäten oder Produkte ermöglichen.	8
8.	Die Geschäftsführung~~leitung~~ ist für die Grundsätze der Kategorisierung verantwortlich. Diese sind durch das Organ für die Oberleitung, Aufsicht und Kontrolle der Bank zu genehmigen.	9*
9.	Die Verfahren der Kategorisierung sind regelmässig durch die Prüfgesellschaft zu überprüfen.	10

Anhang ~~32~~*

Übersicht zur Klassifikation von Ereignistypen

Verlustereignis-kategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
Interner Betrug	Verluste auf Grund von Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum, Umgehung von Gesetzen, Vorschriften oder internen Bestimmungen (unter Beteiligung mindestens einer interner Partei)	Unautorisierte Aktivität	Nicht rapportierte Transaktionen (vorsätzlich) Unautorisierte Transaktionen (mit finanziellem Schaden) Falscherfassung von Positionen (vorsätzlich)
		Diebstahl und Betrug	Betrug, Kreditbetrug, wertlose Einlagen Diebstahl, Erpressung, Veruntreuung, Raub Veruntreuung von Vermögenswerten Böswillige Vernichtung von Vermögenswerten Fälschungen Scheckbetrug Schmuggel Unbefugter Zugriff auf fremde Konten Steuerdelikte Bestechung Insidergeschäfte (nicht auf Rechnung des Arbeitgebers)
Externer Betrug	Verluste auf Grund von Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum oder der Umgehung von Gesetzen bzw. Vorschriften (ohne Beteiligung einer internen Partei)	Diebstahl und Betrug	Diebstahl, Raub Fälschungen Scheckbetrug
		Informatiksicherheit	Schäden durch Hacker-Aktivitäten Unbefugter Zugriff auf Informationen (mit finanziellem Schaden)
Arbeitsplatz	Verluste auf Grund von Widerhandlungen gegen arbeitsrechtliche, sicherheits- oder gesundheitsbezogene Vorschriften oder Vereinbarungen; inkl. aller Zahlungen im Zusammenhang mit solchen Widerhandlungen	Mitarbeiter	Kompensations- und Abfindungszahlungen, Verluste im Zusammenhang mit Streiks etc.
		Sicherheit am Arbeitsplatz	Allgemeine Haftpflicht Verstoss gegen sicherheits- oder gesundheitsbezogene Bestimmungen Entschädigungs- oder Schadenersatzzahlungen an Mitarbeiter

Anhang ~~32~~ 32*

Übersicht zur Klassifikation von Ereignistypen

Verlustereignis-kategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
		Diskriminierung	Schadenersatzzahlungen auf Grund von Diskriminierungsklagen
Kunden, Produkte und Geschäftspraktiken	Verluste auf Grund unbeabsichtigter oder fahrlässiger Nichterfüllung von Verpflichtungen gegenüber Kunden sowie Verluste auf Grund der Art oder Struktur bestimmter Produkte	Angemessenheit, Offenlegung und Treuhandpflichten	Verstoss gegen Treuhandpflichten, Verletzung von Richtlinien Probleme bezüglich Angemessenheit und Offenlegung (Know-your-Customer-Regeln etc.) Verletzung von Informationspflichten gegenüber Kunden Verletzung des Bankkundengeheimnisses bzw. von Datenschutzbestimmungen Aggressive Verkaufspraktiken Inadäquate Generierung von Kommissions- und Courtagenzahlungen Missbrauch vertraulicher Informationen Haftung des Kreditgebers
		Unzulässige Geschäfts- oder Marktpraktiken	Verstoss gegen kartellrechtliche Bestimmungen Unlautere Marktpraktiken Marktmanipulationen Insidergeschäfte (auf Rechnung des Arbeitgebers) Geschäftstätigkeiten ohne entsprechende Bewilligung Geldwäscherei
		Probleme mit Produkten	Produktprobleme (Befugnismängel etc.) Modellfehler
		Kundenselektion, Geschäftsvergabe und Kreditexposition	Nicht mit internen Richtlinien kompatibles Vorgehen bei Kundenprüfungen Überschreitung von Limiten
		Beratungstätigkeiten	Streitigkeiten in Bezug auf Resultate von Beratungstätigkeiten

Anhang ~~32~~*

Übersicht zur Klassifikation von Ereignistypen

Verlustereignis-kategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
Sachschaden	Verluste auf Grund von Schäden an physischen Vermögenswerten infolge Naturkatastrophen oder anderer Ereignisse	Katastrophen oder andere Ereignisse	Naturkatastrophen Terrorismus Vandalismus
Geschäftsunterbrüche und Systemausfälle	Verluste auf Grund von Störungen der Geschäftstätigkeit oder Problemen mit technischen Systemen	Technische Systeme	Hardware Software Telekommunikation Stromausfälle etc.
Abwicklung, Vertrieb und Prozessmanagement	Verluste auf Grund von Fehlern bei der Geschäftsabwicklung oder beim Prozessmanagement; Verluste aus Beziehungen mit Geschäftspartnern, Lieferanten etc.	Erfassung, Abwicklung und Betreuung von Transaktionen	Kommunikationsfehler Fehler bei der Datenerfassung oder im Datenunterhalt Terminüberschreitung Nichterfüllung einer Aufgabe Fehler bei Modell- oder Systemanwendung Buchhaltungsfehler bzw. Zuordnung zur falschen Einheit Fehlerhafte bzw. nichterfolgte Lieferung Fehlerhafte Bewirtschaftung von Absicherungsinstrumenten Fehler im Umgang mit Referenzdaten Fehler bei übrigen Aufgaben
		Überwachung und Meldungen	Nichterfüllung von Meldepflichten Inadäquate Berichte an Externe (mit Verlustfolge)
		Kundenaufnahme und Kundendokumentation	Nichteinhaltung entsprechender interner und externer Vorgaben
		Kontoführung für Kunden	Gewährung eines nichtlegitimierten Kontozugriffs Unkorrekte Kontoführung mit Verlustfolge Verlust oder Beschädigung von Kundenvermögenswerten durch fahrlässige Handlungen

Anhang ~~3~~2*

Übersicht zur Klassifikation von Ereignistypen

Verlustereignis-kategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
		Geschäftspartner	Fehlerhafte Leistung von Geschäftspartnern (Nicht-kunden) Verschiedene Streitigkeiten mit Geschäftspartnern (Nichtkunden)
		Lieferanten und Anbieter	Outsourcing Streitigkeiten mit Lieferanten und Anbietern

Anhang 43*

Vergleich zwischen FINMA-RS und Basler MindeststandardsUmgang mit elektronischen Kundendaten

Rz im RS	§ im Basler Papier[15]	Inhalt mit allfälligem Kommentar zur schweizerischen Umsetzung
1	645	Allgemeiner Gegenstand und Zweck des Rundschreibens
2	644	Begriffsdefinition: operationelle Risiken (OpR)
–	646	Ermutigung zur Bewegung in Richtung komplexerer Ansätze: Fehlt im Rundschreiben.
–	647	Erwartung, dass gewisse Banken nicht den Basisindikatoransatz (BIA) anwenden: Fehlt im Rundschreiben. Erwähnung der Möglichkeit zur partiellen Verwendung.
3	649	Erläuterung der Eigenmittelanforderungen für BIA: verbal
4	–	Definition des Begriffs der vorangegangenen drei Jahre
5	649	Erläuterung der Eigenmittelanforderungen für BIA: Formel
6	649	Erläuterung zu Formel in Rz 5
7	649	Erläuterung zu Formel in Rz 5
8	649	Erläuterung zu Formel in Rz 5
9	650	Schweizerische GI Definition (Beschränkung der Berücksichtigung des Beteiligungsertrags auf nicht zu konsolidierende Beteiligungen)
10	650	GI-Bestandteile: Erfolg aus dem Zinsengeschäft
11	650	GI-Bestandteile: Erfolg aus dem Kommissions- und Dienstleistungsgeschäft
12	650	GI-Bestandteile: Erfolg aus dem Handelsgeschäft
13	650	GI-Bestandteile: Beteiligungsertrag aus nicht zu konsolidierenden Beteiligungen
14	650	Liegenschaftenerfolg
15	–	Erläuterungen zur Konsolidierung des Ertragsindikators GI
16	–	Erläuterungen zu Anpassungen des Ertragsindikators GI nach Änderungen der Struktur einer Bank infolge Ausbau oder Reduktion von Geschäftsaktivitäten (z.B. nach Übernahmen oder Verkäufen von Geschäftsbereichen)
17	–	Möglichkeit der Zulassung anderer Rechnungslegungsstandards als FINMA-RS 08/2 „Rechnungslegung Banken“
18	650	Behandlung von Outsourcing (inkl. Möglichkeit zum Abzug von Outsourcing-Aufwendungen, falls gemeinsame Konsolidierung mit Outsourcing-Dienstleister erfolgt)
20	651	Qualitative Grundanforderungen für BIA (gestützt auf „*Sound Practices for the Management and Supervision of Operational Risk*“): gemäss Rundschreiben nur für Banken ab gewisser Grösse sowie für im Ausland vertretene Banken.
21		Grössenkriterium zu Rz 20
22		Kriterium der Vertretung im Auslang gemäss Rz 20
23	652 und 654	Einteilung der 8 Geschäftsfelder und ihren jeweiligen β-Faktoren
24	654	Erläuterung der Eigenmittelanforderungen im SA: verbal
–	653	Verschiedene Erläuterungen zum Konzept des Standardansatzes (SA): Fehlen im Rundschreiben.
–	Fussnote 97	Alternativer Standardansatz: in der Schweiz nicht umgesetzt.
25	654	Erläuterung der Eigenmittelanforderungen im SA: Formel
26	654	Erläuterung zu Formel in Rz 25
27	654	Erläuterung zu Formel in Rz 25

[15] Vgl. Fussnote 1 im Haupttext.

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

~~Rz im RS~~	~~§ im Basler Papier[15]~~	~~Inhalt mit allfälligem Kommentar zur schweizerischen Umsetzung~~
~~28~~	~~651~~	~~Erfüllung der qualitativen Grundanforderungen (gestützt auf „*Sound Practices for the Management and Supervision of Operational Risk*“)~~
~~29~~	~~662~~	~~Allokation von Geschäftsaktivitäten im SA~~
~~30~~	~~663~~	~~Einleitung zu Anforderungen für im Ausland vertretene Banken im SA~~
~~31~~	~~663a~~	~~Managementsystem im OpR-Bereich~~
~~32~~	~~663a~~	~~Managementsystem im OpR-Bereich~~
~~33~~	~~663a~~	~~Managementsystem im OpR-Bereich~~
~~34~~	~~663a~~	~~Managementsystem im OpR-Bereich~~
~~35~~	~~663a~~	~~Managementsystem im OpR-Bereich~~
~~36~~	~~663b~~	~~System zur Beurteilung von OpR~~
~~37~~	~~663b~~	~~System zur Beurteilung von OpR~~
~~38~~	~~663b~~	~~System zur Beurteilung von OpR~~
~~39~~	~~663b~~	~~System zur Beurteilung von OpR~~
~~40~~	~~663c~~	~~Rapportierung an leitende Stellen~~
~~41~~	~~663d~~	~~Dokumentation~~
~~42~~	~~663d~~	~~Dokumentation~~
~~43~~	~~663e~~	~~Validierung und Überprüfung~~
~~44~~	~~663f~~	~~Externe Revision~~
~~45~~	~~655~~	~~Grundkonzept der institutsspezifischen Ansätze (AMAs)~~
~~46~~	~~655~~	~~Bewilligungspflicht für AMAs; früheste Umsetzung per Anfang 2008~~
~~47~~	~~659~~	~~Vorgängige AMA-Verwendung zu Vergleichs- und Testzwecken („*Parallel Run*“ und „*Impact Studies*“)~~
~~48~~	~~648~~	~~Restriktionen betreffend Wechsel vom AMA zu BIA oder SA~~
~~49~~	~~–~~	~~Kostenbelastung für AMA-Prüfungen~~
~~–~~	~~656~~	~~Anerkennung von Allokationsmechanismen: keine explizite Umsetzung in der Schweiz.~~
~~–~~	~~657~~	~~Anerkennung von Diversifikationseffekten bei ausländischen Banken mit AMA-Bewilligung im Herkunftsland: keine explizite Anerkennung in der Schweiz.~~
~~–~~	~~658~~	~~Überwachung der Adäquanz des verwendeten Allokationsmechanismus: Explizite Regelung erübrigt sich in der Schweiz.~~
~~ERV~~	~~659~~	~~Hinweis auf AMA-Verwendung im Gesamtkontext von Basel III mit entsprechenden Floors~~
~~–~~	~~660~~	~~Drei qualifizierende Anforderungen für SA: keine explizite Erwähnung im Rundschreiben. Abdeckung ist jedoch insbesondere durch Anforderungen aus „*Sound Practices for the Management and Supervision of Operational Risk*“ von Februar 2003 sichergestellt.~~
~~–~~	~~661~~	~~Testphase für SA: Schweizerische Umsetzung verzichtet darauf.~~
~~50~~	~~651~~	~~Erfüllung der qualitativen Grundanforderungen (gestützt auf „*Sound Practices for the Management and Supervision of Operational Risk*“, *Februar 2003*)~~
~~51~~	~~664~~	~~Einleitung zu den qualitativen AMA-Anforderungen~~
~~52~~	~~664, Pkt. 1~~	~~Aktive Involvierung des Organs für die Oberleitung, Aufsicht und Kontrolle in die Überwachung~~
~~53~~		~~Vertrautheit der Geschäftleitung mit Grundkonzept~~
~~54~~	~~664, Pkt. 2~~	~~Konzeptionell solides und integer implementiertes System~~
~~55~~	~~664, Pkt. 3~~	~~Ausreichende Ressourcen~~
~~–~~	~~665~~	~~Verschiedene einleitende Informationen~~

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

~~Rz im RS~~	~~§ im Basler Papier[15]~~	~~Inhalt mit allfälligem Kommentar zur schweizerischen Umsetzung~~
~~56~~	~~666a~~	~~Unabhängige zentrale Einheit für das OpR-Management~~
~~57~~	~~666a~~	~~Aufzählungspunkt zu Rz 56~~
~~58~~	~~666a~~	~~Aufzählungspunkt zu Rz 56~~
~~59~~	~~666a~~	~~Aufzählungspunkt zu Rz 56~~
~~60~~	~~666a~~	~~Aufzählungspunkt zu Rz 56~~
~~61~~	~~666b~~	~~Integration in den Risikomanagementprozess~~
~~62~~	~~666b~~	~~Integration in den Risikomanagementprozess~~
~~63~~	~~666b~~	~~Integration in den Risikomanagementprozess~~
~~64~~	~~666c und d~~	~~Verweis auf Rz 40–42~~
~~65~~	~~666e~~	~~Interne und externe Revision~~
~~66~~	~~666f~~	~~Validierung durch Aufsichtsbehörde und Prüfgesellschaft: in der Schweiz nur durch Prüfgesellschaft.~~
~~67~~	~~666f~~	~~Aufzählungspunkt zu Rz 66~~
~~68~~	~~666f~~	~~Aufzählungspunkt zu Rz 66~~
~~69~~	~~667~~	~~Einleitung zu quantitativen Vorgaben: Idee des liberalen Grundkonzepts~~
~~70~~	~~667~~	~~Hinweis auf 99.9%-Quantil~~
~~–~~	~~668~~	~~Hinweis auf Flexibilität und rigorose Standards sowie allfällige spätere Überarbeitung durch den Basler Ausschuss~~
~~71~~	~~669a~~	~~Kompatibilität der Definitionen~~
~~72~~	~~669b~~	~~Erwähnung der Möglichkeit für einen Abzug erwarteter Verluste~~
~~–~~	~~669c~~	~~Anforderung der *„ausreichenden Granularität“*: Verzicht auf explizite Erwähnung im Rundschreiben. Der Begriff ist problematisch und die Erfüllung der Idee ist durch die übrigen Anforderungen sichergestellt.~~
~~73~~	~~669d~~	~~Berücksichtigung von Korrelationsannahmen: pragmatische Umsetzung im Rundschreiben. Die Basler Formulierung ist wörtlich genommen nicht praktikabel.~~
~~74~~	~~669e~~	~~Berücksichtigung der vier Input-Faktoren~~
~~75~~	~~669f~~	~~Konzept zur Integration der vier Input-Faktoren~~
~~–~~	~~670~~	~~Einleitung zu Anforderungen für Sammlung interner Verlustdaten~~
~~76~~	~~671~~	~~Unterhalt der Verlustdatensammlung~~
~~77~~	~~672~~	~~Mindestlänge der verwendeten Beobachtungszeiträume~~
~~78~~	~~673~~	~~Einleitungen zu Anforderungen an Prozess zur Schaffung einer institutsinternen Datenbank~~
~~79~~	~~673, Pkt. 1~~	~~Kategorisierung in Geschäftsfelder und Ereignistypen~~
~~80~~	~~673, Pkt. 2~~	~~Sicherstellung einer umfassenden Datensammlung; Threshold~~
~~81~~	~~673, Pkt. 3~~	~~Informationen zu Verlustdaten: Erläuterungen zu den Ursachen des Verlustes sind gemäss Rundschreiben nur für Brutto-Verluste von mindestens 1 Mio. CHF erforderlich.~~
~~82~~	~~673, Pkt. 4~~	~~Grundsätze zur Erfassung von Verlustereignissen~~
~~83~~	~~673, Pkt. 5~~	~~OpR-Verluste mit Kreditrisikobezug~~
~~84~~	~~673, Pkt. 6~~	~~OpR-Verluste mit Marktrisikobezug; expliziter Hinweis auf Pflicht zur Berücksichtigung solcher Verluste in einem allfälligen Marktrisikomodell~~
~~85~~	~~–~~	~~Umgang mit negativen OpR-Verlusten: Expliziter Hinweis fehlt im Basler Text.~~
~~86~~	~~674~~	~~Zweck externer Verlustdaten~~
~~87~~	~~674~~	~~Informationen zu einzelnen externen Verlustdaten~~
~~88~~	~~674~~	~~Methodik zur Verwendung externer Verlustdaten~~

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

~~Rz im RS~~	~~§ im Basler Papier[15]~~	~~Inhalt mit allfälligem Kommentar zur schweizerischen Umsetzung~~
~~89~~	~~675~~	~~Pflicht zur Berücksichtigung der Szenarioanalyse~~
~~90~~	~~675~~	~~Grundidee der Szenarioanalyse~~
~~91~~	~~675~~	~~Regelmässige Überprüfung bzw. Aktualisierung der Szenarien: gemäss Rundschreiben mindestens jährlich bzw. unmittelbar bei wesentlichen Veränderungen der Risikolage.~~
~~92~~	~~676~~	~~Grundidee der Faktoren des Geschäftsumfelds und des internen Kontrollsystems~~
~~93~~	~~676~~	~~Einleitung zu den Anforderungen~~
~~94~~	~~676, Pkt. 1~~	~~Auswahl der Faktoren des Geschäftsumfelds und des internen Kontrollsystems~~
~~95~~	~~676, Pkt. 2~~	~~Begründbarkeit und Nachvollziehbarkeit der Sensitivität der Risikoschätzungen in Bezug auf Veränderungen der Faktoren des Geschäftsumfelds und des internen Kontrollsystems~~
~~96~~	~~676, Pkt. 3~~	~~Dokumentation~~
~~97~~	~~676, Pkt. 4~~	~~Validierung~~
~~98~~	~~677~~	~~Grundsätzliche Anerkennung der Absicherungswirkung von Versicherungskontrakten; Limitierung auf 20%~~
~~99~~	~~678~~	~~Einleitung zu den Bedingungen~~
~~100~~	~~678, Pkt. 1~~	~~Mindest-Rating des Versicherungsgebers~~
~~101~~	~~678, Pkt. 2; 679, Pkt. 1~~	~~Mindestursprungslaufzeit, Mindestrestlaufzeit und Präzisierung der entsprechenden „*appropriate haircuts*“: im Rundschreiben linear.~~
~~102~~	~~678, Pkt. 3; 679, Pkt. 2~~	~~Mindestkündigungsfrist von 90 Tagen und Handhabung der Haircuts bei Kündigungsfrist unter einem Jahr: im Rundschreiben linear.~~
~~103~~	~~678, Pkt. 4~~	~~Ausschlussklauseln und Einschränkungen für den Fall einer regulatorischen Intervention~~
~~104~~	~~678, Pkt. 5~~	~~Transparenz der Berechnung der Absicherungswirkung~~
~~105~~	~~678, Pkt. 6~~	~~Versicherung durch nichtexterne Parteien~~
~~106~~	~~678, Pkt. 7~~	~~Orientierung am effektiven Risikotransfer und Dokumentation~~
~~107~~	~~678, Pkt. 8~~	~~Publikationspflicht von Informationen zur Verwendung von Versicherungslösungen~~
~~–~~	~~679, Pkt. 3~~	~~Unsicherheit der Zahlung und allfällige nicht vorhandene Deckung: Verzicht auf explizite Erwähnung im Rundschreiben. Einhaltung ist durch übrige Anforderungen bereits sichergestellt.~~
~~108~~	~~680~~	~~Grundsätzliche Möglichkeit der partiellen AMA-Anwendung~~
~~109~~	~~680, Pkt. 1/2~~	~~Vollständige Abdeckung~~
~~110~~	~~680, Pkt. 3~~	~~Abdeckung zum Zeitpunkt der Implementation~~
~~111~~	~~680, Pkt. 4~~	~~Zeitplan zur Ausdehnung des AMA~~
~~112~~	~~680, Pkt. 4~~	~~BIA und SA dürfen nicht aus Gründen der Eigenmittel-Optimierung in einzelnen Bereichen beibehalten werden: Das Rundschreiben formuliert hier die Idee im letzten Satz von §680, Pkt. 4 explizit aus.~~
~~113~~	~~681~~	~~Abgrenzung zwischen den verschiedenen Ansätzen~~
~~114~~	~~–~~	~~Expliziter Hinweis auf Nichtzulässigkeit der Verwendung verschiedener Verfahren zur Bestimmung der OpR-Eigenmittelanforderungen~~
~~–~~	~~682~~	~~Spezialregelung für AMA bei ausländischer Tochter einer Bank, die konsolidiert auf Gruppenebene keinen AMA anwendet: keine Berücksichtigung im Rundschreiben.~~
~~–~~	~~683~~	~~Hinweis zu zurückhaltender Genehmigungspraxis für Fälle nach §682: in der schweizerischen Umsetzung irrelevant.~~

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

~~Rz im RS~~	~~§ im Basler Papier~~[15]	~~Inhalt mit allfälligem Kommentar zur schweizerischen Umsetzung~~
~~115~~	~~778; Fussnoten 98 u. 99~~	~~Eingriffe unter Pillar II~~
~~116~~	~~–~~	~~Datum des Inkrafttretens~~
~~Anhang 1~~	~~Separates Dokument~~	~~Qualitative Grundanforderungen: Entspricht der schweizerischen Umsetzung der Basler „*Sound Practices for the Management and Supervision of Operational Risk*“, Februar 2003.~~
~~Anhang 2A~~	~~Annex 6~~	~~Kategorisierung der Geschäftsfelder: Übersicht~~
~~Anhang 2B~~	~~Annex 6~~	~~Kategorisierung der Geschäftsfelder: Allokation~~
~~–~~	~~Fussnote 2, Annex 6~~	~~Ergänzende Hinweise zum Mapping auf Geschäftsfelder: Im Rundschreiben nicht explizit erwähnt.~~
~~Anhang 3~~	~~Annex 7~~	~~Übersicht zur Klassifikation von Ereignistypen~~

In diesem Anhang werden Grundsätze und die dazugehörigen Ausführungen für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten natürlicher Personen („Privatkunden“), deren Geschäftsbeziehungen in oder von der Schweiz aus betreut oder geführt werden („Kundendaten“), formuliert. Die Grundsätze sind hauptsächlich auf das Risiko von Vorfällen in Bezug auf die Vertraulichkeit von Kundenmassendaten durch Verwendung elektronischer Systeme zugeschnitten. Sie gehen nur am Rande auf Sicherheitsüberlegungen für physische Daten sowie auf Fragen der Integrität und Verfügbarkeit von Daten ein. Die einschlägigen rechtlichen Bestimmungen finden sich nicht nur im Aufsichtsrecht[16], sondern auch im Datenschutzrecht[17] und Zivilrecht. 1*

Kleine[18] Banken sind von der Erfüllung folgender Randziffern ausgenommen: 2*

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

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

A. Grundsatz 1: Governance

Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten werden systematisch identifiziert, begrenzt und überwacht. Dazu überwacht der Verwaltungsrat die Geschäftsführung zur Sicherstellung einer wirksamen Implementierung von Massnahmen zur Gewährleistung der Vertraulichkeit von Kundendaten. Die Geschäftsführung beauftragt eine unabhängige Kontrollfunkti- 3*

[16] Insb. Art. 3 und 47 BankG sowie Art. 9 BankV; Art. 10 und 43 BEHG sowie Art. 19 f. BEHV.
[17] Insb. 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).
[18] Vgl. Rz 118 des Kapitels IV.A.

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

on, die Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten zu schaffen und aufrechtzuerhalten.

a) Unabhängigkeit und Verantwortung

4*

Die für die Schaffung und Aufrechterhaltung der Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten zuständige Einheit muss unabhängig von jenen Einheiten sein, welche für die Verarbeitung der Daten zuständig sind. Sie kann Teil der Risikokontrollorganisation sein, oder einer gleichwertigen Einheit, die unabhängig ist von jenen Einheiten, welche für die Verarbeitung der Kundendaten zuständig sind. Je nach Grösse und Komplexität der Bank kann die zuständige Einheit auch durch mehrere dezentrale Einheiten unterstützt werden.

5*

Für alle beteiligten Funktionen und Standorte müssen die Verantwortlichkeiten geregelt sein und klare Eskalationsstrukturen geschaffen werden. Insbesondere die Festlegung der Verantwortlichkeiten und ihre Zuteilung an Front-Office-, IT- und Kontrollfunktionen sind von der Geschäftsführung zu definieren und vom Verwaltungsrat zu genehmigen. Die Geschäftsführung informiert den Verwaltungsrat regelmässig über die Wirksamkeit der eingeführten Kontrollen.

b) Vorgaben, Prozesse und Systeme

6*

Es wird erwartet, dass ein formales und umfassendes Rahmenkonzept von Aktivitäten, Prozessen und Systemen zur Datenvertraulichkeit besteht, dessen Struktur der Grösse und Komplexität der Bank Rechnung trägt. Dieses Rahmenkonzept muss in allen Funktionsbereichen und Einheiten, die auf Kundendaten zugreifen oder diese berarbeiten, konsistent umgesetzt werden.

7*

Die Implementierung und Einhaltung des Rahmenkonzepts zur Vertraulichkeit von Kundendaten ist durch den Verwaltungsrat zu überwachen und muss durch regelmässige Kontrollen der für Datensicherheit und -vertraulichkeit zuständigen Einheit sichergestellt werden.

B. Grundsatz 2: Kundenidentifikationsdaten (Client Identifying Data, CID)

8*

Grundlegende Anforderung für ein angemessenes Rahmenkonzept zur Sicherstellung der Vertraulichkeit von Kundendaten ist die Kategorisierung der Kundendaten, die eine Bank verarbeitet. Dies erfordert die unternehmensspezifische Festlegung von Kundenidentifikationsdaten (CID) und deren Klassifizierung bzgl. ihrer Vertraulichkeits- und Schutzstufe. Zudem muss die Zuordnung der Datenverantwortung („*Data Owners*“) geregelt sein.

a) Kundendatenkategorien und CID-Definition

9*

Eine klare und transparente Liste der Kundendatenkategorien, einschliesslich der unternehmensspezifischen Festlegung von CID, muss in der Bank vorliegen und formell dokumentiert werden. Die Kategorisierung und Definition von Kundendaten hat sämtliche direkten Kundenidentifikationsdaten (z.B. Vorname, zweiter Name, Nachname), indirekten Kundenidentifikationsdaten (z.B. Passnummer) und potenziell indirekten Kundenidentifikationsdaten (z.B. Kombinationen aus Geburtsdatum, Beruf, Staatsangehörigkeit usw.) zu umfassen.

10*

Jede Bank muss über eine Kategorisierung und unternehmensspezifische Festlegung von CID

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

verfügen, die ihrem spezifischen Kundenstamm angemessen ist. Kapitel III enthält eine nicht abschliessende Liste von Beispielen.

b) CID-Klassifizierung und Vertraulichkeitsstufen

11* CID müssen nach formalen Klassifizierungskriterien in Vertraulichkeitsstufen zugeordnet werden. Die Kundendatenklassifizierung hat zum Schutz der Vertraulichkeit klare Anforderungen für den Zugriff und entsprechende technische Massnahmen zu enthalten (z.B. Anonymisierung, Verschlüsselung oder Pseudonymisierung) und grundsätzlich zwischen verschiedenen Vertraulichkeits- und Schutzstufen zu unterscheiden.

12* Gemäss den Beispielen in Kapitel III ist davon auszugehen, dass zumindest die direkten CID (Kategorie A) und ausgewählte indirekte CID (z.B. Passnummer der Kategorie B) zu einer höheren[19] Kundendaten-Vertraulichkeits- und -Schutzstufe gehören. Falls eine Bank nur eine einzige Kategorie kennt, ist für sämtliche CID eine höhere Kundendaten-Vertraulichkeits- und -Schutzstufe anzuwenden.

c) CID-Verantwortung

13* Es müssen Kriterien für die Zuordnung der Datenverantwortung festgelegt werden, die gleichermassen für alle Einheiten gelten, die auf CID zugreifen oder diese verarbeiten. Die für CID verantwortlichen Einheiten (*„Data Owners“*) müssen die Überwachung des gesamten Lebenszyklus der Kundendaten abdecken, einschliesslich der Genehmigung der Zugriffsrechte sowie des Löschens und Entsorgens von allen Backup- und operationellen Systemen.

14* Die für CID verantwortlichen Einheiten (*„Data Owners“*) sind für die Implementierung der Datenklassifizierungsrichtlinien sowie die Rechtfertigung und Dokumentierung von Ausnahmen zuständig.

C. Grundsatz 3: Datenspeicherort und -zugriff

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.

a) Datenspeicherort und -zugriff allgemein

16* Ein Inventar der Applikationen und der damit verbundenen Infrastruktur (z.B. Datenbank, Ba-

[19] Die höhere Kundendaten-Vertraulichkeits- und -Schutzstufe muss nicht zwingend die höchste Vertraulichkeits- und -Schutzstufe sein, die ein Institut für Informationen kennt. Sie hat jedoch zu berücksichtigen, dass eine Verletzung der Vertraulichkeit von Kundendaten zu einer schweren Beeinträchtigung der wirtschaftlichen Situation oder gesellschaftlichen Stellung der Betroffenen führen kann.

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

ckups), die CID enthalten oder verarbeiten, muss verfügbar sein und laufend aktualisiert werden. Das Inventar muss auch Applikationen und CID berücksichtigen, die für Testzwecke (z.B. einer neuen IT-Plattform) verwendet werden.

Es wird erwartet, dass die Granularität des Inventars es der Bank erlaubt, zu ermitteln: 17*

- wo CID gespeichert sind, durch welche Anwendungen und IT-Systeme CID verarbeitet werden und wo elektronisch auf CID zugegriffen werden kann (Endbenutzeranwendungen); 18*
- von welchen nationalen und internationalen Standorten und Rechtseinheiten aus auf Daten zugegriffen werden kann (einschliesslich ausgelagerter Dienstleistungen und externer Firmen). 19*

b) Datenspeicherort und -zugriff im Ausland

Falls CID ausserhalb der Schweiz gespeichert werden oder vom Ausland aus auf sie zugegriffen wird (z.B. aufgrund einer Auslagerung spezifischer Aktivitäten innerhalb der Unternehmensgruppe oder an externe Dritte), sind die damit verbundenen erhöhten Risiken in Bezug auf den Kundendatenschutz angemessen zu begrenzen.[20] CID müssen angemessen geschützt (anonymisiert, verschlüsselt oder pseudonymisiert) werden. Es sind die folgenden Massnahmen zu ergreifen: 20*

- Schutzvorkehrungen, ihre Implementierung und Anwendung müssen sachgerecht erfolgen; 21*
- Die Anwendung von Schutzvorkehrungen ist durch die Festlegung von Schlüsselkontrollen, die regelmässig überprüft werden, zu überwachen; 22*
- Die Kunden sind detailliert mittels besonderem Schreiben über die Auslagerung spezifischer Aktivitäten innerhalb der Gruppe oder an externe Dritte, die im Ausland durchgeführt werden, zu informieren und auf die getroffenen Vorkehrungen zum Schutz der Vertraulichkeit hinzuweisen. Lassen die ausserhalb der Schweiz verfügbaren Daten keine Rückschlüsse auf die Identität der betroffenen Kunden zu, so entfällt diese Pflicht. In diesem Fall sind die allgemeinen Anforderungen zur Information über ausgelagerte Aktivitäten im Sinne der Grundsätze 5 und 6 des FINMA-RS 08/7 „Outsourcing Banken“ ausreichend. 23*

c) „Need to know“-Grundsatz

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: 24*

[20] Zudem sind die einschlägigen Bestimmungen des Datenschutzrechts einzuhalten, wie insb. Art. 6 DSG.

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

- Geltungsbereich: Der Zugriff auf CID muss auf Kundengruppen, Segmente, Buchungszentren oder andere geeignete Definitionen von Kundenuntergruppen beschränkt sein, auf die der jeweilige Mitarbeiter im Rahmen seiner Aufgabenerfüllung zwingend zugreifen muss. 25*

- 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). 26*

Die Erteilung von Zugriffsrechten muss regelmässig überprüft werden. 27*

d) Zugriffs-Verzeichnis

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. 28*

Vorkehrungen, wie z.B. das Führen von Log-Dateien, müssen eingeführt werden, um die Identifizierung von Benutzern, die auf Massen-CID zugegriffen haben, zu ermöglichen. 29*

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

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. 30*

a) Sicherheitsstandards

Die Sicherheitsstandards müssen in Bezug auf die Grösse der Bank und den Grad der Komplexität seiner IT-Architektur angemessen sein. Im Falle differenzierter Sicherheitsstandards (z.B. bei nicht identischen Sicherheitsstandards für alle Mitarbeitenden, Prozesse oder Instrumente), ist das Verhältnis zwischen den erhöhten Sicherheitsstandards und der Klassifikation der Kundendaten festzulegen und ausreichend zu dokumentieren. 31*

b) Sicherheitsstandards und Marktpraxis

Die Sicherheitsstandards bilden einen festen Bestandteil des Rahmenkonzept zur Sicherstellung der Vertraulichkeit von Kundendaten. Es wird erwartet, dass sie regelmässig mit der Marktpraxis verglichen werden, um potenzielle Sicherheitslücken zu ermitteln. Auch externe Inputs in Form 32*

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

von unabhängigen Überprüfungen und Prüfberichte müssen berücksichtigt werden.

c) Sicherheit bei Übertragung von CID und bei gespeicherten CID auf dem Endgerät (Endpoint)

Um die Vertraulichkeit von CID sicherzustellen, muss die Bank Schutzmassnahmen (z.B. Verschlüsselung) prüfen und diese soweit erforderlich auf den folgenden Ebenen umsetzen: 33*

a. Sicherheit von CID auf dem Endgerät bzw. am Endpoint (z.B. PCs, Notebooks, portable Datenspeicher und Mobilgeräte); 34*

b. Sicherheit bei Übertragung von CID (z.B. innerhalb eines Netzwerks oder zwischen verschiedenen Standorten); 35*

c. Sicherheit von gespeicherten CID (z.B. auf Servern, in Datenbanken oder auf Backup-Medien). 36*

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

Gut ausgebildete und verantwortungsbewusste Mitarbeitende sind für die Umsetzung erfolgreicher unternehmensweiter Massnahmen zum Schutz der Vertraulichkeit von Kundendaten zentral. Mitarbeitende, die auf CID zugreifen können, sind sorgfältig auszuwählen, zu schulen und zu überwachen. Dies gilt auch für Dritte, die im Auftrag der Bank auf CID zugreifen können. Erhöhte Sicherheitsanforderungen müssen für privilegierte IT-Benutzer und Anwender mit funktionalem Zugriff auf Massen-CID (*„Schlüsselmitarbeitenden“*) gelten. Ihnen ist besondere Aufmerksamkeit zu schenken. 37*

a) Sorgfältig Auswahl der Mitarbeitenden

Mitarbeitende, die auf CID zugreifen können, sind sorgfältig auszuwählen. Insbesondere ist vor der Aufnahme der Tätigkeit zu überprüfen, ob der potentielle Mitarbeiter die Anforderungen für einen angemessenen Umgang mit CID erfüllt. Die Bank hat ferner sicherzustellen, dass die Mitarbeiterauswahl durch Dritte, als auch die Bestimmung von Mitarbeitern von Drittunternehmen, welche im Auftrag der Bank auf CID zugreifen können, einer vergleichbaren, sorgfältigen Auswahlprozess durchlaufen 38*

b) Gezielte Schulungen der Mitarbeitenden

Interne und externe Mitarbeiter müssen im Rahmen gezielter Schulungen in Bezug auf die Kundendatensicherheit sensibilisiert sein. Dabei wird erwartet, dass Mitarbeitende ein Programm zur Sensibilisierung für die Vertraulichkeit von Kundendaten durchlaufen. Sie müssen den Rahmen der Kundendatensicherheit kennen und müssen insbesondere darüber informiert sein, dass die Weitergabe von Kundendaten nach Art. 47 BankG strafbar ist. 39*

c) Sicherheitsanforderungen

Die Bank muss über klare Sicherheitsanforderungen für Mitarbeiter, die auf CID zugreifen, ver- 40*

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

fügen. Es ist regelmässig zu überprüfen, ob die Anforderungen für einen angemessenen Umgang mit CID weiterhin erfüllt sind. Erhöhte Sicherheitsanforderungen müssen für privilegierte IT-Benutzer und Anwender mit funktionalem Zugriff auf Massen-CID („Schlüsselmitarbeitenden“) gelten. Ihnen ist besondere Aufmerksamkeit zu schenken.

d) Liste von Schlüsselmitarbeitenden

41*

Als Ergänzung zu den allgemeinen Anforderungen in Bezug auf Mitarbeitende mit Zugriff auf CID (siehe Rz 28) wird von der Bank die Führung und laufende Aktualisierung einer Liste mit den Namen aller internen und externen privilegierten IT-Benutzer und Anwender (Schlüsselmitarbeitenden) erwartet, die Zugriff auf Massen-CID haben und/oder denen Verantwortlichkeiten hinsichtlich der Kontrolle und Überwachung der Vertraulichkeit von Kundendaten übertragen wurden. Die Identität von privilegierten IT-Benutzern und Anwendern muss dem lokal oder gesamthaft verantwortlichen obersten Management bekannt sein.

e) Weisung

42*

Die Prozesse zur Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben, sind in einer Weisung festzuhalten

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

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[21] 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

a) Risikobeurteilungsprozess

44*

Die Beurteilung des mit der Vertraulichkeit von CID verbundenen inhärenten Risikos (des zugrunde liegenden Risikos bei fehlenden Kontroll- oder Minderungsmassnahmen) und Residualrisikos (unter Berücksichtigung von Kontroll- oder Minderungsmassnahmen) muss auf Basis eines strukturierten Prozesses und unter Einbezug der Geschäfts-, IT- und Kontrollfunktionen erfolgen. Dies kann im Rahmen eines weiter gefassten Prozesses zur Selbstbeurteilung der Risiken und Kontrollen geschehen, der zusätzliche operationelle Risiken berücksichtigt.

b) Risikoszenarien und Schlüsselkontrollen[22]

---

[21] Auf der Grundlage einer Analyse schwerwiegender Vorfälle in Bezug auf die Datensicherheit, die in der eigenen Bank oder bei der Konkurrenz eingetreten sind, oder einer Beschreibung rein hypothetischer schwerwiegender Vorfälle.

[22] Marktpraktiken zu Sicherheitsszenarien und damit verbundenen Schlüsselkontrollen sind umfassend durch die Schweizerische Bankiervereinigung unter dem Titel „Data Leakage Protection – Information

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

45*

Die Definition von Risikoszenarien und entsprechenden Schlüsselkontrollen in Bezug auf die Vertraulichkeit von CID muss der Risikoexposition sowie der Komplexität der Bank angemessen sein und regelmässig überarbeitet werden.

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

46*

Identifizierte Risiken müssen überwacht und angemessen minimiert werden. Dies gilt namentlich in Verbindung mit Aktivitäten, bei denen grosse Mengen von CID verändert oder migriert werden müssen.[23] Solchenfalls bedarf es angemessener und entsprechend erhöhter Sicherheitsmassnahmen, um das Risiko von Vorfällen in Bezug auf die Vertraulichkeit von CID zu mindern. Bei strukturellen Veränderungen (z.B. bedeutende Reorganisationen) muss sich die Bank frühzeitig und vertieft mit Sicherheitsmassnahmen der Vertraulichkeit von CID befassen.

a) Produktionsumfeld, Aktivitäten in Verbindung mit Massen-CID

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.

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

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.

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

49*

Von den Banken wird erwartet, dass sie vordefinierte Prozesse einführen, um rasch auf Vorfälle in Verbindung mit der Vertraulichkeit zu reagieren, einschliesslich einer klaren Strategie zur Kommunikation schwerwiegender Vorfälle. Zudem müssen Ausnahmen, Vorfälle und Prüfergebnisse überwacht, analysiert und in geeigneter Form dem obersten Management gemeldet werden. Dies muss zur laufenden Verfeinerung der Massnahmen zur Sicherstellung der Vertrau-

---

on Best Practice by the Working Group Information Security of the Swiss Bankers Association“ behandelt (verabschiedet im Oktober 2012).

[23] Dazu kommt es in der Regel bei der Weiterentwicklung, Veränderung oder Migration von Systemen infolge von Technologie-Upgrades oder organisatorischen Restrukturierungen.

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

lichkeit von CID beitragen.

a) Identifikation von Vorfällen in Bezug auf die Vertraulichkeit und Reaktion

50* Es muss ein klar definierter Prozess für die Identifikation von Vorfällen in Bezug auf die Vertraulichkeit sowie die Reaktion darauf formalisiert und allen involvierten Stellen kommuniziert werden. Zudem müssen alle relevanten Einheiten und Standorte, die auf CID zugreifen, über Ressourcen verfügen, um auf entsprechende Vorfälle reagieren zu können.

b) Meldung

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

c) Laufende Verfeinerung des Rahmens zur Sicherstellung der Vertraulichkeit von CID

52* Das Rahmenkonzept zur Sicherstellung der Vertraulichkeit von CID (Rz 6 und 7) und die Sicherheitsstandards (Rz 31) müssen regelmässig überprüft werden. Vorfälle, Ausnahmen und Prüfergebnisse müssen zur laufenden Verfeinerung dieses Rahmenkonzeptes beitragen.

d) Externe Kommunikation

53* Die Bank muss über eine klare Kommunikationsstrategie verfügen, wenn schwerwiegende Vorfälle in Bezug auf die Vertraulichkeit von CID auftreten. Darin sind insbesondere die Form und der Zeitpunkt der Kommunikation an die FINMA, Strafverfolgungsbehörden, die betroffenen Kunden und die Medien zu regeln.

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

54* Bei der Auswahl der Anbieter von Outsourcing-Dienstleistungen, welche CID bearbeiten, muss die CID-Vertraulichkeit ein ausschlaggebendes Kriterium sowie integraler Bestandteil der zugrunde liegenden Sorgfaltsprüfung (Due Diligence) sein. Gemäss dem FINMA-RS 08/7 „Outsourcing Banken“ trägt die Bank über den gesamten Lebenszyklus der ausgelagerten Dienstleistungen weiterhin die endgültige Verantwortung für die CID. Die folgenden Anforderungen gelten zwingend für alle Arten von Aktivitäten, die den Zugriff auf Massen-CID beinhalten, worunter sowohl Grossaufträge (z.B. Drittanbieter von IT-Services, Support für die Installation und den Unterhalt extern entwickelter IT-Plattformen, Hosting von Anwendungen) als auch Nicht-IT-Dienstleistungen (z.B. Outsourcing von Kundenveranstaltungen usw.) fallen.

a) Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID

55* Die Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID muss Teil des Prozesses für die Auswahl von Outsourcing-Dienstleistern und Anbietern von Grossaufträge sein. Es muss klare Kriterien für die Beurteilung der Sicherheits- und Vertraulichkeitsstandards solcher Dritter definiert werden. Die Prüfung in Bezug auf die CID-Sicherheits- und -Vertraulichkeitsstandards muss vor der Vertragsvereinbarung erfolgen und regelmässig wiederholt werden. Zudem muss

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

das oberste Management über relevante Änderungen der Vertraulichkeitsstandards und -lösungen, die intern und/oder von Dritten angewandt werden, orientiert werden.

56*

Es wird erwartet, dass die Due Diligence in Bezug auf die Sicherheit und Vertraulichkeit von CID durch unabhängige Informationen gestützt wird (z.B. aufgrund zertifizierter Standards oder anhand externer Wirtschaftsprüfungen). Die Bank muss sicherstellen, dass Dritte mit Zugriff auf CID über das nötige Know-how und die nötige Erfahrung im Bereich Datenschutz und -sicherheit verfügen sowie genügend Ressourcen bereitstellen, um die Sicherheits- und Vertraulichkeitsstandards während der gesamten Vertragslaufzeit (einschliesslich des Vertragsendes und der Übergangsphase) zu erfüllen.

b) Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID und Dienstleistungsvereinbarungen

57*

Dritte müssen über die internen Sicherheits- und Vertraulichkeitsstandards der Bank informiert werden und diese als Mindestanforderung erfüllen. In den Dienstleistungsvereinbarungen ist klar festzuhalten, wie Dritte eine allfällige Erweiterung der internen Sicherheits- und Vertraulichkeitsstandards des Intituts erfüllen werden.

c) Allgemeine Verantwortung

58*

Die Bank muss für jede ausgelagerte Aktivität, die Zugriff auf CID beinhaltet, einen oder mehrere interne(n) Mitarbeitende(n) bestimmen, der/die dafür verantwortlich ist/sind, dass die Sicherheits- und Vertraulichkeitsstandards in Bezug auf die Vertraulichkeit von CID eingehalten werden. Der/Die Mitarbeitende(n) ist/sind auch für die Schaffung eines Kommunikationssystems mit dem Outsourcing-Dienstleister verantwortlich, das es ihm/ihnen erlaubt, jegliche Vorfälle in Verbindung mit CID, die beim Dienstleister eintreten, zu melden, zu überwachen und zu dokumentieren. Die intern verantwortliche Person, muss im Einklang mit der allgemeinen Kommunikationsstrategie (siehe Rz 54 dieses Anhangs), in der Lage sein, die Umstände und Auswirkungen eines schwerwiegenden Vorfalls jederzeit wiederzugeben.

d) Ausgestaltung der Kontrollen und Wirksamkeitstests

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.

II. Glossar

60*

Kundenidentifikationsdaten (Client Identifying Data, CID): Kundendaten, die Personendaten nach Art. 3 Bst. a DSG darstellen und es ermöglichen, die betroffenen Kunden zu identifizieren.

61*

Grossaufträge: Alle durch Dritte erbrachten Dienstleistungen, die Zugriff auf Massen-CID erfor-

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

dern oder potenziell zum Zugriff auf Massen-CID führen (z.B. bei der Implementierung von Zugriffsrechtsprofilen durch Mitarbeitende eines Dritten). Ein CID-Risiko kann beispielsweise auftreten bei der Installation von Anwendungen oder der Implementierung von lokalen Einstellungen (z.B. Zugriffsrechten), der Datenspeicherung oder dem laufenden Systemunterhalt (z.B. Drittanbieter von IT-Services, extern entwickelte IT-Plattformen). Dies umfasst auch interne Prüfarbeiten und externe Prüfungen. Gewöhnlich sind solche Grossaufträge langfristiger Natur.

62*

Mitarbeitende Dritter: Alle Mitarbeitenden, die für Beauftragte der Bank arbeiten (z.B. Auftragnehmer, Berater, externe Prüfer, externe Unterstützung usw.), die Zugriff auf CID haben und nicht interne Mitarbeitern sind.

63*

Schlüsselmitarbeitende: Alle internen und externen im IT-Bereich sowie in weiteren Unternehmensbereichen tätigen Mitarbeitenden, die aufgrund ihres Tätigkeitsprofils und ihrer Aufgaben privilegierten Zugriff auf CID im grossen Umfang haben (z.B. Datenbankadministratoren, Mitglieder des obersten Managements).

64*

Schwerwiegender Vorfall in Bezug auf die Vertraulichkeit von Kundendaten / Leck von Kundenmassendaten: Ein Vorfall in Bezug auf die Vertraulichkeit von Kundendaten, der ein bedeutendes Leck von CID impliziert (im Vergleich zur Gesamtzahl der Konten/Gesamtgrösse des Kundenportfolios).

65*

Reversible Datenverarbeitungstechniken:

- Pseudonymisierte Daten (Pseudonymisierung): Unter Pseudonymisierung versteht man den Vorgang der Trennung der identifizierenden (z.B. Name, Foto, E-Mail Adresse, Telefonnummer) von anderen Daten (z.B. Kontostand, Kreditwürdigkeit). Das Bindeglied zwischen den beiden Datenbereichen bilden sogenannte Pseudonyme und eine Zuordnungsregel (Konkordanztabelle). Beispielsweise können Pseudonyme durch einen Zufallszahlengenerator erzeugt und mittels einer Konkordanztabelle den identifizierenden Personendaten bei Bedarf zugeordnet werden.
- Verschlüsselte Daten: In der Praxis wird die Pseudonymisierung auch mittels Verschlüsselungsverfahren umgesetzt. Das Pseudonym wird in diesem Fall durch Verschlüsselung von identifizierenden Personendaten mit einem kryptographischen Schlüssel erzeugt. Die Re-identifikation erfolgt aufgrund der Entschlüsselung mit Hilfe des geheimen Schlüssels.

66*

Irreversible Datenverarbeitungstechniken:

- Anonymisierte Daten: Bei der Anonymisierung von Personendaten werden sämtliche Elemente, die eine Identifizierung einer Person ermöglichen, unwiederbringlich entfernt oder verändert (z.B. durch Löschung oder Aggregierung), so dass die Daten nicht mehr mit einer bestimmten oder bestimmbaren Person verknüpft werden können. Solche Daten sind/enthalten gemäss Definition keine CID mehr und fallen nicht unter das DSG[24].

[24] Vgl. EDÖB, Anhang zu Mindestanforderungen DSMS, 5.

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

III. Beispiel zu Kundenidentifikationsdaten

67*

Die folgende Liste enthält anschauliche Beispiele für Kundendatenkategorien und -elemente, die für die Definition der Kundenidentifikationsdaten zu berücksichtigen sind. Die Liste ist nicht abschliessend.

A: Direkte Kundenidentifikationsdaten	B: Indirekte Kundenidentifikationsdaten	C: Potenziell indirekte Kundenidentifikationsdaten
Persönliche Identifikation: - Vorname - Nachname - Zweiter Name - Unterschrift - Mädchenname - Name Ehepartner(in)/Partner(in) - Name(n) Kind(er) **Unternehmensidentifikation:** - Name des Unternehmens - Börsensymbol **Physische Adressdaten:** - Privatadressen - Geschäftsadressen - Postadressen **Elektronische Adressdaten:** - Private Adressen (privat, geschäftlich) - Telefonnummern (privat, geschäftlich, Handy usw.) - Faxnummern (privat, geschäftlich) - Social-Network-IDs, einschliesslich biometrischer Daten wie Fotos - IP-Adressen - Geolokalisation	**Persönliche IDs/Nummern in öffentlichen Registern:** - Passnummer - Identitätskartennummer - Sozialversicherungsnummer - Nummer Militärausweis - Steuernummer - Autokennzeichen - Bloomberg-ID - Unternehmensregister - Grundbuch - Eigentum an Unternehmen/Trusts **Kundenidentifikatoren:** - Kundennummer - IBAN/BIC - Kontonummern - Schliessfachnummern - Schlüsselwort (Nummernkonten) - Vertragsnummern - Hypotheken - Benutzer-IDs und Passwörter (z.B. E-Banking-Anwendungen) - Portfolio-ID - Kartennummern - Freie Textfelder (die potenziell CID enthalten) - Elektronische Dokumente (die potenziell CID enthalten) - Bankdetails Kunde bei Dritten **Berufliche Eckdaten:** - Unternehmen - Funktionale Stellung	**Geburtsdaten:** - Geburtsdatum - Geburtsort - Staatsangehörigkeit bei der Geburt (Nationalitätscode) - Alter - Geschlecht **Familiendaten:** - Heiratsdatum **Persönliche Angaben:** - Sprache (Sprachcode) - Anrede/Titel (Frau, Herr, Dr. usw). - Andere Nationalitäten (Nationalitätscode) - Familienstand - Diplomatenkennzeichen - Hobbys - Mitgliedschaften (beruflich, wohltätige Organisationen, Vereinigungen) - Herkunft des Vermögens - Lebenszyklusdaten **Persönliche Wohnsitzangaben:** - Wohnsitzland/-länder (Ländercode) - Land/Länder des steuerlichen Wohnsitzes **Berufliches Profil:** - Berufliche Qualifikationen - Beruf, Funktion - Datum Unternehmensgründung/-liquidierung/Börsengänge **Unternehmensidentifikatoren:** - Bezeichnung der Management-

Anhang 43*

~~Vergleich zwischen FINMA-RS und Basler Mindeststandards~~Umgang mit elektronischen Kundendaten

		funktion in einer Publikumsgesellschaft, z.B. CRO - Hauptaktionär (J/N) **Nichtidentifizierende Angaben zum Unternehmen:** - Rechtsform des Unternehmens - Gründungsjahr - Branche (NOGA-Code) - Namen von Mitbewerbern **Identifikationsdaten Beziehung:** - Kundensegment - Name/Abkürzung des internen Kundenkontakts - Kontowährung - Niederlassung - Kundenperformance **Kundenbedürfnisse und Produktnutzung:** - Anlageverhalten/-typ - Lebenszyklusphase - Unternehmensstrategie - Produktdaten - Kreditrating - Transaktions-/Bewegungsdaten ohne CID - Portfoliopositionen - Kontostand

Verzeichnis der Änderungen

Das Rundschreiben wird wie folgt geändert:

Diese Änderungen wurden am 1.6.2012 beschlossen und treten am 1.1.2013 in Kraft.

Geänderte Rz	84

Zudem wurden die Verweise auf die Eigenmittelverordnung (ERV; SR 952.03) an die am 1.1.2013 in Kraft tretende Fassung angepasst.

Diese Änderungen wurden am xx.yy.2013 beschlossen und treten am 1.1.2015 in Kraft (mit Ausnahme von Rz 116, welche per 1.1.2014 in Kraft tritt).

Neu eingefügte Rz	2.1, 116, 117 – 136, 137
Geänderte Rz	1, 29, 50, 53, 71, 79
Aufgehobene Rz	20 – 22, 28, 30 – 44, 64

Die Anhänge des Rundschreibens werden wie folgt geändert:

Diese Änderungen wurden am xx.yy.2013 beschlossen und treten am 1.1.2015 in Kraft.

Geändert / Neu	Anhang 3
Aufgehoben	Anhang 1 und 4

Zudem wurde die Nummerierung der Anhänge angepasst.