Rundschreiben 2023/1 Operationelle Risiken und Resilienz – Banken

Management der operationellen Risiken und Sicherstellung der operationellen Resilienz

Referenz: FINMA-RS 23/1 „Operationelle Risiken und Resilienz – Banken“

Erlass: 7. Dezember 2022
Inkraftsetzung: 1. Januar 2024
Konkordanz: vormals FINMA-RS 08/21 „Operationelle Risiken – Banken“ vom 20. November 2008
Rechtliche Grundlagen: FINMAG Art. 7 Abs. 1 Bst. b und 29 Abs. 1 BankG Art. 1b Abs. 3 Bst. b, Art. 3 Abs. 2 Bst. a und 3f BankV Art. 12 und 14e
FINIG Art. 9 und 49
FINIV Art. 12 und 68
Anhang 1: Erläuternde Graphik zur operationellen Resilienz

FINMA RS OpRisk (Notes)

Erläuterungen

4.1.1 Vorbemerkungen

Das im neuen Rundschreiben beschriebene Management der operationellen Risiken ist Bestandteil des institutsweiten Risikomanagements nach dem FINMA-Rundschreiben 2017/1 „Corporate Governance – Banken“ (FINMA- RS 17/1) und soll sich demnach in das institutsweite Risikomanagement einbetten.

Das Management der operationellen Risiken (Kapitel IV des neuen Rundschreibens) ist übergreifend und umfasst unter anderem die IKT- und Cyber- Risiken, mit kritischen Daten verbundene Risiken, Risiken aus der Ausgestaltung und Implementierung des BCM und die Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft.

Die Erwartungen an das übergreifende Management der operationellen Risiken sind in Kapitel IV Buchstabe A des Rundschreibens dargelegt. Die nachfolgenden Kapitel IV Buchstaben B bis F zu den IKT-Risiken, den Cyber-Risiken, den Risiken kritischer Daten, den Risiken aus der Ausgestaltung und Implementierung des BCM und den Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft geben zusätzliche Konkretisierungen zu den Erwartungen an das Management dieser jeweiligen, spezifischen Risiken. Das neue Rundschreiben hat nicht den Anspruch, jede Art von operationellen Risiken umfassend und im Detail zu behandeln.

Die Anforderungen an die Sicherstellung der operationellen Resilienz sind in Kapitel V geregelt. Während das BCM die spezifische Wiederherstellung des Geschäftsbetriebs bei bedeutenden Störungen oder Unterbrechungen behandelt (d. h., die Reaktion auf solche bedeutenden Störungen oder Unterbrechungen), bezieht sich die operationelle Resilienz auf die strategische Identifikation und Stärkung der für das Institut und den Finanzplatz wichtigsten Funktionen, die sogenannten „kritischen Funktionen“. Hierbei geht es auch darum, den Aufbau des Instituts bzw. seines Betriebsmodells so zu gestalten, dass das Institut widerstandsfähiger gegenüber Unterbrechungen wird. Die operationelle Resilienz baut auf einem robusten Management der operationellen Risiken und dem BCM auf.

Alle Grundsätze der qualitativen Anforderungen des bisherigen FINMA-RS 08/21 wurden überprüft und angepasst. Die Grundsätze 6 (neu Kapitel VI) und 7 (neu Kapitel IV Buchstabe F) wurden dabei nahezu unverändert ins neue Rundschreiben übernommen.

Für das gesamte Rundschreiben gilt das Proportionalitätsprinzip, d. h. die Randziffern sind abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen. Zusätzlich wenden sich einige Randziffern nicht an die Banken und Wertpapierhäuser der FINMA-Kategorien 4 und 5 sowie die Institute im Kleinbankenregime, die Personen nach Art. 1b BankG und die nicht-kontoführenden Wertpapierhäuser. Diese Institute haben also noch mehr Flexibilität bei der Ausgestaltung und Umsetzung.

Da das Rundschreiben prinzipienbasiert und technologieneutral gestaltet ist, geht es bewusst nicht auf die Besonderheiten spezifischer Technologien, wie den Umgang mit Cloud-Auslagerungen, ein.

7.2 Auswirkungen des FINMA-Rundschreibens „Operationelle Risiken und Resilienz – Banken“

Die Art und das Ausmass der Wirkung des neuen Rundschreibens unterscheidet sich je nach angepasstem Themenbereich. Im Folgenden wird pro angepasstem Themenbereich auf die wichtigsten Aspekte eingegangen:

- **Übergreifendes Management der operationellen Risiken**: Die Revision führt nicht zu wesentlichen Anpassungen der Anforderungen. Die Revision zielt darauf ab, den in der Praxis häufig festgestellten Fehlinterpretationen und Mängeln im Zusammenhang mit den bisherigen Grundsätzen 1–3 des FINMA-RS 08/21 entgegenzuwirken. Somit wird ein neu entstehender Implementierungsaufwand als gering und vertretbar eingeschätzt. Durch die Revision wird insbesondere ein klareres Verständnis der Rolle der Risikotoleranz im Bereich der operationellen Risiken und der Wichtigkeit der Effektivität der Kontroll-und Minderungsmassnahmen gefördert.
- **Management der IKT-Risiken**: Dieses Kapitel ersetzt einen Teil des Grundsatzes 4 „Technologieinfrastruktur" des FINMA-RS 08/21 und präzisiert diesen, basierend auf den BCBS-Papieren. Er stellt die wesentlichen Grundlagen einer funktionierenden IKT dar und reflektiert damit die bereits bestehende Aufsichtspraxis der FINMA, die lediglich expliziter ausformuliert wird. Daher wird der Implementierungsaufwand als gering und vertretbar eingeschätzt.
- **Management der Cyber-Risiken**: Die einzige wesentliche Anpassung zum Umgang mit Cyber-Risiken im Vergleich zum FINMA-RS 08/21 (Grundsatz 4) ist die Einführung szenariobasierter Cyber-Übungen als eine der Möglichkeiten zum Schutz der IKT und der kritischen Daten. Auch wurde die Meldung wesentlicher Cyber-Attacken in Abstimmung mit der FINMA-Aufsichtsmitteilung 05/2020 „Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG" aufgenommen. Der Rest der Revision zielt darauf ab, den in der Praxis häufig festgestellten Fehlinterpretationen und Mängeln im Zusammenhang mit FINMA-RS 08/21 entgegenzuwirken. Der Einsatz der szenariobasierten Cyber-Übungen oder der anderen genannten Tests (bspw. Penetrationstests) unterliegt – wie alle andern Randziffern auch – dem Proportionalitätsprinzip. Es ist nicht davon auszugehen, dass jedes Institut alle genannten Tests durchführen sollte. Für grössere, komplexe Institute sind szenariobasierte Cyber- Übungen bereits Bestandteil eines angemessenen Umgangs mit den Cyber-Risiken, während von kleineren Instituten im Rahmen des Proportionalitätsprinzips keine komplexen Übungen erwartet werden. Somit wird ein zusätzlicher Implementierungssaufwand insgesamt als gering eingeschätzt.
- **Management der Risiken kritischer Daten**: Während mit diesem neuen Kapitel auf die Granularität des Anhangs 3 des FINMA-RS 08/21 verzichtet wird, so erweitert es den Umfang der schützenswerten Daten in Abstimmung mit den BCBS-Papieren, weg von nur elektronischen Kundendaten hin zu Daten, die in Bezug auf Vertraulichkeit, Integrität oder Verfügbarkeit als kritisch eingeschätzt werden. Es ist davon auszugehen, dass die Mehrheit der Institute bereits über entsprechende Schutzmassnahmen für ihre kritischen Daten verfügen, auch da diese bereits im bestehenden Grundsatz 4 des FINMA-RS 08/21 verlangt wurden; dennoch kann hier mindestens bei einigen Instituten ein zusätzlicher Implementierungsaufwand entstehen.
- **Business Continuity Management (BCM)**: Dieses Kapitel ist eine prinzipienbasierte, aktualisierte Version der bisherigen SBVg Empfehlungen für das Business Continuity Management (BCM) in Abstimmung mit den BCBS-Papieren. Sein Inhalt ist nicht grundsätzlich neu und unterliegt keinen wesentlichen Anpassungen abgesehen von seiner Abstimmung mit dem Thema "Sicherstellung der operationellen Resilienz", die vom BCBS neu eingeführt wurde. Somit wird ein neu entstehender Implementierungsaufwand als gering eingeschätzt.
- **Operationelle Resilienz**: Dieses Kapitel ist neu und es wird ein zusätzlicher Implementierungsaufwand erwartet. Je nach Maturität des bereits vorhandenen BCM wird der Aufwand insbesondere bei kleineren Instituten jedoch als gering eingeschätzt, da möglicherweise vorhandene Kenntnisse über die kritischen Prozesse, granular durchgeführte BIA, sowie bestehende Tests und Berichterstattungen bereits einen Grossteil der benötigen Bausteine liefern können.

Die Verhältnismässigkeit der Totalrevision ergibt sich einerseits dadurch, dass die Einhaltung der Grundsätze sachdienlich ist, um die operationellen Risiken (inkl. Risiken von Unterbrechungen) adäquat erfassen, begrenzen und überwachen zu können.

Andererseits würde ein länger währender Verzicht auf eine Revision des Rundschreibens zu erheblichen Lücken und Rechtsunsicherheiten führen. Des Weiteren bestünde ein erhöhtes Risiko, bei künftigen Assessments durch das BCBS als „nicht (vollständig) compliant" angeprangert zu werden, was der Reputation des Finanzplatzes schaden würde.

Es wurden im Vorfeld verschiedene Varianten geprüft, insbesondere die Variante einer Teilrevision. Diese wurde verworfen aufgrund der Fülle an zu aktualisierenden Themen und ihrer Wichtigkeit.

Auch wurde geprüft, den neuen Grundsatz der operationellen Resilienz aufzuspalten und in einen oder mehrere der bestehenden Grundsätze zu integrieren. Diese Variante wurde jedoch nicht implementiert, um den schärferen Fokus auf die kritischen Funktionen sowie die strategischen und präventiven Aspekte der operationellen Resilienz nicht zu verlieren. Zusätzlich würde die Schweiz mit einer derartigen

Zusammenlegung als Ausreisser gegenüber anderen Jurisdiktionen wirken, was wiederum der Reputation des Finanzplatzes schaden würde. Auch greift z. B. das bisher vorhandene BCM oftmals – wenn auch nicht zwangsläufig bei allen Instituten – zu kurz1 1. Es wird typischerweise eine sogenannte „asymmetrische" Herausforderung angenommen, bei der nur das Institut selbst, ein Teil des Instituts oder eine geringe Anzahl an Instituten betroffen wäre. Die Corona-Pandemie hat gezeigt, dass auch sogenannte „symmetrische" Herausforderungen realistisch sind, in der die Finanzmarktbeteiligten gleichzeitig betroffen sein können. Solche symmetrischen Herausforderungen sind unter anderem auch als Konsequenz von weitreichenden Cyber-Attacken oder langanhaltenden Stromausfällen oder Strommangellagen denkbar. Bei der Sicherstellung der operationellen Resilienz geht es vereinfacht gesagt darum, auch solche Szenarien überstehen zu können.

11 Unter anderem ist dies der Fall, wenn Abhängigkeiten und die benötigten Ressourcen ungenügend erfasst sind, die Verbindungen zwischen DRP und BCPs nicht oder ungenügend hergestellt werden oder Tests nur sehr punktuelle Verluste an Ressourcen berücksichtigen.

I. Gegenstand und Geltungsbereich

1 Dieses Rundschreiben bezieht sich auf die Vorschriften über die Funktionentrennung, das Risikomanagement und die interne Kontrolle der Bankenverordnung (Art. 12 und 14e BankV; SR 952.02) und der Finanzinstitutsverordnung (Art. 12 und 68 FINIV; SR 954.11) und konkretisiert die entsprechende Aufsichtspraxis. Es berücksichtigt die Basler Grundsätze zum einwandfreien Management der operationellen Risiken1 und/ der operationellen Resilienz2 .

1 BCBS Revisions to the Principles for the Sound Management of Operational Risk (31 March 2021)
2 BCBS Principles for Operational Resilience (31 March 2021)

2 Das Rundschreiben richtet sich an Banken nach Art. 1a und Personen nach Art. 1b Bankengesetz (BankG; SR 952.0), Wertpapierhäuser nach Art. 2 Abs. 1 Bst. e und Art. 41 des Finanzinstitutsgesetzes (FINIG; SR 954.1) sowie an Finanzgruppen und Finanzkonglomerate nach Art. 3c BankG und Art. 49 FINIG. Im Folgenden werden Banken, Personen nach Art. 1b BankG, Wertpapierhäuser, Finanzgruppen und Finanzkonglomerate unter dem Begriff „**Institute**" zusammengefasst.

II. Begriffe

3 Operationelle Risiken sind in Art. 89 ERV definiert. Es handelt sich um die Gefahr von finanziellen Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Prozessen oder Systemen, des unangemessenen Handelns von Menschen oder durch sie begangene Fehler, oder in Folge von externen Ereignissen eintreten. Dies beinhaltet die finanziellen Verluste, die aus Rechts- oder Compliance-Risiken entstehen können. Das Management der operationellen Risiken berücksichtigt typischerweise auch andere Schadensdimensionen3, sofern diese letztendlich auch in finanziellen Verlusten resultieren können. Dabei ausgeschlossen sind die strategischen Risiken.

3 Bspw. negative Auswirkungen auf die Reputation, möglicher Vertrauensverlust und Verlust von Kundinnen und Kunden, negative Auswirkungen auf den Markt, negative regulatorische Auswirkungen (z. Bsp. möglicher Verlust der Lizenz).

Anhörungsbericht
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.

4 Inhärente Risiken sind operationelle Risiken, denen das Institut durch seine Produkte, Aktivitäten, Prozesse und Systeme ausgesetzt ist, ohne Berücksichtigung von Kontrollund Minderungsmassnahmen.

5 Residuale Risiken sind operationelle Risiken, denen das Institut nach der Berücksichtigung von Kontrollund Minderungsmassnahmen ausgesetzt ist.

6 Die **Informations- und Kommunikationstechnologie (IKT)** bezeichnet den physischen und logischen (elektronischen) Aufbau von IT- und Kommunikationssystemen, die einzelnen Hardund Softwarekomponenten, Netzwerke, Daten und Betriebsumgebungen.

7 Kritische Daten sind Daten, die in Anbetracht der Grösse, der Komplexität, der Struktur, des Risikoprofils sowie des Geschäftsmodells des Instituts von so wesentlicher Bedeutung sind, dass sie einen erhöhten Sicherheitsanspruch erfordern. Dabei handelt es sich um Daten, die für die erfolgreiche und nachhaltige Erbringung der Dienstleistungen des Instituts oder für regulatorische Zwecke wesentlich sind. Bei der

Beurteilung und Festlegung der Kritikalität von Daten sind sowohl die Vertraulichkeit als auch die Integrität und Verfügbarkeit zu berücksichtigen. Jeder dieser drei Aspekte kann ausschlaggebend dafür sein, dass Daten als kritisch klassifiziert werden.

Anhörungsbericht

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 „kritischen 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.

8 Kritische Prozesse sind Prozesse, deren bedeutende Störung oder Unterbrechung die Erbringung kritischer Funktionen gefährden. Sie sind ein Bestandteil der kritischen Funktionen.

9 Das **Business Continuity Management (BCM)** bezeichnet den institutsweiten Ansatz, um im Falle einer über das Vorfallmanagement hinausgehenden, bedeutenden Störung oder Unterbrechung den Betrieb der kritischen Prozesse wiederherzustellen. Es definiert die Reaktion auf bedeutende Störungen oder Unterbrechungen. Ein effektives BCM vermindert die residualen Risiken im Zusammenhang mit bedeutenden Störungen oder Unterbrechungen.

10 Die **Recovery Time Objective (RTO)** ist die Zeit bis zur Wiederherstellung einer Anwendung, eines Systems und/oder eines Prozesses. Die Recovery Point Objective (RPO) ist die maximal tolerierbare Zeitspanne eines Datenverlusts.

11 Der **Business Continuity Plan (BCP)** ist ein vorausschauender Plan, der die notwendigen Vorgehensweisen, Wiederherstellungsoptionen und Ersatzressourcen (die Wiederherstellungsprozesse) zur Sicherstellung der Kontinuität und zur Wiederherstellung der kritischen Prozesse festlegt.

12 Der **Disaster Recovery Plan (DRP)** definiert die Wiederherstellungsprozesse, um im Fall eines schwerwiegenden Ausfalls oder einer Zerstörung der IKT und unter Berücksichtigung des möglichen Ausfalls von Schlüsselpersonen, die Wiederherstellungsziele zu erreichen.

13 Krisensituationen sind ausserordentliche, potenziell existenzbedrohende Situationen, welche nicht mit ordentlichen Massnahmen und Entscheidungskompetenzen bewältigt werden können. Sie unterscheiden sich von Vorfällen (Incidents bzw. Störungen) und bedeutenden Störungen oder Unterbrechungen, welche mit dem Vorfallmanagement im Normalbetrieb oder den festgelegten BCPs und DRPs bewältigt werden können.

14 Kritische Funktionen beinhalten:

15 *a.* die Aktivitäten, Prozesse und Dienstleistungen, inklusive die für ihre Erbringung notwendigen zugrundeliegenden Ressourcen, deren Unterbrechung die Weiterführung des Instituts oder seine Rolle im Finanzmarkt und damit die Funktionsfähigkeit der Finanzmärkte gefährden würde; und

16 *b.* die systemrelevanten Funktionen nach Art. 8 BankG.

Anhörungsbericht

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 Anhö- rungsvorlage 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 unterstützt 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.

17 Die **Unterbrechungstoleranz** ist das Ausmass (bspw. Dauer oder erwarteter Schaden) der Unterbrechung einer kritischen Funktion, das das Institut unter Berücksichtigung von schwerwiegenden, aber plausiblen Szenarien zu akzeptieren bereit ist. Für jede kritische Funktion ist eine Unterbrechungstoleranz zu definieren.

18 Operationelle Resilienz bezeichnet die Fähigkeit des Instituts, seine kritischen Funktionen bei Unterbrechungen innerhalb der Unterbrechungstoleranz wiederherstellen zu können. D. h., die Fähigkeit des Instituts, Bedrohungen und mögliche Ausfälle zu identifizieren, sich davor zu schützen und darauf zu reagieren, bei Unterbrechungen den ordentlichen Geschäftsbetrieb wiederherzustellen und daraus zu lernen, um die Auswirkungen von Unterbrechungen auf die Erbringung der kritischen Funktionen zu minimieren. Ein operationell resilientes Institut hat sein Betriebsmodell so aufgebaut4 , dass es in Bezug auf seine kritischen Funktionen dem Risiko von Unterbrechungen weniger ausgesetzt ist. Die operationelle Resilienz verringert somit nicht nur die residualen Risiken von Unterbrechungen, sondern auch das inhärente Risiko, dass es zu Unterbrechungen kommt. Ein effektives Management der operationellen Risiken trägt dazu bei, die operationelle Resilienz des Instituts zu stärken.

4 Häufig auch Resilience by Design genannt.

III. Proportionalitätsprinzip

19 Dieses Rundschreiben gilt grundsätzlich für alle seiner Adressaten. Die Anforderungen sind jedoch im Einzelfall abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen. Die FINMA ordnet im Einzelfall Erleichterungen oder Verschärfungen an.

20 Banken und Wertpapierhäuser der FINMA-Kategorien 4 und 5 sind von der Erfüllung der Rz 33–38, 41–46, 48, 51, 57, 73, 74, 76–78, 80, 87, 92, 93, 96, 103, 104 und 110–112 ausgenommen.

21 Institute nach Art. 47a–47e ERV, Personen gemäss Art. 1b BankG, sowie nicht-kontoführende Wertpapierhäuser sind zusätzlich von der Erfüllung der Rz 72, 75, 79 und 105–109 ausgenommen.

Anhörungsbericht

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. 47a–47e ERV, Personen gemäss Art. 1b 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. 47a–47e ERV, Personen gemäss Art. 1b 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.

IV. Management der operationellen Risiken

Erläuterungen

A. Übergreifendes Management der operationellen Risiken

4.1.2 Übergreifendes Management der operationellen Risiken (Kapitel IV Buchstabe A)

Das Kapitel IV Buchstabe A umfasst eine Überarbeitung der im FINMA-RS 08/21 bisher enthaltenen Grundsätze 1–3 zu den Themen „Kategorisierung und Klassifizierung von operationellen Risiken", „Identifizierung, Begrenzung und Überwachung", sowie „Interne und Externe Berichterstattung". Er legt somit die für ein wirksames Management der operationellen Risiken grundlegendsten Komponenten dar.

Bei der Überarbeitung wurden die folgenden Stossrichtungen verfolgt:

- **Abgleich und Aktualisierung entlang der revidierten PSMOR**: Da die Revision dieses BCBS-Papiers auf sehr granularer Ebene erfolgte, erwies sich sein Einfluss auf das neue Rundschreiben jedoch als zweitrangig in Bezug auf das übergreifende Management der operationellen Risiken. Relevanter für das neue Rundschreiben war das neu im BCBS Papier eingeführte Prinzip zur IKT, welches in die Kapitel IV Buchstaben B bis D eingeflossen ist.
- **Aktualisierung und Klarstellungen aufgrund der Erfahrungen aus der Aufsichtspraxis der FINMA**: Die Revision zielt primär darauf ab, den in der Praxis häufig festgestellten Fehlinterpretationen und Mängeln im Bereich des Managements der operationellen Risiken entgegenzuwirken. So wird, wie unten erläutert, insbesondere mehr Klarheit in Bezug auf die Aufsichtspraxis zur Risikotoleranz für operationelle Risiken geschaffen (Rz 23, 32, 38). Auch werden die Schlüsselkontrollen als wichtige Komponente des internen Kontrollsystems behandelt (Rz 31). Der Bezug zum institutsweiten Risikomanagement nach FINMA-RS 17/1 wird klarer ausgeführt (Rz 22–25).

Die Definition der operationellen Risiken (Rz 3) bleibt inhaltlich insgesamt unverändert und aligniert mit der Definition des BCBS, sowie aligniert mit der ERV. Aufgrund des Bezugs zu den Eigenmittelanforderungen bezieht sie sich historisch gesehen rein auf finanzielle Verluste. Die Reputationsrisiken wurden historisch gesehen ausgeschlossen, da sie schwierig zu quantifizieren sind. Dieser Ausschluss bedeutet jedoch nicht, dass 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 (z. B. 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 z. B. 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. In der Definition der operationellen Risiken klar nicht eingeschlossen sind die strategischen Risiken (z. B. das Risiko, dass das Anbieten eines neuen Produktes nicht zu den gewünschten und erwarteten Erträgen führt).

Das Management der operationellen Risiken ist als eine der Komponenten des institutsweiten Risikomanagements nach FINMA-RS 17/1 zu verstehen (Rz 22). Die im FINMA-RS 17/1 vorgegebenen Funktionentrennungen sind somit auch hier unter Anwendung des Proportionalitätsprinzips umzusetzen, weshalb im neuen Rundschreiben nicht auf Details der Funktionentrennungen (oftmals mit 1st und 2nd line of defence bezeichnet) im Kontext des Managements der operationellen Risiken eingegangen wird.

Die im FINMA-RS 17/1 dargelegte Rolle und Verantwortung des Oberleitungsorgans wird im neuen Rundschreiben in Bezug auf die operationellen Risiken präzisiert, unter anderem in Bezug auf die Risikotoleranz. Dem Oberleitungsorgan muss eine transparente und aktuelle Sicht über die inhä- renten und residualen Risiken des Instituts vorgelegt werden, auf deren Basis die Risikotoleranz definiert und vom Oberleitungsorgan genehmigt wird (Rz 23).

Während auf Stufe der Geschäftsleitung oder der Geschäftseinheiten im Detail über die Reaktion auf Risiken (Vermeidung, Transfer, Minimierung, Akzeptanz) und zu ergreifende Massnahmen entschieden werden kann, so liegt es in der Verantwortung des Oberleitungsorgans, strategische Richtungswechsel vorzugeben, wenn es gewisse inhärente oder residuale Risiken als nicht oder nicht mehr tolerierbar ansieht. Strategische Richtungswechsel können etwa Änderungen des Geschäftsmodells sein (bspw. Verzicht auf grenzüberschreitende Aktivitäten oder auf Geschäfte in gewissen Ländern, Einstellungen gewisser Produkte, Verzicht auf Investment Banking oder Kundenzielgruppen) oder Anpassungen des Organisationsmodells bzw. des Operating Models (bspw. starke Umorientierung zu Automatisierung und Reduktion manueller Prozesse oder wesentliche neue Auslagerungen).

Bei der Durchführung der Risiko- und Kontrollbeurteilungen sind alle relevanten Informationen zu berücksichtigen (Rz 30). Ausserdem sollen sich die Verantwortlichen bei der Beurteilung der Kontrollund Minderungsmassnahmen nicht alleine auf „reaktive“ Inputs verlassen (Rz 31). Z. B. sollten Kontroll- und Minderungsmassnahmen nicht einfach deshalb als effektiv beurteilt werden, weil es in den letzten Jahren keine (Verlust-)Ereignisse gab. Stattdessen sollen mindestens die Schlüsselkontrollen regelmässig und systematisch getestet werden und die Resultate dieser Tests einbezogen werden. In Bezug auf die Tests der Schlüsselkontrollen ist es wichtig, dass die Schlüsselkontrollen mindestens stichprobenhaft periodisch durch eine unabhängige Kontrollinstanz wie die Risikokontrolle oder die Compliance-Funktion getestet werden, komplementär zu den Beurteilungen durch die Organisationseinheiten, die die Schlüsselkontrollen definieren, „besitzen“ und durchführen (control owners und control performers).

Im Falle wesentlicher Änderungen ist die Risiko- und Kontrollbeurteilung zu aktualisieren (Rz 32). Beispiele von potentiell wesentlichen Änderungen sind Umstellungen auf ein anderes IT-System mit neuen Abläufen, Veränderungen in den Prozessabläufen, Einführung neuer oder Abschaffung bestehender Produkte, Einführung oder Aufgabe bestimmter Geschäftstätigkeiten, Änderungen der Zielkundengruppen (z. B. anderes Land, anderer Typ Kunden), Inkrafttreten neuer Regulierungen oder eine ansteigende Bedrohungslage.

Die interne Berichterstattung zu den operationellen Risiken soll unter anderem Informationen zu wesentlichen internen Verlusten aus operationellen Risiken umfassen (Rz 39). Dies bedeutet nicht, dass zwangsläufig jedes Institut eine systematische Verlustdatensammlung nach Rz 34 oder nach den Anforderungen an die internen Verlustdaten der Berechnung der Mindesteigenmittel für operationelle Risiken nach den finalen Basel III Regeln umsetzen muss. Eine systematische Verlustdatensammlung wird zwar empfohlen, aber in Anwendung des Proportionalitätsprinzips nicht bei jedem Institut erwartet.

22 Das Management der operationellen Risiken ist Teil des institutsweiten Risikomanagements nach FINMA-Rundschreiben 2017/1 „Corporate Governance – Banken“.

23 Das Oberleitungsorgan genehmigt die Grundzüge des Managements der operationellen Risiken, die für das Institut relevant sind, und überwacht deren Einhaltung. Darunter fallen unter anderem die IKT-Risiken, die Cyber-Risiken, die Risiken hinsichtlich kritischer Daten, die Risiken aus der Ausgestaltung und Implementierung des BCM und gegebenenfalls die Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft. Es genehmigt mindestens jährlich die Risikotoleranz für operationelle Risiken nach Massgabe der Risikopolitik in Anbetracht der strategischen und finanziellen Ziele des Instituts. Dabei berücksichtigt es die Ergebnisse aus den Risiko- und Kontrollbeurteilungen nach Rz 30. Es akzeptiert entweder das Ausmass, in dem das Institut den operationellen Risiken ausgesetzt ist, oder entscheidet über eine Anpassung der Risikotoleranz und die dafür notwendigen, strategischen Änderungen5 .

5 Zum Beispiel eine Änderung des Geschäftsmodells

24 Das Oberleitungsorgan genehmigt regelmässig Strategien für den Umgang mit der IKT, den Cyber-Risiken, den kritischen Daten und dem BCM, und überwacht deren Einhaltung.

25 Die Geschäftsleitung stellt nachvollziehbar sicher, dass die operationellen Risiken identifiziert, beurteilt, begrenzt und überwacht werden, und dass die Effektivität sowohl der Ausgestaltung als auch der Implementierung dieses Managements der operationellen Risiken regelmässig überprüft wird. Für die Begrenzung der als wesentlich beurteilten, inhärenten Risiken6 ergreift sie situativ risikospezifische ergänzende oder verschärfende Massnahmen.

6 Häufig Top-Risiken oder Schlüsselrisiken (Key Risks) genannt.

Anhörungsbericht

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.

26 Zur Stärkung des Bewusstseins der Mitarbeitenden zur Reduktion von relevanten operationellen Risiken, insbesondere der IKT-Risiken, der Cyber-Risiken, der Risiken hinsichtlich kritischer Daten und der Risiken aus der Ausgestaltung und Implementierung des BCM, sind unter Berücksichtigung ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) Massnahmen zu implementieren7 .

7 Dies beinhaltet unter anderem die sorgfältige Auswahl und Qualifikation von Mitarbeitenden für ihre AKV und ihre kontinuierliche Weiterbildung im Rahmen ihrer Aktivitäten.

27 Falls notwendig, definiert die FINMA im Rahmen der laufenden Aufsicht für spezifische Themen weitergehende Anforderungen an das Management der operationellen Risiken. Dies geschieht zurückhaltend und unter Anwendung des Proportionalitätsprinzips.

Anhörungsbericht

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.

28 Die operationellen Risiken sind institutsweit einheitlich zu kategorisieren und in einem Inventar aufzuführen. Diese Kategorisierung kann in Anlehnung an die für die Berechnung der Mindesteigenmittel für operationelle Risiken verwendete Kategorisierung der Ereignistypen oder mittels einer internen Taxonomie erfolgen. Die Kategorisierung ist in allen Bereichen des Instituts und in allen Komponenten des Managements der operationellen Risiken konsistent anzuwenden.

29 Für die Identifikation der operationellen Risiken werden interne8 und externe9 Faktoren berücksichtigt. Die identifizierten operationellen Risiken werden sowohl aus Sicht der inhärenten als auch der residualen Risiken nachvollziehbar beurteilt.

8 Interne Faktoren sind beispielsweise Änderungen in den Produkten, Aktivitäten, Prozessen und Systemen, Prüfergebnisse und interne Verluste aus operationellen Risiken.

9 Externe Faktoren sind beispielsweise erkannte Verlustereignisse anderer Institute, Änderungen in der Sicherheitslage (bspw. durch Umwelteinflüsse, Cyber-Attacken oder Terrorismus) oder Änderungen in den regulatorischen Anforderungen.

30 Die Identifikation und Beurteilung der operationellen Risiken stützt sich mindestens auf Prüfergebnisse1 0 und regelmässig durchzuführende Risiko- und Kontrollbeurteilungen. Die Risiko- und Kontrollbeurteilungen berücksichtigen die inhärenten Risiken, die Effektivität der bestehenden Kontrollund Minderungsmassnahmen und die residualen Risiken.

10 Prüfergebnisse umfassen hier Resultate der internen Revision und der externen Prüfgesellschaft, sofern vorhanden, sowie Ergebnisse von Überprüfungen durch bspw. die Geschäfts- und Organisationsbereiche, die Risikokontrolle, die Compliance-Funktion oder Aufsichtsbehörden.

31 Für die Beurteilung der bestehenden Kontrollund Minderungsmassnahmen wird insbesondere eine regelmässige Beurteilung der Effektivität der Schlüsselkontrollen durch eine unabhängige Kontrollinstanz vorgenommen und dokumentiert (Design Effectiveness und Operating Effectiveness Testing). Dabei sind Schlüsselkontrollen diejenigen Kontrollund Minderungsmassnahmen, die die als wesentlich beurteilten, inhärenten Risiken minimieren. Auch wird die Trennung der AKV zur Sicherstellung der Unabhängigkeit und Vorbeugung vor Interessenskonflikten regelmässig beurteilt.

Anhörungsbericht

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 Risks2 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.

2 <https://www.bis.org/bcbs/publ/d5 15.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.").

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

32 Vor wesentlichen Änderungen in den Produkten, Aktivitäten, Prozessen und Systemen sind ad hoc Risiko- und Kontrollbeurteilungen durchzuführen. Diese berücksichtigen die mit dem Änderungsprozess einhergehenden operationellen Risiken und die operationellen Risiken des Zielzustands. Bei Bedarf werden die Risikotoleranz angepasst und Kontrollund Minderungsmassnahmen implementiert.

33 In Abhängigkeit von Art, Umfang, Komplexität und Risiko der institutsspezifischen Produkte, Aktivitäten, Prozesse und Systeme sind folgende weiteren Instrumente und Methoden anzuwenden:

34 *a.* Systematische Erhebung und Analyse interner Verlustdaten und relevanter externer Ereignisse, die mit operationellen Risiken verbunden sind;

35 *b.* Risiko- und Kontrollindikatoren für die Überwachung der operationellen Risiken und zeitnahe Identifikation von relevanten Risikoerhöhungen;

36 *c.* Szenarioanalysen und/oder Abschätzung des Verlustpotenzials in Anbetracht der bzw. in Gegenüberstellung mit den Mindesteigenmitteln für operationelle Risiken;

37 *d.* Vergleichende Analysen (Read-across), beispielsweise Analysen der Relevanz von Prüfergebnissen für andere Bereiche des Instituts oder Vergleiche zwischen den Ergebnissen der Risiko- und Kontrollbeurteilungen verschiedener Bereiche.

38 Die Risikotoleranz für operationelle Risiken berücksichtigt sowohl die Toleranz in Bezug auf inhärente1 1 als auch auf residuale operationelle Risiken und wird anhand von Risikooder Kontrollindikatoren überwacht.

11 Die Risikotoleranz in Bezug auf inhärente Risiken berücksichtigt strategische Entscheidungen in Bezug auf das Geschäfts- oder Betriebsmodell, bspw. Toleranz für die inhärenten Risiken, die mit der Bedienung gewisser Kundensegmente oder Länder einhergehen, mit dem Angebot gewisser Produkte, mit der Anwendung vorwiegend manueller Prozesse, mit der Abstützung auf eine komplexe IT-Infrastruktur oder mit gewissen Auslagerungen (Outsourcing).

Anhörungsbericht

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.

39 Die Risikokontrolle erstattet dem Oberleitungsorgan mindestens jährlich und der Geschäftsleitung mindestens halbjährlich nach Rz 75–76 FINMA-RS 17/1 Bericht über die operationellen Risiken entlang der obersten Stufe1 2 der nach Rz 28 definierten Kategorisierung, über deren Vergleich mit der festgelegten Risikotoleranz, sowie über Einzelheiten zu wesentlichen internen Verlusten.

12 Die oberste Stufe der Kategorisierung wird häufig Stufe 1 oder Level 1 genannt. Die Berichterstattung kann auch auf einer detaillierteren Stufe erfolgen.

40 In Bezug auf die relevanten IKT- und Cyber-Risiken beinhaltet die mindestens jährlich erfolgende Berichterstattung an die Geschäftsleitung zudem Informationen zur Entwicklung dieser Risiken, zur Effektivität der entsprechenden Schlüsselkontrollen und zu wesentlichen internen und externen Ereignissen im Zusammenhang mit diesen Risiken.

41 Die interne Berichterstattung nach Rz 39 enthält ergänzend folgende Informationen:

- **42** relevante, externe Faktoren nach Fussnote 9,
- **43** zusammenfassende Gesamtübersicht über die Effektivität der Schlüsselkontrollen nach Rz 31,
- **44** neu aufkommende operationelle Risiken,
- **45** Ergebnisse aus der Anwendung zusätzlicher Instrumente und Methoden nach Rz 33.

46 Entsprechend dem Proportionalitätsprinzip wird für die systemrelevanten Banken auch auf Ebene der Geschäfts- oder Organisationsbereiche, die relevanten oder wesentlichen operationellen Risiken ausgesetzt sind, eine regelmässige Berichterstattung zu den operationellen Risiken vorgenommen.

Anhörungsbericht

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 Kontrollund 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.

B. Management der IKT-Risiken

Erläuterungen

4.1.3 Management der IKT-Risiken (Kapitel IV Buchstabe B)

Die IKT-Risiken sind ein spezifischer Typ von operationellen Risiken. Auf Basis der allgemeinen Anforderungen nach Kapitel IV Buchstabe A gibt Kapitel IV Buchstabe B weitergehende Präzisierungen für das Management der IKT-Risiken.

In den Grundsätzen zum Management der IKT- und Cyber-Risiken sowie der Risiken kritischer Daten wurde im Sinne einer guten Lesbarkeit auf den expliziten Bezug zu FINMA-RS 18/3 „Outsourcing" und FINMA-RS 17/1 verzichtet. Jedoch gelten deren Prinzipien weiterhin. So sind insbesondere die Anforderungen an die organisatorischen Strukturen, die Risikopolitik und die Grundzüge des institutsweiten Risikomanagements nach FINMA-RS 17/1 anzuwenden.

Das neue Rundschreiben präzisiert insbesondere die unterschiedlichen Verantwortlichkeiten des Oberleitungsorgans (mit Fokus auf Genehmigung und Überwachung) und der Geschäftsleitung (mit Fokus

auf Implementation) in den Bereichen der IKT-Strategie, des Managements der IKT-Risiken sowie der Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit der IKT (Rz 47, 49).

Die IKT stellt einen wesentlichen Bestandteil der Geschäftstätigkeit der Institute dar. Unter Berücksichtigung der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts ist daher ein angemessenes System für das Management der IKT-Risiken zu entwickeln und zu implementieren. Das Management dieser Risiken erfordert bei den Instituten angemessene Fachkenntnisse der Mitglieder der Geschäftsleitung und des Oberleitungsorgans. Die Verfahren, Prozesse und Massnahmen zur Kontrolle der IKT-Risiken sollen in Abstimmung mit den institutsspezifischen Bedingungen auch allgemeine, international anerkannte Standards berücksichtigen (Rz 48).

Mit dem stark gestiegenen Volumen an Entwicklungen im Bereich der IKT, wozu auch Entwicklungsmethoden wie Agile gehören, hat das IKT Change Management an Bedeutung gewonnen (Rz 50-52). Das Rundschreiben hebt somit das Change Management als Behandlung jeder Art von Veränderungen (Change) an einer IKT-Infrastruktur hervor. Ein strukturierter, wohldefinierter und kontrollierter Change Management-Prozess ermöglicht die wirksame Implementierung von Veränderungen und trägt somit zur Risikominimierung bei. Dabei müssen die Auswirkungen der durch einen Change Request beantragten Veränderungen ermittelt und die Veränderungen klassifiziert und priorisiert werden. Der Change Management-Prozess beinhaltet typischerweise die Aktivitäten Annahme, Klassifizierung, Genehmigung4 , Autorisierung, Planung, Testen und Freigabe des Tests sowie die tatsächliche Freigabe in die produktive Umgebung. Ein bekannter Erfolgsfaktor für ein wirksam implementiertes Change Management ist eine enge Zusammenarbeit zwischen den Disziplinen Change Management, Projektmanagement und Release Management.

4 Typischerweise durch ein Gremium wie ein Change Review Board oder eine andere Change Authority.

Zur Vermeidung unautorisierter Eingriffe wird auch die Trennung der Produktions- und der Test- bzw. Entwicklungsumgebungen hervorgehoben (Rz 51). Das Institut muss hierbei mit Hilfe von geeigneten Verfahren, Prozessen und Kontrollen eine Aufgabentrennung sicherstellen. Dazu können beispielsweise Code-Reviews, Freigabe von Build-Artefakten durch Product Owner, Embedded und Independent Testing oder Logging-Mechanismen dienen. Klassischerweise ist die Funktionentrennung die wichtigste Präventivkontrolle zum Schutz vor unautorisierten Eingriffen in die Produktionsumgebung. Aufgrund der steigenden Verbreitung agiler Entwicklungsmethoden wurde im Rundschreiben darauf verzichtet, die Funktionentrennung zu nennen. Auch ist diese bei sehr kleinen Instituten häufig nicht umsetzbar und es wird stattdessen auf kompensierende Kontrollen gesetzt.

Ein strukturierter, wohldefinierter und kontrollierter IKT-Betrieb (Run, Maintenance) stellt die Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Produktionsumgebung sicher (Rz 53–57). Je komplexer die IKT-Landschaft eines Instituts ist, desto grösser ist das Risiko, dass Komponenten der IKT-Infrastruktur das sogenannte End of Life erreichen und nicht mehr vom Hersteller unterstützt werden. Die Institute müssen daher einen risikoorientierten und kontrollierten Umgang mit Systemen sicherstellen, deren Betriebsende naht oder deren Dekommissionierung nicht durchgeführt wurde.

Das neue Rundschreiben präzisiert die grundlegende Bedeutung der IKT- Inventarisierung, die Hardware- und Software-Komponenten sowie kritische Daten umfasst (Rz 53). Dabei müssen sowohl interne Abhängigkeiten als auch Schnittstellen zu wesentlichen externen Dienstleistern berücksichtigt werden. Die IKT-Inventarisierung soll eine strukturierte Bewertung der physischen und virtuellen IKT-Elemente erlauben, die einem Institut zur Verfügung stehen. Das Vorliegen vollständiger und richtiger IKT-Inventarinformationen ist wesentlich für die zeitnahe Reaktion auf IKT- und Cyber-Vorfälle sowie bei Problemen innerhalb eines bestimmten IT-Systems und zukünftigen Anschaffungen für die Wartung oder Erweiterung des Betriebs (Rz 54, 62–67). Zudem bildet die IKT-Inventarisierung die Grundlage bei Beurteilungen, ob nicht mehr standardgemässe oder funktionsgestörte Elemente der IKT-Infrastruktur eine neue Konfiguration (Patching) erhalten oder ausgetauscht, komplett abgebaut oder dekommissioniert werden sollen.

Der IKT-Betrieb steht nicht isoliert da, sondern ist in enger Verknüpfung mit den Aspekten BCM und DRP (Kapitel IV Buchstabe E) zu betrachten. Die Institute müssen sicherstellen, dass das Institut bei bedeutenden Störungen oder Unterbrechungen reibungslos vom IKT-Betrieb in ihre BCP- und DRP- Prozesse übergehen kann, um den Betrieb auch bei Unterbrechungen und in Krisensituationen aufrechtzuerhalten (Rz 56). Dies bedeutet, dass entsprechende Back-up- und Wiederherstellungsprozesse mindestens einmal jährlich getestet werden müssen. Dazu gehört auch das Testen von Sicherheitsmechanismen, die fehlerhafte Wiedererstellungsschritte sowie mögliche Datenkorruptionen feststellen und eingrenzen.

Das neue Rundschreiben präzisiert auch die Grundzüge des IKT-Vorfallmanagements (Incident Management, Rz 58–60). Das Incident Management umfasst den gesamten organisatorischen und technischen Prozess

zum Umgang mit erkannten oder vermuteten Betriebsstörungen oder Sicherheitsvorfällen in IKT-Bereichen, inklusive vorbereitende Massnahmen und Prozesse der Reaktion und Eskalation. Im Incident Management ist der gesamte Lebenszyklus von IKT-Vorfällen zu berücksichtigen, um Rückschlüsse zu ziehen und aus vorherigen Vorfällen zu lernen.

a) IKT-Strategie und Governance

47 Die grundsätzlichen Erwartungen an die Strategie, Governance und Stärkung des Bewusstseins in Bezug auf die IKT sind in Rz 23–26 und 40 festgehalten.

48 Das Management der IKT-Risiken berücksichtigt relevante international anerkannte Standards und Practices sowie den Einfluss von neuen technologischen Entwicklungen auf die IKT-Risiken.

49 Die Geschäftsleitung stellt sicher, dass sowohl für das Änderungsmanagement (Change Management) als auch für den IKT-Betrieb (Run, Maintenance) Verfahren, Prozesse und Kontrollen sowie AKV implementiert und dokumentiert sind. Diese sind mit qualifizierten und angemessenen Ressourcen ausgestattet.

b) Änderungsmanagement (Change Management)

50 Für alle Phasen der Entwicklung oder Beschaffung von IKT definiert das Änderungsmanagement Verfahren, Prozesse, und Kontrollen. In jeder dieser Phasen berücksichtigt es die Auswirkungen der Änderung auf die IKT-Risiken. Dabei stehen insbesondere auch die Anforderungen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit im Fokus.

51 Es ist eine Trennung zwischen den Umgebungen für die Entwicklung oder das Testen und der Umgebung für die IKT-Produktion sicherzustellen. Dies umfasst auch eine eindeutige Zuweisung von AKV und eine Regelung der damit einhergehenden Zugangsberechtigungen.

52 Bei Entwicklung und Beschaffung von IKT werden funktionale und nicht-funktionale Anforderungen1 3 klar definiert und genehmigt und gemäss ihrer Kritikalität getestet und validiert.

13 Bspw. im Hinblick auf die Architektur oder die Anforderungen an die Informationssicherheit.

c) IKT-Betrieb (Run, Maintenance)

53 Das Institut führt ein oder mehrere Inventar(-e) der Bestandteile der IKT. Das Inventar umfasst Hardwareund Software-Komponenten sowie Ablageorte kritischer Daten. Dabei werden sowohl Abhängigkeiten innerhalb des Instituts als auch Schnittstellen zu wesentlichen externen Dienstleistern berücksichtigt.

54 Das Inventar ist zeitnah verfügbar und wird regelmässig hinsichtlich Vollständigkeit und Richtigkeit überprüft und aktualisiert.

55 Das Institut verfügt über Verfahren, Prozesse, und Kontrollen, die die Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Produktionsumgebung unter Berücksichtigung der jeweiligen Risikotoleranz sicherstellen.

56 Das Institut stellt sicher, dass es bei bedeutenden Störungen oder Unterbrechungen reibungslos vom IKT-Betrieb in seine BCP- und DRP-Prozesse übergehen kann. Es implementiert angemessene Back-up-Prozesse und Wiederherstellungsprozesse, die regelmässig getestet und validiert werden.

57 Das Institut verfügt über Verfahren, Prozesse und Kontrollen, die einen risikoorientierten Umgang mit IKT, deren Betriebsende naht oder deren geplante Dekommissionierung überschritten wurde, sicherstellt.

d) Vorfallmanagement (Incident Management)

58 Das Institut verfügt über Verfahren, Prozesse und Kontrollen zur Behandlung wesentlicher IKT-Vorfälle, einschliesslich solcher, die auf Abhängigkeiten von wesentlichen externen Dienstleistern und konzerninternen Auslagerungen zurückzuführen sind. Dabei ist der gesamte Lebenszyklus von wesentlichen IKT-Vorfällen zu berücksichtigen und AKV zur Behandlung dieser Vorfälle sind zu definieren.

59 Die Behandlung wesentlicher IKT-Vorfälle ist mit den Prozessen zum BCM und dem DRP abzustimmen und zu verknüpfen.

60 IKT-Vorfälle, die vom Institut als wesentliche Störung bei der Erbringung seiner kritischen Prozesse erachtet werden und für die Aufsicht von wesentlicher Bedeutung sind, müssen der FINMA unverzüglich gemeldet werden.

Anhörungsbericht

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 EXPERT- suisse 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 EXPERT-suisse 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.

C. Management der Cyber-Risiken

Erläuterungen

4.1.4 Management der Cyber-Risiken (Kapitel IV Buchstabe C)

Cyber-Risiken gehören zu den operationellen Risiken, welche im Allgemeinen unter dem übergreifenden Management der operationellen Risiken behandelt werden, während das Management der Cyber-Risiken Präzisierungen der Anforderungen zu einem angemessenen Umgang mit Cyber-Risiken beinhaltet. Bei den Cyber-Risiken besteht ein enger Zusammenhang mit den unter dem Management der IKT-Risiken aufgeführten Anforderungen, da die Materialisierung von IKT-Risiken zu höheren Cyber-Risiken führen kann und umgekehrt. Cyber-Risiken können aber nicht mit IKT-Risiken gleichgesetzt werden. Cyber-Risiken haben stärkere externe Einflussfaktoren wie die Ausnutzung von Schwachstellen über unterschiedliche Angriffsvektoren, etwa bei Ransomwareoder Distributed Denial of Service (DDoS)-Attacken sowie Insider-Bedrohungen. Die Institute haben daher eine eigenständige Definition von Cyber-Risiken in ihrem Risikomanagement aufzuführen, die der Art des Risikos gerecht wird.

Die Überarbeitung der Cyber-Sicherheitsanforderungen im neuen Rundschreiben basiert im Wesentlichen auf den Erfahrungen aus der Aufsichtspraxis der FINMA. Für eine effektive Handhabung von Cyber-Risiken sollten die Institute ihr IKS grundsätzlich nach einem international anerkannten Standard und Practices aufbauen (Rz 62–67), etwa nach dem Cybersicherheitsrahmenwerk des National Institute of Standards and Technology (NIST) oder den entsprechenden Standards der Internationalen Organisation für Normung (ISO). Auch ist eine jährliche Berichterstattung an die Geschäftsleitung über Entwicklungen des Threatund Risikoprofils, allfällige Schäden bei einer erfolgreichen Cyber-Attacke sowie über die operative Wirksamkeit von Schlüsselkontrollen in diesem Bereich sicherzustellen (Rz 61 bzw. Rz 40).

Die zu implementierenden Massnahmen wurden präzisiert, um einen ganzheitlichen Ansatz zu verfolgen (Rz 62–67). Bei der Identifikation von Cyber- Attacken wurde der Fokus auf die Einführung geeigneter Verfahren, Prozesse und Kontrollen für eine umfassende Inventarisierung der IKT gelegt, mit dem Ziel sicherzustellen, dass Schwachstellen zeitnah erkannt werden und im Falle einer Cyber-Attacke Zusammenhänge schneller analysiert und unterbunden werden können. Dazu gehört auch die angemessene Implementierung von Verfahren, Prozessen und Kontrollen, um einen solchen Cyber-Angriff zu erkennen, einzudämmen und zu beseitigen.

Um die Wirksamkeit der implementierten Cyber-Schutzmassnahmen zu überprüfen, soll die Geschäftsleitung neben Schwachstellenscans und Penetrationstests veranlassen, dass Cyber-Übungen auf Basis der institutsspezifischen Bedrohungspotenziale durchgeführt werden (Rz 70). Ergänzend können weitere, im Rundschreiben nicht explizit aufgelistete Verfahren für die Überprüfung von Cyber-Schutzmassnahmen wie z. B. die Teilnahme an Bug Bounty-Programmen oder Quellcode-Sicherheitsüberprüfungen durchgeführt werden. Der Mindestumfang für Verwundbarkeitsanalysen und Penetrationstests wurde in Rz 69 näher definiert. Dieser umfasst Applikationen, Systeme oder Schnittstellen, welche vom Institut gehostet sind oder an Dritte ausgelagert wurden (entweder mittels direkter Prüfungen oder Assurance Berichten). Bezogene Drittservices, wie z.B. Twitter, Instragram, LinkedIn etc. fallen nicht unter diese Definition.

Das Kapitel IV Buchstabe C beschreibt auch die Meldepflicht einer Cyber- Attacke an die FINMA (Rz 68). Die Details zum Meldeprozess wurden in der Aufsichtsmitteilung 05/2020 „Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG“ festgehalten.

61 Die grundsätzlichen Erwartungen an die Strategie, Governance und Stärkung des Bewusstseins in Bezug auf die Cyber-Risiken sind in Rz 23–26 und 40 festgehalten.

62 Das Institut definiert eindeutige AKV. Es hat mindestens die folgenden Aspekte nach international anerkannten Standards und Practices abzudecken und deren effektive Umsetzung durch geeignete Verfahren, Prozesse und Kontrollen zu gewährleisten und kontinuierlich weiter zu entwickeln und zu verbessern:

63 *a.* Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken1 4 und Beurteilung der möglichen Auswirkungen der Ausnützung von Schwachstellen bezüglich der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten (gemäss Rz 53, 54 und 7);

64 *b.* Schutz der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten vor Cyber-Attacken durch die Implementierung angemessener Schutzmassnahmen, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit;
65 *c.* Zeitnahe Aufzeichnung und Erkennung von Cyber-Attacken auf Basis eines Prozesses zur systematischen und durchgängigen Überwachung der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten;
66 *d.* Reaktion auf identifizierte Schwachstellen und Cyber-Attacken durch die Entwicklung und Implementierung angemessener Prozesse, um zeitnah Massnahmen für die Eindämmung und Beseitigung einzuleiten; und
67 e. Sicherstellung einer zeitnahen Wiederherstellung des ordentlichen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen.

14 Angriffe auf die Vertraulichkeit, die Integrität und die Verfügbarkeit von IKT sowie auf die elektronischen kritischen Daten, welche durch die Ausnutzung von Schwachstellen oder Umgehung von Schutzmassnahmen durch externe oder interne Angreifende stattfinden.

68 Das Management der Cyber-Risiken hat sicherzustellen, dass eine erfolgreiche oder teilweise erfolgreiche Cyber-Attacke nach seiner Wesentlichkeit für kritische inventarisierte IKT-Bestandteile bzw. elektronische kritische Daten sowie kritische Prozesse (inkl. ausgelagerte Dienstleistungen und Funktionen) analysiert wird und die Meldepflicht nach FINMAG eingehalten wird. Nach erfolgter Erstbeurteilung und der Vororientierung an die zuständige Stelle bei der FINMA innerhalb von 24 Stunden ist die Meldung gemäss dem Anforderungskatalog der Erhebungsplattform EHP (Pflichtfelder) innerhalb von 72 Stunden zu übermitteln. Nach Abschluss der institutsseitigen Fallbearbeitung ist ein dem Schweregrad entsprechender abschliessender Ursachenbericht an die zuständige Stelle bei der FINMA einzureichen.
69 Die Geschäftsleitung lässt regelmässig Verwundbarkeitsanalysen1 5 und Penetrationstests1 6 durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen ausgeführt werden. Dabei sind alle inventarisierten Bestandteile der IKT, die über das Internet erreichbar sind, zu berücksichtigen. Zudem sind inventarisierte Bestandteile der IKT, welche nicht über das Internet erreichbar, aber für die Erbringung von kritischen Prozessen notwendig sind, oder welche elektronische kritische Daten beinhalten, zu berücksichtigen.

15 Analyse zur Identifikation von derzeit bestehenden Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur gegenüber Cyber-Attacken

16 Gezielte Prüfung und das Ausnützen von Software-Schwachstellen und Sicherheitslücken in der IKT

70 Auf Basis der institutsspezifischen Bedrohungspotenziale müssen risikobasiert szenariobezogene Cyber-Übungen1 7 durchgeführt werden. Das Ergebnis der Übungen ist in geeigneter Form zu dokumentieren und zu rapportieren.

17 Unter Berücksichtigung der Rz 19 könnten solche Cyber-Übungen beispielsweise beinhalten, Table-Top-, Red Teaming-Übungen usw.

Anhörungsbericht

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.

D. Management der Risiken kritischer Daten

Erläuterungen

4.1.5 Management der Risiken kritischer Daten (Kapitel IV Buchstabe D)

Neue Technologien und die Digitalisierung bewirken grundlegende Veränderungen im Finanzsektor. Damit einhergehend wird die Qualität, Integrität, Sicherheit und Nutzung von Daten immer entscheidender für die strategische Ausrichtung der Institute. Das neue Rundschreiben trägt dem Rechnung, indem es den bisherigen Fokus auf die Vertraulichkeit im Rahmen von Kundenidentifikationsdaten nun auch auf die Dimensionen der Integrität und Verfügbarkeit kritischer Daten allgemein erweitert.

Kritische Daten sind Daten, die besonders zu schützen und somit vom Institut risikobasiert zu definieren sind (Rz 7). Kritische Daten können sowohl in Bezug auf Vertraulichkeit als auch auf Integrität oder Verfügbarkeit kritisch sein und unterliegen daher unterschiedlichen Kritikalitätsstufen:

- Kritische Daten in Bezug auf **Vertraulichkeit**, d. h. vertrauliche Daten, sind Geschäftsinformationen, Kunden- oder personenbezogene Daten, die vor unberechtigtem Zugriff geschützt werden müssen, um die Privatsphäre oder Sicherheit einer Person oder einer Organisation zu schützen.
- Kritische Daten in Bezug auf **Integrität und Verfügbarkeit** sind vom Institut risikobasiert zu definieren. Die Kritikalität dieser Daten bezieht sich auf die Fähigkeit des Instituts, effizient und effektiv zu arbeiten - oder in einigen Fällen überhaupt zu arbeiten. Kritische Daten sind somit lebensnotwendig für das Funktionieren des Instituts („missionskritische Daten“). Missionskritische Daten sind beispielsweise Daten, die in Finanzberichten (sowohl intern als auch extern), regulatorischen Berichten, für einen Entscheidungsprozess, eine technische Realisierung oder zur Messung der Unternehmensleistung verwendet werden. Wenn diese Art von Daten beschädigt oder zerstört werden oder nicht mehr zugänglich sind, können das Institut und seine Einheiten und Mitarbeitende ihre Aufgaben möglicherweise nicht mehr erfüllen.

Die Einhaltung weitergehender gesetzlicher Verpflichtungen, wie bspw. des Datenschutzrechts bleibt vorbehalten. Die FINMA verfügt über keine Zuständigkeit betreffend die Anwendung des Datenschutzrechts.

Die Beaufsichtigten können gestützt auf das jeweils anwendbare Datenschutzrecht (z. B. das revidierte DSG) bei einem Vorfall auch gegenüber dem zuständigen Datenschutzbeauftragten eine Meldepflicht haben, welche sie neben der Meldepflicht gegenüber der FINMA zu erfüllen haben. Die Aufsichtskompetenz der zuständigen Datenschutzbeauftragten im Bereich des Datenschutzes bleibt unberührt.

Diese Präzisierung des Umgangs mit kritischen Daten geht auch einher mit einer Erhöhung des angestrebten Schutzniveaus im Vergleich zum Anhang 3 des bisherigen FINMA-RS 08/21. Dazu zählen folgende Elemente:

- Die Definition und Implementierung einer Datenstrategie durch die Institute, die u. a. die Strategie-Definition, Governance und Organisation, Prozesse, Datenund Informationsarchitektur sowie Datenschutz umfasst (Rz 71 bzw. 24);
- Während des Betriebs, der Entwicklung, der Veränderung und Migration von Systemen müssen die kritischen Daten besonders vor dem Zugriff und der Nutzung durch Unberechtigte geschützt werden (Rz 76).
- Ein hoher Schutz von Berechtigungsstrukturen ergibt sich nicht automatisch aus einer Risikobetrachtung heraus. Daher sind die (logischen und physischen) Bestandteile der IKT, die kritische Daten speichern oder verarbeiten, besonders zu schützen (Rz 77).

Die kritischen Daten werden entlang ihres gesamten Lebenszyklus verwaltet. Der Lebenszyklus umfasst Datenverantwortlichkeiten, Datensammlung, Ablageort, Unterhalt, Aufbewahrung (Retention), Löschung und Entsorgung. Er berücksichtigt Aspekte der Produktion, Anreicherung, Verarbeitung und Übertragung von kritischen Daten.

Auch wenn die Institute zunehmend ihre Daten und IT-Prozesse an Dritte auslagern, die nicht von der FINMA beaufsichtigt werden, bleiben die Institute für das Risikomanagement, die Datensicherheit und die Einhaltung von Gesetzen und Vorschriften verantwortlich. Outsourcing wird im FINMA-RS 18/3 behandelt. Das neue Rundschreiben schränkt somit weder die Implementierung noch die Nutzung von Cloud-Lösungen oder anderen Technologien ein, sondern legt fest, dass Daten ihrer Kategorisierung und vom Institut festgelegten Kritikalitätsstufen entsprechend zu schützen sind.

71 Die grundsätzlichen Erwartungen an die Strategie, Governance und Stärkung des Bewusstseins in Bezug auf die Risiken kritischer Daten sind in Rz 23–26 festgehalten.

72 Die Geschäftsleitung definiert geeignete Prozesse, Verfahren und Kontrollen sowie eindeutige AKV zum Umgang mit den vom Institut identifizierten kritischen Daten. Darüber hinaus beauftragt die Geschäftsleitung eine Einheit, um Rahmenbedingungen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von kritischen Daten zu schaffen und ihre Einhaltung zu überwachen.

73 Das Institut identifiziert seine kritischen Daten systematisch und vollständig, kategorisiert diese nach ihrer Kritikalität und definiert eindeutige Datenverantwortlichkeiten.

74 Die vom Institut definierten kritischen Daten werden entlang ihres gesamten Lebenszyklus verwaltet.

75 Dabei wird insbesondere die Einhaltung der Vertraulichkeit, Integrität und Verfügbarkeit bei der Verwaltung von kritischen Daten durch geeignete Prozesse, Verfahren und Kontrollen gewährleistet.

76 Kritische Daten sind im Betrieb und während der Entwicklung, Veränderung und Migration von IKT vor dem Zugriff und der Nutzung durch Unberechtigte angemessen zu schützen. Dies gilt auch für kritische Daten in Testumgebungen.

77 Die Bestandteile der IKT, die kritische Daten speichern oder verarbeiten, sind besonders zu schützen. Dabei ist der Zugriff auf diese Daten systematisch zu regeln und laufend zu überwachen.

78 Der Zugriff auf kritische Daten und verarbeitende Funktionalitäten ist auf Personen beschränkt, welche diesen zur Erfüllung ihrer Aufgaben benötigen1 8. Dabei muss das Institut über ein Autorisierungssystem verfügen. Der Zugang zu diesem Autorisierungssystem ist besonders zu schützen und regelmässig zu überprüfen. Die im Autorisierungssystem enthaltenen Berechtigungen sind regelmässig zu überprüfen.

18 Bspw. Need-to-knowund Least Privilege-Prinzip

79 Falls kritische Daten ausserhalb der Schweiz gespeichert werden1 9 oder vom Ausland aus auf sie zugegriffen werden kann, sind die damit verbundenen erhöhten Risiken angemessen zu begrenzen und mit geeigneten Massnahmen zu überwachen sowie die Daten besonders zu schützen.

19 Bspw. im Rahmen von Cloudoder Hosting-Lösungen

80 Sowohl interne wie externe Personen, die auf kritische Daten zugreifen oder diese verändern können, sind sorgfältig auszuwählen. Diese Personen sind mit geeigneten Massnahmen zu überwachen2 0 und regelmässig im Umgang mit diesen Daten zu schulen. Für Personen mit erhöhten Privilegien2 1 gelten erhöhte Sicherheitsanforderungen. Es ist zudem eine Liste aller Personen mit erhöhten Privilegien zu führen und laufend zu aktualisieren.

20 Bspw. Auswertung von Log-Dateien, Vier-Augen-Prinzip usw.
21 Bspw. Personen mit Administratorenrechten, Anwender mit funktionalem Zugriff auf eine grosse Menge an kritischen Daten usw.

81 Vorfälle, die die Vertraulichkeit, Integrität oder Verfügbarkeit von kritischen Daten wesentlich beeinträchtigen, müssen der FINMA unverzüglich gemeldet werden.

82 Bei der Auswahl von Dienstleistern, die kritische Daten bearbeiten2 2 oder einsehen können, ist der Sorgfaltsprüfung (Due Diligence) eine hohe Bedeutung beizumessen. Es sind klare Kriterien für die Beurteilung des Umgangs der Dienstleister mit kritischen Daten zu definieren und vor Vertragsvereinbarung

zu prüfen. Die Dienstleister sind im Rahmen des internen Kontrollsystems des Instituts risikoorientiert periodisch zu überwachen und zu kontrollieren.

22 Bearbeiten: jeder Umgang mit kritischen Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

Anhörungsbericht

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. 47a–47e ERV, Personen gemäss Art. 1b 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 geschützt 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.

E. Business Continuity Management (BCM)

Erläuterungen

4.1.6 Business Continuity Management (BCM; Kapitel IV Buchstabe E)

Dieser Abschnitt umfasst eine Überarbeitung des im FINMA-RS 08/21 bisher enthaltenen Grundsatzes 5 „Kontinuität bei Geschäftsunterbrechung" und ist im Wesentlichen eine prinzipienbasierte, aktualisierte Version der bisherigen SBVg Empfehlungen für das Business Continuity Management (BCM) in Abstimmung mit den BCBS-Papieren. Hierzu wird auch auf Kapitel 3 verwiesen.

Das BCM zielt darauf ab, dass bei bedeutenden Störungen oder Unterbrechungen von kritischen Prozessen, die über das Vorfallmanagement (Incident Management) hinausgehen, der Betrieb der kritischen Prozesse wieder hergestellt wird5 (Rz 9). Es besteht nicht unbedingt die Erwartung, dass bei jedem einzelnen Geschäfts- und Organisationsbereich kritische Prozesse bestehen (Rz 84).

5 Dies beinhaltet die bisher in den SBVg Empfehlungen für das Business Continuity Management (BCM) vom August 2013 definierten Ziele der Aufrechterhaltung der Kundendienstleistungen, der Einhaltung der regulatorischen Verpflichtungen des Unternehmens und/oder der Bewirtschaftung von Risikopositionen und dadurch Vermeidung kritischer (direkter oder indirekter) Schäden (vgl. Definition "Kritische Geschäftsprozesse" im Glossar der SBVg-Empfehlungen).

Eine Aktualisierung in Abstimmung mit den PSMOR betrifft die Transparenz über die für die kritischen Prozesse benötigten Ressourcen sowie die Verbindungen und Abhängigkeiten der Ressourcen und Prozesse untereinander (Rz 84). Die wie bisher in den SBVg-Empfehlungen genannten vier Kategorien6 wirken möglicherweise etwas einschränkend. Z. B. nennen die PSMOR auch die Abhängigkeiten zu Zentralbanken und Clearinghäusern. Daher wird innerhalb des neuen Rundschreibens auf eine Auflistung dieser vier Kategorien verzichtet. Eine Übersicht über möglicherweise benötigte Ressourcen wird im nachfolgenden Kapitel 4.1.7 gegeben. Aufgrund ihrer Relevanz für die kritischen Funktionen (siehe Kapitel 4.1.7) ist ein breiteres und detaillierteres Verständnis als bisher über die für die kritischen Prozesse benötigten Ressourcen nötig.

6 Ausfall von Personal, Ausfall von Gebäuden, Ausfall von IT-Systemen oder IT-Infrastruktur (inkl. Kommunikationssystemen), Ausfall von externen Dienstleistern und Lieferanten (Outsourcing) wie z.B.

Informationsprovider.

In ähnlicher Weise wird das Testen neu auf „schwerwiegende, aber plausible Szenarien“ bezogen (Rz 94). Damit soll verhindert werden, dass nur auf punktuelle Ausfälle oder Ausfälle einzelner Ressourcen aus einer der bisherigen vier Kategorien fokussiert wird. Auch soll durch die Verwendung dieser Begrifflichkeit eine Verbindung zu Kapitel 4.1.7 hergestellt werden, da das BCM einen Baustein für die Sicherstellung der operationellen Resilienz liefert.

Abhängig von der Grösse und Komplexität des Instituts kann es einen institutsweiten Business Continuity Plan (BCP) oder mehrere BCP geben (Rz 11, 86), sowie einen oder mehrere Disaster Recovery Plans (DRP; Rz 12, 88)

Abhängig von der Organisation des Instituts kann der Disaster Recovery Plan (DRP)7 im BCP enthalten sein oder separat erfasst werden. Er fungiert jedoch in jedem Fall als Teil eines BCP, d. h., die Präzisierungen des neuen Rundschreibens in Bezug auf den BCP gelten auch für den DRP (Rz 12, 88).

Im Bereich der IKT umfassen potenzielle Wiederherstellungsoptionen (wie in Rz 11 oder auch Rz 12 genannt) beispielsweise eine Hot Site-, eine Cold Site- oder eine Warm Site-Lösung. Diese Optionen haben im Allgemeinen unterschiedliche Wiederherstellungszeiten, Kosten und Funktionen. Die Bewertung der erwarteten Verfügbarkeitszeiten wird mit den in den Wiederherstellungsoptionen angegebenen Ressourcen und ihren RTO abgeglichen.

Schulungen und Trainingsmassnahmen zum BCM werden, wo nötig, auf die Interessensgruppen zugeschnitten und regelmässig auf den neuesten Stand gebracht (Rz 96).

In Antwort auf eine eintretende Krisensituation erfordert das BCM, bzw. die Aktivierung des Krisenstabs, die volle Aufmerksamkeit und das volle Engagement des Oberleitungsorgans und der Geschäftsleitung (Rz 89). Mögliche Beispiele von Krisensituationen sind Naturereignisse und Katastrophen, der Ausbruch einer Pandemie, gezielte Cyber-Attacken oder länger wirkende vollständige IKT-Unterbrechungen. Wichtig ist, dass das Institut bereits vorgängig geregelt hat, wie mit Krisensituationen umzugehen ist (bspw. Trigger, Krisenstab, Krisenorganisation).

Für Krisensituationen ist auch eine Kommunikationsstrategie zu definieren (Rz 90). Diese legt fest, wann welche Art von Kommunikation an welche internen und externen Interessensgruppen benötigt wird (bspw. Information der Mitarbeitenden, Kunden und Kundinnen, Gegenparteien und Dienstleistern, Medienmitteilungen sowie Meldepflicht an die Aufsichtsbehörde).

83 Die grundsätzlichen Erwartungen an die Strategie, Governance und Stärkung des Bewusstseins in Bezug auf Risiken aus der Ausgestaltung und Implementierung des BCM sind in Rz 23–26 festgehalten.

84 Jeder relevante Geschäfts- und Organisationsbereich hat im Rahmen der Business Impact Analyse (**BIA**) seine kritischen Prozesse und die dafür benötigten Ressourcen2 3 zu identifizieren.

23 Personal, Einrichtungen (bspw. Gebäude, Arbeitsplatzinfrastruktur), Informationen, IT-Systeme oder IT-Infrastruktur (inkl. Kommunikationssysteme), Abhängigkeiten zu andern Bereichen des Instituts und zu Drittparteien, bspw. externen Dienstleistern und Lieferanten (Outsourcing), Zentralbanken oder Clearinghäusern.

85 Für die kritischen Prozesse definiert das Institut die RTO und RPO nach Rz 10. Diese sind mit den dafür erforderlichen Leistungserbringern2 4 abgestimmt und die Einhaltung der RTO und RPO wird durch Service Level Agreements oder Verträge geregelt oder durch andere geeignete Verfahren, Prozesse und Kontrollen sichergestellt.

24 Bspw. mit der IT-Abteilung, anderen Bereichen des Instituts oder Externen

86 Das Institut definiert mindestens einen BCP nach Rz 11, der auch die den Plan auslösenden Gegebenheiten und Entscheidungsprozesse beschreibt und den Verlust der Ressourcen nach Rz 84 berücksichtigt. Die Akzeptanz von residualen Risiken wird angemessen dokumentiert.

87 Die BIA und BCP werden einer institutsweiten Vorgabe folgend auf konsistente Art erstellt und dokumentiert. Sie sind jährlich sowie ad hoc im Falle wesentlicher Änderungen im Geschäftsbetrieb (Reorganisationen, Aufbau eines neuen Geschäftsfelds, usw.) zu überprüfen und zu aktualisieren.

88 Das Institut definiert als Teil des BCP mindestens einen DRP. Wenn kritische Prozesse oder Teile davon ausgelagert sind, berücksichtigt der DRP die externen Abhängigkeiten und vertraglichen Regelungen sowie alternative Lösungen. Der DRP wird ad hoc im Falle wesentlicher Änderungen und mindestens jährlich überprüft und aktualisiert.

89 In Krisensituationen hat ein Krisenstab die Aufgabe der Krisenbewältigung bis zur Wiederherstellung eines ordnungsgemässen Zustands zu übernehmen. Die eine Krise auslö- senden Gegebenheiten und die AKV des Krisenstabs sind vorgängig zu regeln, und die Krisenorganisation auf die Geschäftstätigkeit und geographische Struktur des Instituts auszurichten. Die Erreichbarkeit der Verantwortungsträger in Krisensituationen ist sicherzustellen.

90 Das Institut definiert eine Kommunikationsstrategie für die interne und externe Kommunikation in Krisensituationen.

91 Mit Tests wird die Umsetzung der BCP und des DRP sowie die Funktionsfähigkeit der Krisenorganisation regelmässig beurteilt. Dafür wird eine systematische Planung erstellt, die die regelmässige Abdeckung sicherstellt. Es können verschiedene Vorgehen zum Testen von unterschiedlicher Intensität und Effektivität gewählt werden, so auch bspw. Table-Top-Übungen.

92 Die gemäss BCP und DRP wichtigsten Massnahmen und die Krisenorganisation werden mindestens einmal jährlich getestet.

93 Relevante Anspruchsgruppen, einschliesslich diejenigen in Fachund IT-Funktionen, nehmen an den Tests teil, um sich mit den Wiederherstellungsprozessen vertraut zu machen.

94 Die Tests umfassen verschiedene schwerwiegende, aber plausible Szenarien und berücksichtigen Wiederherstellungsabhängigkeiten, einschliesslich solcher, die zu internen oder externen Drittparteien bestehen.

95 Eine regelmässige Berichterstattung an das Oberleitungsorgan und die Geschäftsleitung informiert über die durchgeführten Testund Überprüfungsaktivitäten und deren Ergebnisse. Sie zeigt vorgenommene Priorisierungen (bspw. Priorisierung der für die Erbringung der kritischen Funktionen nach Rz 14 benötigten kritischen Prozesse) und erkannte Lücken in der Abdeckung anderer kritischer Prozesse klar auf.

96 Die Mitarbeitenden sowie die Mitglieder der Krisenorganisation werden hinsichtlich ihrer AKV, die sich aus den diversen BCM Aktivitäten ergeben, ausreichend geschult, sowohl bei Neueintritt von Mitarbeitenden als auch als Teil regelmässiger Schulungen.

Anhörungsbericht

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.

F. Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft

Erläuterungen

4.1.7 Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft (Kapitel IV Buchstabe F)

Die Rz 97–100 wurden im Wesentlichen unverändert aus dem bisherigen Rundschreiben (Grundsatz 7, Rz 136.2–146.5) übernommen.

Eine Anpassung stellt die Streichung des folgenden Satzes dar: „Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Institute ausländisches Aufsichtsrecht einhalten". Es handelt sich dabei um eine Hervorhebung in Bezug auf ausländisches Aufsichtsrecht, da dieses für die betroffenen Institute von besonderer Relevanz sein kann. Die im besagten Satz formulierte Erwartungshaltung geht letztlich zurück auf die generelle Anforderung, die Risiken im grenzüberschreitenden Dienstleistungsgeschäft zu erfassen, zu begrenzen und zu kontrollieren, wobei nicht nur Aufsichtsrecht, sondern sämtliche im spezifischen Fall relevanten Rechtsnormen erfasst sind. Diesem Satz kommt also neben den generellen Ausführungen zu den aufsichtsrechtlichen Anforderungen an das Management der Rechtsrisiken keine eigenständige Bedeutung zu, weshalb er gestrichen werden kann. Der Massstab zur Beurteilung einer Verletzung von schweizerischem Aufsichtsrecht infolge Nichteinhaltung ausländischen Rechts orientiert sich weiterhin an den generellen Anforderungen, wie sie den Rz 97–100, den aufsichtsrechtlichen Organisationsvorschriften und den Anforderungen an die Gewähr für eine einwandfreie Geschäftstätigkeit zu entnehmen sind. Insofern bewirkt die Streichung des erwähnten Satzes keine materiell-regulatorische Änderung.

Der Begriff „Finanzdienstleistungen" wurde durch den Begriff „Dienstleistungen" ersetzt, da nach Art. 3 Bst. c FIDLEG der Begriff „Finanzdienstleistungen" so eng definiert ist, dass gewisse banktypische Dienstleistungen (Depotgeschäft und Zahlungsdienstleistungen) nicht erfasst wären. Abgesehen davon gab es keine Anpassungen.

97 Wenn Institute oder ihre Gruppengesellschaften grenzüberschreitend Dienstleistungen erbringen oder Finanzprodukte vertreiben, sind auch die aus einer Anwendung ausländischer Rechtsvorschriften (Steuer-, Straf-, Geldwäschereirecht usw.) resultierenden Risiken angemessen zu erfassen, begrenzen und kontrollieren.

98 Die Institute unterziehen ihr grenzüberschreitendes Dienstleistungsgeschäft 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 spezifische Dienstleistungsmodelle für die bedienten Länder, schulen die Mitarbeitenden und stellen durch entsprechende organisatorische Massnahmen, Weisungen, Vergütungs- und Sanktionsmodelle die Einhaltung der Vorgaben sicher.

99 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.

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

Anhörungsbericht

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 Anhö- rung sieht die FINMA keinen Anpassungsbedarf der Randziffern

zum grenz- überschreitenden Dienstleistungsgeschäft.

V. Sicherstellung der operationellen Resilienz

Erläuterungen

4.1.8 Operationelle Resilienz (Kapitel V)

Seit der Finanzkrise von 2007–2009 stärkte das BCBS mit seinen Reformen die finanzielle Resilienz der Banken. Während seine Anforderungen an die Eigenmittel und Liquidität die Fähigkeit der Banken zur Absorption von finanziellen Schocks verbesserten, wurde die operationelle Resilienz bisher noch nicht ausreichend berücksichtigt. Hierbei geht es um die Fähigkeit, signifikante operationelle Schocks mit möglichst geringen negativen Auswirkungen überstehen und zeitnah überwinden zu können. Operationelle Schocks entstehen dabei bspw. durch Ereignisse wie Pandemien, Cyber-Attacken, Systemausfälle, Versagen von Lieferketten, grossflächige oder andauernde Stromausfälle oder Naturkatastrophen. Die Wahrscheinlichkeit und die Auswirkungen solcher Ereignisse haben sich in den letzten Jahren erhöht.

Eines von mehreren Konzepten, die die operationelle Resilienz unterstützen, ist das BCM. Dieses wird jedoch als insgesamt noch zu kurz greifend aufgefasst, da der Fokus auf Wiederherstellungsplänen nach einer Unterbrechung liegt. Die neuen POR des BCBS zielen darauf ab, zusätzlich folgende Aspekte miteinzubringen:

1. Strategischer Fokus mit einer Top-Down-Sicht auf die strategisch wichtigsten Operationen oder Leistungserbringungen, im Rundschreiben als „kritische Funktionen“ bezeichnet.
2. Präventiver Fokus mit gezielten vorbeugenden Massnahmen, Aufbau des Betriebsmodells und kontinuierlichem Lernen und Verbesserungen, um die kritischen Funktionen so widerstandsfähig wie möglich zu gestalten (Resilience by Design).

Auch das Management der operationellen Risiken unterstützt die operationelle Resilienz. Wenn die Risikotoleranz für operationelle Risiken klar definiert ist und operationelle Risiken entsprechend minimiert werden, so sinkt tendenziell auch das Risiko von signifikanten Unterbrechungen und deren Auswirkungen.

Das erwähnte BCBS Papier definiert die als besonders schützenswerten Objekte im Rahmen der Sicherstellung der operationellen Resilienz des Instituts mit „critical operations“. Mehrere Begriffe könnten hierzu als Übersetzung der „operations“ gewählt werden, unter anderem die Begriffe „Operationen“, „Dienstleistungen“ (wie von den britischen Behörden angewendet) oder „Funktionen“. Die Interpretationen dieser Begriffe im schweizerischen Raum sind nicht scharf voneinander getrennt. Aus den folgenden Gründen wurde für die Übersetzung der Begriff „Funktionen“ gewählt:

- Abstimmung mit der FINMA-Aufsichtsmitteilung 05/2020 „Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG“, die den Begriff „kritische Funktionen“ verwendet.
- Abstimmung mit Art. 8 Abs. 1 BankG, in dem „systemrelevante Funktionen“ definiert werden. Diese sind namentlich das inländische Einlagenund Kreditgeschäft sowie der Zahlungsverkehr.
- Keine Verwendung des Begriffs „Dienstleistungen“ zur Vermeidung von Missverständnissen, da dieser Begriff eine zu einschränkende Assoziation rein mit Produkten oder Kundendienstleistungen haben könnte.
- Abgrenzung zu „kritischen Geschäftsprozessen“ oder „kritischen Prozessen“ wie im BCM bis anhin bzw. neu verwendet. Solche Prozesse können die kritischen Funktionen unterstützen, sind dann aber nur Teilkomponenten davon.

Die „kritischen Funktionen“ des neuen Rundschreibens umfassen (Rz 14– 16):

a. für alle Institute: die Aktivitäten, Prozesse, Dienstleistungen und die für ihre Erbringung notwendigen zugrundeliegenden Ressourcen, deren Unterbrechung die Weiterführung des Instituts oder seine Rolle im Finanzmarkt und damit die Funktionsfähigkeit der Finanzmärkte gefährden würde; und

b. für systemrelevante Banken nach Art. 8 BankG: die systemrelevanten Funktionen nach Art. 8 Abs. 1 BankG.

Bei den unter Buchstabe a. genannten „Prozessen“ ist davon auszugehen, dass die für die Erbringung kritischer Funktionen notwendigen Prozesse immer „kritische Prozesse“ nach der im BCM verwendeten Terminologie sind.

Der Schutz der Rolle im Finanzmarkt bedeutet nicht, dass der Fokus des Instituts alleine auf sich gerichtet sein soll (Rz 14–16). Die Ziele der Finanzmarktaufsicht nach Art. 4 FINMAG sind auch in Hinblick auf die Sicherstellung der operationellen Resilienz relevant, d. h. der Schutz der Gläubigerinnen und

Gläubiger, der Anlegenden und der Versicherten sowie der Schutz der Funktionsfähigkeit der Finanzmärkte.

Eine kritische Funktion beinhaltet eine End-to-End bzw. Front-to-Back Sicht der gesamten für ihre Erbringung notwendigen Lieferkette und der dazu benötigten Ressourcen (Rz 107). Es ist somit möglich, dass für das Erbringen einer kritischen Funktion mehrere kritische Prozesse benötigt werden. Tendenziell erfassen die Institute in ihrem BCM viele (teils hunderte) kritische Prozesse. Eine Gleichsetzung der kritischen Prozesse mit den kritischen Funktionen ist nicht angedacht. Es sollte pro Institut nur eine geringe und leicht überschaubare Anzahl an kritischen Funktionen geben. Falls kleinere Institute eine sehr überschaubare Anzahl kritischer Prozesse definiert haben, ist im Rahmen des Proportionalitätsprinzips jedoch eine Verbindung eins-zu-eins zwischen den kritischen Prozessen und den kritischen Funktionen denkbar.

Die Abbildung 1 zeigt auf, wie für die Erbringung kritischer Funktionen gewisse zu identifizierende Prozesse (bzw. kritische Prozesse), Aktivitäten und Dienstleistungen benötigt werden. Auch zeigt sie vereinfacht die dafür benö- tigten, zu identifizierenden, zugrundeliegenden Ressourcen und die Abhängigkeiten all dieser Komponenten untereinander. Die Begriffe „Aktivitäten“ und „Dienstleistungen“ werden nicht weitergehend definiert, um zu berücksichtigen, dass es Differenzen in den von den Instituten verwendeten Begrifflichkeiten gibt und eine gewisse Flexibilität diesbezüglich zuzulassen.

Abbildung 1: Komponenten für die Erbringung der kritischen Funktion

Bei der Identifizierung der benötigten, zugrundeliegenden Ressourcen soll granular vorgegangen und das Netz weit ausgebreitet werden, um ein möglichst transparentes Verständnis der benötigten Ressourcen zu erhalten (Rz 107). Mögliche Ressourcen können etwa sein:

- **Externe**: Service Providers, Cloud-Anbieter, relevante Inputs liefernde Gegenparteien (z. B. Zentralbanken, Clearinghäuser, andere Banken usw.), Stromzufuhr, Gebäudeoder Einrichtungsvermieter, Consultants
- **IKT**: IT-Anwendungen in den Geschäftsbereichen, IT-Basissysteme, die zugrundeliegende IT-Infrastruktur (z. B. Rechenzentren und alternative Sites), Telekommunikation
- **Informationen**: Inputs, Daten und Datensätze, die für die Erbringung kritischer Funktionen benötigt werden
- **Einrichtungen**: Gebäude und Arbeitsplätze, Arbeitsplatzeinrichtung inkl. Laptops und Work-from-Home-Organisation, Trading Desk-Vorrichtung
- **Personal**: relevante Teams, verschiedene zur Erbringung der kritischen Funktion beisteuernde Bereiche des Instituts, Schlüsselpersonen, spezifische benötigte Fähigkeiten des Personals

Das Verständnis der vorhandenen Verbindungen und Abhängigkeiten sowohl innerhalb des Instituts als auch nach aussen zu relevanten Input liefernden externen Parteien ist wichtig. Aufgrund dessen können Auswirkungen verschiedenartiger Unterbrechungen verstanden und Massnahmen ergriffen werden, um trotz solcher Unterbrechungen die kritische Funktion weiterhin erbringen zu können.

Bei der Identifizierung der benötigten Ressourcen und der Verbindungen und Abhängigkeiten ist es denkbar, dass verschiedene Ressourcen sich als wichtiger herausstellen als andere und daher speziell geschützt werden müssen.

Für die Sicherstellung der operationellen Resilienz wird der Begriff der „Unterbrechungstoleranz“ eingeführt (Rz 17). Diese wird für jede kritische Funktion definiert und beschreibt das Ausmass, in dem die Unterbrechung der kritischen Funktion vom Institut toleriert werden kann. Dieses Ausmass kann auf verschiedene Arten gemessen werden. Als Beispiele können etwa genannt werden: eine maximal tolerierbare Zeitspanne der Unterbrechung, ein maximal tolerierbarer entstehender finanzieller Verlust, eine maximal tolerierbare Beeinträchtigung von Kundenaktivitäten oder ein maximal tolerierbarer Verlust an Geschäften oder Kunden. Das Oberleitungsorgan ist sich über die Auswirkungen von Unterbrechungen und die definierten Unterbrechungstoleranzen im Klaren und genehmigt diese (Rz 101, 103). Die Fähigkeit, kritische Funktionen innerhalb der Unterbrechungstoleranz zu erbringen, wird sichergestellt, indem wo nötig zusätzliche Massnahmen getroffen werden, die das Einhalten der Unterbrechungstoleranz ermöglichen (Rz 102).

Bei Unterbrechungen der kritischen Funktionen wird von „schwerwiegenden, aber plausiblen“ Szenarien ausgegangen (Rz 17). Hierbei kann es sich in einem ersten Schritt um den Verlust einzelner, wichtiger Ressourcen handeln; es sollte jedoch alsbald zu weitergehenden Szenarien übergegangen werden, in denen der Verlust mehrerer Ressourcen oder ganzer Abhängigkeitsketten berücksichtigt wird. Als ein Beispiel sei angenommen, dass die externe Stromzufuhr aus dem öffentlichen Netz längere Zeit grossflächig unterbrochen wird und die Laufzeiten der im Rahmen des BCM bereitgestellten unterbrechungsfreien Stromversorgung (Uninterruptible Power Supply) nicht ausreichen. Dann fallen die ganze oder ein Grossteil der dem Personal und Kunden zur Verfügung stehenden Telekommunikation und IT-

Systeme aus und viele Prozesse können nicht mehr erbracht werden; somit voraussichtlich auch die kritischen Funktionen nicht mehr. Zur Sicherstellung der operationellen Resilienz sind Massnahmen zu ergreifen, die die Erbringung der kritischen Funktionen innerhalb der Unterbrechungstoleranz gewährleisten (Rz 102). Es kann nicht ausgeschlossen werden, dass manche Szenarien 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 (Fussnote 25).

Unterbrechungstoleranzen sind nicht mit den im BCM definierten RTO oder RPO (Rz 10) gleichzusetzen, da letztere eher pro IT-System definiert werden. Die Unterbrechungstoleranzen der kritischen Funktionen sollen stattdessen unter Berücksichtigung aller benötigten Ressourcen, Verbindungen und Abhängigkeiten gewählt werden. Die im BCM bestimmten RTO und RPO sollten so gewählt sein, dass sie der Unterbrechungstoleranz nicht widersprechen. Wenn für eine bestimmte kritische Funktion eine Unterbrechungstoleranz von z. B. einem Tag gewählt wird, dann sollte die RTO eines für die Erbringung dieser kritischen Funktion benötigten IT-Systems nicht länger als ein Tag sein.

Es ist möglich, dass pro kritischer Funktion die Definition mehrerer Unterbrechungstoleranzen nötig ist, um verschiedene zugrundeliegende Aspekte der kritischen Funktion abzudecken (Rz 17).

Die Fähigkeit, kritische Funktionen innerhalb ihrer Unterbrechungstoleranz unter schwerwiegenden, aber plausiblen Szenarien erbringen zu können, ist regelmässig zu testen (Rz 110). Dabei können verschiedene Vorgehen zum Testen von unterschiedlicher Intensität und Effektivität gewählt werden. Beispiele sind Walk-Through, Table Top-Übungen, lokalisierte oder auf den Ausfall einzelner Ressourcen beschränkte Tests, vollumfängliche Tests (Annahme eines Komplettausfalls). Bei der Testplanung wird die Effektivität der Tests mit den Risiken der Tests abgewogen. Es ist davon auszugehen, dass manche schwerwiegende, aber plausible Szenarien nicht vollständig live getestet werden können, bspw. eine langanhaltende Stromunterbrechung. In solchen Fällen kann im Rahmen von Trockenübungen wie Table Top-Übungen verfahren werden; jedoch ist es wichtig, die diversen identifizierten Verbindungen und Abhängigkeiten zu berücksichtigen.

101 Das Institut identifiziert seine kritischen Funktionen und deren Unterbrechungstoleranzen. Diese werden vom Oberleitungsorgan genehmigt. Ausserdem genehmigt und überwacht das Oberleitungsorgan regelmässig das Vorgehen zur Sicherstellung der operationellen Resilienz.

102 Das Institut trifft Massnahmen zur Sicherstellung der operationellen Resilienz unter Berücksichtigung schwerwiegender, aber plausibler Szenarien2 5.

25 Es kann nicht ausgeschlossen werden, dass manche Szenarien nicht ohne Einbezug des Staates bewältigt werden können (bspw. Pandemien, Kriege, langanhaltende Strommangellage). Für solche Szenarien sind durch das Institut Vorarbeiten zwecks Stärkung seiner operationellen Resilienz gegenüber diesen Szenarien im Rahmen seiner Möglichkeiten zu leisten.

103 Die kritischen Funktionen und die damit verbundenen Unterbrechungstoleranzen nach Rz 14 sind mindestens jährlich durch das Oberleitungsorgan zu genehmigen.

104 Das Institut koordiniert die relevanten Bestandteile eines umfassenden Risikomanagements wie beispielsweise das Management der operationellen Risiken, inklusive das Management der IKT- und Cyber-Risiken, das Business Continuity Management, das Management von Auslagerungen (Outsourcing; vgl. das FINMA-Rundschreiben 2018/3 „Outsourcing“), und die Notfallplanung (Kapitel VI) dahingehend, dass diese zu einer Stärkung der operationellen Resilienz des Instituts beitragen. Dies beinhaltet einen angemessenen Austausch relevanter Informationen zwischen diesen verschiedenen Bereichen.

105 Zur operationellen Resilienz hat mindestens jährlich eine Berichterstattung an das Oberleitungsorgan und die Geschäftsleitung zu erfolgen, sowie bei wesentlichen Kontrollschwächen oder Vorfällen, die die operationelle Resilienz gefährden.

106 Für die kritischen Funktionen werden interne und externe Bedrohungen sowie die entsprechende Ausnützung von Verwundbarkeiten identifiziert und beurteilt. Die daraus resultierenden operationellen Risiken werden im Rahmen des Managements der operationellen Risiken identifiziert, beurteilt, begrenzt und überwacht.

107 Das Institut führt ein Inventar seiner kritischen Funktionen, das mindestens jährlich überprüft und aktualisiert wird. Dieses Inventar beinhaltet die Unterbrechungstoleranzen der kritischen Funktionen, sowie

die Verbindungen und Abhängigkeiten zwischen den benö- tigten kritischen Prozessen und deren Ressourcen2 6 zur Erbringung der kritischen Funktionen.

26 Inklusive die für die kritischen Funktionen relevanten Bestandteile des Inventars nach Rz 53

108 Für die kritischen Funktionen werden mindestens die wesentlichen operationellen Risiken und die Schlüsselkontrollen dokumentiert.

109 Die kritischen Funktionen und die dafür benötigten kritischen Prozesse und Ressourcen sind durch BCPs nach Kapitel IV Bst. E abgedeckt.

110 Die Fähigkeit, kritische Funktionen innerhalb ihrer Unterbrechungstoleranz unter schwerwiegenden, aber plausiblen Szenarien erbringen zu können, wird regelmässig getestet oder geübt. Dazu gehören auch Szenarien, die sich von kürzeren und eher begrenzt wirkenden Unterbrechungen unterscheiden und sich durch eine längere Zeitdauer (bspw. über Monate hinweg) und einen Ausfall grundlegender Ressourcen auszeichnen2 7. Die Tests bzw. Übungen werden dabei so gestaltet sein, dass sie das Institut nicht grundlegend gefährden.

27 Beispiele sind eine Pandemie, eine Strommangellage, ein längerer Ausfall durch die Insolvenz eines wichtigen Dienstleisters (als Beispiel für einen Stressed Exit eines Dienstleisters) oder ein längeranhaltendes Verbot ausländischer Regierungen, gemäss dem auslandsbasierte Cloud-Anbieter oder andere Dienstleister schweizerische Firmen nicht mehr bedienen dürfen.

111 Für systemrelevante Banken sind die für die Weiterführung der kritischen Funktionen nach Rz 14 relevanten BCP, DRP und die Krisenorganisation nach Kapitel IV Bst. E. mit der Notfallplanung nach Kapitel VI abzustimmen.

Anhörungsbericht

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.

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, branchenbzw. 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.

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 verschmol
zen 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 Continuityund 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.

VI. Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken

112 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 in diesem Zusammenhang von internationalen Standardsettern erlassenen Vorgaben.

Erläuterungen

4.1.9 Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken (Kapitel VI)

Bis auf eine sprachliche Umformulierung ohne inhaltliche Relevanz wurden keine Änderungen durchgeführt. Die in diesem Grundsatz genannten systemrelevanten Banken sind die systemrelevanten Banken nach Art. 8 Abs. 3 BankG.

Anhörungsbericht

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.

VII. Übergangsbestimmungen

A. Betreffend die Sicherstellung der operationellen Resilienz

113 Die Identifikation der kritischen Funktionen, die Definition der Unterbrechungstoleranzen und erste Genehmigungen nach Rz 101 und 103, sowie eine erste Berichterstattung nach Rz 105, werden ab Inkrafttreten des Rundschreibens erwartet. Für die Erfüllung der Anforderungen nach den Rz 106–109 sowie erste Tests nach Rz 110 gilt eine Übergangsfrist von einem Jahr ab Inkrafttreten. Die Sicherstellung der operationellen Resilienz nach Rz 102 sowie die Erfüllung der Anforderungen nach den Rz 104 und 111 werden innert einer Übergangsfrist von zwei Jahren erwartet.

B. Betreffend die Eigenmittelanforderungen für operationelle Risiken

114 Die Eigenmittelanforderungen für operationelle Risiken nach Art. 89 ff. ERV richten sich bis zum Inkrafttreten der im Rahmen des Revisionspakets „Basel III final" revidierten ERV und der ausführenden FINMA-Verordnung dazu nach den Rz 3–116 des FINMA-Rundschreibens 2008/21 „Operationelle Risiken – Banken".

Anhörungsbericht

3.13 Übergangsfristen

Stellungnahmen

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

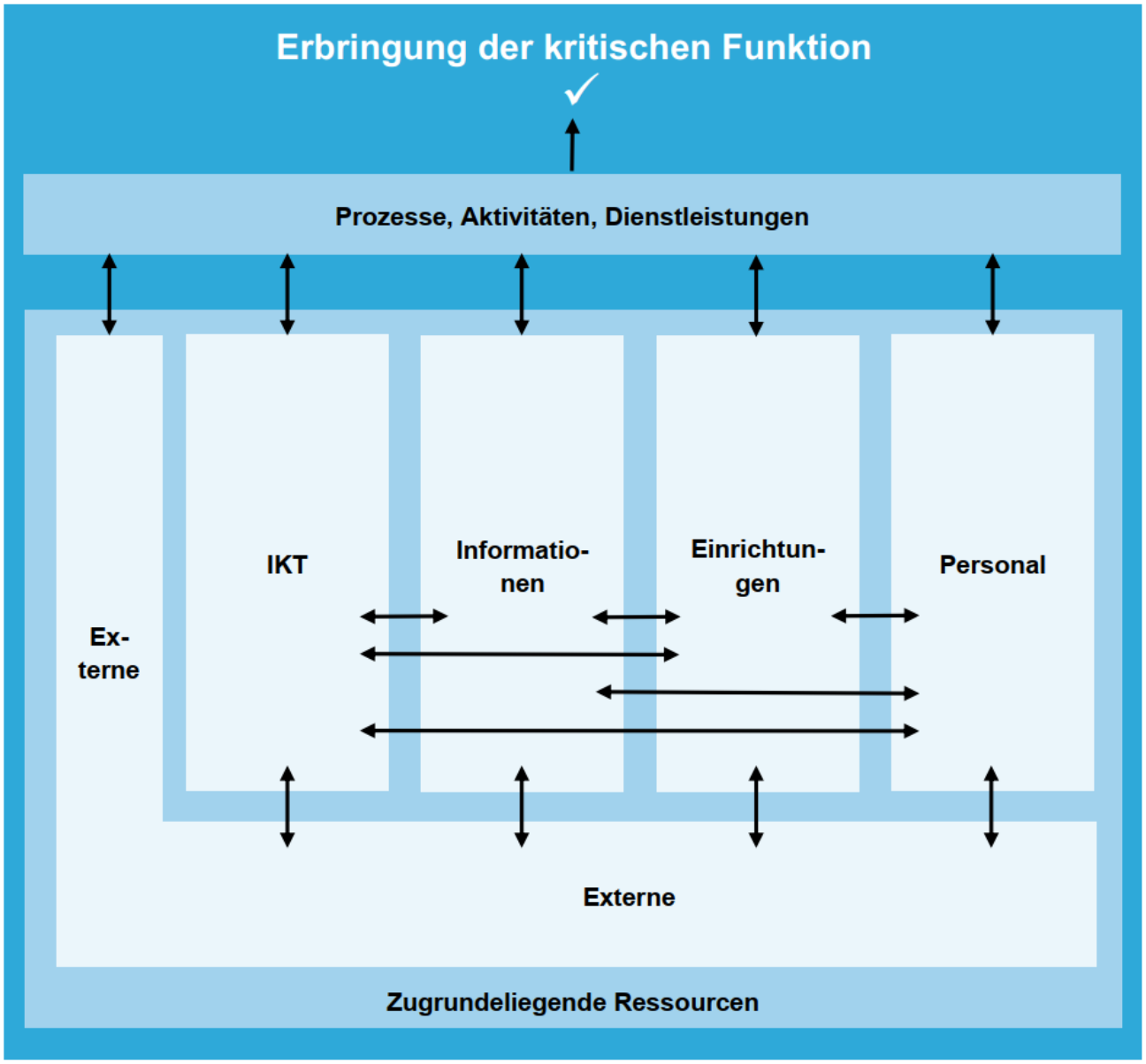
So empfehlen die SBVg und der VSKB eine Verlängerung der Übergangsfristen für die operationelle Resilienz um ein Jahr sowie eine einjährige
Übergangfrist zu allen restlichen Grundsätzen. IIAS und eine weitere Eingabe empfehlen eine Übergangsfrist von mindestens einem Jahr für das Management der Risiken 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.

Anhang 1 - Erläuternde Graphik zur operationellen Resilienz



Komponenten für die Erbringung der kritischen Funktion