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

# Rundschreiben 2008/21 „Operationelle Risiken – Banken“ – Totalrevision

# Rundschreiben 2013/3 „Prüfwesen“ – Teilrevision

Erläuterungen

7. Dezember 2022

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

# Inhaltsverzeichnis

## Kernpunkte

1. Die FINMA nimmt eine Totalrevision des FINMA-Rundschreibens 2008/21 „Operationelle Risiken – Banken“ vor. Dieses wird durch das neue FINMA-Rundschreiben „Operationelle Risiken und Resilienz – Banken“ ersetzt.

2. Die Anpassungen der qualitativen Anforderungen des FINMA-Rundschreibens 08/21 bestehen aus Konkretisierungen der Aufsichtspraxis einerseits in Bezug auf das Management der operationellen Risiken im Allgemeinen, das Management der Risiken im Zusammenhang mit der Informations- und Kommunikationstechnologie (IKT) und kritischen Daten sowie der Cyber-Risiken im Speziellen und andererseits in Bezug auf das Business Continuity Management (BCM) sowie die operationelle Resilienz.

3. Die Anpassungen der qualitativen Anforderungen basieren auf den *Revisions to the Principles for the Sound Management of Operational Risk* (PSMOR) und den neuen *Principles for Operational Resilience* (POR) des *Basel Committee on Banking Supervision* (BCBS) vom März 2021.

4. Die Anpassungen der qualitativen Anforderungen sind prinzipienbasiert und technologieneutral. Die Proportionalität wird angemessen berücksichtigt.

5. Die Eigenmittelanforderungen des aktuellen FINMA-Rundschreibens 08/21 werden im Rahmen der Umsetzung der finalen Basel III Regeln durch Anforderungen in der zu revidierenden Eigenmittelverordnung und der dazugehörigen FINMA-Ausführungsbestimmungen ersetzt. Sie sind daher nicht Gegenstand des neuen Rundschreibens.

6. Die Totalrevision führt auch zu Anpassungen des FINMA-Rundschreiben 2013/3 „Prüfwesen“, welches somit zeitgleich teilrevidiert wird. Das neue Rundschreiben „Operationelle Risiken und Resilienz – Banken“ tritt per 1. Januar 2024 in Kraft, mit Übergangsfristen über zwei Jahre für die Sicherstellung der operationellen Resilienz. Das teilrevidierte FINMA-Rundschreiben 13/3 soll auf den 1. Januar 2024 in Kraft treten.

## Abkürzungsverzeichnis

| | |
|---|---|
| BankG | Bankengesetz vom 8. November 1934 (SR 952.0) |
| BankV | Bankenverordnung vom 30. April 2014 (SR 952.02) |
| BCBS | *Basel Committee on Banking Supervision* |
| BCM | *Business Continuity Management* |
| BRP | *Business Recovery Plan* |
| DRP | *Disaster Recovery Plan* |
| DSG | Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz) (SR 235.1) |
| ERV | Eigenmittelverordnung vom 1. Juni 2012 (SR 952.03) |
| FIDLEG | Finanzdienstleistungsgesetz vom 15. Juni 2018 (SR 950.1) |
| FINIG | Finanzinstitutsgesetz vom 15. Juni 2018 (SR 954.1) |
| FINIV | Finanzinstitutsverordnung vom 6. November 2019 (SR 954.11) |
| FINMAG | Finanzmarktaufsichtsgesetz vom 22. Juni 2007 (SR 956.1) |
| IKT | Informations- und Kommunikationstechnologie |
| IOSCO | *International Organization of Securities Commissions* |
| POR | BCBS *Principles for Operational Resilience* vom 31. März 2021 |
| PSMOR | BCBS *Revisions to the Principles for the Sound Management of Operational Risk* vom 31. März 2021 |
| RPO | *Recovery Point Objective* |
| RTO | *Recovery Time Objective* |
| SBVg | Schweizerische Bankiervereinigung |

# 1 Inhalt und Ziel der Vorlage

Das FINMA-Rundschreiben 2008/21 „Operationelle Risiken – Banken“ (FINMA-RS 08/21) legte u. a. die qualitativen Anforderungen an das Management der operationellen Risiken dar. Es konkretisierte damit die bestehenden Gesetze und Bundesratsverordnungen (insb. Art. 3 Abs. 2 Bst. a und 3*f* BankG sowie Art. 12 BankV, Art. 9 FINIG und Art. 68 FINIV) in Bezug auf die Organisation, die Funktionentrennung, das Risikomanagement und die interne Kontrolle im Zusammenhang mit den operationellen Risiken.

Die neuen POR und die revidierten PSMOR des BCBS, sowie die starken Entwicklungen im Bereich der Digitalisierung und der IKT gaben den Auslöser für eine Totalrevision des FINMA-RS 08/21.

Ziel des neuen Rundschreibens „Operationelle Risiken und Resilienz - Banken“ ist es, in Bezug auf die operationellen Risiken und die operationelle Resilienz Transparenz zu schaffen über die Anwendung des Finanzmarktrechts durch die FINMA. Dies erfolgt möglichst schlank, prinzipienbasiert, proportional, technologieneutral und in Abstimmung mit internationalen Standards.

Durch das neue Rundschreiben benötigte Anpassungen am Prüfwesen bei den Banken und Wertpapierhäusern werden durch eine Teilrevision des FINMA-Rundschreiben 2013/3 „Prüfwesen“ (FINMA-RS 13/3) vorgenommen.

# 2 Handlungsbedarf

Die Umsetzung internationaler Standards ist Teil der Finanzmarktstrategie des Bundesrats und in Art. 7 Abs. 2 Bst. d FINMAG verankert. Dazu gehören auch neue Standards des BCBS.

Folgende internationale Standards des BCBS sollen mit vorliegender Totalrevision umgesetzt werden:

- *Basel III: Finalising Post-Crisis Reforms*[1], Dezember 2017. Dieses Papier beinhaltet eine neue Methodik zur Berechnung der Mindesteigenmittel für operationelle Risiken, die auf Verordnungsstufe umgesetzt wird. Die Eigenmittelanforderungen des FINMA-RS 08/21 sind somit nicht mehr Teil des neuen Rundschreibens. Die Umsetzung der finalen Basel III Regeln ist Gegenstand eines separaten Prozesses auf Stufe

[1] Abrufbar unter https://www.bis.org/bcbs/publ/d424.htm

Bundesrat (ERV) sowie FINMA (ausführende Verordnungen dazu). Betreffend die Aufhebung der Eigenmittelanforderungen sowie die Übergangsregelung vgl. Kapitel 8.

- *Principles for Operational Resilience*[2] (POR), März 2021. Dies ist ein neues Papier, mit dem eine Stärkung der operationellen Widerstandsfähigkeit (Resilienz) der Banken angestrebt wird angesichts gestiegener und komplexerer Bedrohungslagen, insbesondere im Zusammenhang mit der zunehmenden Digitalisierung.

- *Revisions to the Principles for the Sound Management of Operational Risk*[3] (PSMOR), März 2021. Es handelt sich hierbei um eine Revision der bereits bestehenden Grundsätze zum Management der operationellen Risiken. Das BCBS hat die bestehenden Grundsätze auf ihre fortwährende Angemessenheit überprüft, aktualisiert und durch einen neuen Grundsatz zur IKT ergänzt.

Mit dem neuen Rundschreiben schafft die FINMA Transparenz über die Umsetzung dieser internationalen Standards des BCBS zum Management der operationellen Risiken und zur Sicherstellung der operationellen Resilienz im Rahmen der Finanzmarktgesetzgebung. Das Rundschreiben dient ausschliesslich der Rechtsanwendung und enthält keine rechtsetzenden Bestimmungen.

Eine Aktualisierung des FINMA-RS 08/21 ist ausserdem angebracht, um den starken Entwicklungen im Technologieumfeld seit Erlass des Rundschreibens Rechnung zu tragen. Die Abhängigkeiten von einer reibungslos funktionierenden IKT sind gestiegen, während Systemlandschaften und Lieferketten tendenziell komplexer geworden sind, wodurch sich neue Fragestellungen ergeben. Zudem sind grössere Ausfälle sowie Cyber-Angriffe häufiger geworden. Als Teil dieser Entwicklungen haben sich auch Herausforderungen im Zusammenhang mit dem Management der Daten in Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit verdeutlicht.

Durch die Anpassungen am FINMA-RS 08/21 ergibt sich auch ein Handlungsbedarf für das FINMA-RS 13/3 zum Prüfwesen bei den Banken und Wertpapierhäusern. So werden die Anpassungen am FINMA-RS 08/21 insbesondere durch Anpassungen an den Prüffeldern mit Bezug auf die Neufassung des FINMA-RS 08/21 nachvollzogen.

[2] Abrufbar unter https://www.bis.org/bcbs/publ/d516.htm

[3] Abrufbar unter https://www.bis.org/bcbs/publ/d515.htm

# 3 Nationales und internationales Umfeld

Die Totalrevision des FINMA-RS 08/21 orientiert sich an den Standards der in Kapitel 2 genannten Papiere des BCBS. Soweit vorhanden und thematisch relevant wurden auch Vorlagen anderer Länder zum Vergleich beigezogen.

Die operationelle Resilienz und die IKT- und Cyber-Risiken entwickelten sich bereits vor Ausbruch der Corona-Pandemie zu internationalen Fokusthemen, die mit der Pandemie an noch erhöhter Wichtigkeit und Dringlichkeit gewannen. Viele Behörden anderer Länder, insbesondere im Bereich der Finanzmarktaufsicht, haben daher in der Zwischenzeit neue oder revidierte Vorgaben veröffentlicht. So haben die britischen Behörden seit 2018 diverse Papiere zur Sicherstellung der operationellen Resilienz veröffentlicht. Die amerikanischen Behörden publizierten ihr *U.S. Interagency Paper on Sound Practices to Strengthen Operational Resilience* im November 2020. Die Europäische Union erarbeitet den *Digital Operational Resilience Act.* Die IOSCO erarbeitet ein Papier zur operationellen Resilienz der Handelsplätze und Marktvermittler.

Durch die Umsetzung der in Kapitel 2 genannten Papiere des BCBS wurde unter anderem eine Aktualisierung der Angaben für das BCM nötig. Das FINMA-RS 08/21 umfasste hierzu lediglich eine Randziffer, da gleichzeitig einige Kapitel der *Empfehlungen für das Business Continuity Management (BCM)* der SBVg vom August 2013 als Selbstregulierung nach Art. 7 Abs. 3 FINMAG anerkannt waren. Auf Anfrage der FINMA konsultierte die SBVg im Jahr 2021 ihre Mitgliedsbanken und kam dabei zum Schluss, dass künftig eine ausschliessliche Behandlung des Themas im neuen Rundschreiben vorzuziehen sei und somit von einer Aktualisierung der bestehenden Empfehlungen abgesehen würde. Dementsprechend sind die als Selbstregulierung anerkannten Passagen der erwähnten Empfehlungen der SBVg neu durch das neue Rundschreiben abgedeckt und die Anerkennung der erwähnten Selbstregulierung als Mindeststandard wird mit Inkrafttreten des neuen Rundschreibens aufgehoben.

# 4 Erläuterungen zu den einzelnen Bestimmungen

## 4.1 FINMA-Rundschreiben „Operationelle Risiken und Resilienz – Banken“

### 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. 1*b* 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.

#### 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 inhärenten 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 Kontroll- und 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.

### 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, Genehmigung[4], 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*.

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

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

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.

### 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 *Ransomware- oder 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 *Threat*- und 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.

#### 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, Daten- und 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.

### 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 wird[5] (Rz 9). Es besteht nicht unbedingt die Erwartung, dass bei jedem einzelnen Geschäfts- und Organisationsbereich kritische Prozesse bestehen (Rz 84).

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 Kategorien[6] 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.

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

[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).

[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.

(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).

#### 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 Hervorhe-

[7] Manchmal auch *Business Recovery Plan* (BRP) genannt.

bung 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.

### 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 Einlagen- und 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 benötigten, 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.

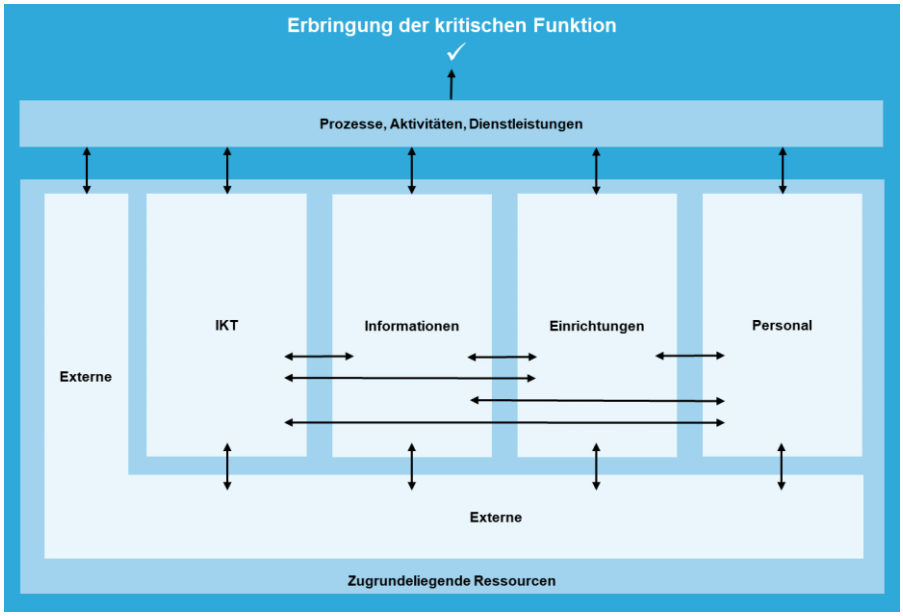


Abbildung 1: Komponenten für die Erbringung der kritischen Funktion

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, Gebäude- oder 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 Auswirkun-

gen 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.

#### 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.

### 4.2 FINMA-Rundschreiben 2013/3 „Prüfwesen“

Die Totalrevision des FINMA-RS 08/21 hat Auswirkungen auf das FINMA-RS 13/3 „Prüfwesen“, welche im Bereich Banken und Wertpapierhäuser nachvollzogen werden sollen. Für andere mittelbar durch Anpassungen im Bereich operationelle Risiken tangierte Aufsichtsbereiche werden analoge Anpassungen mittelfristig gesondert geprüft.

Es werden im Prüfwesen für Banken und Wertpapierhäuser gewisse bestehende Prüffelder umbenannt, zwei neue Prüffelder erstellt und gewisse Standardprüfstrategien angepasst.

Insbesondere wird das Prüffeld „Informatik (IT)“ in zwei Prüffelder unterteilt, eines zum „Management der IKT-Risiken“ und eines zum „Management der Cyber-Risiken“. Damit wird die Zuordnung zu den entsprechenden Themenbereichen und deren Abgrenzung voneinander klargestellt, sowie erhöhte Transparenz über die Abdeckung des Managements der Cyber-Risiken geschaffen. Für das Prüffeld zu den IKT-Risiken gilt neu eine graduelle Abdeckung über vier Jahre statt bisher sechs Jahre; dies einerseits aufgrund des Bedürfnisses, mit den rapiden technologischen Entwicklungen durch einen schnelleren Prüfzyklus mitzuhalten, andererseits aus konzeptioneller Perspektive, da das Kapitel IV Buchstabe B „Management der IKT-Risiken“ neu in vier Bereiche aufgeteilt ist und sich somit eine Abdeckung über vier Jahre eignet. Die vorhandenen „Prüfpunkte zur Informatik“ werden durch neue „Prüfpunkte zum Management der Cyber-Risiken“ ersetzt.

Das Prüffeld „Umgang mit elektronischen Kundendaten“ welches sich auf den Anhang 3 des bisherigen FINMA-RS 08/21 bezieht, wird abgeändert in Einklang mit Kapitel IV Buchstabe D in „Management der Risiken kritischer Daten“ und die vorhandenen „Prüfpunkte zur Vertraulichkeit von Kundendaten“ werden entsprechend revidiert und umbenannt.

Das Prüffeld „Qualitative Anforderungen an das Management operationeller Risiken“ wird in Einklang mit Kapitel IV Buchstabe A des neuen Rundschreibens ohne wesentliche inhaltliche Anpassungen umbenannt in „Übergreifendes Management der operationellen Risiken“. Für das Prüffeld „BCM (business continuity management)“ sind keine Anpassungen nötig.

Zur Abdeckung des Kapitels V zur operationellen Resilienz wird das neue Prüffeld „Operationelle Resilienz“ eingeführt, für das die übliche Standardprüfstrategie nach den Rz 87.1–90 des FINMA-RS 13/3 gilt. Aufgrund der konzeptionellen Unterschiede zu den bereits bestehenden Prüffeldern und um Transparenz zur Abdeckung der operationellen Resilienz zu schaffen, wurde von einer Integration des Themas in ein bereits bestehendes Prüffeld abgesehen.

Ferner ist die Übergangsbestimmung in Rz 150 obsolet und wird aufgehoben.

# 5 Regulierungsprozess

Die FINMA steht für einen transparenten, berechenbaren und glaubwürdigen Regulierungsprozess unter frühzeitigem Einbezug der Betroffenen sowie interessierten Kreisen, wie Behörden und allenfalls der Wissenschaft. Für Änderungen an Verordnungen und Rundschreiben (ausser bei rein formalen Anpassungen) wird eine öffentliche Anhörung durchgeführt. Die Möglichkeit zur Stellungnahme im Rahmen dieser Anhörungen wird von den Betroffenen rege genutzt. Der FINMA-Verwaltungsrat als zuständiges Organ wertet die Stellungnahmen aus, gewichtet sie und legt jeweils in einem Bericht (Ergebnisbericht) dar, inwiefern diese umgesetzt werden. Sämtliche Unterlagen zu Anhörungen, einschliesslich des Ergebnisberichts, werden veröffentlicht.[8]

## 5.1 Vorkonsultation

Vor der Eröffnung der Anhörung führt die FINMA grundsätzlich Vorkonsultationen mit den Betroffenen und interessierten Kreisen durch. Sie klärt dabei die relevanten Sachverhalte und erhebt die notwendigen Informationen, erläutert die Stossrichtungen des Regulierungsvorhabens und nimmt Einschätzungen dazu entgegen. Dabei können auch der Handlungsbedarf und mögliche Handlungsoptionen Gegenstand des Austausches sein.

Im Oktober und November 2021 führte die FINMA im Rahmen einer Arbeitsgruppe eine Vorkonsultation mit rund 20 Branchenvertretenden durch. Auf Basis eines ersten Entwurfs des Rundschreibens reichten die Teilnehmenden schriftliche Rückmeldungen ein. Anschliessend wurden die wichtigsten Anliegen im Rahmen einer Telefonkonferenz besprochen. Gegenstand der Vorkonsultation waren das Management der operationellen Risiken, der IKT-Risiken, der Cyber-Risiken und der Risiken kritischer Daten, sowie das Business Continuity Management und die operationelle Resilienz. Die Kapitel zum Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft und zur Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken wurden ohne wesentliche Änderungen aus dem bisherigen FINMA-RS 08/21 übernommen.

Wo die Teilnehmenden Anpassungsbedarf oder Klärungen angeregt haben, konnten diese zu einem grossen Teil im Anhörungsentwurf umgesetzt werden, soweit diese mit den Bestimmungen des übergeordneten Rechts und den Zielen der Finanzmarktaufsicht vereinbar waren. So wurden etwa Begriffsdefinitionen überarbeitet und Übergangsbestimmungen für die Sicherstellung der operationellen Resilienz eingeführt.

[8] Unterlagen betreffend die Anhörungen zu Revisionen von FINMA-Verordnungen und Rundschreiben sind auf der FINMA-Webseite publiziert (www.finma.ch > Dokumentation > Anhörungen).

Die Eigenmittelanforderungen für operationelle Risiken, die nicht mehr Gegenstand des neuen Rundschreibens sind, wurden separat im Rahmen der „Nationalen Arbeitsgruppe Basel III final“ diskutiert.

### 5.2 Erste Konsultation der mitinteressierten Verwaltungseinheiten

Vom 14. Februar bis 8. März 2022 führte die FINMA eine erste Konsultation der mitinteressierten Verwaltungseinheiten durch.

### 5.3 Öffentliche Konsultation

Die vorliegenden Regelungen sind nicht von grosser Tragweite im Sinne des Vernehmlassungsgesetzes vom 18. März 2005 (SR 172.061). Entsprechend führte die FINMA dazu eine Anhörung nach Art. 10 Abs. 2 Verordnung vom 13. Dezember 2019 zum Finanzmarktaufsichtsgesetz (SR 956.11) durch. Die Anhörungsfrist betrug zwei Monate.

### 5.4 Zweite Konsultation der mitinteressierten Verwaltungseinheiten

Vom 3. bis 21. Oktober 2022 führte die FINMA eine zweite Konsultation der mitinteressierten Verwaltungseinheiten durch.

## 6 Regulierungsgrundsätze[9]

Den regulatorischen Handlungsbedarf betreffend wird auf Kapitel 2 hiervor verwiesen.

Die im Rundschreiben dargelegten Konkretisierungen der Aufsichtspraxis der FINMA basieren auf den internationalen Standards des BCBS. Damit waren die Möglichkeiten von Varianten bei der Ausgestaltung der Regulierung auf Stufe FINMA eingeschränkt. Wo solche bestanden haben, werden diese in den obenstehenden Erläuterungen zu den einzelnen Bestimmungen diskutiert. Dabei hat die FINMA jene Varianten verfolgt, die dem Grundsatz der Verhältnismässigkeit am besten entsprochen haben. Soweit einschlägig, hat sie dabei die Auswirkungen auf die Zukunftsfähigkeit und die internationale Wettbewerbsfähigkeit des Finanzplatzes berücksichtigt.

Die getroffenen Regulierungen sind wettbewerbs- und technologieneutral ausgestaltet. Die Differenzierung einer Regulierung nach Art. 7 Abs. 2 Bst. c FINMAG orientiert sich am mit der Regulierung angestrebten Ziel und am

[9] Gemäss Art. 6 Verordnung zum Finanzmarktaufsichtsgesetz

Risiko (vgl. zum Proportionalitätsprinzip auch Kapitel 4.1.1). Internationale Standards im Finanzmarktbereich und deren Umsetzung in anderen wichtigen Finanzstandorten wurden, soweit relevant, berücksichtigt. Für die Einzelheiten wird auf die Erläuterungen zu den einzelnen Bestimmungen verwiesen.

# 7 Wirkungsanalyse[10]

## 7.1 Allgemeines

Grundsätzlich sind die Auswirkungen von Regulierungen bereits auf Gesetzesstufe umfassend aufzuzeigen. Auch im Rahmen des Erlasses von Bundesratsverordnungen werden die Auswirkungen (mit Bezugnahme auf die Wirkungsanalyse auf Gesetzesstufe) dargestellt. Wir verweisen hierzu auf die hiervor unter Kapitel 1 genannten Gesetze und Bundesratsverordnungen.

Die im Vergleich zum bisherigen FINMA-RS 08/21 ergänzten Anforderungen an das Management der operationellen Risiken und die Sicherstellung der operationellen Resilienz haben primär präzisierenden Charakter.

## 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

[10] Gemäss Art. 7 Verordnung zum Finanzmarktaufsichtsgesetz.

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 kurz[11]. 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.

## 7.3 Auswirkungen der Vorlage auf das Prüfwesen

Der Anpassungsbedarf des FINMA-RS 13/3 „Prüfwesen“ im Bereich Banken und Wertpapierhäuser aufgrund der Totalrevision des FINMA-RS 08/21 ist in Kapitel 4.2 beschrieben. Die darin genannten Prüfstrategien sind insbesondere für die Institute der Kategorien 3–5 relevant. Ohne Berücksichtigung der Initialaufwände für die Anpassungen wird mit einer leichten Erhöhung der Prüfkosten gerechnet.

Das neue Prüffeld „Operationelle Resilienz“ resultiert in einer Erhöhung der Gesamtprüfkosten, die auf 1% pro Jahr geschätzt wird. Der Prüfaufwand wird als mit dem Prüfaufwand für BCM vergleichbar eingeschätzt. Im BCM sind die Anforderungen für voraussichtlich viele oder mehrere kritische Prozesse zu prüfen, für die operationelle Resilienz sind sehr wenige kritische Funktionen zu prüfen, dafür aber mehr in der Tiefe. Für die operationelle Resilienz sind die Herabskalierung für kleinere Institute und die Anwendung des Proportionalitätsprinzips stark ausgeprägt. Je simpler das Setup, desto einfacher und weniger umfangreich die notwendige Prüfung.

Der Prüfaufwand des neuen Prüffeld „Management der IKT-Risiken“ reduziert sich auf etwa 60–80 % des vormaligen Prüffelds „Informatik (IT)“ aus zwei Gründen: 1) konzeptionelle Revision und Fokus auf 4 Themenbereiche, Wegfall der Prüfpunkte zur Informatik und somit Wegfall der detaillierten Prüfung gewisser Themenbereiche, und 2) die Abtrennung des Managements der Cyber-Risiken in ein separates Prüffeld.

Die Reduktion des Prüfaufwands im IKT-Bereich hält sich jedoch die Waage mit dem Prüfaufwand für das neue Prüffeld „Management der Cyber-Risiken“, sodass die Aufspaltung des Prüffelds „Informatik (IT)“ in zwei Prüffelder sich insgesamt kostenneutral gestaltet.

Wiederum ohne den Einbezug von Initialaufwänden werden auch die restlichen Anpassungen als kostenneutral eingeschätzt. Der Fokus des „Managements der kritischen Daten“ wird zwar ausgeweitet, jedoch nimmt die Granularität der Anforderungen aufgrund des Wegfalls von Anhang 3 ab. Das Prüffeld BCM umfasste vormals formell lediglich die Abdeckung der als Mindeststandard anerkannten Selbstregulierung, d. h. die Abdeckung gewisser Kapitel der SBVg-Empfehlungen für das BCM. Jedoch wurden typischerweise in der Praxis bereits die ganzen SBVg-Empfehlungen abgedeckt, welche nun in gestraffter und aktualisierter Form durch den neuen Grundsatz 6 gegeben sind. Am Prüfumfang für die qualitativen Anforderungen an das Management der operationellen Risiken (bzw. neu "Übergreifendes Management der operationellen Risiken" genannt) ändert sich nichts.

## 8 Weiteres Vorgehen

Das FINMA-Rundschreiben "Operationelle Risiken und Resilienz – Banken" tritt am 1. Januar 2024 in Kraft. Über zwei Jahre verteilt, d.h. bis zum 1. Januar 2026, gelten Übergangsbestimmungen zur Sicherstellung der operationellen Resilienz. Das FINMA-RS 08/21 wird – unter Ausschluss der Randziffern zu den Eigenmittelanforderungen – per 1. Januar 2024 ausser Kraft gesetzt. Die bisherigen Randziffern zu den Eigenmittelanforderungen (Rz 3–116 FINMA-RS 08/21) gelten bis zum Inkrafttreten der finalen Basel III Regeln vorübergehend weiterhin und treten anschliessend ebenfalls ausser Kraft. Hierauf wird im neuen Rundschreiben in den Übergangsbestimmungen hingewiesen.

Das teilrevidierte FINMA-RS 13/3 "Prüfwesen" mit Anpassungen zum Nachvollzug der Totalrevision des FINMA-RS 08/21 tritt per 1. Januar 2024 in Kraft und wird erstmals für das Prüfjahr 2024 angewendet.