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“ – Totalrevision

Rundschreiben 2013/3 „Prüfwesen“ – Teilrevision

Bericht über die Ergebnisse der Anhörung vom 10. Mai 2022 bis 11. Juli 2022

7. Dezember 2022

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Inhaltsverzeichnis

Kernpunkte

1. Die Initiative zur Totalrevision des FINMA-Rundschreibens 2008/21 „Operationelle Risiken – Banken“ stiess auf breite Zustimmung. Auch begrüsst wurde, dass das neue Rundschreiben die Basler Prinzipien, die Aufsichtspraxis der FINMA und die Inhalte der Selbstregulierung der Schweizerischen Bankiervereinigung im Bereich des *Business Continuity Management* (BCM) konsolidiert.

2. An der öffentlichen Anhörung vom 10. Mai 2022 bis 11. Juli 2022 haben Verbände von Banken und Prüfgesellschaften, Berufsorganisationen sowie individuelle Banken und Dienstleister teilgenommen. Ihre Eingaben hat die FINMA ausgewertet und – sofern stringent – aufgenommen.

3. Die Teilnehmenden begrüssten die technologieneutrale Ausgestaltung des Rundschreibens und die Anwendung des Proportionalitätsprinzips. Zu Letzterem forderten einige Teilnehmende mehr Erleichterungen, andere hingegen punktuelle Verschärfungen. Die FINMA hat die betroffenen Randziffern, wo stringent und in Einklang mit den Aufsichtserwartungen, angepasst.

4. Der Zeitplan wurde von mehreren Teilnehmenden als zu ambitioniert angesehen. Die FINMA verschiebt daher den Zeitpunkt des Inkrafttretens um ein Jahr, auf den 1. Januar 2024.

5. Die kritischen Daten wurden vielfach als zu breit definiert angesehen, sodass je nach Betrachtungsweise fast alle Daten darunterfallen könnten. Die FINMA hat diese Definition daher entlang der zahlreichen eingegangenen Vorschläge angepasst.

6. Zahlreiche Fragen ergaben sich zu Abgrenzungen und Abhängigkeiten, insb. zwischen verschiedenen Risikokategorien, zwischen dem BCM und der operationellen Resilienz sowie zwischen Inventarisierungen. Die FINMA erklärt die Abgrenzungen und Abhängigkeiten im Anhörungsbericht und hat die entsprechenden Randziffern, wo sinnvoll und stringent, angepasst.

7. Das neue FINMA-Rundschreiben „Operationelle Risiken und Resilienz – Banken“ und die Teilrevision des FINMA-RS 13/3 „Prüfwesen“ treten am 1. Januar 2024 in Kraft, mit Übergangsfristen für die Sicherstellung der operationellen Resilienz.

Abkürzungsverzeichnis

BankG	Bankengesetz vom 8. November 1934 (SR 952.0)
BCM	*Business Continuity Management*
DRP	*Disaster Recovery Plan*
ERV	Eigenmittelverordnung vom 1. Juni 2012 (SR 952.03)
ESG	*Environmental Social Governance*
FINMAG	Finanzmarktaufsichtsgesetz vom 22. Juni 2007 (SR 956.1)
IKT	Informations- und Kommunikationstechnologie
ITSCM	*IT Service Continuity Management*
MPDT	*Maximum Period of Downtime*
RTO	*Recovery Time Objective*

1 Einleitung

Vom 10. Mai 2022 bis 11. Juli 2022 wurden das von der FINMA vorgeschlagene, totalrevidierte Rundschreiben 2008/21 „Operationelle Risiken – Banken“ sowie die Anpassungen am Rundschreiben 2013/3 „Prüfwesen“ einer Anhörung unterzogen.

2 Eingegangene Stellungnahmen

Folgende Personen haben im Rahmen der Anhörung eine Stellungnahme eingereicht und sich für deren Publikation[1] ausgesprochen (in alphabetischer Reihenfolge):

- Amazon Web Services (AWS)
- Clientis AG
- Credit Suisse Group AG (Credit Suisse)
- EXPERTsuisse
- Institute of Internal Auditing Switzerland (IIAS)
- NCC Group
- Raiffeisen Schweiz
- Schweizerische Bankiervereinigung (SBVg)
- SIX Group AG (SIX)
- Verband Schweizerischer Kantonalbanken (VSKB)

3 Ergebnisse der Anhörung und Beurteilung durch die FINMA

Im vorliegenden Bericht werden die eingegangenen Stellungnahmen von der FINMA zusammengefasst, gewichtet und ausgewertet. Ohne weitere Angabe beziehen sich die Verweise auf Randziffern auf die Anhörungsversionen der Rundschreiben.

Der Bericht wurde vom Verwaltungsrat der FINMA verabschiedet (Art. 11 Abs. 4 der Verordnung zum Finanzmarktaufsichtsgesetz). Er wird zusammen mit den verabschiedeten Regulierungen und den Stellungnahmen der Anhörung veröffentlicht.

[1] Nicht aufgeführt sind diejenigen Anhörungsteilnehmenden, die sich gegen eine Veröffentlichung ihrer Stellungnahme durch die FINMA ausgesprochen haben.

3.1 Allgemeines, Titelseite, Gegenstand und Geltungsbereich (Rz 1 und 2)

Stellungnahmen

Die EXPERTsuisse weist darauf hin, dass die Personen nach Art. 1*b* BankG auch auf der Titelseite als Adressaten genannt werden und in Rz 2 unter den Sammelbegriff „Institute“ fallen sollten.

Der Clientis AG erscheint die Organisation des Rundschreibens in verschiedene Grundsätze als nicht zweckmässig, da einzelne Fachgebiete und nicht Grundsätze geregelt würden. Stattdessen solle mit aussagekräftigen Kapitelüberschriften gearbeitet werden.

Würdigung

Die FINMA stimmt mit der EXPERTsuisse überein, dass die Personen nach Art. 1*b* BankG auch genannt werden sollen. Auch stimmt sie der Clientis zu und verwendet neu Kapitelüberschriften statt „Grundsätze“.

Fazit

Die Personen nach Art. 1*b* BankG werden in Rz 2 genannt. In Kapitel IV werden die Titel der Unterkapitel ersetzt und der Begriff der „Grundsätze“ wird gestrichen.

3.2 Proportionalitätsprinzip

Stellungnahmen

Zusätzlich zu den Erleichterungen für die Banken der Kategorien 4 und 5 wünschen sich die SBVg, der VSKB und die Clientis AG auch Erleichterungen für die Banken der Kategorie 3. Die SBVg merkt an, dass mit dem Rundschreiben die Basler Standards für alle Banken in der Schweiz umgesetzt würden, diese sich aber nur an sehr grosse, internationale Banken (in der Schweiz: die Grossbanken) richten würden. Entsprechend sei eine proportionale und prinzipienbasierte Umsetzung umso wichtiger.

Die SBVg stellt insbesondere fest, dass spezifische Aspekte aus den Rz 68, 84–85 und 97 für manche Institute der Kategorie 3 einen unverhältnismässigen Aufwand bedeuten könnten. Der VSKB wünscht sich konkret, dass die Rz 31, 33, 34, 61, 68, 84, 85, 88, 90, 91 und 97 nicht auf Institute der Kategorie 3 angewendet würden. Die EXPERTsuisse erläutert, warum die Rz 69 (Meldung von Vorfällen in Bezug auf kritische Daten) auch für die Institute nach Art. 47*a*–47*e* ERV, Personen gemäss Art. 1*b* BankG, sowie nicht-kontoführende Wertpapierhäuser von Relevanz ist und daher die Meldepflicht für diese Institute wieder aufgenommen werden solle. Ferner empfiehlt die

Clientis AG eine Umordnung der Randziffern, sodass zu Beginn jedes Themenbereichs zuerst die grundlegenden und für alle Institute relevanten Aspekte aufgeführt werden.

Würdigung

Die Basler Standards richten sich an international aktive Banken; dies beinhaltet in der Schweiz nicht nur die Grossbanken. Die Umsetzung internationaler Standards wie den Basler Standards ist Teil der Finanzmarktstrategie des Bundesrats und in Art. 7 Abs. 2 Bst. d FINMAG verankert.

Es wird auf Rz 17 hingewiesen, laut der die Grundsätze im Einzelfall abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen sind. Dieser Proportionalitätsgedanke gilt für alle Randziffern und insbesondere auch für die Institute der Kategorie 3. Daher wird von der Einführung einer weiteren Abstufung mit Erleichterungen für die Kategorie 3 Institute abgesehen.

Die Rz 97 wurde nicht sinngemäss verstanden und wird daher zur Klärung angepasst und ergänzt; siehe Kapitel 3.11.2. Die Rz 84 ist eine Weiterführung des Status Quo, da sie bereits sinngemäss Teil der *Empfehlungen für das Business Continuity Management (BCM)* der SBVg vom August 2013 ist. Die Rz 34 wird auf die systemrelevanten Banken (Kategorien 1 und 2) eingeschränkt; siehe Kapitel 3.5.4.

Die restlichen, speziell erwähnten Randziffern werden auch für die Institute der Kategorie 3 als sehr relevant angesehen und daher beibehalten. Die Meldung von Vorfällen (Rz 69) wird für Institute nach Art. 47*a*–47*e* ERV, Personen gemäss Art. 1*b* BankG, sowie nicht-kontoführende Wertpapierhäuser wieder aufgenommen. Bei der Anordnung der Randziffern wird eine inhaltlich sinnvolle Struktur vorgezogen; daher wird keine Staffelung der Randziffern nach Kategorien vorgenommen.

Fazit

Die Rz 34 wird für die Institute der Kategorie 3 ausgenommen und die Rz 97 wird angepasst. Die Rz 69 wird für die Institute nach Art. 47*a*–47*e* ERV, Personen gemäss Art. 1*b* BankG, sowie die nicht-kontoführenden Wertpapierhäuser wieder aufgenommen.

3.3 Begriffe

3.3.1 Definition der operationellen Risiken (Rz 3)

Stellungnahmen

Die SBVg bittet um Klärung, ob es sich bei dem genannten „Verlust“ rein um einen finanziellen Verlust handelt oder auch um Auswirkungen in anderen Dimensionen, bspw. Auswirkungen auf die Reputation. Unklar sei auch, ob Rechts- und Reputationsrisiken als eigenständige Risikokategorien zu behandeln seien oder als Schadensdimensionen (Auswirkungen). In ersterem Fall bittet die SBVg um eine Abgrenzung der Rechtsrisiken von den *Compliance*-Risiken. Diese Abgrenzung ist auch für den VSKB wichtig, da der Erläuterungsbericht (S. 10–11) hierzu als widersprüchlich empfunden wird. Ausserdem bittet die SBVg um eine Abgrenzung zu den ESG- und insbesondere Klimarisiken. Die EXPERTsuisse erachtet eine blosse Wiederholung der Definition der operationellen Risiken aus Art. 89 ERV als nicht ausreichend und schlägt vor, dass die Definition expliziter ausgeführt wird, so unter anderem durch expliziten Einschluss der *Compliance*-Risiken.

Auch die Raiffeisen Schweiz bittet um weitere Details zur Definition und genaueren Abgrenzungen sowie um die Klärung der Frage, ob Fälle mit Bezug auf Rechts- oder *Compliance*-Risiken mit einer möglichen Reputationsauswirkung von den operationellen Risiken auszuschliessen sind. Sie wünscht zusätzlich eine exemplarische Aufzählung aller operationellen Risiken (darunter insbesondere auch der *Tax*-Risiken), die Einbettung der Ausführungen zum grenzüberschreitenden Dienstleistungsverkehr in die Beschreibung der *Compliance*-Risiken sowie eine Klarstellung dazu, welche Risiken von der Risikokontrolle und welche von der *Compliance*-Funktion zu überwachen sind, da letztere nach dem FINMA-Rundschreiben 2017/1 „*Corporate Governance* – Banken“ jährlich die *Compliance*-Risiken einschätzen soll.

Würdigung

Die FINMA stützt sich grundsätzlich auf die Basler Standards und hat daher in der Anhörungsvorlage exakt deren Definition der operationellen Risiken übernommen. Diese Definition basiert auf den Basler Standards für die Bestimmung der Eigenmittelanforderungen. Daher bezieht sie sich historisch gesehen rein auf finanzielle Verluste. Die Reputationsrisiken wurden historisch gesehen in Bezug auf Eigenmittelanforderungen ausgeschlossen, da sie schwierig zu quantifizieren sind. Dieser Ausschluss bedeutet jedoch nicht, dass im Management der operationellen Risiken Ereignisse aufgrund operationeller Risiken auszuschliessen sind, sobald sie möglicherweise negative Auswirkungen auf die Reputation haben. Die FINMA begrüsst und unterstützt, dass sich das Management der operationellen Risiken weiterentwickelt hat und nebst finanziellen Auswirkungen auch andere Schadensdimensionen zur Beurteilung der operationellen Risiken verwendet werden, so

bspw. Auswirkungen auf die Reputation, Auswirkungen auf die Kundinnen und Kunden oder den Markt oder regulatorische Auswirkungen (bspw. mögliche Aufsichtsmassnahmen, Verlust der Banklizenz).

Aus Sicht der FINMA ist der Bezug auf den finanziellen Verlust nach wie vor sinnvoll, da auch andere Schadensdimensionen wiederum in finanziellen Verlusten resultieren können, wenn auch möglicherweise auf eine indirekte Art. Selbst wenn bspw. die Auswirkungen einer Cyber-Attacke nicht direkt gut quantifizierbar sind, so kann es dennoch zu einem Vertrauensverlust der Kundinnen und Kunden kommen, der in Umsatzeinbussen resultiert. Auch andere negative Auswirkungen auf die Reputation und/oder der Verlust von Kundinnen und Kunden können letztendlich in Umsatzeinbussen resultieren.

Aus Sicht der FINMA ist es nicht zielführend, eine Kategorisierung der operationellen Risiken und scharfe Abgrenzungen zwischen Rechtsrisiken und *Compliance*-Risiken vorzudefinieren oder spezifische Risikotypen (wie *Tax*-Risiken) genauestens zu definieren. Den Instituten ist hier Freiheit und Flexibilität gegeben, die Kategorisierung passend nach ihren Bedürfnissen zu definieren (vgl. Proportionalitätsprinzip). Wichtig ist aus Sicht der Aufsicht letztendlich, dass alle relevanten operationellen Risiken gemäss einer definierten Kategorisierung erfasst wurden und die gewählte Kategorisierung konsequent und konsistent angewendet wird. Für das Management der operationellen Risiken kann sich die gewählte Kategorisierung an öffentlich verfügbaren Referenztaxonomien orientieren, muss sie aber nicht. ESG- bzw. Klima- und Nachhaltigkeitsrisiken sollten nicht konsequent von den operationellen Risiken ausgeschlossen werden, da ein starker Konnex zwischen physischen Risiken oder auch Risiken als Teil von Transformationsprojekten und den operationellen Risiken besteht. Auch hier steht es dem Institut frei, seine Kategorisierung und Kategorisierungskriterien selbst zu wählen.

Unter *Compliance*-Risiko versteht man grob gesagt das Risiko, dass Gesetze, Regeln und Weisungen nicht eingehalten werden. Diese Art von Risiko wird, wie im FINMA-RS 17/1 definiert, von der *Compliance*-Funktion überwacht, die auch eine jährliche, unabhängige Einschätzung vornimmt. Sofern das *Compliance*-Risiko auch als operationelles Risiko fungieren kann, soll eine Integration bzw. ein Informationsfluss ins Management der operationellen Risiken stattfinden.

Fazit

Die Definition der operationellen Risiken wird angepasst, um den Bezug zu finanziellen Verlusten klarzustellen, sowie die Relevanz der Berücksichtigung auch anderer Schadensdimensionen im Management der operationellen Risiken hervorzuheben.

3.3.2 Definition der kritischen Daten (Rz 7)

Stellungnahmen

Die SBVg, der VSKB, die IIAS, die Raiffeisen Schweiz und eine weitere Eingabe sehen die Definition der kritischen Daten aus der Anhörungsvorlage als zu weit gefasst an. Laut SBVg und dem VSKB soll die Definition geschärft werden, damit nicht quasi alle Daten darunterfallen. Unklar für die SBVg ist auch, ob mit Daten nur elektronische oder auch physische Daten gemeint sind. Verschiedene der in der Anhörungsvorlage erwähnten Daten seien bereits durch das Datenschutzgesetz (Personendaten), das Strafgesetzbuch (Geschäftsgeheimnisse) oder das Bankkundengeheimnis nach Art. 47 BankG geschützt. Deshalb wird eine zusätzliche Regulierung durch die FINMA als weder sinnvoll noch nötig empfunden. Jedes Institut solle selbst in Anwendung von vernünftigem Ermessen unter Würdigung seiner konkreten Verhältnisse entscheiden, zwischen welchen Datensätzen risikoadäquat zu unterscheiden ist. Die IIAS bittet um eine Präzisierung der Definition, damit für die Revision klarer sei, was geprüft werden soll. Der Raiffeisen Schweiz ist insbesondere der Passus „Daten, die für regulatorische Zwecke aufbewahrt werden müssen" zu allgemein formuliert. Das Prinzip der Wesentlichkeit solle auch bei diesen Daten gelten. Eine weitere Eingabe bemerkt, dass die breite Definition der kritischen Daten aufgrund der Rz 68 dazu führen würde, dass ein sehr breites Monitoring ausgerollt werden müsse, welches unverhältnismässig und nicht notwendig sei, um die Ziele des Rundschreibens zu erfüllen. Auch wird die Inventarisierung nach Rz 45 als sehr breit kritisiert.

Die Credit Suisse schlägt vor, dass die Definition der kritischen Daten sich auf einen „angemessenen Schutz" statt auf einen „besonderen Schutz" beziehen soll. Auch sollten die Begriffe „Personendaten" und „Geschäftsgeheimnisse" in Einklang mit dem Datenschutzgesetz, bzw. dem Strafgesetzbuch definiert werden. Die EXPERTsuisse schlägt vor, dass die Vertraulichkeit, Integrität und Verfügbarkeit zusätzlich durch die Rückverfolgbarkeit ergänzt werden. Eine weitere Eingabe bittet darum, dass nur die Daten, die zur Erbringung kritischer Funktionen relevant sind, als „kritische Daten" gelten.

Würdigung

Es ist darauf hinzuweisen, dass die Verwendung des Begriffs „kritischer Daten" nicht grundsätzlich neu ist. So verwendet das FINMA-RS 08/21 bereits den Begriff „kritische und/oder sensitive Daten" in den Rz 135.3, 135.7, 135.8 und 135.12, in denen es um die Technologieinfrastruktur und den Schutz der Verfügbarkeit, Integrität und Vertraulichkeit der „kritischen und/oder sensitiven Daten" geht. Für das neue Rundschreiben ist der Begriff der „kritischen Daten" grundsätzlich gleich zu verstehen wie die im FINMA-RS 08/21 genannten „kri-

tischen und/oder sensitiven Daten“. So wurde aus Sicht der FINMA die Definition aus der Anhörungsvorlage von den Anhörungsteilnehmenden als breiter interpretiert als sie angedacht ist. Daher präzisiert die FINMA die Definition der kritischen Daten mit dem Fokus auf Wesentlichkeit entlang der eingegangenen Formulierungsvorschläge. Kritische Daten sind Daten, die ein Institut – in eigenem Ermessen – als wesentlich erachtet. Dabei sind sowohl elektronische als auch physische Daten gemeint. Es ist denkbar, dass ein Institut keine physischen Daten als kritisch erachtet.

Die FINMA wird jedoch im Rahmen der Aufsichtstätigkeiten nicht akzeptieren, dass ein Institut keine seiner Daten als kritisch einschätzt. Eine solche Einschätzung wird voraussichtlich als unrealistisch und mit ungenügendem Risikomanagement einhergehend angesehen werden. Auch sind die bereits durch Gesetze abgedeckten Daten (wie Personendaten nach dem Datenschutzgesetz, Geschäftsgeheimnisse nach dem Strafgesetzbuch oder Bankkundengeheimnisse nach dem Bankengesetz) nicht konsequent auszuschliessen. Die erwähnten Gesetzgebungen und das neue Rundschreiben verfolgen unterschiedliche Ziele, insbesondere da es beim neuen Rundschreiben um das Risikomanagement geht. Der Fokus des neuen Rundschreibens auf das Management der Risiken hinsichtlich kritischer Daten trägt den sich rasch veränderten Marktbedingungen, insbesondere der fortschreitenden Digitalisierung und internationalen *Practices* Rechnung.

Eine Einschränkung der kritischen Daten auf nur diejenigen Daten, die zur Erbringung der kritischen Funktionen (im Sinne der Sicherstellung der operationellen Resilienz) notwendig sind, sieht die FINMA als zu einschränkend an; siehe hierzu auch Kapitel 3.11.1. Einen konkreten Einbezug der „Rückverfolgbarkeit“ als zusätzliches Ziel sieht die FINMA in Bezug auf ihre Aufsichtserwartungen jedoch als zu weitgehend an, wobei den Instituten es natürlich freisteht, dieses zusätzlich zu integrieren.

Fazit

Die Definition der kritischen Daten und insbesondere der Fokus auf Wesentlichkeit werden präzisiert.

3.3.3 Begriffe zum BCM (Rz 8–10, 12, 13), zur operationellen Resilienz (Rz 14–16), und deren Abgrenzung voneinander

Stellungnahmen

Die IIAS wünscht eine Präzisierung des Begriffs „kritische Prozesse“ (Rz 8) und schlägt vor, zusätzlich den Begriff der *Business Impact Analysis* im Kapitel II zu definieren. Eine weitere Eingabe bittet um eine Verengung der Definition der kritischen Prozesse, da das Erreichen der Geschäftsziele als Grundlage für die Definition zu breit sei. Stattdessen solle es bei den kritischen Prozessen um die Aufrechterhaltung des Betriebs gehen.

Die SBVg merkt an, dass der Begriff „wesentliche Unterbrechung“ aus Rz 9 bisher nicht gebräuchlich gewesen sei und eine Lesart zulasse, gemäss der die Institute bei einer solchen Unterbrechung neu im operativen Modus (Notfallstufe) und nicht im klassisch definierten BCM-Umfeld (strategisch, Krisenstufe) agieren müssten, was zu grossen Auswirkungen auf die bisherigen Aufgaben, Kompetenzen und Verantwortlichkeiten führen könne. Auch solle der Begriff „wesentlich“ mittels einer risikogerechten Abstufung geklärt werden. Weiter bringt die SBVg an, dass die Abgrenzung oder Abhängigkeit der RTO (Rz 10) sowie der in der Anhörungsvorlage nicht genannten *Maximum Period of Downtime* (MPDT) zur Unterbrechungstoleranz (Rz 15) zu klären sei.

Laut EXPERTsuisse sollen die *Disaster Recovery Plans* (Rz 12) auch Drittparteien und kritische Daten berücksichtigen, die zur Erreichung der Wiederherstellungsziele benötigt würden.

In Bezug auf die Definition der Krisensituationen (Rz 13) weisen die SBVg, der VSKB und die Credit Suisse auf die Bedeutung des Anhangs B der *Empfehlungen für das Business Continuity Management (BCM)* der SBVg vom August 2013 hin. Dieser Anhang zeige den Unterschied zwischen Krisen und Störungen auf und sei in der Anhörungsvorlage nicht berücksichtigt worden. Die Unterscheidung sei insbesondere relevant, um Lieferanten zu einem Krisenmanagement statt nur einem Störungsmanagement (*Incident Management*) verpflichten zu können. Auch soll eine Krisensituation nicht von der Art der Bewältigung abhängig gemacht werden, sondern von der Art der Bedrohung.

Laut SBVg sollten die in der Definition der kritischen Funktionen (Rz 14) aufgeführten Ressourcen nicht auf einer Ebene neben den Aktivitäten, Prozessen und Dienstleistungen genannt werden, da sie nicht Teil der kritischen Funktion an sich, sondern für deren Erbringung benötigt würden. Auch solle die Definition der operationellen Resilienz klarer vom BCM, dem *IT Service Continuity Management* (ITSCM) und der *IT Security* (beide in der Anhörungsvorlage nicht genannt) abgegrenzt werden, sowie die Abhängigkeiten aufgezeigt werden. Es sei nicht klar, wie bei der operationellen Resilienz die „schwerwiegenden, aber plausiblen Szenarien“ hineinspielten (Rz 83). Die ausführlicheren Erläuterungen dazu im Erläuterungsbericht (S. 24 f.) sollten besser im Rundschreiben reflektiert werden. Auch sollten die schwerwiegenden, aber plausiblen Szenarien zwischen SNB und FINMA abgestimmt sein.

Würdigung

Die Rz 76 beinhaltet bereits den Kern einer *Business Impact Analysis*, sodass eine zusätzliche, explizite Definition duplizierenden Charakter hätte. Die Definition des Begriffs der „kritischen Prozesse“ wird revidiert und eingegrenzt, sodass nun nicht mehr die Geschäftsziele, sondern die Verbindung zu den kritischen Funktionen im Vordergrund steht. So werden die kritischen

Prozesse als diejenigen angesehen, welche für die Erbringung kritischer Funktionen wesentlich sind. Hintergrund bei der Unterscheidung der kritischen Prozesse von den kritischen Funktionen ist die Erwartung, dass sich kritische Funktionen voraussichtlich meist aus mehreren Prozessen und allenfalls komplementär auch noch aus anderen Aktivitäten oder Dienstleistungen zusammensetzen (welche ein Institut möglicherweise nicht als „Prozess" bezeichnet). Bei kleineren Instituten mit geringer Komplexität kann es vorkommen, dass eine kritische Funktion genau nur einem kritischen Prozess entspricht.

Der Vergleich zwischen der RTO und der Unterbrechungstoleranz im Erläuterungsbericht wird in den Erläuterungen gelöscht, da er aufgrund der eingegangenen Stellungnahmen als nicht zielführend eingeschätzt wird. Die *Maximum Period of Downtime* (MPDT) wird bewusst weiterhin nicht eingeführt, da dieser Begriff nicht zwingend und allerorts ein integraler Bestandteil des BCM ist. Den Beaufsichtigten steht es frei, diesen Begriff zu verwenden. Beim Definieren der Unterbrechungstoleranz geht es darum, zu entscheiden, ab welchem Punkt negative Auswirkungen des Ausfalls einer kritischen Funktion nicht mehr tolerierbar sind.

Laut Rz 80 der Anhörungsvorlage gibt der DRP Auskunft über die „externen Abhängigkeiten". Darin enthalten sind die Abhängigkeiten zu Drittparteien. Die Rz 46 der Anhörungsvorlage präzisiert, dass angemessene Back-up-Prozesse und Wiederherstellungsprozesse implementiert werden. Darin enthalten sind die Back-up-Anforderungen an die kritischen Daten. Die FINMA sieht hier daher eine explizitere Nennung der Drittparteien und der kritischen Daten als nicht notwendig.

Die FINMA anerkennt die Bedeutung des Unterschieds zwischen Störungen und Krisen und passt die Definition der Krisensituationen entlang der Vorschläge der SBVg, des VSKB und der Credit Suisse an. Auch wird der Begriff „wesentliche Unterbrechung" durch „bedeutende Störung" ersetzt. Die Definition der kritischen Funktionen wird entsprechend dem Vorschlag der SBVg angepasst.

Die Begriffe des ITSCM und der *IT Security* werden bewusst nicht explizit eingeführt. Es handelt sich hierbei um *Frameworks*, deren Nutzung selbstverständlich nicht durch das Rundschreiben verhindert werden soll. Das Rundschreiben hat nicht den Anspruch, ein umfassendes Rahmenwerk inklusive aller verfügbaren *Best Practices* zu sein. Stattdessen soll es auf so einfache Art wie möglich die Mindesterwartungen der Aufsicht widerspiegeln, wobei bei der detaillierten Ausgestaltung das Proportionalitätsprinzip gilt und somit eine gewisse Flexibilität zugelassen wird, je nach Grösse, Komplexität, Struktur und Risikoprofil des Instituts. Das ITSCM unterstützt die Erbringung der *IT Services* und somit das BCM, welches wiederum seinerseits die operationelle Resilienz unterstützt. Die *IT Security* hingegen un-

terstützt das Management der Cyber-Risiken oder kann als Teil davon angesehen werden. Ein robustes Management der Cyber-Risiken unterstützt die operationelle Resilienz des Instituts. Die Abgrenzung zwischen dem BCM und der operationellen Resilienz wird durch Anpassungen bzw. Ergänzungen der jeweiligen Definitionen klarer herausgearbeitet.

Die schwerwiegenden, aber plausiblen Szenarien werden nicht von der FINMA vordefiniert. Wo gemeinsame Aufsichtstätigkeiten mit der SNB bestehen, besteht eine enge Koordination zwischen FINMA und SNB, als Teil derer auch die Sicherstellung der operationellen Resilienz überwacht werden wird.

Fazit

Die Definitionen der Krisensituationen und der kritischen Funktionen werden entlang der eingegangenen Vorschläge angepasst. Auch wird die Definition der kritischen Prozesse eingegrenzt, sodass neu ihre Verbindung zu den kritischen Funktionen im Vordergrund steht. Die Abgrenzung zwischen dem BCM und der operationellen Resilienz wird durch Anpassungen und Ergänzungen der jeweiligen Begriffsdefinitionen klarer herausgearbeitet. Von einer zusätzlichen, expliziten Definition der *Business Impact Analyse*, einer Anpassung der Definition des DRP und expliziten Nennungen der MPDT, des ITSCM und der *IT Security* wird abgesehen.

3.4 Oberleitungsorgan und Geschäftsleitung (Rz 21–23, 35, 39, 53, 59–60, 75, 89)

Stellungnahmen

Die SBVg merkt an, dass gewisse Aufgaben und Kompetenzen, die dem Oberleitungsorgan und der Geschäftsleitung übertragen werden, als zu detailliert und daher nicht stufengerecht erscheinen würden. Insbesondere die wiederkehrende Wortwahl „implementieren“ solle ersetzt werden, bspw. durch „sicherstellen“. Es sei weiterhin nicht klar, ob das Oberleitungsorgan alle operationellen Risiken oder nur die „Top-Risiken“ verabschieden solle. Der Clientis AG sind die Kapitel zum Management der IKT-Risiken, dem BCM und der operationellen Resilienz bezüglich *Governance* und Prozesse zu detailliert geregelt.

Laut der IIAS fehle eine Präzisierung der Rolle des Oberleitungsorgans in Bezug auf die (wesentlichen und nicht-wesentlichen) Auslagerungen. Das FINMA-Rundschreiben 2018/3 „Outsourcing“ sei hierzu nicht ausreichend ausführlich und auch die Anhörungsvorlage behandle diese Thematik nicht. Die IIAS empfiehlt daher zusätzlich eine Revision des FINMA-RS 18/3.

Würdigung

In Sachen *Governance* bezweckt das neue Rundschreiben, die Erwartungen an das Oberleitungsorgan und die Geschäftsleitung in Bezug auf das Management der operationellen Risiken und neu auch der Sicherstellung der operationellen Resilienz zu präzisieren. Die Notwendigkeit dieser Präzisierungen ergibt sich aus den Erfahrungswerten der FINMA, da es Fälle gibt, in denen das Oberleitungsorgan und die Geschäftsleitung ihre Pflichten nicht im erwarteten Ausmass wahrnehmen und das Bewusstsein für ihre Verantwortung in diesem Teilgebiet des institutsweiten Risikomanagements fehlt.

Zwecks besserer Übersichtlichkeit konsolidiert die FINMA neu die bisher einzeln aufgeführten aber sich überlappenden Erwartungen an das Oberleitungsorgan und die Geschäftsleitung in wenigen Randziffern zu Beginn des Kapitels zum Management der operationellen Risiken. Nur sehr spezifische Erwartungen in Bezug auf die jeweiligen Themenbereiche verbleiben in den entsprechenden Unterkapiteln. Auch die jeweiligen Texte wurden revidiert, um mehr Klarheit über die Erwartungen zu schaffen. Das Wort „implementieren“ wird wie vorgeschlagen durch „sicherstellen“ ersetzt.

Bezüglich den von der IIAS genannten Entscheiden über die Auslagerungen geht die FINMA davon aus, dass sie Teil der vom Oberleitungsorgan zu genehmigenden Strategien sind. Mindestens in der Strategie für die IKT ist zu erwarten, dass sie Entscheide zu Auslagerungen enthält. Aber auch für die Strategien zu den Cyber-Risiken, den kritischen Daten und dem BCM können Entscheide zu Auslagerungen relevant sein. Auch geht die FINMA davon aus, dass die mit Auslagerungen verbundenen Risiken als Teil des Managements der operationellen Risiken identifiziert, beurteilt, begrenzt und überwacht werden. Somit sollten sie in der vom Oberleitungsorgan zu genehmigenden Risikotoleranz berücksichtigt werden. Ein mögliches Resultat eines Entscheids über die Risikotoleranz ist, dass das Oberleitungsorgan die mit einer Auslagerung assoziierten Risiken nicht zu tragen bereit ist und daher den strategischen Entscheid trifft, auf die Auslagerung zu verzichten.

Fazit

Die Randziffern zu den Erwartungen an das Oberleitungsorgan und die Geschäftsleitung werden revidiert sowie konsolidiert, wo sinnvoll. Eine Revision des FINMA-RS 18/3 ist derzeit nicht geplant.

3.5 Management der operationellen Risiken

3.5.1 Risikotoleranz für operationelle Risiken (Rz 22, 31)

Stellungnahmen

Die SBVg weist darauf hin, dass eine Überwachung der Risikotoleranz für operationelle Risiken im Bereich der inhärenten Risiken insbesondere im Bereich der Cyber-Risiken als schwer umsetzbar erscheine. Sie empfiehlt daher die Prüfung alternativer Ansätze, welche bspw. auf Strategien zum Umgang mit entsprechenden Risiken abstellten. Die Credit Suisse merkt an, dass Kontrollindikatoren nicht dazu verwendet werden könnten, inhärente Risiken zu bemessen. Dies könnten nur Risikoindikatoren.

Laut EXPERTsuisse herrscht bei vielen Instituten Unklarheit über die Begrifflichkeiten „Risikotoleranz“ und „Risikoappetit“. Sie empfiehlt, neu nur den Begriff des „Risikoappetits“ zu verwenden und diesen ausdrücklich zu definieren. Aufgrund der von ihr beobachteten Unsicherheiten in der Umsetzung empfiehlt sie zudem die Einführung einer erläuternden Fussnote zur Risikotoleranz in Bezug auf inhärente Risiken.

Würdigung

Der Begriff der „Risikotoleranz“ stammt aus dem FINMA-RS 17/1. Das neue Rundschreiben legt die zu berücksichtigenden Aspekte der Risikotoleranz im Bereich der operationellen Risiken dar. In der Praxis wenden die Beaufsichtigten häufig zusätzliche Begrifflichkeiten an, bspw. Risikoappetit und Risikokapazität. Die FINMA ist offen gegenüber der Verwendung anderer Begrifflichkeiten oder der detaillierteren Ausgestaltung, solange das zugrundeliegende Konzept abgedeckt ist. Daher sieht sie von einer Umbenennung des Begriffes „Risikotoleranz“ oder der Einführung weiterer damit verwandter Begriffe ab.

Im Bereich der Cyber-Risiken merkt die FINMA an, dass die Überwachung des inhärenten Risikos möglich ist, etwa durch die Überwachung von *Threat Intelligence* und der Bedrohungslage oder weitere Überlegungen dazu, wo erhöhte inhärente Risiken bestehen (bspw. bei den über das Internet erreichbaren IT-Systemen). Die FINMA stimmt der Credit Suisse zu, dass zur Bemessung der inhärenten Risiken nur Risikoindikatoren sinnvoll sind, während für die Bemessung von residualen Risiken sowohl Risiko- als auch Kontrollindikatoren verwendet werden können. Basierend auf Erfahrungswerten aus Vor-Ort-Kontrollen stimmt die FINMA ausserdem der Einschätzung der EXPERTsuisse zu, dass häufig Unsicherheiten in der Umsetzung der Risikotoleranz in Bezug auf die inhärenten Risiken bestehen und sich hierzu weitere Präzisierungen lohnen.

Fazit

Die Rz 31 wird angepasst und eine Fussnote ergänzt.

3.5.2 Weitergehende Anforderungen durch die FINMA (Rz 24)

Stellungnahmen

Die SBVg und der VSKB schlagen eine Ergänzung der Rz 24 vor. Diese Randziffer solle nun laut SBVg und VSKB so ergänzt werden, dass die FINMA weitergehende Anforderungen definiert, falls „zur Steuerung einer für das Institut einschneidenden Risikolage notwendig". Dies, da sie derzeit offen und allgemein formuliert sei und der FINMA einen zu grossen Handlungsspielraum gäbe. Laut Raiffeisen Schweiz soll die Randziffer angeben, dass die FINMA sich dabei auf bestehenden gesetzlichen oder regulatorischen Anforderungen basiert.

Würdigung

Die Rz 24 der Anhörungsvorlage besteht bereits sinngemäss im aktuellen FINMA-RS 08/21 (Rz 138) im Kontext der operationellen Risiken mit weitreichender Tragweite. Laut dieser Randziffer definiert die FINMA im Rahmen der laufenden Aufsicht für spezifische Themen weitergehende Anforderungen an das Management der operationellen Risiken, falls notwendig. Dies geschieht zurückhaltend und unter Anwendung des Proportionalitätsprinzips. Erfahrungsgemäss wird diese Rz extrem selten angewendet und nur aufgrund sehr hoher operationeller Risiken, deren Management als ungenügend eingeschätzt wird. Die seitens SBVg und VSKB vorgeschlagene Formulierung wirft aus Sicht der FINMA möglicherweise zusätzliche Fragen nach der Definition einer „einschneidenden Risikolage" auf. So gab es im Rahmen der Anhörung vielfach Wünsche nach genaueren Definitionen von Begriffen, bspw. der Begriffe „Risikogehalt" oder „Aktivitäten". Die seitens Raiffeisen Schweiz vorgeschlagene Formulierung ist selbstverständlich, sodass sie aus Sicht der FINMA keinen Mehrwert bringt. Daher sieht die FINMA von den vorgeschlagenen Ergänzungen ab.

Fazit

Die Rz 24 wird unverändert beibehalten.

3.5.3 Unabhängige Beurteilung der Schlüsselkontrollen (Rz 28)

Stellungnahmen

Die SBVg, der VSKB, die Credit Suisse, die EXPERTsuisse und die IIAS merken an, dass der Begriff der Unabhängigkeit in Bezug auf die „unabhängige" Beurteilung der Effektivität der Schlüsselkontrollen weiter auszuführen

sei. Insbesondere stellen sie Fragen dazu, ob i) die unabhängige Beurteilung durch ein Teammitglied oder den Linienvorgesetzten durchgeführt werden dürfte oder durch eine separate Abteilung innerhalb der ersten Verteidigungslinie, ob ii) die Unabhängigkeit sich auf die zweite und dritte Verteidigungslinie beziehe oder nur auf eine der beiden Verteidigungslinien.

Weiter bringt die EXPERTsuisse an, dass die Ergebnisse der unabhängigen Beurteilung nachvollziehbar dokumentiert und allfällig identifizierte Schwachstellen zeitnah adressiert werden sollten.

Würdigung

Es ist darauf hinzuweisen, dass die risikotragenden Einheiten (die sogenannte erste Verteidigungslinie, darunter insbesondere die ertragsorientierten Geschäftseinheiten) jeweils für die Sicherstellung der Effektivität der Schlüsselkontrollen zu den von ihnen eingegangenen operationellen Risiken verantwortlich sind und geeignete Massnahmen (wie bspw. die strukturierte Beurteilung der Effektivität der Schlüsselkontrollen) dafür ergreifen müssen.

Im Sinne der *Revisions to the Principles for the Sound Management of Operational Risks*[2] des *Basel Committee on Banking Supervision*, an denen sich das neue Rundschreiben orientiert, präzisiert die FINMA, dass es sich bei der in Rz 28 genannten „unabhängigen" Beurteilung um eine Beurteilung durch die unabhängigen Kontrollinstanzen nach FINMA-RS 17/1 handeln soll. Dies bedeutet, dass die unabhängige Beurteilung durch die Risikokontrolle und/oder die *Compliance*-Funktion durchgeführt wird, bzw. – wo vorhanden – durch die Einheit, die die Risikokontrolle und die *Compliance*-Funktion vereint.

Basierend auf Erfahrungswerten aus Vor-Ort-Kontrollen stimmt die FINMA mit EXPERTsuisse überein, dass die unabhängigen Beurteilungen nachvollziehbar dokumentiert werden sollen. Ohne angemessene Dokumentation sind die Einschätzungen zur Effektivität der Schlüsselkontrollen nicht nachweisbar und nachvollziehbar, welches zu einer Infragestellung der Effektivität des internen Kontrollsystems führen kann.

Die FINMA sieht jedoch entgegen der Empfehlung von EXPERTsuisse davon ab, zu präzisieren, dass allfällig identifizierte Schwachstellen zeitnah adressiert werden sollen. Solche Schwachstellen müssen erkannt und trans-

[2] https://www.bis.org/bcbs/publ/d515.pdf; siehe insbesondere Rz 10 "*A functionally independent CORF is typically the second line of defence. The responsibilities of an effective second line of defence should include: a) developing an independent view regarding business units' […] (ii) design and effectiveness of key controls, […]*", wobei es sich beim genannten CORF um eine "Compliance and Operational Risk Function" handelt (siehe Fussnote 6 "*In addition to an independent Operational Risk Management function, the second line of defense also typically includes a Compliance function.*").

parent kommuniziert werden (Rz 33), jedoch kann eine der möglichen Antworten darauf auch die ausdrückliche Akzeptanz des daraus entstehenden Risikos sein.

Fazit

Der erste Satz der Rz 28 der Anhörungsvorlage wird angepasst.

3.5.4 Weitere Stellungnahmen zum Management der operationellen Risiken

Stellungnahmen

Die EXPERTsuisse schlägt vor, dass die mit dem BCM und der operationellen Resilienz verbundenen Risiken ebenfalls als Teil des Managements der operationellen Risiken berücksichtigt werden sollen (Rz 21). Der SBVg bleibt unklar, ob die Kategorisierung der operationellen Risiken nach Rz 25 eindeutig bleibt und die Rapportierung entlang dieser Kategorisierung verlaufen muss.

Laut EXPERTsuisse sei es notwendig, dass die Risiken „formell und nachvollziehbar" beurteilt würden (Rz 26). Cyber-Angriffe sollten als ein Beispiel möglicher externer Faktoren aufgeführt werden (Fussnote 5). Der Raiffeisen Schweiz ist der Unterschied zwischen Prüfergebnissen und Kontrollbeurteilungen nicht klar (Rz 27), da es das Ziel einer Prüfung sei, die Angemessenheit und Wirksamkeit einer Kontrolle zu beurteilen. Sie empfiehlt die Zusammenfassung der beiden Begriffe.

Für den VSKB ist der Begriff „Aktivitäten" in Rz 29 nicht nachvollziehbar, er solle abschliessend definiert werden. Die EXPERTsuisse merkt zu dieser Randziffer an, dass ad-hoc Risiko- und Kontrollbeurteilungen vor der Vornahme wesentlicher Änderungen durchgeführt werden und anschliessend neue Kontroll- und Minderungsmassnahmen implementiert werden sollen. Für den VSKB ist weiterhin der Begriff „Risikogehalt" aus Rz 30 nicht klar definiert und solle durch „Risiko" ersetzt werden.

Der VSKB weist darauf hin, dass die in Rz 32 erwähnte Berichterstattung der Risikokontrolle zu wesentlichen Prüfergebnissen nicht angemessen sei und mit den Vorgaben aus FINMA-RS 17/1 zur Würdigung der Revisionsberichte durch das Oberleitungsorgan zu einer Duplikation führen würde. Die Raiffeisen Schweiz empfiehlt das Löschen der Berichterstattungspflicht auf Stufe der Geschäfts- oder Organisationsbereiche (Rz 34), da die Verantwortlichkeiten auf Stufe der Geschäftsleitung festgelegt würden.

Würdigung

Die FINMA erachtet die Vorschläge der EXPERTsuisse als zielführend, und übernimmt diese (Rz 21, 26, 29). So auch die Vorschläge des VSKB zu Rz 30 und 32.

Die operationellen Risiken sollten jeweils eindeutig den Kategorien der Kategorisierung nach Rz 25 zugewiesen werden können, anhand eines vom Institut definierten Vorgehens bzw. anhand von vom Institut definierten Kriterien. Die gewählte Kategorisierung soll konsistent in allen Komponenten des Managements der operationellen Risiken angewendet werden, d.h. auch in der Berichterstattung über die operationellen Risiken.

Die Risiko- und Kontrollbeurteilungen (Rz 27) unterscheiden sich klar von Prüfungen. Risiko- und Kontrollbeurteilungen werden von den risikotragenden (inkl. den ertragsorientierten) Geschäfts- und Organisationseinheiten durchgeführt für die operationellen Risiken, welche für die jeweilige Einheit relevant sind. Prüfungen werden von der internen Revision, der externen Prüfgesellschaft oder sonstigen unabhängigen Parteien durchgeführt und umfassen ein oder mehrere spezifische, im Voraus zu definierende Themengebiete.

Aufgrund der Vielfalt der vom neuen Rundschreiben betroffenen Beaufsichtigten und ihrer Geschäftsmodelle sieht die FINMA davon ab, den Begriff „Aktivitäten“ (Rz 29) genauer zu definieren. Eine genauere Definition wäre zwangsläufig zu eng und könnte der Heterogenität der Beaufsichtigten nicht gerecht werden.

Die Berichterstattung auf Stufe der Geschäfts- oder Organisationsbereiche (Rz 34) ist vor allem für Institute von hoher Komplexität und mit einer Gruppenstruktur relevant. Die FINMA schränkt diese Randziffer daher auf die systemrelevanten Banken ein, wobei sich das Proportionalitätsprinzip– wie auf alle Randziffern des Rundschreibens – auch auf diese Randziffer anwendet.

Fazit

Die Rz 21, 26, 29, 30 und 32 werden auf Basis der eingegangenen Formulierungsvorschläge angepasst. Die Rz 25 zur Kategorisierung bleibt unverändert bestehen, jedoch wird Rz 32 zur Berichterstattung ergänzt, um die Verwendung der Kategorisierung in der Berichterstattung klar zu stellen. Die Rz 34 wird auf systemrelevante Banken beschränkt in Abhängigkeit ihrer Komplexität und Struktur. Die Rz 27 bleibt unverändert bestehen.

3.6 Management der IKT-Risiken

Stellungnahmen

Die EXPERTsuisse empfiehlt in der Rz 35 die Ergänzung, dass die Geschäftsleitung ausreichende Ressourcen sicherstellen müsse zwecks Erreichung der IKT-Strategie. Die Raiffeisen Schweiz fragt in Bezug auf das Management der IKT-Risiken in Rz 36 (aber auch mit Verweis auf das Management der Cyber-Risiken), ob zusätzliche Anforderungen zur Überwachung und insbesondere Berichterstattung vorzunehmen sind, wenn die gesamten IKT-Prozesse ausgelagert sind.

Für die SBVg und den VSKB ist die Erwartung an die Berücksichtigung neuer technologischer Entwicklungen in der Rz 37 unklar. Die EXPERTsuisse schlägt in dieser Randziffer vor, konkrete international anerkannte Standards zu benennen, bspw. COSO und COBIT, während die Raiffeisen Schweiz empfiehlt, statt „Best Practices" von „Good Practices" zu sprechen, da es sich hierbei üblicherweise um gute Branchenstandards handle und nicht alle Institute mittels „Best Practices" mit den Besten mithalten müssten.

Die SBVg und der VSKB hinterfragen die Formulierung von Rz 43 in Bezug auf die Trennungen der Umgebungen für die Entwicklung, das Testen und die Produktion als zu pauschal und zu wenig risikoorientiert. Die EXPERTsuisse empfiehlt, nur die Trennung zur Produktion sicherzustellen, um Entwicklungsmethoden wie DevOps zu berücksichtigen. Auch zu mehreren anderen Randziffern gibt sie Anpassungsvorschläge.

Die SBVg und der VSKB merken an, dass der Begriff „Schutzbedürfnis" aus Rz 47 neu sei und nicht klar sei, wie er sich von der Risikotoleranz abgrenze. Auch der Begriff der „Schutzmassnahmen" aus Rz 55 sei neu.

Für ein effektives Management der operationellen Risiken, inklusive der IKT-Risiken, empfiehlt die AWS den Instituten, ein institutsweites, holistisches Verständnis ihrer Geschäftsaktivitäten und ihrer jeweiligen Priorisierungen aufzustellen, inklusive der dazu benötigten Personen, Prozesse, und Technologien.

Würdigung

Die FINMA erachtet die Forderung nach ausreichenden Ressourcen bereits durch die Rz 41 der Anhörungsvorlage als ausreichend abgedeckt. Die Rz 36 stellt den Rahmen des Managements der IKT-Risiken und adressiert sowohl die IKT- und Cyber-Risiken wie auch Technologie-Risiken, die in Verbindung mit Externalisierungen (*Outsourcing*) stehen. Diesbezüglich soll eine regelmässige Berichterstattung an die Geschäftsleitung hinsichtlich der Entwicklung der IKT-Risiken, Massnahmen und Kontrollen sowie Ereignisse erfolgen. In dieser Hinsicht betrachtet die FINMA eine jährliche Frequenz als

Minimum. Eine höhere Frequenz (bspw. quartalsweise) liegt im Ermessen des Instituts.

Die Idee der Rz 37 ist, dass die mit neuen technologischen Entwicklungen einhergehenden Risiken in der Risikobetrachtung und im IKS der Institute reflektiert werden müssen. Von einer expliziten Nennung international anerkannter Standards und Best (bzw. Good) Practices im Rundschreiben wird abgesehen. Breit bekannt und anerkannt sind insbesondere COBIT, ITIL, COSO und diverse ISO-Standards. Die Begrifflichkeit international anerkannter „Practices“ wird übernommen.

Die Idee der Rz 43 (Trennung der Umgebungen) ist, dass ungeachtet der Verbreitung agiler Entwicklungsmethoden (bspw. DevOps und CI/CD - *Continuous Implementation – Continuous Deployment* Modelle) jedoch weiterhin eine klare Trennung zwischen den IKT-Umgebungen für die Entwicklung, das Testen und die IKT-Produktion notwendig ist. Dies umfasst, soweit möglich, eine eindeutige Zuweisung von Aufgaben, Funktionen und Verantwortlichkeiten und eine Regelung der damit einhergehenden Zugangsberechtigungen. Es muss sichergestellt werden, dass die Entwickler und Tester von Codes bzw. von neuen oder angepassten Teilen von Software diese nicht eigenständig in die Produktionsumgebung freigeben dürfen. Hierbei handelt es sich um eine grundlegende Präventivkontrolle zum Schutz des Betriebs. Die Randziffer wird dementsprechend angepasst. Auch die anderen Anpassungsvorschläge der EXPERTsuisse werden übernommen, soweit sie die Klarheit der betroffenen Randziffern aus Sicht der FINMA verbessern.

In Rz 47 wird der Begriff „Schutzbedürfnis“ gelöscht, da seine Nennung nicht absolut notwendig ist. Es geht dabei um die Aspekte „Vertraulichkeit, Integrität und Verfügbarkeit“. Die „Schutzmassnahmen“ in Rz 55 werden beibehalten und benötigen aus Sicht der FINMA keine weitergehende Definition.

Fazit

Die grundsätzlichen Erwartungen an die Strategie, *Governance* und Stärkung des Bewusstseins in Bezug auf die IKT werden neu zusammengefasst im Kapitel zum übergreifenden Management der operationellen Risiken. Dies betrifft die Rz 35–36 und 38–40 der Anhörungsvorlage. Die Rz 37, 42–43, und 45–48 werden auf Basis der eingegangenen Rückmeldungen angepasst, soweit die Kommentare begründet bzw. relevant sind. Die Rz 41 wird entsprechend erweitert und präzisiert („Trennung der Umgebungen“).

3.7 Management der Cyber-Risiken

Stellungnahmen

Die Clientis AG wünscht sich eine Zusammenlegung der Kapitel „Management der IKT Risiken“ und „Management der Cyber-Risiken“, da diese beiden Themen viele Überschneidungen hätten.

Für die drei ersten Randziffern im Management der Cyber-Risiken wünscht sich die IIAS eine klarere Regelung der Rollen und Zuständigkeiten für das Oberleitungsorgan für den Umgang mit Cyber-Risiken sowie eine Harmonisierung mit den anderen Kapiteln im Rundschreiben. Für die Rz 54 fordert die SIX eine mindestens quartalsweise Berichterstattung an die Geschäftsleitung anstatt einer mindestens jährlichen.

In Bezug auf die Fussnote 8 der Rz 55 wird von der SBVg und dem VSKB gefordert, dass die Definition einer Cyber-Attacke auf Angriffe von extern nach intern, bspw. durch das Überwinden des Perimeters, eingegrenzt wird. Die EXPERTsuisse wünscht sich eine explizitere Aussage, ob Angriffe durch Mitarbeitende von intern ebenfalls in die Definition einer Cyber-Attacke fallen.

Die EXPERTsuisse schlägt für die Rz 55 Bst. a vor, dass nicht von Bedrohungspotentialen gesprochen wird, sondern von Risiken.

Für die Rz 55 Bst. b schlägt die EXPERTsuisse vor, die Implementation angemessener Schutzmassnahmen nicht nur auf kritische Prozesse zu beschränken, sondern ebenfalls Systeme und Daten aufzuführen. Die SIX schlägt vor, neben den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit ebenfalls noch die Verbindlichkeit/Nichtabstreitbarkeit (sog. *Non-repudiation*) hinzuzufügen.

Der VSKB sieht in der Aufzählung unter Rz 55 Bst. c betreffend die vollumfängliche Überwachung der IKT eine Verletzung des Proportionalitätsprinzips und dem Risikoansatz. Die SIX merkt weiter an, dass in derselben Randziffer die Erkennung und Aufzeichnung in der logischen Abfolge verdreht seien.

Die in der Rz 56 präzisierte Meldepflicht zu Cyber-Attacken nach FINMAG wünscht sich der VSKB zentralisiert für alle Behördenstellen. Eine weitere Eingabe schlägt hier vor, den expliziten Verweis auf den FINMAG-Artikel über die Meldepflicht zu streichen.

Die SBVg, die Raiffeisen Schweiz, die EXPERTsuisse sowie eine weitere Eingabe fordern eine Präzisierung zu den szenariobasierten Cyber-Übungen in Rz 58. Die Formulierung erlaube die Interpretation, dass diese Übungen im selben Umfang wie Verwundbarkeitsanalysen und Penetrationstests

durchgeführt werden müssten. Ebenfalls für die Rz 58 fordert die SBVg eine klarere Abgrenzung, wie weit der von der FINMA neu präzisierte Mindestumfang für Verwundbarkeitsanalysen und Penetrationstests für vom Internet erreichbare IT-Systeme gehen soll

Die AWS hebt hervor, dass bei ihren Dienstleistungen die Verantwortlichkeiten mit ihren Kundinnen und Kunden geteilt werden (*shared responsibility model*). So seien die Kundinnen und Kunden verantwortlich für die Sicherheit innerhalb der AWS-*Cloud*, d. h. die Sicherheit der darin enthaltenen Inhalte, Applikationen, Systeme und Netzwerke. Die AWS hingegen sei verantwortlich für die Sicherheit der *Cloud* selbst, d. h. sie schütze die zugrundeliegende Infrastruktur und gewährleiste die Performance der Dienstleistungen.

Würdigung

Die grundsätzlichen Erwartungen an die Strategie, die *Governance* und die Stärkung des Bewusstseins in Bezug auf die Cyber-Risiken werden neu zusammengefasst im Kapitel zum übergreifenden Management der operationellen Risiken.

Auf den Änderungswunsch des SBVg und des VSKB, Insiderbedrohungen explizit auszuschliessen, wird nicht eingegangen. Angriffe auf die IKT und kritische Daten durch die Ausnutzung von Schwachstellen oder Umgehung von Schutzmassnahmen können auch von innerhalb des Perimeters gestartet werden. Solche Angriffe sollen ebenfalls durch geeignete Mittel und technische Kontrollen entdeckt werden können. Die Fussnote wurde aufgrund der eingegangenen Rückmeldung etwas präzisiert.

In Rz 55 Bst. a geht es darum, dass Institute zuerst die allgemeine Bedrohungslage analysieren (bspw. durch bekannt gewordene Cyber-Attacken auf andere Unternehmen und die dabei verwendeten Angriffswerkzeuge bzw. ausgenutzten Schwachstellen) und danach die Bedrohungspotentiale für das eigene Institut ableiten (*Threat Intelligence*). Erst danach können die institutsspezifischen Risiken identifiziert werden, falls zum Beispiel ein Asset mit entsprechender Verwundbarkeit im Inventar aufgeführt ist.

Infolge der Rückmeldung der EXPERTsuisse wird Rz 55 Bst. b leicht angepasst. Die Rückmeldung der SIX, neben Cyber-Attacken auf die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von kritischen Daten und IT-Systemen ebenfalls die Nichtabstreitbarkeit zu ergänzen, wird als nicht zielführend erachtet. Durch Angriffe auf die Nichtabstreitbarkeit kann nicht mehr garantiert werden, dass der Urheber Informationen erstellt bzw. diese versendet hat. Die FINMA stimmt überein, dass die Nichtabstreitbarkeit sehr wichtig ist im Bereich der Informationssicherheit. Sie wird jedoch im Kontext der Cyber-Risiken bzw. Attacken bereits durch den Punkt Integrität abgedeckt.

Die Rückmeldung des VSKB zum Umfang der zu überwachenden Systeme in Rz 55 Bst. c kann nachvollzogen werden. „Vollumfänglich“ wird ersetzt durch „durchgängig“, mit einem Verweis auf die inventarisierten Bestandteile der IKT. Das Feedback der SIX über die Reihenfolge des Ablaufs der Detektion wird ebenfalls übernommen.

Die in Rz 56 beschriebene Meldepflicht wurde von der FINMA-Aufsichtsmitteilung 05/2020 übernommen, welche wiederum den Wesentlichkeitscharakter und die Unverzüglichkeit für den Cyber-Kontext gemäss den Anforderungen in Art 29 Absatz 2 FINMAG präzisiert. Seit der Veröffentlichung der Aufsichtsmitteilung haben andere Behörden ebenfalls angekündigt, dass sie die Einführung einer Meldepflicht für kritische Infrastrukturen planen. Die entsprechende Gesetzesvorlage ist aktuell in der Ausarbeitung. Sobald der Gesetzestext zur Meldepflicht final definiert ist, wird die FINMA prüfen ob und wie, unter Berücksichtigung des Amtsgeheimnisses gemäss FINMAG, ein behördenübergreifendes zentrales Eingangsfenster für Cyber-Attacken Meldungen umsetzbar ist. Aufgrund der weiteren Eingabe wird der Verweis auf den entsprechenden Artikel und Abschnitt im FINMAG entfernt.

Die Rz 58 ist eine Folgeaktivität der Rz 55 Bst. a. Sobald die Institute Ihre Bedrohungspotentiale für das eigene Institut ermittelt haben, geht es darum, zu analysieren, welche Auswirkungen diese auf das eigene Institut haben. Der Abschnitt zu den szenariobasierten Cyber-Übungen wurde aufgrund der Rückmeldungen in eine eigene Randziffer verschoben um den Grundsatz der Risikobasiertheit beizubehalten. Verwundbarkeitsanalysen und Penetrationstests sollen weiterhin regelmässig auf den mindestens spezifizierten Applikationen, Systemen oder Schnittstellen durchgeführt werden. Auf eine detailliertere Erläuterung zum Mindestumfang für Verwundbarkeitsanalysen und Penetrationstests für genutzte Drittservices (wie bspw. Twitter) wird im Erläuterungsbericht eingegangen.

Fazit

Die grundsätzlichen Erwartungen an die Strategie, *Governance* und Stärkung des Bewusstseins in Bezug auf die Cyber-Risiken werden neu zusammengefasst im Kapitel zum übergreifenden Management der operationellen Risiken. Dies betrifft Rz 48, 49 und 52 der Anhörungsvorlage. Die Fussnote 8, welche die Definition einer Cyber-Attacke umfasst, wird präzisiert. Der Umfang für die Überwachung der IKT wird in Rz 55 Bst. c angepasst. In Rz 51 wird der FINMAG-Verweis gestrichen. Ausserdem werden die Anforderungen an die szenariobezogenen Cyber-Übungen aus der Rz 53 herausgelöst und in eine eigene Randziffer verschoben. Der Mindestumfang für Verwundbarkeitsanalysen und Penetrationstests wird präzisiert.

3.8 Management der Risiken kritischer Daten

Stellungnahmen

Laut der Clientis AG soll das Management der Risiken kritischer Daten sich konsequent an die neue Datenschutzgesetzgebung ausrichten und, wo immer möglich, darauf verweisen. Die EXPERTsuisse bittet um Klarheit, ob die in Rz 59 genannte Datenstrategie durch das Oberleitungsorgan zu erlassen sei, während die IIAS darauf hinweist, dass die Rolle des Oberleitungsorgans in Bezug auf das Management der Risiken kritischer Daten auch genannt werden solle.

Die SBVg merkt an, dass die unabhängige Kontrollfunktion aus Rz 60 nicht selbst dafür verantwortlich sein soll, die genannten Rahmenbedingungen zu schaffen und aufrecht zu erhalten. Auch stellen die SBVg und eine weitere Eingabe die Frage, ob es sich dabei um eine der zwei unabhängigen Kontrollinstanzen nach FINMA-RS 17/1 handle (d. h. die Risikokontrolle oder die *Compliance*-Funktion). Die SBVg und der VSKB fragen nach der Bedeutung des Begriffs „Kritikalitätsstufe“ in Rz 61 und ob damit gemeint sei, dass kritische Daten noch in Subkategorien eingeteilt werden müssten.

Laut SBVg könne die Verfügbarkeit und Integrität von Daten (bspw. Kontostand, Kreditbetrag) davon abhängig sein, ob sich diese Daten in einem kritischen Bereich der Bank (bspw. Kernbankensystem) befänden und so nur für einen Moment ihres Lebenszyklus als kritisch einzustufen seien. Daher mache die in Rz 62 genannte Verwaltung dieser Daten über den gesamten Lebenszyklus keinen Sinn. Da nicht klar sei, was mit einer vollständigen Datenstrategie gemeint sei, solle das Wort „vollständig“ gestrichen werden.

Die SBVg und der VSKB regen an, den Begriff der „Echtdaten“ aus Rz 64 abschliessend zu definieren oder alternativ von „Daten in Testumgebungen“ zu sprechen. Die Credit Suisse schlägt vor, hier von einem „angemessenen Schutz“ zu sprechen statt nur von „Schutz“, während die EXPERTsuisse vorschlägt, deutlicher hervorzuheben, dass Rz 64 auch im Normalbetrieb gelte. Die SBVg bemängelt, dass Rz 66 eine *Role Based Access Control* vorschreibe, die nicht immer das optimale Modell für die Zugriffsverwaltung sei. Stattdessen sollen die Prinzipien des *Need-to-know* und *Least Privilege* vorgeschrieben werden.

Die SBVg bittet um Löschung der Rz 67, da das Erfordernis betreffend den Schutz kritischer Daten, die im Ausland gespeichert werden, sich bereits aus den Rz 59 und 63 der Anhörungsvorlage ergebe und auch auf das FINMA-RS 18/3 verwiesen werden könne. Die Credit Suisse empfiehlt, dass in dieser Randziffer von einem „angemessenen“ statt „besonderen“ Schutz die Rede sein soll und dass der Begriff „erhöhte Risiken“ genauer umrissen werde soll. Die SIX bittet um Klarstellung, was mit „besonderem Schutz“ gemeint ist, dies auch in Rz 65.

In Rz 68 ist es der SBVg nicht abschliessend klar, wen die genannte Liste betreffe und wie das Element „Anwender mit funktionalem Zugriff auf eine grosse Menge an kritischen Daten“ als mögliches Element zur Qualifizierung als Person mit erhöhten Privilegien zu interpretieren sei. Die EXPERTsuisse weist darauf hin, dass der in Rz 70 genannte Begriff des Bearbeitens der Daten bereits in Art. 3 Bst. e des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (SR 235.1) definiert sei. Ein Ausschluss dieser Randziffer für die Institute nach Art. 47*a*–47*e* ERV, Personen gemäss Art. 1*b* BankG, sowie nicht-kontoführende Wertpapierhäuser widerspräche aus Sicht der EXPERTsuisse ausserdem der Anforderung nach einer Überwachung der Dienstleister nach Rz 24 FINMA-RS 18/3, da es sich bei Zugriffen externer Dienstleister auf kritische Daten voraussichtlich häufig um Auslagerungen wesentlicher Funktionen handle.

Würdigung

Die FINMA ist nicht zuständig, die Tragweite und Anwendung des Datenschutzrechts zu bestimmen. Die Aufsicht im Bereich des Datenschutzrechts obliegt dem zuständigen Datenschutzbeauftragten. Beim neuen Rundschreiben handelt es sich dementsprechend nicht um Präzisierungen der Datenschutzgesetzgebung. Diese ist unabhängig vom Rundschreiben zu beachten, so wie andere Gesetze auch. Das Rundschreiben befasst sich mit dem Management der Risiken, die sich in Bezug auf den Umgang mit Daten ergeben, mit Fokus einerseits auf sogenannte „kritische Daten“ zwecks Eingrenzung und anderseits auf die Wesentlichkeit. Daher wird das Rundschreiben weder an die Datenschutzgesetzgebung angepasst noch auf diese verwiesen. Die Rolle des Oberleitungsorgans wird neu unter dem Kapitel zum übergreifenden Management der operationellen Risiken behandelt, dies insbesondere auch in Bezug auf die Datenstrategie und das Management der Risiken kritischer Daten.

Die Positionierung der unabhängigen Einheit als Kontrollfunktion aus Rz 60 ist dem Institut überlassen, so wie dies bereits im Anhang 3 des FINMA-RS 08/21 in Bezug auf elektronische Kundendaten der Fall war. Auch die Formulierung der Rz 60 wurde aus diesem Anhang übernommen, wird nun jedoch abgeändert. Bei der in Rz 61 genannten Kritikalitätsstufe geht es darum, dass die Daten hinsichtlich ihrer Kritikalität gegenüber den drei Aspekten „Vertraulichkeit“, „Integrität“, inklusive Rückverfolgbarkeit („Non-repudiation“), und/oder „Verfügbarkeit“ eingestuft werden. Hier sind auch detailliertere Abstufungen der Kritikalität möglich bzw. je nach Grösse, Komplexität, Struktur und Risikoprofil des Instituts sinnvoll, aber nicht zwangsläufig für jedes Institut notwendig (vgl. Proportionalitätsprinzip). Der Bezug zur „Vertraulichkeitsstufe“ wird gelöscht, da die Kritikalität bzw. Kritikalitätsstufe diese umfasst.

Aus der Sicht der FINMA sind Daten, die vom Institut als „kritisch“ definiert, während ihres gesamten Lebenszyklus kritisch und müssen entsprechend ge-

schützt werden. Zum Beispiel werden kritische Kontodaten über den gesamten Lebenszyklus (von der Entstehung, über Verarbeitung bis hin zur Löschung) kritisch bleiben. Der FINMA ist wichtig, dass Institute ihre kritischen Daten als solche definieren und diese über ihren Lebenszyklus (Lebensdauer) entsprechend überwachen.

Die „Echtdaten“ aus Rz 64 werden entsprechend dem Vorschlag der SBVg und des VSKB „Daten“ ersetzt. Auch die Vorschläge der Credit Suisse und der EXPERTsuisse werden in dieser Randziffer übernommen. Die Rz 66 wird angepasst, damit nicht auf eine *Role Based Access Control* beschränkt werden muss.

In Rz 67 wird der Bezug zum Ausland beibehalten, da er sich nicht klar genug aus den anderen Randziffern ergibt und nicht nur im *Outsourcing*-Fall relevant ist, sodass ein Verweis auf FINMA-RS 18/3 hier aus Sicht der FINMA nicht ausreicht. In den Rz 7, 65 und 67 wurde der Begriff *besonders* anstatt *angemessen* bewusst ausgewählt, um den speziellen Schutz dieser Daten hervorzuheben. Somit wird mit Nachdruck zum Ausdruck gebracht, dass ein höherer Schutz als bei anderen nicht-kritischen Daten sichergestellt werden muss. Die Institute müssen ihre Ressourcen sinnvoll einsetzen und dafür sorgen, dass ihre kritischen Daten durch besondere Massnahmen wie privilegierte Zugangsregelungen, Einhaltung des *Need-to-Know*-Prinzips sowie Datenverschlüsselung gesichert werden. Die Institute müssen ein geeignetes Zugriffsmodell implementieren, welches die Einhaltung der Prinzipien *Need-to-Know* und *Least Privilege* ermöglicht. Die darin hinterlegten Zugriffsrechte müssen regelmässig überprüft werden.

Die Vorschläge der EXPERTsuisse in Bezug auf das Bearbeiten der kritischen Daten in der Rz 70 werden übernommen.

Fazit

Die grundsätzlichen Erwartungen an die Strategie, *Governance* und Stärkung des Bewusstseins in Bezug auf die kritischen Daten werden neu zusammengefasst im Kapitel zum übergreifenden Management der operationellen Risiken. Dies betrifft Rz 59 der Anhörungsvorlage. Rz 60 wird angepasst, um klarzustellen, dass die Positionierung der genannten Einheit dem Institut überlassen wird. Rz 61 und 64–70 werden auf Basis der eingegangenen Formulierungsvorschläge angepasst.

3.9 Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft

Stellungnahmen

Die IIAS merkt an, dass die Rolle des Oberleitungsorgans in diesen Anforderungen nicht präzisiert werde. Jedoch würde sich die Erwähnung einiger zusätzlicher Aspekte lohnen, so insbesondere die Risikoanalyse, das Festlegen des Perimeters des geografischen Tätigkeitsbereichs und die Berichterstattung der Geschäftsleitung an das Oberleitungsorgan. Die Credit Suisse empfiehlt, dass in Rz 72 statt von einer „vertieften" Analyse von einer „angemessenen" Analyse die Rede ist.

Die SBVg stellt fest, dass nach Ablauf der einschlägigen Übergangsfristen sowohl Banken als auch unabhängige Vermögensverwalter (UVV) jeweils als vollumfänglich lizenzierte und beaufsichtigte Finanzinstitute operieren würden. Die Depotbanken hätten jeweils nur Einblick in einen Teil der Aktivitäten der UVV. Infolgedessen hätten sie in gewissen Bereichen keine Möglichkeit, die Vollständigkeit und Plausibilität der gelieferten Informationen zu überprüfen. Sie würden somit Informationen dazu benötigen, welche Prüfungen die neuen Aufsichtsorganisationen bezüglich der Einhaltung der sich aus dem Finanzdienstleistungsgesetz vom 15. Juni 2018 (SR 950.1) sowie dem Finanzinstitutsgesetz vom 15. Juni 2018 (SR 954.1) ergebenden Verpflichtungen der UVV vornehmen werden. Diese Angaben würden in die künftige Ausgestaltung der Bewirtschaftung der Risiken aus den Geschäftsbeziehungen mit UVV einfliessen. Die SBVg erwartet, dass eine Abgrenzung der Verantwortlichkeiten der Depotbanken gegenüber denjenigen der UVV und ihren eigenen Aufsichtsorganisationen und der FINMA gemacht wird. Diesbezüglich sei ein Austausch mit der FINMA aufgegleist worden.

Würdigung

Die FINMA erwartet, dass die Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft Teil der Entscheide des Oberleitungsorgans zur Risikotoleranz sind. Auch sollten sie Teil der Risiko- und Kontrollbeurteilungen sein, deren Resultate dem Oberleitungsorgan vorgelegt werden. Ein mögliches Resultat eines Entscheids des Oberleitungsorgans zur Risikotoleranz ist, dass es nicht mehr dazu bereit ist, die Risiken zu tragen, die sich aus den Tätigkeiten des Instituts in einem bestimmten Land ergeben, und daher den strategischen Entscheid fällt, die geografische Präsenz des Instituts zu verändern. Die FINMA erachtet deshalb eine explizite Nennung der Rolle des Oberleitungsorgans in diesem Unterkapitel zum Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft als nicht notwendig.

Hingegen hat sich gezeigt, dass dem Satz "Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Institute ausländisches Aufsichtsrecht

einhalten" neben den generellen Ausführungen zu den aufsichtsrechtlichen Anforderungen an das Management der Rechtsrisiken aus dem grenzüberschreitenden Dienstleistungsgeschäft keine eigenständige Bedeutung zukommt. Er ergibt sich bereits aus den generellen Anforderungen an das Management der Rechtsrisiken und kann daher gestrichen werden. Der Massstab zur Beurteilung einer Verletzung von schweizerischem Aufsichtsrecht infolge Nichteinhaltung ausländischen Rechts orientiert sich also weiterhin an den generellen Anforderungen, wie sie dem Kapitel F und den Anforderungen an die Gewähr für eine einwandfreie Geschäftstätigkeit zu entnehmen sind. Eine Streichung des erwähnten Satzes bewirkt also keine materiell-regulatorische Änderung.

In Bezug auf die Stellungnahme der SBVg besteht – wie bereits von der SBVg erwähnt – ein laufender Dialog mit der FINMA. Auf Basis der Anhörung sieht die FINMA keinen Anpassungsbedarf der Randziffern zum grenzüberschreitenden Dienstleistungsgeschäft.

Fazit

Der Satz "Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Institute ausländisches Aufsichtsrecht einhalten" wird gestrichen. Die übrigen Randziffern zum Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft bleiben unverändert.

3.10 *Business Continuity Management*

Stellungnahmen

Laut SBVg soll neben dem Begriff „Test“ jeweils auch der Begriff „Übung“ genannt werden, da manche Überprüfungen nur in Form von bspw. *Table-Top*-Übungen vorgenommen werden könnten.

Ausserdem merken die SBVg und der VSKB an, dass jährliche Tests (bzw. Übungen) einen zu hohen Aufwand darstellten (Rz 84). Stattdessen sollen diese regelmässig risikobasiert durchgeführt werden und ihre Frequenz somit mit der regelmässigen Berichterstattung nach Rz 87 abgestimmt sein. Die IIAS empfiehlt hingegen, auch für die Genehmigung der BCM-Strategie (Rz 75) und die Berichterstattung (Rz 87) eine fixe Mindestfrequenz zu definieren.

Die SBVg merkt ferner an, dass nach ihrem Verständnis „schwerwiegende, aber plausible Szenarien“ ein Abgrenzungsmerkmal zwischen dem BCM und der operationellen Resilienz darstellten. Daher sollten Tests im BCM nicht auf solche Szenarien bezogen werden (Rz 86).

Die SBVg und eine weitere Eingabe interpretieren die Rz 80 so, dass es nur einen DRP pro Institut geben dürfe. Es solle stattdessen für grössere Institute auch möglich sein, mehrere DRPs zu definieren. Die EXPERTsuisse empfiehlt, in Rz 80 von ausgelagerten „kritischen Prozessen" zu sprechen statt von ausgelagerten „Teilen der Technologieinfrastruktur". Sie empfiehlt ausserdem eine Präzisierung der Rz 79, nach der die *Business Impact Analyse* (BIA) und der *Business Continuity Plan* (BCP) klar auch dann ad hoc zu aktualisieren sind, wenn es zu wesentlichen Änderungen kommt.

Laut Clientis AG sollte das Kapitel konsequent dem FINMA-RS 18/3 angeglichen werden. Wenn immer möglich, sollte auf das FINMA-RS 18/3 verwiesen werden, statt zusätzliche Regelungen zu erlassen, so insbesondere in Bezug auf Rz 80. Dem Umstand, dass die Banken der Kategorien 3 bis 5 die Mehrheit ihrer Infrastruktur und zahlreiche kritische Prozesse an externe Dienstleister ausgelagert hätten, sollte Rechnung getragen werden.

Würdigung

Aus Sicht der FINMA beinhaltet der Begriff „Tests" auch „Übungen", insbesondere auch *Table-Top*-Übungen, *Desktop Reviews* und *Walkthroughs*. Dies reflektiert die Rz 83 der Anhörungsvorlage („Es können verschiedene Vorgehen zum Testen von unterschiedlicher Intensität und Effektivität gewählt werden."). Für mehr Klarheit führt sie gemäss dem Wunsch der SBVg den Begriff der „Übungen" jedoch zusätzlich ein, integriert ihn jedoch nach wie vor unter den „Tests".

Die *Empfehlungen für das Business Continuity Management (BCM)* der SBVg vom August 2013 enthielten bereits die Empfehlung, dass die wichtigsten Massnahmen und die Krisenorganisation mindestens einmal jährlich getestet werden. Die entsprechend formulierte Rz 84 der Anhörungsvorlage entspricht somit dem Status Quo. Jedoch wird sie nur auf die Institute der Kategorien 1–3 angewendet, sodass kleinere Institute hier mehr Flexibilität haben. Die Häufigkeit der Genehmigung der Strategie für das BCM und die Berichterstattung wird an die anderen Themenbereiche (IKT, Cyber-Risiken, Risiken kritischer Daten) angeglichen. Zwecks Angleichung wird auch die Definition der BCM-Strategie gestrichen.

Da das BCM eine wichtige Komponente zur Unterstützung der operationellen Resilienz bildet, ist es aus Sicht der FINMA sachlogisch und zielführend, sich bereits im BCM mit den schwerwiegenden, aber plausiblen Szenarien auseinanderzusetzen.

Die FINMA sieht es als selbstverständlich an, dass es auch mehrere DRPs geben kann, je nach Grösse, Komplexität und Struktur des Instituts. Zur Klarstellung definiert sie jedoch in Rz 80 neu, dass es „mindestens einen DRP" geben soll. Wichtig bei der Verwendung mehrerer DRPs ist, dass

diese sich zu einer ausreichenden und in sich stimmigen Abdeckung zusammenfügen. Bspw. soll es nicht zu Konflikten zwischen den in verschiedenen DRPs festgehaltenen Wiederherstellungsprozessen kommen. Auch sollen keine wichtigen Komponenten verloren gehen, weil einzelne Organisationseinheiten jeweils nur „ihre“ Wiederherstellungsprozesse beachten, aber insgesamt keine Gesamtsicht über das Institut besteht. Auch die Anpassungsvorschläge der EXPERTsuisse für die Rz 79–80 werden übernommen.

In Bezug auf Auslagerungen nennt das FINMA-RS 18/3 die grundsätzlichen Erwartungen. Im neuen Rundschreiben werden Präzisierungen in Bezug auf das BCM inklusive dem DRP vorgenommen, die nicht mit derselben Klarheit bereits im FINMA-RS 18/3 enthalten sind und gemäss Erfahrungswerten auch häufig übersehen werden. Daher erachtet die FINMA einen expliziten Verweis auf externe Abhängigkeiten nach wie vor als wertvoll.

Fazit

Die grundsätzlichen Erwartungen an die Strategie, die *Governance* und die Stärkung des Bewusstseins in Bezug auf das BCM werden neu zusammengefasst im Kapitel zum übergreifenden Management der operationellen Risiken. Der Begriff der „Übungen“ wird als ein Beispiel von Tests der Umsetzung des BCP und DRP eingeführt. Die Mindestfrequenz für das Testen kritischer Prozesse bei den Kategorie 1–3 Instituten wird beibehalten. Die Genehmigung der Strategie für das BCM soll regelmässig eingeholt werden, die Berichterstattung soll mindestens jährlich erfolgen. Die Behandlung der schwerwiegenden, aber plausiblen Szenarien im BCM wird beibehalten. Es wird klargestellt, dass es mindestens einen DRP geben soll, d.h. dass es auch mehrere geben darf. Es wird präzisiert, dass die BIA, BCP und DRP mindestens jährlich, aber auch ad hoc bei wesentlichen Änderungen überprüft und wo nötig, aktualisiert werden. Die Behandlung von vereinzelten Auslagerungsthemen wird beibehalten.

3.11 Operationelle Resilienz und Anhang 1

3.11.1 Abgrenzungen und Abhängigkeiten (Rz 45, 76, 93–94, sowie FINMA-RS 18/3)

Stellungnahmen

Die SBVg und der VSKB weisen in Bezug auf Rz 89 bzw. 93 darauf hin, dass die BIA nach Rz 76 bereits eine Identifikation von den Ereignissen beinhalte, die Pläne auslösen könne. Weiter zu präzisieren ist gemäss SBVg die Abgrenzung zwischen dem Inventar der kritischen Funktionen (Rz 94) und der Inventarisierung kritischer Daten nach Rz 45.

Eine weitere Eingabe bittet um Klarstellung, ob Auslagerungen, die für die Erbringung kritischer Funktionen relevant sind, automatisch auch unter die

Auslagerungen von wesentlichen Funktionen nach FINMA-RS 18/3 fallen würden. Die Terminologien sollten international gleich sein. Derzeit gäbe es viele verschiedene Begriffe, um Materialität darzustellen, so insbesondere *critical*, *important* und *material*.

Würdigung

Da das BCM die operationelle Resilienz unterstützt, ist es sinnvoll, sich an den in den BIA (Rz 76) gewonnenen Erkenntnissen zu orientieren, bzw. sich darauf zu stützen, wenn es um die Identifikation der Bedrohungen und Verwundbarkeiten der kritischen Funktionen (Rz 93) geht. Jedoch erachtet die FINMA die Beibehaltung beider Randziffern als wertvoll, da es sich dennoch nicht um eine Duplikation handelt. Ferner besteht keine eins-zu-eins Überlappung zwischen der Inventarisierung der Bestandteile der IKT (Rz 45) und dem Inventar der kritischen Funktionen (Rz 94), da die beiden unterschiedliche Zwecke erfüllen. Jedoch geht die FINMA davon aus, dass die Inventarisierung der IKT in der Praxis eine wichtige Quelle von Informationen zum Erstellen des Inventars der kritischen Funktionen ist. In Bezug auf die kritischen Daten sieht die FINMA bewusst davon ab, einen Automatismus zu erstellen, gemäss dem die für kritische Funktionen relevanten Daten automatisch kritische Daten sein müssen oder umgekehrt kritische Daten nur diejenigen Daten sind, die für die Erbringung kritischer Funktionen benötigt werden. Dies wäre kurzsichtig und wichtige Risiken könnten damit aus dem Sichtfeld verschwinden.

Auch sieht die FINMA bewusst davon ab, einen Automatismus herzustellen, nach dem für kritische Funktionen relevante Auslagerungen automatisch auch wesentliche Auslagerungen nach FINMA-RS 18/3 sein müssen. In vielen Fällen wird dies vermutlich so sein, aber es gibt auch Gegenbeispiele. So ist es möglich, dass gewisse Auslagerungen, die im Sinne des FINMA-RS 18/3 tendenziell nicht als Auslagerungen von wesentlichen Funktionen gelten (bspw. physische Geldlieferungen und Geldautomatenversorgung) dennoch relevant zur Erbringung kritischer Funktionen sind (bspw. für den Zahlungsverkehr).

Die FINMA ist offen gegenüber der Verwendung verschiedener Begriffe zur Darstellung der Materialität (kritisch, materiell, signifikant usw.). So ist es bspw. nicht notwendig, dass ein Institut die kritischen Funktionen in seinen Dokumenten unbedingt als „kritische Funktionen“ bezeichnet. Stattdessen sind bspw. auch abweichende Bezeichnungen wie „important business services“ in Ordnung, solange die zugrundeliegenden Konzepte des Rundschreibens damit abgedeckt werden.

Fazit

Die Rz 45, 76 und 93–94 werden nicht zwecks schärferer Abgrenzungen angepasst.

3.11.2 Tests und Bewältigung schwerwiegender, aber plausibler Szenarien

Stellungnahmen

Die SBVg merkt an, dass die Bewältigung länger anhaltender Szenarien (Rz 97) nur mit Vorarbeit und Garantien von Seiten des Staates möglich seien. Je nach Szenario müssten übergeordnete, branchen- bzw. schweizweite Katastrophenpläne ausgelöst werden.

Das Testen längerer Unterbrechungen wird als nicht praktikabel und zielführend angesehen. Es seien niederschwelligere Sensibilisierungsmassnahmen zu wählen. Eine weitere Eingabe merkt an, dass aus Rz 97 möglicherweise eine grosse und nicht mehr handhabbare Anzahl Szenarien hervorgehen könnte.

Die IIAS empfiehlt, für die Tests eine fixe Mindestfrequenz vorzugeben.

Würdigung

Die FINMA anerkennt, dass die Institute nicht für jedes schwerwiegende, aber plausible Szenario in der Lage sind, dieses bewältigen zu können und sich gegebenenfalls die Frage der Notwendigkeit des Einbezugs des Staates stellt (bspw. Pandemien, Kriege, langanhaltende Strommangellage). Die Erwartung der FINMA ist jedoch, dass mindestens Vorarbeiten und Denkarbeiten durchgeführt werden, sowie Massnahmen zur Stärkung der operationellen Resilienz getroffen werden, sodass die Institute so bereit wie möglich für den Fall systemweiter Krisen (welche auch zu den schwerwiegenden, aber plausiblen Szenarien zählen) sind.

Das Testen von längeren Unterbrechungen nach Rz 97 wurde missverstanden. Selbstverständlich sollen für einen Test eines länger anhaltenden Szenarios nicht grundlegende Ressourcen für mehrere Monate tatsächlich abgestellt werden. Das aus dem BCM bekannte Prinzip, dass Tests den Betrieb des Instituts nicht gefährden sollen, gilt nach wie vor. Stattdessen ist hier eine weniger intensive Art an Tests angedacht, etwa eine *Table-Top*-Übung bzw. ein Durchdenken des Szenarios. Entlang solcher Tests soll überlegt werden, inwiefern die benötigten Aktivitäten, Prozesse, Dienstleistungen und Ressourcen anhand der bestehenden Pläne innerhalb der Unterbrechungstoleranz der kritischen Funktion wiederhergestellt werden können bzw. ob sie überhaupt wiederhergestellt werden können. Die Rz 97 wird daher so angepasst, dass sie zusätzlich auch Übungen erwähnt. Auch wird klargestellt, dass es Fälle gibt, in denen die Beihilfe des Staates benötigt wird. Die Szenarien mit den schlimmsten Auswirkungen sind tendenziell diejenigen, die lange anhalten. Daher sieht die FINMA davon ab, die länger anhaltenden Szenarien aus der Rz 97 zu streichen.

Da bei den Tests bzw. Übungen davon ausgegangen wird, dass sie eine gewisse Komplexität beinhalten (insbesondere bei mittleren bis grossen Instituten), sieht die FINMA davon ab, anstelle einer „regelmässigen“ Testfrequenz eine Mindestfrequenz (bspw. jährlich) zu fixieren. Damit soll vermieden werden, dass die Tests aufgrund des hohen Zeitdrucks mit einer ungenügenden Qualität durchgeführt werden.

Fazit

Es wird ergänzt, dass manche Szenarien gegebenenfalls nicht ohne Einbezug des Staates bewältigt werden können (bspw. Pandemien, Kriege, langanhaltende Strommangellage). Für solche Szenarien sind durch das Institut Vorarbeiten zu leisten zwecks Stärkung seiner operationellen Resilienz gegenüber diesen Szenarien im Rahmen seiner Möglichkeiten. Weiter wird präzisiert, dass die Tests auch durch Übungen durchgeführt werden können und die Tests bzw. Übungen so zu gestalten sind, dass sie das Institut nicht grundlegend gefährden.

3.11.3 Weitere Stellungnahmen zur operationellen Resilienz

Der VSKB bittet darum, dass die Banken der Kategorie 3 von der Rz 90 ausgenommen würden oder das Oberleitungsorgan die entsprechende Genehmigung der kritischen Funktionen und Unterbrechungstoleranzen nicht jährlich, sondern periodisch oder bei wesentlichen Veränderungen geben sollten.

Laut Clientis AG sollte das Kapitel mit dem Kapitel zu BCM verschmolzen werden.

Die EXPERTsuisse empfiehlt, in Rz 91 zusätzlich die IKT- und die Cyber-Risiken aufzuführen und die Berichterstattung nach Rz 92 auch bei wesentlichen Änderungen im Geschäftsbetrieb zu fordern.

Die Credit Suisse fragt, ob die in Rz 95 genannten operationellen Risiken und Schlüsselkontrollen sich ausschliesslich auf die Weiterführung der kritischen Funktionen beziehen würden. Eine weitere Eingabe bemerkt, dass die in Rz 96 geforderte Abdeckung der Komponenten der kritischen Funktionen durch BCPs nicht ausreichend sei, um die operationelle Resilienz sicherzustellen.

Die NCC Group empfiehlt, dass *Resilience by Design* einen stärkeren Stellenwert erhalten solle. Insbesondere relevant seien die Forderung nach *Escrow*-Lösungen und die vertragliche Regelung mit Drittanbietern in Bezug auf Testanforderungen sowie Exit-Pläne (insbesondere *Stressed Exit*). Für ein besseres Verständnis von Konzentrations- und Cyber-Risiken solle es mehr Informationsaustausch geben, insbesondere in Bezug auf anonyme

Prüfungen von Outsourcing-Arrangements, Beurteilungen von nicht-wesentlichen Auslagerungen und gescheiterte *Business Continuity*- und *Stressed Exit*-Pläne, vor allem von grösseren Anbietern.

In Bezug auf die Graphiken des Anhang 1 empfiehlt der VSKB einen erläuternden Text hinzuzufügen, während die Clientis AG die Graphiken für wenig aussagekräftig hält und empfiehlt, sie zu löschen.

Würdigung

Aufgrund der Wichtigkeit der Institute der Kategorie 3, ihrer Präsenz und Wirkung im Schweizer Finanzplatz sowie ihrer meist grossen Kundenstämme, erachtet die FINMA die Aufmerksamkeit des Oberleitungsorgans in Bezug auf die kritischen Funktionen als so relevant, dass sie an der jährlichen Genehmigungsfrequenz festhält.

Wie bereits im Erläuterungsbericht aufgeführt, hat die FINMA die Möglichkeit eines Zusammenlegens des BCM und der operationellen Resilienz geprüft, musste diese jedoch verwerfen. Vereinfacht gesagt definiert das BCM die Reaktionen auf Unterbrechungen (reaktiv; auf Unterbrechungen reagierend), während die operationelle Resilienz im Kern auf einen bereits resilienten Aufbau des Betriebsmodells abzielt (präventiv; Unterbrechungen vermeidend). Es handelt sich somit um unterschiedliche Konzepte. Auch würde ein Zusammenlegen falsche Signale senden.

Das Management der IKT-Risiken und die Cyber-Risiken werden gemäss Vorschlag der EXPERTsuisse zur Rz 91 hinzugefügt; jedoch reicht nach Ansicht der FINMA eine jährliche Berichterstattung an das Oberleitungsorgan.

Zur Beantwortung der Frage der Credit Suisse nach den operationellen Risiken der kritischen Funktionen (Rz 95) präzisiert die FINMA, dass es sich um wesentliche operationelle Risiken handeln soll. Jedoch beinhaltet dies nicht nur die Risiken in Bezug auf die Verfügbarkeit. Auch wurde die Definition des Begriffs der operationellen Resilienz angepasst und ergänzt, um klarzustellen, dass für die Sicherstellung der operationellen Resilienz nicht nur BCPs benötigt werden, wie dies durch Rz 96 suggeriert wird.

Der Gedanke der *Resilience by Design* war bereits in der Definition der operationellen Resilienz enthalten, wird nun neu aber noch stärker hervorgehoben. Auch das Thema des *Stressed Exit* enthält explizit Einzug in das Rundschreiben. Unter *Stressed Exit* versteht man den ungeplanten und ungeordneten Wegfall eines Dienstleisters, bspw. aufgrund seiner Insolvenz, aufgrund von Sanktionen oder aufgrund des Ausfalls grundlegender Ressourcen, die der Dienstleister benötigt.

Aufgrund der Anpassungen und Ergänzungen an den Definitionen des BCM und der operationellen Resilienz sieht die FINMA die Graphik I aus Anhang 1 als nicht mehr notwendig an. Daher wird diese gelöscht.

Fazit

An der jährlichen Genehmigungsfrequenz wird festgehalten. Die Sicherstellung der operationellen Resilienz wird nach wie vor in einem separaten Kapitel behandelt. Die Definition der operationellen Resilienz wird angepasst und ergänzt. Die Begriffe *Resilience by Design* und *Stressed Exit* werden im Rundschreiben explizit benannt. Die Graphik I aus dem Anhang 1 wird gelöscht.

3.12 Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken

Stellungnahmen

Die Clientis AG schlägt vor, den Grundsatz 8 zur Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken in den Grundsatz 6 zu BCM zu integrieren.

Würdigung

Beim Grundsatz 8 geht es nur um die systemrelevanten Banken, im Gegensatz zum Grundsatz 6. Abgesehen davon behandeln die zwei Grundsätze auch zwei unterschiedliche Situationen: Wenn die Bank in Abwicklung oder Sanierung ist, so soll sie die systemrelevanten Funktionen in dieser Phase noch erbringen können. Beim BCM geht es hingegen unter anderem darum, abzuwehren, dass es überhaupt zu einer solchen Situation der Abwicklung oder Sanierung kommen wird.

Fazit

Die Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken wird weiterhin separat behandelt.

3.13 Übergangsfristen

Stellungnahmen

Die SBVg, der VSKB, die Clientis AG, EXPERTsuisse, IIAS sowie eine weitere Eingabe schätzen die Übergangsfristen als nicht ausreichend ein.

So empfehlen die SBVg und der VSKB eine Verlängerung der Übergangsfristen für die operationelle Resilienz um ein Jahr sowie eine einjährige

Übergangfrist zu allen restlichen Grundsätzen. IIAS und eine weitere Eingabe empfehlen eine Übergangsfrist von mindestens einem Jahr für das Management der Risiken kritischer Daten, eine weitere Eingabe empfiehlt eine solche zusätzlich für das Management der IKT-Risiken. Die Clientis AG wünscht sich eine flächendeckende Übergangsfrist von zwei Jahren.

Würdigung

Die FINMA anerkennt das Bedürfnis der Stellungnehmenden nach einer Erweiterung der Übergangsfristen. Im Rahmen ihrer Erläuterungen und Wirkungsanalyse hielt die FINMA fest, dass das Rundschreiben für einige der Grundsätze zwar umfangreiche Umformulierungen vornimmt, die zugrundeliegende Aufsichtspraxis sich dadurch jedoch nicht materiell verändert. Dies ist namentlich der Fall beim Management der operationellen Risiken, dem Management der Cyber-Risiken und dem *BCM*. Weiterhin wurden die Grundsätze zum Management der Risiken grenzüberschreitender Dienstleistung sowie zur Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken bis auf unwesentliche sprachliche Anpassungen aus dem FINMA-RS 08/21 übernommen. Auch das Konzept der kritischen Daten ist nicht grundlegend neu, da es bereits Bestandteil des Grundsatzes 4 „Technologieinfrastruktur“ des FINMA-RS 08/21 ist. Dennoch anerkennt die FINMA, dass durch die vorgenommenen Umformulierungen bei den Beaufsichtigten ein vertieftes Abklärungsbedürfnis (bspw. *Gap Assessment* und Schliessung allfälliger Lücken) entstehen kann.

Die Übergangfrist für die operationelle Resilienz wird jedoch nicht von drei auf vier Jahre erweitert, da die drei Jahre in Abstimmung mit den Übergangsfristen der britischen Aufsichtsbehörden definiert wurden.

Fazit

Das Datum des Inkrafttretens des Rundschreibens wird vom 1. Januar 2023 auf den 1. Januar 2024 verschoben, womit auch für die Anforderungen an das Management der operationellen Risiken genügend Umsetzungszeit zur Verfügung steht. Die Übergangsfrist bis zur Sicherstellung der operationellen Resilienz beträgt anschliessend noch zwei Jahre. Diese Frist bleibt also letztlich unverändert.

3.14 Prüfwesen

Stellungnahmen

Laut IIAS sei die graduelle Abdeckung des Managements der IKT-Risiken über vier Jahre, mit einer Prüftiefe im Ermessen der Prüfgesellschaft, nicht optimal und nicht konsistent im Vergleich mit der Abdeckung verwandter Themen, darunter insbesondere das BCM und das Management der Cyber-

Risiken. Sie empfiehlt, die Abdeckung den anderen Themenbereichen des Rundschreibens anzugleichen.

Würdigung

Die graduelle Abdeckung für das Management der IKT-Risiken wurde bewusst gewählt, da es sich um einen grossen und häufig komplexen Themenbereich handelt, dessen vollständige Prüfung innerhalb eines Jahres zumeist nicht möglich ist. Daher wird die Prüfung wie auch bisher über mehrere Jahre verteilt. Basierend auf den Resultaten der Ex-Post Evaluation des FINMA-RS 13/3 kann es jedoch noch zu Anpassungen an den Mehrjahreszyklen kommen.

Fazit

Die Prüfstrategie für das Management der IKT-Risiken wird basierend auf der Anhörung nicht angepasst.

4 Auswirkungen

Die in Erwägung der Anhörungseingaben vorgenommen Präzisierungen an der Vorlage ändern die Einschätzung der im Erläuterungsbericht vorgenommenen Wirkungsanalyse nicht[3].

5 Weiteres Vorgehen

Das totalrevidierte Rundschreiben „Operationelle Risiken und Resilienz – Banken“ tritt am 1. Januar 2024 in Kraft.

Für die Sicherstellung der operationellen Resilienz gelten Übergangsfristen von zwei Jahren ab Inkrafttreten. Die Sicherstellung der operationellen Resilienz soll somit bis 1. Januar 2026 gegeben sein.

Das teilrevidierte FINMA-RS 13/3 „Prüfwesen“ tritt ab 1. Januar 2024 in Kraft.

[3] Betreffend die Auswirkungen siehe Erläuterungsbericht vom 10. Mai 2022, Kapitel 7 “Wirkungsanalyse“, S. 29ff.