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:	~~22. September 2016~~ … [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. 12 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:	Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV
Anhang 2:	Übersicht zur Kategorisierung von Ereignistypen
Anhang 3:	Umgang mit elektronischen Kundendaten

Laupenstrasse 27, 3003 Bern
Tel. +41 (0)31 327 9100, Fax +41 (0)31 327 9101
www.finma.ch

Adressaten																										
BankG			VAG			BEHG	FinfraG						KAG									GwG			Andere	
Banken	Finanzgruppen und -kongl.	Andere Intermediäre	Versicherer	Vers.-Gruppen und -Kongl.	Vermittler	Effektenhändler	Handelsplätze	Zentrale Gegenparteien	Zentralverwahrer	Transaktionsregister	Zahlungssysteme	Teilnehmer	Fondsleitungen	SICAV	KmG 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; SR 952.03) und definiert die qualitativen Grundanforderungen an das Management der operationellen Risiken beruhend auf Art. 12 BankV sowie Art. 19–20 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

Operationelle Risiken sind gemäss Art. 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 Rechts- bzw. Compliance-Risiken, soweit sie einen direkten, finanziellen Verlust darstellen, d.h. inklusive Bussen durch Aufsichtsbehörden und Vergleiche. 2*

Aufgehoben 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. Juni 2006, 1. Juli 2006 bis 30. Juni 2007 und 1. Juli 2007 bis 30. Juni 2008. 4

Damit ergeben sich die Eigenmittelanforderungen K_{BIA} als 5

[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.

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

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 125 ff. FINMA-RS 15/1 „Rechnungslegung Banken“: 9*

- Brutto-Erfolg Zinsengeschäft (Rz 131 FINMA-RS 15/1 „Rechnungslegung Banken“); 10*
- Erfolg aus dem Kommissions- und Dienstleistungsgeschäft[2] (Rz 139 FINMA-RS 15/1 „Rechnungslegung Banken“); 11*
- Erfolg aus dem Handelsgeschäft und der *Fair-Value*-Option (Rz 140 FINMA-RS 15/1 „Rechnungslegung Banken“); 12*
- Beteiligungsertrag (Rz 143 FINMA-RS 15/1 „Rechnungslegung Banken“) aus nicht zu konsolidierenden Beteiligungen; und 13*
- Liegenschaftenerfolg (Rz 144 FINMA-RS 15/1 „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 der schweizerischen Rechnungslegungsvorschriften international anerkannte Rechnungslegungsstandards verwenden, sofern die FINMA dafür die Bewilligung erteilt (vgl. Art. 91 Abs. 4 ERV). 17

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

[2] Die Berücksichtigung des Kommissionsaufwandes nach Rz 138 FINMA-RS 15/1 „Rechnungslegung Banken“ unterliegt den Restriktionen von Rz 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

Aufgehoben 20*

Aufgehoben 21*

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 Summanden gleich null gesetzt werden müssen (vgl. Art. 93 Abs. 1 ERV). 24

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

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

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

Aufgehoben 28*

Jede Bank muss nach Massgabe von Anhang 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) Aufgehoben

Aufgehoben 30*-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 qualitative Anforderungen

Banken, die einen institutsspezifischen Ansatz verwenden, müssen die qualitativen Grundanforderungen gemäss 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 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

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 Bewilligungsprozesses. Dieser findet unter Leitung der FINMA und unter Einbezug der Prüfgesellschaft statt. 69

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 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

[3] Vgl. Fussnote 1

- 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 Beobachtungszeitraum von mindestens drei Jahren umfassen. Spätestens zwei Jahre nach erstmaliger Verwendung des Ansatzes muss sich der Beobachtungszeitraum dauerhaft über mindestens fünf Jahre erstrecken. 77

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 2 zuordnen können. Sie muss über dokumentierte und objektive Kriterien für diese Kategorisierung verfügen. 79*

- Die internen Verlustdaten einer Bank müssen gestützt auf einen integren 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 aufgrund 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 Risk Measure* noch aus dem *Backtesting* ausgeschlossen werden. 84*

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 Grundprinzipien 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 98

operationelle Risiken berücksichtigen. Die Anerkennung solcher Absicherungswirkungen ist jedoch auf eine Reduktion von maximal 20 % der mittels eines institutsspezifischen Ansatzes berechneten Eigenmittelanforderungen beschränkt.

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. 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. 102

- 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 Einheiten und Geschäftsfelder ergibt. 111

- 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 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 bestimmt die FINMA im institutsspezifischen Einzelfall, wie eine angemessene approximative Berechnung der theoretischen Basel I-Anforderungen vorgenommen werden kann. Für operationelle Risiken orientiert sie sich am Standardansatz gemäss Art. 93 ERV. 116*

IV. Qualitative Anforderungen an den Umgang mit operationellen Risiken

A. Proportionalitätsprinzip

Die Anforderungen dieses Kapitels gelten grundsätzlich für alle Adressaten dieses Rundschreibens. Die Anforderungen dieses Kapitels sind jedoch im Einzelfall abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen. Die Rz 119 listet die Randziffern auf, von deren Umsetzung kleine Institute gänzlich ausgenommen sind. 117*

Kleine Institute im Sinne der Rz 117 sind Banken und Effektenhändler der FINMA-Kategorien[6] 4 und 5. Die FINMA kann im Einzelfall Erleichterungen oder Verschärfungen anordnen. 118*

B. Qualitative Grundanforderungen

Kleine Institute gemäss Rz 117 und 118 sind von der Erfüllung von Rz 129 und 132–134 ausgenommen. 119*

Die qualitativen Grundanforderungen basieren auf den „Principles for the Sound Management of Operational Risk“ des Basel Committee on Banking Supervision (Juni 2011).[7] 120*

a) Grundsatz 1: Kategorisierung und Klassifizierung von operationellen Risiken

Die operationellen Risiken sind zur Gewährleistung der Konsistenz im Rahmen der Risikoidentifikation, der Risikobeurteilung und der Zielsetzung im operativen Risikomanagement einheitlich zu kategorisieren[8]. 121*

[4] Vgl. Pressemitteilung des Basler Ausschusses vom 13. Juli 2009: 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, AS **1998** 16).
[6] Vgl. den Anhang im FINMA-RS 11/2 „Eigenmittelpuffer und Kapitalplanung Banken“.
[7] www.bis.org/publ/bcbs195.pdf
[8] Diese einheitliche Kategorisierung kann in Anlehnung an Anhang 2 dieses Rundschreibens oder mittels einer internen Terminologie oder Taxonomie erfolgen.

Die einheitliche Klassifizierung der operationellen Risiken erfolgt auf Basis der Kategorisierung der operationellen Risiken gemäss Rz 121 und umfasst eine Beurteilung sowohl der inhärenten Risiken[9] als auch der Residualrisiken[10]. ~~Typischerweise erfolgt die Beurteilung entlang den Dimensionen „Eintrittswahrscheinlichkeit“ und „Schadensausmass“.~~ Die Klassifizierung kann sowohl auf Basis einer qualitativen wie quantitativen Beurteilung erfolgen. Die Klassifizierung dient insbesondere auch der Bestimmung der Risiken mit weitreichender Tragweite im Sinne von Rz 137. 122*

Aufgehoben 123*-124*

b) Aufgehoben

Aufgehoben 125*-127*

c) Grundsatz 2: Identifizierung, Begrenzung und Überwachung

Eine wirksame Risikoidentifikation, welche die Grundlage für die Begrenzung und Überwachung der operationellen Risiken bildet, berücksichtigt sowohl interne[11] als auch externe[12] Faktoren. Hierzu gehören mindestens Risiko- und Kontrollbeurteilungen sowie Revisionsergebnisse. 128*

In Abhängigkeit von den institutsspezifischen Geschäftsaktivitäten und deren Art, Umfang, Komplexität und Risikogehalt, ist die Berücksichtigung weiterer Instrumente und Methoden zu prüfen und sind diese gegebenenfalls anzuwenden: 129*

a. Erhebung und Analyse interner Verlustdaten;

b. Erhebung und Analyse externer Ereignisse, die mit operationellen Risiken verbunden sind;

c. Analyse der Zusammenhänge zwischen Risiken, Prozessen und Kontrollen;

d. Risiko- und Performance-Indikatoren für die Überwachung von operationellen Risiken und Indikatoren für die Wirksamkeit des internen Kontrollsystems;

e. Szenarioanalysen;

f. Abschätzung des Verlustpotenzials;

g. Vergleichende Analysen[13].

Die Begrenzung und Überwachung erfolgt mittels der im Rahmenkonzept für das institutsweite Risikomanagement gemäss dem FINMA-Rundschreiben 2017/1 „Corporate Governance – Banken“ definierten Instrumente, Strukturen, Ansätze usw. von den hierfür vorgesehenen Organisationseinheiten. 130*

[9] Vgl. Anhang 3, Rz 59
[10] Vgl. Anhang 3, Rz 60
[11] Beispielsweise Unternehmensstruktur, Art der Aktivitäten, Qualifikationen der Mitarbeitenden, organisatorische Veränderungen und Personalfluktuation einer Bank.
[12] Beispielsweise Veränderungen des weiteren Umfelds und der Branche sowie technologische Fortschritte.
[13] Bei einer vergleichenden Analyse werden die Resultate der verschiedenen Beurteilungsinstrumente verglichen, um sich ein umfassenderes Bild der operationellen Risiken der Bank zu verschaffen.

d) Grundsatz 3: Interne und externe Berichterstattung

Aufgehoben 131*

Die interne Berichterstattung über operationelle Risiken muss sowohl Finanz-, Betriebs- und Compliance-Daten, aber auch wesentliche risikorelevante externe Informationen über Ereignisse und Bedingungen umfassen. Die Berichterstattung über operationelle Risiken muss dabei mindestens folgende Punkte abdecken und deren mögliche Auswirkungen auf das Institut und das für die operationellen Risiken erforderliche Eigenkapital darstellen: 132*

a. Wesentliche Verstösse gegen die in Bezug auf die inhärenten und Residualrisiken definierte Risikotoleranz des Instituts sowie Überschreitungen von diesbezüglich festgesetzten Risikobegrenzungen; 132.1*

b. Einzelheiten zu wesentlichen internen operationellen Risikoereignissen und/oder Verlusten; 132.2*

c. Informationen zu externen Ereignissen, welche für das Institut relevant sein können, und potentiellen Risiken sowie deren mögliche Auswirkungen auf das Institut. 132.3*

Ein Institut muss über eine formelle, vom Oberleitungsorgan genehmigte Offenlegungspolitik verfügen, aus der hervorgeht, wie die Bank ihre operationellen Risiken offenlegt und welche Kontrollprozesse bezüglich der Offenlegung anzuwenden sind. 133*

Von den Instituten 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 muss den Anspruchsgruppen eine Beurteilung der Wirksamkeit der Identifikation, Begrenzung und Überwachung der operationellen Risiken ermöglichen. 134*

e) Grundsatz 4: Technologieinfrastruktur[14]

Die Geschäftsleitung hat ~~ein IT-Risikomanagement-Konzept~~ den Umgang mit Risiken aus der Technologieinfrastruktur in Übereinstimmung mit der IT-Strategie und der definierten Risikotoleranz sowie unter Berücksichtigung von für das jeweilige Institut relevanten Aspekte gemäss international anerkannten Standards ~~zu implementieren~~in geeigneter Form zu dokumentieren. 135*

Die Geschäftsleitung stellt dabei sicher, dass im Umgang mit Risiken aus der Technologieinfrastruktur ~~das IT-Risikomanagement-Konzept~~ mindestens die folgenden ~~minimalen~~ Aspekte ~~beinhaltet~~abgedeckt sind: 135.1*

a. Aktuelle Übersicht über die wesentlichsten Bestandteile der Netzwerkinfrastruktur und ein Inventar aller kritischen Applikationen und der damit verbundenen IT-Infrastruktur sowie Schnittstellen mit Dritten, 135.2*

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

b. Eindeutige Festlegung von Rollen, Aufgaben und Verantwortlichkeiten in Bezug auf die kritischen Applikationen sowie damit verbundener IT-Infrastruktur und kritischen und/oder sensitiven Daten und Prozesse, 135.3*

c. Systematischer Prozess im Hinblick auf die Identifikation und Beurteilung von IT-Risiken im Rahmen der Sorgfaltsprüfung (Due Diligence) insbesondere bei Akquisitionen bzw. Auslagerungen im IT-Bereich sowie bei der Überwachung von Dienstleistungsvereinbarungen, 135.4*

d. Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Verantwortung zur Reduktion von IT-Risiken sowie Einhaltung und Stärkung der IT-Informationssicherheit. 135.5*

Die Geschäftsleitung hat zudem ~~ein Risikomanagement-Konzept für~~ den Umgang mit Cyber-Risiken[15] ~~zu implementieren~~in geeigneter Form zu dokumentieren. ~~Dieses Konzept~~Dieser Umgang hat mindestens die folgenden Aspekte abzudecken und eine effektive Umsetzung durch geeignete Prozesse sowie eine eindeutige Festlegung von Aufgaben, Rollen und Verantwortlichkeiten zu gewährleisten: 135.6*

a. Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken[16], insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme, 135.7*

b. Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen und/oder sensitiven Daten und IT-Systeme, 135.8*

c. Zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken auf Basis eines Prozesses zur systematischen Überwachung der Technologieinfrastruktur, 135.9*

d. Reaktion auf Cyber-Attacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyber-Attacken in Abstimmung mit dem BCM, und 135.10*

e. Sicherstellung einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen. 135.11*

[15] Operationelle Risiken in Bezug auf mögliche Verluste durch Cyber-Attacken.
[16] Sind Angriffe aus dem Internet und vergleichbaren Netzen, auf die Integrität, die Verfügbarkeit und die Vertraulichkeit der Technologieinfrastruktur, insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme.

Die Geschäftsleitung lässt zum Schutz der kritischen und/oder sensitiven Daten und IT-Systemen vor Cyber-Attacken regelmässig Verwundbarkeitsanalysen[17] und *Penetration Testings*[18] durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen durchgeführt werden. 135.12*

f) Grundsatz 5: Kontinuität bei Geschäftsunterbrechung

Die Geschäftsleitung hat über Pläne zur Fortführung der Geschäfte des Instituts zu verfügen, welche die Kontinuität der Tätigkeiten und die Schadensbegrenzung im Falle einer schwerwiegenden Geschäftsunterbrechung gewährleisten.[19] 136

g) Grundsatz 6: Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken

Systemrelevante Banken treffen im Rahmen ihrer Notfallplanung die für die unterbruchsfreie Weiterführung von systemrelevanten Funktionen nötigen Massnahmen (Art. 9 Abs. 2 Bst. d BankG i.V.m. Art. 60 ff. BankV). Sie identifizieren die zur Fortführung der systemrelevanten Funktionen im Fall der Abwicklung, Sanierung oder Restrukturierung notwendigen Dienstleistungen („kritische Dienstleistungen“) und ergreifen die für deren Weiterführung nötigen Massnahmen. Dabei berücksichtigen sie die von internationalen Standardsettern erlassenen Vorgaben in diesem Zusammenhang. 136.1*

h) Grundsatz 7: Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft

Wenn Institute oder ihre Gruppengesellschaften grenzüberschreitend Finanzdienstleistungen erbringen oder Finanzprodukte vertreiben, sind auch die aus einer Anwendung ausländischer Rechtsvorschriften (Steuer-, Straf-, Geldwäschereirecht usw.) resultierenden Risiken angemessen zu erfassen, begrenzen und kontrollieren. Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Institute ausländisches Aufsichtsrecht einhalten. 136.2*

Die Institute unterziehen ihr grenzüberschreitendes Finanzdienstleistungsgeschäft sowie den grenzüberschreitenden Vertrieb von Finanzprodukten einer vertieften Analyse der rechtlichen Rahmenbedingungen und der damit verbundenen Risiken. Gestützt auf diese Analyse treffen die Institute die erforderlichen strategischen und organisatorischen Massnahmen zur Risikoeliminierung und -minimierung und passen diese laufend geänderten Bedingungen an. Insbesondere verfügen sie über das notwendige länderspezifische Fachwissen, definieren sie spezifische Dienstleistungsmodelle für die bedienten Länder, schulen die Mitarbeiter und stellen durch entsprechende organisatorische Massnahmen, Weisungen, Vergütungs- und Sanktionsmodelle die Einhaltung der Vorgaben sicher. 136.3*

[17] Analyse zur Identifikation von derzeit bestehenden Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur gegenüber Cyber-Attacken.
[18] Gezielte Prüfung und das Ausnützen von Software-Schwachstellen und Sicherheitslücken in der Technologieinfrastruktur, um unberechtigten Zugang zu dieser Technologieinfrastruktur zu erhalten.
[19] Vgl. die im FINMA-Rundschreiben 2008/10 „Selbstregulierung als Mindeststandard“ als Mindeststandard anerkannten Ziffern der SBVg-Empfehlungen für das *Business Continuity Management* (BCM).

Auch die durch externe Vermögensverwalter, Vermittler und andere Dienstleister generierten Risiken sind zu berücksichtigen. Entsprechend ist bei der Auswahl und Instruktion dieser Partner sorgfältig vorzugehen. 136.4*

Von diesem Grundsatz werden auch Konstellationen erfasst, in denen eine im Ausland ansässige Tochtergesellschaft, Zweigniederlassung oder dergleichen eines Schweizer Finanzinstituts Kunden grenzüberschreitend bedient. 136.5*

C. Risikospezifische qualitative Anforderungen

Die Steuerung und Kontrolle spezifischer operationeller Risiken mit weitreichender Tragweite hat umfassender und intensiver zu erfolgen als dies in den qualitativen Grundanforderungen vorgegeben ist. Die Geschäftsleitung hat hierfür ergänzende risikospezifische Massnahmen oder eine Verschärfung bestehender Massnahmen situativ zu bestimmen und umzusetzen. 137*

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. 138*

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. 139*

Anhang 1

Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV

I. Übersicht

1

1. Ebene	2. Ebene	Aktivitäten
Unternehmensfinanzierung/-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[20]	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
	Unternehmens-stiftungen	
Institutionelle Vermögensverwaltung	Freie Vermögensverwaltung	Im Pool, segmentiert, Retail-bezogen, institutionell, geschlossen, offen, *Private Equity*

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

Anhang 1

Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV

	Gebundene Vermögensverwaltung	Im Pool, segmentiert, Retail-bezogen, individuell, privat, institutionell, geschlossen, offen
Wertpapierprovisionsgeschäft	Ausführung von Wertschriftenaufträgen	Ausführung, inkl. sämtlicher damit verbundenen Dienstleistungen

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 Geschäftsleitung 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 2

Übersicht zur Kategorisierung 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)

Anhang 2

Übersicht zur Kategorisierung von Ereignistypen

Verlustereignis-kategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
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 usw.
		Sicherheit am Arbeitsplatz	Allgemeine Haftpflicht Verstoss gegen sicherheits- oder gesundheitsbezogene Bestimmungen Entschädigungs- oder Schadenersatzzahlungen an Mitarbeiter
		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 usw.) 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

Anhang 2

Übersicht zur Kategorisierung von Ereignistypen

Verlustereignis-kategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
		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 usw.) Modellfehler
		Kundenselektion, Geschäftsvergabe und Kreditexposition	Nicht mit internen Richtlinien kompatibles Vorgehen bei Kundenprüfungen Überschreitung von Limiten
		Beratungstätigkeiten	Streitigkeiten in Bezug auf Resultate von Beratungstätigkeiten
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 usw.

Anhang 2

Übersicht zur Kategorisierung von Ereignistypen

Verlustereignis-kategorie (Stufe 1)	Definition	Subkategorien (Stufe 2)	Beispiele von Aktivitäten (Stufe 3)
Abwicklung, Vertrieb und Prozessmanagement	Verluste auf Grund von Fehlern bei der Geschäftsabwicklung oder beim Prozessmanagement; Verluste aus Beziehungen mit Geschäftspartnern, Lieferanten usw.	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. nicht erfolgte 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 nicht-legitimierten Kontozugriffs Unkorrekte Kontoführung mit Verlustfolge Verlust oder Beschädigung von Kundenvermögenswerten durch fahrlässige Handlungen

Anhang 2

Übersicht zur Kategorisierung von Ereignistypen

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

Anhang 3*

Umgang mit elektronischen Kundendaten

In diesem Anhang werden die Grundsätze und die dazugehörigen Ausführungen für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten natürlicher Personen („Privatkunden“[21]), 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[22], sondern auch im Datenschutzrecht[23] und Zivilrecht. 1*

Kleine Banken[24] sind von der Erfüllung folgender Randziffern ausgenommen: 2*

- Rz 15, 17–19 sowie 22 des Grundsatzes 3;
- Alle Randziffern der Grundsätze 4–6;
- Rz 41 des Grundsatzes 7.

Banken des Kleinbankenregimes sowie Institute gemäss Art. 1*b* BankG können sich hinsichtlich Umsetzung der Anforderungen in Anhang 3 auf die Rz 3 beschränken. Dabei ist die Anforderung in Rz 3 im Einzelfall abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen. 2.1*

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 das Oberleitungsorgan die Geschäftsleitung zur Sicherstellung einer wirksamen Implementierung von Massnahmen zur Gewährleistung der Vertraulichkeit von Kundendaten. Die Geschäftsleitung beauftragt eine unabhängige Einheit als Kontrollfunktion, die Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten zu schaffen und aufrechtzuerhalten. 3*

a) Unabhängigkeit und Verantwortung

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. 4*

[21] Unter „Privatkunden“ werden auch solche Geschäftsbeziehungen verstanden, bei denen die natürliche Person mittels einer juristischen Person (z.B. als wirtschaftlich Berechtigter einer Sitzgesellschaft, Domizilgesellschaft, Stiftung) oder Trust eine Geschäftsbeziehung mit der Bank eingeht.
[22] Insbesondere Art. 3 und 47 BankG sowie Art. 12 BankV; Art. 10 und 43 BEHG sowie Art. 19 f. BEHV.
[23] Insbesondere Art. 7 DSG sowie Art. 8 ff. VDSG (vgl. dazu auch die Leitfäden des EDÖB~~; abrufbar unter www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=de~~).
[24] Vgl. Rz 118

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 Geschäftsleitung zu definieren und vom Oberleitungsorgan zu genehmigen. Die Geschäftsleitung informiert das Oberleitungsorgan regelmässig über die Wirksamkeit der eingeführten Kontrollen. 5*

b) Vorgaben, Prozesse und Systeme

Es wird vorausgesetzt, 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 bearbeiten, konsistent umgesetzt werden. 6*

Die Massnahmen und die Periodizität deren Durchführung sind aufgrund der von der Bank festgelegten Risikotoleranz schriftlich, nachvollziehbar und verbindlich festzulegen. 7*

Die Implementierung und Einhaltung des Rahmenkonzepts zur Vertraulichkeit von Kundendaten ist durch das Oberleitungsorgan zu überwachen und muss durch regelmässige Kontrollen der für Datensicherheit und -vertraulichkeit zuständigen Einheit sichergestellt werden. 8*

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

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. 9*

a) Kundendatenkategorien und CID-Definition

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 verfügen, die ihrem spezifischen Kundenstamm angemessen ist. 11*

b) CID-Klassifizierung und Vertraulichkeitsstufen

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*

c) CID-Verantwortung

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. 13*

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

C. Grundsatz 3: Datenspeicherort und -zugriff

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. 15*

a) Datenspeicherort und -zugriff allgemein

Ein Inventar der Applikationen und der damit verbundenen Infrastruktur, die CID enthalten oder verarbeiten, muss verfügbar sein und laufend aktualisiert werden. Die Aktualisierung des Inventars hat insbesondere bei strukturellen Änderungen (z.B. neue Standorte oder Erneuerung der technischen Infrastruktur) zeitnah zu erfolgen. Änderungen von geringer Tragweite sind regelmässig nachzuführen. 16*

Es wird vorausgesetzt, dass die Granularität des Inventars 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, sind die damit verbundenen erhöhten Risiken in Bezug auf den Kundendatenschutz angemessen zu begrenzen.[25] CID müssen angemessen geschützt (z.B. anonymisiert, verschlüsselt oder pseudonymisiert) werden. 20*

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

c) *Need to know*-Grundsatz

Personen dürfen nur auf diejenigen Informationen oder Funktionalitäten Zugriff haben, die für die Wahrnehmung ihrer Aufgaben erforderlich sind. 21*

d) Zugriffsberechtigung

Die Bank hat über ein rollen- und funktionsspezifisches Autorisierungssystem zu verfügen, welches die Zugriffsberechtigungen von Mitarbeitenden und Dritten auf CID eindeutig regelt. Um sicherzustellen, dass nur aktuell autorisierte Personen auf CID Zugriff haben, sind Berechtigungen regelmässig zu bestätigen. 22*

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 ihrer 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. 23*

a) Sicherheitsstandards

Die Sicherheitsstandards müssen in Bezug auf die Grösse der Bank und den Grad der Komplexität seiner IT-Architektur angemessen sein. 24*

b) Sicherheitsstandards und Marktpraxis

Die Sicherheitsstandards bilden einen festen Bestandteil des Rahmenkonzepts 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 von unabhängigen Überprüfungen und Prüfberichte müssen berücksichtigt werden. 25*

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

Um die Vertraulichkeit von CID sicherzustellen, hat die Bank Schutzmassnahmen (z.B. Verschlüsselung) abzuwägen und diese soweit erforderlich auf den folgenden Ebenen umsetzen: 26*

a. Sicherheit von CID auf dem Endgerät bzw. am Endpoint (z.B. PCs, Notebooks, portable Datenspeicher und Mobilgeräte); 27*

b. Sicherheit bei Übertragung von CID (z.B. innerhalb eines Netzwerks oder zwischen verschiedenen Standorten); 28*

c. Sicherheit von gespeicherten CID (z.B. auf Servern, in Datenbanken oder auf Backup-Medien). 29*

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 (hoch-)privilegierte IT-Benutzer (bspw. Systemadministratoren) und Anwender mit funktionalem Zugriff auf Massen-CID („Schlüsselmitarbeitenden*"*) gelten. Ihnen ist besondere Aufmerksamkeit zu schenken. 30*

a) Sorgfältige Auswahl der Mitarbeitenden

Mitarbeitende, die auf CID zugreifen können, sind sorgfältig auszuwählen. Insbesondere ist vor der Aufnahme der Tätigkeit zu überprüfen, ob der potentielle Mitarbeitende die Anforderungen für einen angemessenen Umgang mit CID erfüllt. Die Bank hat ferner vertraglich zu regeln wie die Auswahl von Mitarbeitenden durch Dritte, als auch die Bestimmung von Mitarbeitenden von Drittunternehmen, welche im Auftrag der Bank auf CID zugreifen können erfolgt, damit alle Mitarbeitenden einen vergleichbaren, sorgfältigen Auswahlprozess durchlaufen. 31*

b) Gezielte Schulungen der Mitarbeitenden

Interne und externe Mitarbeitende müssen im Rahmen gezielter Schulungen in Bezug auf die Kundendatensicherheit sensibilisiert werden. 32*

c) Sicherheitsanforderungen

Die Bank muss über klare Sicherheitsanforderungen für Mitarbeitende, die auf CID zugreifen, verfügen. Es ist regelmässig zu überprüfen, ob die Anforderungen für einen angemessenen Umgang mit CID weiterhin erfüllt sind. Erhöhte Sicherheitsanforderungen müssen für (hoch-) privilegierte IT-Benutzer und Anwender mit funktionalem Zugriff[26] auf Massen-CID („Schlüsselmitarbeitenden") gelten. 33*

d) Liste von Schlüsselmitarbeitenden

Als Ergänzung zu den allgemeinen Anforderungen in Bezug auf Zugriffsberechtigungen für Mitarbeitende und Dritte (siehe Rz 22) wird von der Bank die Führung und laufende Aktualisierung einer Liste mit den Namen aller internen und externen (hoch-) privilegierten IT-Benutzer und Anwender (Schlüsselmitarbeitenden) erwartet, die Zugriff auf Massen-CID[27] haben und/oder denen 34*

[26] Bei erweiterten Zugriffsrechten wie z.B. die Abfrage und Extraktion/Migration von Massen-CID.
[27] Einzelabfragen mit eingegrenzten Zugriffsrechten (z.B. von Schaltermitarbeitern) fallen nicht unter den Begriff des Zugriffs auf Massen-CID.

Verantwortlichkeiten hinsichtlich der Kontrolle und Überwachung der Vertraulichkeit von Kundendaten übertragen wurden.

Vorkehrungen, wie z.B. das Führen von Log-Dateien, sind einzuführen, um die Identifizierung von Benutzern, die auf Massen-CID zugreifen, zu ermöglichen. 35*

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

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[28] 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 auf Adäquanz geprüft und gegebenenfalls angepasst werden. 36*

a) Risikobeurteilungsprozess

Die Beurteilung des mit der Vertraulichkeit von CID verbundenen inhärenten Risikos und Residualrisikos muss auf Basis eines strukturierten Prozesses und unter Einbezug der Geschäfts-, IT- und Kontrollfunktionen erfolgen. 37*

b) Risikoszenarien und Schlüsselkontrollen[29]

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. 38*

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

Identifizierte Risiken müssen überwacht und angemessen minimiert werden. Dies gilt namentlich in Verbindung mit Datenbearbeitungsaktivitäten, bei denen grosse Mengen von CID verändert oder migriert werden müssen.[30] Bei strukturellen Veränderungen (z.B. bedeutende Reorganisationen) muss sich die Bank frühzeitig und vertieft mit Sicherheitsmassnahmen der Vertraulichkeit von CID befassen. 39*

a) Produktionsumfeld, Datenbearbeitung in Verbindung mit Massen-CID

[28] 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.

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

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

Die Datenbearbeitung, die im Produktionsumfeld mit nicht anonymisierten, nicht verschlüsselten und nicht pseudonymisierten Massen-CID durchgeführt wird, muss geeigneten Verfahren unterliegen (z.B. Vier-Augen-Prinzip oder Log-Dateien), einschliesslich der Benachrichtigung der für die Datensicherheit und -vertraulichkeit zuständigen Einheit. 40*

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

Während der Entwicklung, Veränderung und Migration von Systemen müssen die CID angemessen vor dem Zugriff und der Nutzung durch Unberechtigte geschützt werden. 41*

Wendet ein Institut bei der Entwicklung, Veränderung und Migration von Systemen (bspw. bei der Generierung von Testdaten oder bei der Zwischenspeicherung von Daten während der Datenmigration) keine Methoden zur Anonymisierung, Pseudonymisierung oder Verschlüsselung an (Arbeiten „in Klartext"), so wendet es bei diesen Tätigkeiten die Vorgaben gemäss Rz 40 an. 41.1*

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

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, Kontroll- und Prüfergebnisse überwacht, analysiert und in geeigneter Form dem obersten Management gemeldet werden. Dies muss zur laufenden Verfeinerung der Massnahmen zur Sicherstellung der Vertraulichkeit von CID beitragen. 42*

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

Es ist ein klar definierter Prozess für die Identifikation von Vorfällen in Bezug auf die Vertraulichkeit sowie die Reaktion darauf zu formalisieren und dieser allen innerhalb des Instituts involvierten Stellen zu kommunizieren. 43*

b) Meldung

Es wird erwartet, dass das Risiko der Verletzung der Vertraulichkeit von CID und diesbezügliche Compliance-Meldungen in den internen Berichterstattungen angemessen abgebildet sind oder alternativ sichergestellt ist, dass eine systematische Erfassung und Eskalierung an geeignete Stellen erfolgt, falls dies die Geheimhaltung solcher Vorkommnisse erfordert. 44*

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

Das Rahmenkonzept zur Sicherstellung der Vertraulichkeit von CID (Rz 6, 7 und 8) und die Sicherheitsstandards (Rz 24) sind regelmässig zu kontrollieren. Vorfälle, Ausnahmen, Kontroll- und Prüfergebnisse müssen zur laufenden Verfeinerung dieses Rahmenkonzeptes beitragen. 45*

d) Externe Kommunikation

Anhang 3*

Umgang mit elektronischen Kundendaten

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. 46*

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

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. 47*

a) Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID

Die Sorgfaltspflicht in Bezug auf die Vertraulichkeit von CID muss Teil des Prozesses für die Auswahl von Outsourcing-Dienstleistern und Anbietern von Grossaufträgen sein. Es müssen 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. 48*

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

Dritte müssen über die internen Sicherheits- und Vertraulichkeitsstandards der Bank sowie deren allfällige Erweiterungen informiert werden und diese als Mindestanforderung erfüllen. 49*

c) Allgemeine Verantwortung

Die Bank muss für jede ausgelagerte Aktivität, die Zugriff auf CID beinhaltet, mindestens einen internen Mitarbeitenden bestimmen, der dafür verantwortlich ist, dass die Sicherheits- und Vertraulichkeitsstandards in Bezug auf die Vertraulichkeit von CID eingehalten werden. 50*

d) Ausgestaltung der Kontrollen und Wirksamkeitstests

Die Bank muss wissen und verstehen, welche Schlüsselkontrollen der Outsourcing-Dienstleister in Verbindung mit der Vertraulichkeit von CID durchzuführen hat. Die Einhaltung interner Anforderungen sowie die Wirksamkeit der Schlüsselkontrollen sind dabei zu prüfen und zu beurteilen. 51*

Anhang 3*

Umgang mit elektronischen Kundendaten

II. Glossar

Kundenidentifikationsdaten (*Client Identifying Data,* CID): Kundendaten, die Personendaten nach Art. 3 Bst. a DSG darstellen und es ermöglichen, die betroffenen Kunden zu identifizieren. 52*

Massen-CID: Menge von CID, welche im Vergleich zur Gesamtzahl der Konten/Gesamtgrösse des Privatkundenportfolios bedeutend ist. 53*

Grossaufträge: Alle durch Dritte erbrachten Dienstleistungen, die Zugriff auf Massen-CID erfordern 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. 54*

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 Mitarbeitende sind. 55*

Schlüsselmitarbeitende: Alle internen und externen im IT-Bereich sowie in weiteren Unternehmensbereichen tätigen Mitarbeitenden, die aufgrund ihres Tätigkeitsprofils und ihrer Aufgaben (hoch-)privilegierten Zugriff auf CID im grossen Umfang haben (z.B. Datenbankadministratoren, Mitglieder des obersten Managements). 56*

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). 57*

Schlüsselkontrolle: Eine Kontrolle, die, falls sachgerecht definiert, implementiert und durchgeführt, das Risiko der Verletzung der Vertraulichkeit von CID massgeblich senkt. 58*

Inhärentes Risiko: Risiko vor Kontroll- oder Minderungsmassnahmen. 59*

Residualrisiko: Risiko nach Berücksichtigung von Kontroll- oder Minderungsmassnahmen. 60*

Reversible Datenbearbeitungstechniken: 61*

- 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. 62*

Anhang 3*

Umgang mit elektronischen Kundendaten

- 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. 63*

Irreversible Datenbearbeitungstechniken: 64*

- 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[31]. 65*

[31] Vgl. EDÖB, Anhang zu den Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem, 5.

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 29.8.2013 beschlossen und treten am 1.1.2014 in Kraft.

Neu eingefügte Rz	116

Diese Änderungen wurden am 29.8.2013 beschlossen und treten am 1.1.2015 in Kraft.

Neu eingefügte Rz	2.1, 117–139
Geänderte Rz	1, 29, 50, 53, 71, 79
Aufgehobene Rz	20–22, 28, 30–44, 64
Übrige Änderungen	Neuer Haupttitel vor Rz 3 und Neugliederung der Titel Titeländerung vor Rz 50

Diese Änderungen wurden am 27.3.2014 beschlossen und treten am 1.1.2015 in Kraft.

Geänderte Rz	1, 9, 10, 11, 12, 13, 14

Diese Änderungen wurden am 22.9.2016 beschlossen und treten am 1.7.2017 in Kraft.

Neu eingefügte Rz	132.1–132.3, 135.1–135.12, 136.1–136.5
Geänderte Rz	2, 53, 117, 118, 119, 121, 122, 128, 129, 130, 132, 133, 134, 135, 136, 137
Aufgehobene Rz	2.1, 123, 124, 125, 126, 127, 131
Übrige Änderungen	Kap. IV.B: Neunummerierung der Grundsätze

Diese Änderungen wurden am … beschlossen und treten am ... in Kraft.

Geänderte Rz	

Die Anhänge des Rundschreibens wurden wie folgt geändert:

Diese Änderungen wurden am 29.8.2013 beschlossen und treten am 1.1.2015 in Kraft.

Die Nummerierung der Anhänge wird angepasst: Anhang 2 "Kategorisierung der Geschäftsfelder nach Art. 93 Abs. 2 ERV" wird neu zum Anhang 1 und Anhang 3 "Übersicht zur Klassifikation von Ereignistypen" wird neu zum Anhang 2.

Neu	Anhang 3

Verzeichnis der Änderungen

Aufgehoben	Anhänge 1 und 4

Diese Änderungen wurden am 22.9.2016 beschlossen und treten am 1.7.2017 in Kraft.

Neu	Anhang 3: Rz 41.1
Geändert	Anhang 1: Rz 9 Anhang 2: Titel des Anhangs Anhang 3: Rz 2, 3, 5, 6,7, 8, 16, 17, 30, 33, 34, 56

Diese Änderungen wurden am … beschlossen und treten am … in Kraft.

Neu	