Rundschreiben 22xx/xx
Operationelle Risiken und Resilienz – Banken

Management der operationellen Risiken und Sicherstellung der operationellen Resilienz

Referenz:	FINMA-RS 22/xx „Operationelle Risiken und Resilienz – Banken“
Erlass:	...
Inkraftsetzung:	1. Januar 2023
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. 3 Abs. 2 Bst. a und 3f BankV Art. 12 FINIG Art. 9 FINIV Art. 12 und 68
Anhang 1:	Erläuternde Graphiken zur operationellen Resilienz

Adressaten

BankG			**VAG**			**FINIG**						**FinfraG**						**KAG**						**GwG**		**Andere**	
Banken	Finanzgruppen und -kongl.	Andere Intermediäre	Versicherer	Vers.-Gruppen und -Kongl.	Vermittler	Vermögensverwalter	Trustees	Verwalter von Koll.vermögen	Fondsleitungen	Kontoführende Wertpapierhäuser	Nicht kontoführ. Wertpapierhäuser	Handelsplätze	Zentrale Gegenparteien	Zentralverwahrer	Transaktionsregister	Zahlungssysteme	Teilnehmer	SICAV	KmG für KKA	SICAF	Depotbanken	Vertreter ausl. KKA	Andere Intermediäre	SRO	SRO-Beaufsichtigte	Prüfgesellschaften	Ratingagenturen
X	X									X	X																

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

Inhaltsverzeichnis

I. Gegenstand und Geltungsbereich

Dieses Rundschreiben bezieht sich auf die Vorschriften über die Funktionentrennung, das Risikomanagement und die interne Kontrolle der Bankenverordnung (Art. 12 BankV; SR 952.02) und der Finanzinstitutsverordnung (Art. 12 und 68 FINIV; SR 954.11) und konkretisiert die entsprechende Aufsichtspraxis. Die Grundsätze berücksichtigen die Basler Grundsätze zum einwandfreien Management der operationellen Risiken[1] und der operationellen Resilienz[2]. 1

Das Rundschreiben richtet sich an Banken nach Art. 1*a* und Personen nach Art. 1*b* 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. 3*c* BankG und Art. 49 FINIG. Im Folgenden werden Banken, Wertpapierhäuser, Finanzgruppen und Finanzkonglomerat unter dem Begriff „Institute“ zusammengefasst. 2

II. Begriffe

Operationelle Risiken sind definiert als die Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Prozessen, Menschen oder Systemen oder in Folge von externen Ereignissen eintreten. Eingeschlossen sind Rechtsrisiken, nicht aber strategische Risiken und Reputationsrisiken. 3

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

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

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

Kritische Daten sind Daten, die ein Institut für eine erfolgreiche und nachhaltige Erbringung seiner Dienstleistungen als wesentlich erachtet, oder Daten, die für regulatorische Zwecke aufbewahrt werden müssen. Daten können sowohl hinsichtlich Vertraulichkeit, als auch Integrität oder Verfügbarkeit kritisch sein. Daten, die hinsichtlich der Vertraulichkeit kritisch sind (vertrauliche Daten), sind dabei solche, die besonders vor unautorisierter Offenlegung geschützt werden müssen (bspw. Personendaten, Kundendaten, Geschäftsgeheimnisse). 7

Kritische Prozesse sind diejenigen, deren Unterbrechung das Erreichen der Geschäftsziele des Instituts wesentlich gefährdet. Dabei werden die finanziellen, operationellen, rechtlichen und reputationellen Auswirkungen beachtet. 8

[1] BCBS Principles for Operational Resilience; https://www.bis.org/bcbs/publ/d516.pdf

[2] BCBS Revisions to the Principles for the Sound Management of Operational Risk; https://www.bis.org/bcbs/publ/d515.htm

Das *Business Continuity Management (BCM)* bezeichnet den institutsweiten Ansatz, um im Falle einer wesentlichen Unterbrechung den Betrieb der kritischen Prozesse wiederherzustellen. Das BCM behandelt somit auch, aber nicht nur, diejenigen kritischen Prozesse, die für die Erbringung der kritischen Funktionen nach Rz 14 und die Sicherstellung der operationellen Resilienz nach Rz 16 benötigt werden. Die *BCM Strategie* legt das grundlegende Vorgehen des Instituts für das BCM fest. Dazu gehört die für das BCM relevante Organisation und Governance, die Definition der Aufgaben, Verantwortungen und Kompetenzen, und der Rahmen für die Ausgestaltung der in Grundsatz 6 aufgeführten Komponenten des BCM. 9

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. 10

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. 11

Der *Disaster Recovery Plan (DRP)* definiert die Wiederherstellungsprozesse, um im Fall eines schwerwiegenden Ausfalls oder Zerstörung der Technologieinfrastruktur (bspw. Hardware, Netzwerke, Primär- oder Produktionsstandort, Rechenzentren) und unter Berücksichtigung des möglichen Ausfalls von Schlüsselpersonen die Wiederherstellungsziele zu erreichen. 12

Krisensituationen sind Situationen, welche nicht mit ordentlichen Massnahmen und Entscheidungskompetenzen bewältigt werden können. 13

Kritische Funktionen beinhalten: 14

a. 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. die systemrelevanten Funktionen nach Art. 8 BankG.

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. 15

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. 16

III. Proportionalitätsprinzip

Die Grundsätze dieses Rundschreibens gelten grundsätzlich für alle Adressaten dieses Rundschreibens. Die Grundsätze sind jedoch im Einzelfall abhängig von der Grösse, der Komplexität, der Struktur und des Risikoprofils des Instituts umzusetzen. 17

Banken und Wertpapierhäuser der FINMA-Kategorien 4 und 5 sind von der Erfüllung der Rz 30–31, 33–34, 37, 43, 49, 61–62, 64–66, 68, 79, 84–85, 88, 90–91 und 97–99 ausgenommen. Die FINMA ordnet im Einzelfall Erleichterungen oder Verschärfungen an. 18

Institute nach Art. 47a–47e ERV, Personen gemäss Art. 1*b* BankG, sowie nicht-kontoführende Wertpapierhäuser sind zusätzlich von der Erfüllung der Rz 60, 63, 67, 69–70 und 92–96 ausgenommen. 19

IV. Grundsätze

A. Grundsatz 1: Generelle Anforderungen an das Management der operationellen Risiken

Die Anforderungen an die organisatorischen Strukturen, die Risikopolitik und die Grundzüge des institutsweiten Risikomanagements nach FINMA-Rundschreiben 2017/1 „*Corporate Governance* – Banken“ gelten insbesondere auch für das Management der operationellen Risiken. 20

Die Geschäftsleitung implementiert und dokumentiert ein Management der operationellen Risiken, das alle für das Institut relevanten operationellen Risiken behandelt, darunter insbesondere die Risiken, die weiterführend in den Grundsätzen 2 bis 5 behandelt werden. 21

Das Oberleitungsorgan nach Kapitel IV FINMA-RS 17/1 genehmigt und überwacht das Management der operationellen Risiken regelmässig und entscheidet mindestens jährlich über die Risikotoleranz für operationelle Risiken in Anbetracht der strategischen und finanziellen Ziele des Instituts. Dabei berücksichtigt es die Ergebnisse aus den Risiko- und Kontrollbeurteilungen nach Rz 27. 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 Änderungen[3]. 22

Die Geschäftsleitung hat für die Steuerung und die Kontrolle der als wesentlich beurteilten, inhärenten Risiken ergänzende risikospezifische Massnahmen oder eine Verschärfung bestehender Massnahmen situativ zu bestimmen und umzusetzen. 23

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. 24

Die operationellen Risiken sind institutsweit einheitlich zu kategorisieren und in einem Inventar aufzuführen. Diese einheitliche Kategorisierung kann in Anlehnung an die für die Berechnung der Mindesteigenmittel für operationelle Risiken verwendete Kategorisierung 25

[3] Zum Beispiel eine Änderung des Geschäftsmodells.

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.

Für die Identifikation der operationellen Risiken werden interne[4] und externe[5] Faktoren berücksichtigt. Die identifizierten operationellen Risiken werden sowohl aus Sicht der inhärenten als auch der residualen Risiken beurteilt. 26

Die Identifikation und Beurteilung der operationellen Risiken stützt sich mindestens auf Prüfergebnisse[6] und regelmässig durchzuführende Risiko- und Kontrollbeurteilungen. Die Risiko- und Kontrollbeurteilungen berücksichtigen die inhärenten Risiken, die Effektivität der bestehenden Kontroll- und Minderungsmassnahmen und die residualen Risiken. 27

Für die Beurteilung der bestehenden Kontroll- und Minderungsmassnahmen wird insbesondere eine regelmässige, unabhängige Beurteilung der Effektivität der Schlüsselkontrollen vorgenommen (*Design Effectiveness* und *Operating Effectiveness Testing*). Dabei sind Schlüsselkontrollen diejenigen Kontroll- und Minderungsmassnahmen, die die als wesentlich beurteilten, inhärenten Risiken minimieren. Auch wird die Trennung der Aufgaben, Verantwortungen und Kompetenzen zur Sicherstellung der Unabhängigkeit und Vorbeugung vor Interessenskonflikten regelmässig beurteilt. 28

Für wesentliche Änderungen in den Produkten, Aktivitäten, Prozessen und Systemen sind Risiko- und Kontrollbeurteilungen durchzuführen. Diese berücksichtigen die mit dem Änderungsprozess einhergehenden operationellen Risiken und die operationellen Risiken des Zielzustands. Bei Bedarf wird die Risikotoleranz angepasst. 29

In Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt der institutsspezifischen Produkte, Aktivitäten, Prozesse und Systeme sind folgende weiteren Instrumente und Methoden anzuwenden: 30

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

b. Risiko- und Kontrollindikatoren für die Überwachung der operationellen Risiken und zeitnahe Identifikation von relevanten Anstiegen im Ausmass, in dem das Institut den Risiken ausgesetzt ist;

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

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.

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

[5] Externe Faktoren sind beispielsweise erkannte Verlustereignisse anderer Institute, Änderungen in der Sicherheitslage (bspw. durch Umwelteinflüsse oder Terrorismus) oder Änderungen in den regulatorischen Anforderungen.

[6] Prüfergebnisse umfassen Ergebnisse von Prüfungen 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.

Die Risikotoleranz für operationelle Risiken berücksichtigt sowohl die Toleranz in Bezug auf inhärente als auch auf residuale operationelle Risiken und wird anhand von Risiko- und Kontrollindikatoren überwacht. 31

Die Risikokontrolle erstattet dem Oberleitungsorgan und der Geschäftsleitung nach Rz 75–76 FINMA-RS 17/1 mindestens Bericht über die operationellen Risiken, denen das Institut ausgesetzt ist, über deren Vergleich mit der festgelegten Risikotoleranz, sowie über Einzelheiten zu wesentlichen internen Verlusten und wesentlichen Prüfergebnissen nach Fussnote 6. 32

Die interne Berichterstattung nach Rz 32 enthält ergänzend folgende Informationen: 33

- relevante, externe Faktoren nach Fussnote 5,
- Effektivität der Schlüsselkontrollen nach Rz 28,
- neu aufkommende operationelle Risiken,
- Ergebnisse aus der Anwendung zusätzlicher Instrumente und Methoden nach Rz 30.

Auch auf Ebene der Geschäfts- oder Organisationsbereiche, die relevanten oder wesentlichen operationellen Risiken ausgesetzt sind, wird eine regelmässige Berichterstattung zu den operationellen Risiken vorgenommen. 34

B. Grundsatz 2: Management der IKT-Risiken

a) IKT-Strategie und Governance

Das Oberleitungsorgan legt eine IKT-Strategie fest, die mit der Geschäftsstrategie abgestimmt ist. Die Geschäftsleitung implementiert und dokumentiert das Management der IKT-Risiken, das eng abgestimmt ist mit der IKT-Strategie und der jeweiligen Risikotoleranz. 35

Das Management der IKT-Risiken stellt sicher, dass die IKT-Risiken im Zusammenhang mit den kritischen Prozessen des Instituts identifiziert, beurteilt, begrenzt und überwacht werden. Zudem trägt es zur Wirksamkeit des internen Kontrollsystems bei. 36

Bei der Erstellung des Managements der IKT-Risiken sind relevante international anerkannte Standards und *Best Practices* zu berücksichtigen, sowie neue technologische Entwicklungen. 37

Entsprechend der festgelegten Risikotoleranz hat das Management der IKT-Risiken Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Funktion und Verantwortung zur Reduktion von IKT-Risiken zu beinhalten[7]. 38

Das Oberleitungsorgan überwacht regelmässig die Effektivität des Managements der IKT-Risiken. Die Geschäftsleitung beurteilt regelmässig die Ausgestaltung und die Implementierung des Managements der IKT-Risiken. 39

Das Management der IKT-Risiken beinhaltet eine regelmässige Berichterstattung an die Geschäftsleitung hinsichtlich der Entwicklung der IKT-Risiken, -Kontrollen und -Ereignissen. 40

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

Die Geschäftsleitung stellt sicher, dass sowohl für das Änderungsmanagement (*Change Management*) als auch für den IKT-Betrieb (*Run, Maintenance*) Verfahren, Prozesse und Kontrollen sowie Aufgaben, Funktionen und Verantwortlichkeiten implementiert und dokumentiert sind. Diese sind mit qualifizierten und angemessenen Ressourcen ausgestattet. 41

b) Änderungsmanagement (*Change Management*)

Das Änderungsmanagement definiert für alle Phasen der Entwicklung und Beschaffung von IKT Verfahren, Prozesse, und Kontrollen und berücksichtigt in jeder dieser Phasen die Auswirkungen und Veränderungen auf die IKT-Risiken. Dabei stehen insbesondere auch die Ziele hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit im Fokus. 42

Es ist eine Trennung zwischen den IKT-Umgebungen für die Entwicklung und das Testen und denjenigen für die IKT-Produktion sicherzustellen. Dies umfasst auch eine eindeutige Zuweisung von Aufgaben, Funktionen und Verantwortlichkeiten und eine Regelung der damit einhergehenden Zugangsberechtigungen. 43

Bei Entwicklung und Beschaffung von IKT werden funktionale und nicht-funktionale Anforderungen (bspw. im Hinblick auf die Architektur, Anforderungen an die Informationssicherheit) klar definiert und genehmigt und gemäss ihrer Kritikalität getestet und validiert. 44

c) IKT-Betrieb (*Run*, *Maintenance*)

Das Institut führt eine Inventarisierung der Bestandteile der IKT. Die Inventarisierung umfasst Hardware- und Software-Komponenten sowie Ablageorte kritischer Daten. Dabei werden sowohl interne Abhängigkeiten als auch Schnittstellen zu wesentlichen externen Dienstleistern berücksichtigt. 45

Die Inventarisierung ist zeitnah verfügbar und wird regelmässig überprüft und aktualisiert. 46

Das Institut verfügt über Verfahren, Prozesse, und Kontrollen, die die Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Produktionsumgebung unter Berücksichtigung des jeweiligen Schutzbedürfnisses sicherstellen. 47

Das Institut stellt konsistente Übergänge vom IKT-Betriebsmanagement in seine BCM- und DRP-Prozesse sicher. Es implementiert angemessene Back-up und Wiederherstellungsprozesse, die regelmässig getestet und validiert werden. 48

Das Institut verfügt über Verfahren, Prozesse und Kontrollen, die einen risikoorientierten Umgang mit IKT, deren Betriebsende naht oder deren geplante Dekommissionierung überschritten wurde, sicherstellt. 49

d) Vorfallmanagement (*Incident Management*)

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 Aufgaben, Rollen und Verantwortlichkeiten zur Behandlung dieser Vorfälle sind zu definieren. 50

Die Behandlung wesentlicher IKT-Vorfälle ist mit den Prozessen zum BCM und dem DRP abzustimmen und zu verknüpfen. 51

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 (vgl. Art. 29 Abs. 2 FINMAG). 52

C. Grundsatz 3: Management der Cyber-Risiken

Die Geschäftsleitung stellt ein Management der Cyber-Risiken sicher, das die Identifikation, Beurteilung, Begrenzung und Überwachung unter Berücksichtigung der jeweiligen Risikotoleranz und in Übereinstimmung mit der Strategie im Umgang mit Cyber-Risiken umfasst. Das Management der Cyber-Risiken ist in das Management der operationellen Risiken zu integrieren und nachvollziehbar zu dokumentieren. 53

Das Management der Cyber-Risiken beinhaltet eine mindestens jährliche Berichterstattung an die Geschäftsleitung über die Entwicklung der Cyber-Risiken, die Wirksamkeit von Schlüsselkontrollen und die wesentlichen internen sowie externen Ereignisse. 54

Weiter definiert es eindeutige Aufgaben, Rollen und Verantwortlichkeiten. Es hat mindestens die folgenden Aspekte nach international anerkannten Standards und *Best Practices* abzudecken und deren effektive Umsetzung durch geeignete Verfahren, Prozesse und Kontrolle zu gewährleisten und kontinuierlich weiter zu entwickeln und zu verbessern: 55

a. Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken[8] und Beurteilung der möglichen Auswirkungen der Ausnützung von Schwachstellen bezüglich der inventarisierten Bestandteile der IKT (gemäss Rz 45 und 46);

b. Schutz der kritischen Prozesse vor Cyber-Attacken durch die Implementierung angemessener Schutzmassnahmen, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen Daten und IT-Systeme;

c. Zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken auf Basis eines Prozesses zur systematischen und vollumfänglichen Überwachung der IKT;

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

e. Sicherstellung einer zeitnahen Wiederherstellung des ordentlichen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen.

Das Management der Cyber-Risiken hat sicherzustellen, dass eine erfolgreiche oder teilweise erfolgreiche Cyber-Attacke nach seiner Wesentlichkeit für kritische Systeme und Prozesse (inkl. ausgelagerte Dienstleistungen und Funktionen) analysiert wird und die Meldepflicht nach Art. 29 Abs. 2 FINMAG eingehalten wird. Nach erfolgter Erstbeurteilung und der Vororientierung an die FINMA innerhalb von 24 Stunden ist die Meldung gemäss dem Anforderungskatalog der Erhebungsplattform (Pflichtfelder) innerhalb von 72 Stunden an die zuständige Stelle bei der FINMA zu übermitteln. Nach Abschluss der institutsseitigen Fallbearbeitung ist ein dem Schweregrad entsprechender abschliessender Ursachenbericht einzureichen. 56

[8] Angriffe aus dem internen Netzwerk, dem Internet und vergleichbaren Netzen auf die Vertraulichkeit, Integrität und Verfügbarkeit der IKT sowie kritischen Daten.

Weiter hat es Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf ihre Funktion und Verantwortung zur Reduktion von Cyber-Risiken zu implementieren. 57

Die Geschäftsleitung lässt regelmässig Verwundbarkeitsanalysen[9], Penetrationstests[10] und auf Basis der institutsspezifischen Bedrohungspotenziale szenariobasierte Cyber-Übungen[11] durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen und risikobasiert durchgeführt werden und mindestens die IT-Systeme umfassen, welche für die Erbringung von kritischen Prozessen notwendig sind, beziehungsweise kritische Daten beinhalten, oder die darüberhinaus über das Internet erreichbar sind. 58

D. Grundsatz 4: Management der Risiken kritischer Daten

Die Geschäftsleitung implementiert und dokumentiert ein Management der Risiken kritischer Daten, das die Identifikation, Beurteilung, Begrenzung und Überwachung der Risiken hinsichtlich kritischer Daten sicherstellt. Dies erfolgt in enger Abstimmung mit einer systematischen und vollständigen Datenstrategie, mit dem Management der operationellen und IKT- und Cyber-Risiken und mit der jeweiligen Risikotoleranz. 59

Die Geschäftsleitung definiert geeignete Prozesse, Verfahren und Kontrollen sowie eindeutige Aufgaben, Rollen und Verantwortlichkeiten zum Umgang mit den vom Institut identifizierten kritischen Daten. Darüber hinaus beauftragt die Geschäftsleitung eine unabhängige Einheit als Kontrollfunktion, um Rahmenbedingungen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von kritischen Daten zu schaffen und aufrechtzuerhalten. 60

Das Institut identifiziert seine kritischen Daten systematisch und vollständig, kategorisiert diese auf der Grundlage einer Vertraulichkeits- bzw. Kritikalitätsstufe und definiert eindeutige Datenverantwortlichkeiten. 61

Die vom Institut definierten kritischen Daten werden entlang ihres gesamten Lebenszyklus verwaltet. 62

Dabei wird insbesondere die Einhaltung der Vertraulichkeit, Integrität und Verfügbarkeit bei der Verwaltung von kritischen Daten durch geeignete Prozesse, Verfahren und Kontrollen gewährleistet. 63

Kritische Daten sind während der Entwicklung, Veränderung und Migration von IKT vor dem Zugriff und der Nutzung durch Unberechtigte zu schützen. Dies gilt auch für kritische Echtdaten in Testumgebungen. 64

Die physische und logische IKT, die kritische Daten speichert oder verarbeitet, ist besonders zu schützen. Dabei ist der Zugriff auf diese Daten systematisch zu regeln und laufend zu überwachen. 65

Der Zugriff auf kritische Daten und verarbeitende Funktionalitäten ist auf Personen beschränkt, welche diesen zur Erfüllung ihrer Aufgaben benötigen[12]. Dabei muss das Institut 66

[9] Analyse zur Identifikation von derzeit bestehenden Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur gegenüber Cyber-Attacken.

[10] Gezielte Prüfung und das Ausnützen von Software-Schwachstellen und Sicherheitslücken in der IKT.

[11] Unter Berücksichtigung der Rz 17 könnten solche beispielsweise beinhalten, *Table-Top*-, *Red Teaming*-Übungen usw.

[12] Bspw. *Need-to-know*-Prinzip

über ein rollen- und funktionsspezifisches Autorisierungssystem verfügen, dessen Berechtigungen regelmässig zu überprüfen sind.

Falls kritische Daten ausserhalb der Schweiz gespeichert werden[13] oder vom Ausland aus auf sie zugegriffen werden kann, sind die damit verbundenen erhöhten Risiken angemessen zu begrenzen und die Daten besonders zu schützen. 67

Sowohl interne wie externe Personen, die auf kritische Daten zugreifen oder diese verändern können, sind sorgfältig auszuwählen. Diese Personen sind mit geeigneten Massnahmen zu überwachen[14] und regelmässig im Umgang mit diesen Daten zu schulen. Für Personen mit erhöhten Privilegien[15] gelten erhöhte Sicherheitsanforderungen. Es ist zudem eine Liste dieser Personen zu führen und laufend zu aktualisieren. 68

Vorfälle, die die Vertraulichkeit, Integrität oder Verfügbarkeit von kritischen Daten wesentlich beeinträchtigen, müssen der FINMA unverzüglich gemeldet werden (Art. 29 Abs. 2 FINMAG). 69

Bei der Auswahl von Dienstleistern, die auf kritische Daten zugreifen können oder solche verwalten, 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 auslagernden Instituts risikoorientiert periodisch zu überwachen und zu kontrollieren. 70

E. Grundsatz 5: Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft

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. Insbesondere erwartet die FINMA als Aufsichtsbehörde, dass die Institute ausländisches Aufsichtsrecht einhalten. 71

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. 72

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. 73

[13] Bspw. im Rahmen von Cloud- oder Hosting-Lösungen

[14] Bspw. Auswertung von Log-Dateien, Vier-Augen-Prinzip usw.

[15] Bspw. Personen mit Administratorenrechten, Anwender mit funktionalem Zugriff auf eine grosse Menge an kritischen Daten usw.

Von diesem Grundsatz werden auch Konstellationen erfasst, in denen eine im Ausland ansässige Tochtergesellschaft, Zweigniederlassung oder dergleichen eines Schweizer Finanzinstituts Kunden grenzüberschreitend bedient. 74

F. Grundsatz 6: Business Continuity Management (BCM)

Das Oberleitungsorgan genehmigt in regelmässigen Abständen die BCM Strategie, und überwacht deren Einhaltung. Die Geschäftsleitung ist für die Implementierung der Strategie verantwortlich. 75

Jeder relevante Geschäfts- und Organisationsbereich hat im Rahmen der *Business Impact Analyse* (BIA) seine kritischen Prozesse und die dafür benötigten Ressourcen[16] zu identifizieren. 76

Für die kritischen Prozesse definiert das Institut die RTO und RPO nach Rz 10. Diese sind mit den dafür erforderlichen Leistungserbringern[17] 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. 77

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 76 berücksichtigt. Die Akzeptanz von residualen Risiken wird angemessen dokumentiert. 78

Die BIA und BCP werden einer institutsweiten Vorgabe folgend auf konsistente Art erstellt und dokumentiert. Sie sind jährlich sowie im Falle wesentlicher Änderungen im Geschäftsbetrieb (Reorganisationen, Aufbau eines neuen Geschäftsfelds usw.) zu überprüfen. 79

Das Institut definiert als Teil des BCP einen DRP. Wenn Teile der Technologieinfrastruktur ausgelagert sind, gibt der DRP Auskunft über die externen Abhängigkeiten und vertraglichen Regelungen sowie alternative Lösungen. Der DRP wird im Falle wesentlicher Änderungen und mindestens jährlich überprüft. 80

In Krisensituationen hat ein Krisenstab die Aufgabe der Krisenbewältigung bis zur Wiederherstellung eines ordnungsgemässen Zustands zu übernehmen. Die eine Krise auslösenden Gegebenheiten, die Zuständigkeiten und Kompetenzen 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. 81

Das Institut definiert eine Kommunikationsstrategie für die interne und externe Kommunikation in Krisensituationen. 82

Mit Tests wird die Umsetzung der BCP und des DRP sowie die Funktionsfähigkeit der Krisenorganisation regelmässig getestet. Dafür wird eine systematische Testplanung erstellt, die die regelmässige Abdeckung sicherstellt. Es können verschiedene Vorgehen zum Testen von unterschiedlicher Intensität und Effektivität gewählt werden. 83

Die gemäss BCP und DRP wichtigsten Massnahmen und die Krisenorganisation werden 84

[16] Personal, Einrichtungen (bspw. Gebäude, Arbeitsplatzinfrastruktur), IT-Systeme oder IT-Infrastruktur (inkl. Kommunikationssysteme), Abhängigkeiten zu andern Bereichen des Instituts und zu Drittparteien, bsp. externe Dienstleister und Lieferanten (Outsourcing), Zentralbanken oder Clearinghäusern.

[17] Bspw. mit der IT-Abteilung, anderen Bereichen des Instituts oder Externen.

mindestens einmal jährlich getestet.

Relevante Anspruchsgruppen, einschliesslich diejenigen in Fach- und IT-Funktionen, nehmen an den Tests teil, um sich mit den Wiederherstellungsprozessen vertraut zu machen. 85

Die Tests umfassen verschiedene schwerwiegende, aber plausible Szenarien und berücksichtigen Wiederherstellungsabhängigkeiten, einschliesslich solcher die zu internen oder externen Drittparteien bestehen. 86

Eine regelmässige Berichterstattung an das Oberleitungsorgan und die Geschäftsleitung informiert über die durchgeführten Test- und 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. 87

Die Mitarbeitenden sowie die Mitglieder der Krisenorganisation werden hinsichtlich ihrer Aufgaben, Verantwortlichkeiten und Kompetenzen, die sich aus den diversen BCM Aktivitäten ergeben, ausreichend geschult, sowohl bei Neueintritt von Mitarbeitenden als auch als Teil regelmässiger Schulungen zur Auffrischung. 88

G. Grundsatz 7: Operationelle Resilienz

Das Institut identifiziert seine kritischen Funktionen und deren Unterbrechungstoleranzen, und trifft Massnahmen zur Sicherstellung der operationellen Resilienz unter Berücksichtigung schwerwiegender, aber plausibler Szenarien. Das Oberleitungsorgan genehmigt und überwacht das Vorgehen zur Sicherstellung der operationellen Resilienz regelmässig. 89

Die kritischen Funktionen und die damit verbundenen Unterbrechungstoleranzen nach Rz 14 sind mindestens jährlich durch das Oberleitungsorgan zu genehmigen. 90

Das Institut koordiniert die relevanten Bestandteile eines umfassenden Risikomanagements wie beispielsweise das Management der operationellen Risiken, das Business Continuity Management, das Management von Auslagerungen (Outsourcing; vgl. das FINMA-Rundschreiben 2018/3 „Outsourcing“), und die Notfallplanung (Grundsatz 8) dahingehend, dass diese zu einer Stärkung der operationellen Resilienz des Instituts beitragen. Dies beinhaltet einen angemessenen Austausch relevanter Informationen zwischen diesen verschiedenen Bereichen. 91

Zur operationellen Resilienz hat eine Berichterstattung an die Geschäftsleitung und das Oberleitungsorgan regelmässig zu erfolgen, sowie bei wesentlichen Kontrollschwächen oder Vorfällen, die die operationelle Resilienz gefährden. 92

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. 93

Das Institut führt ein Inventar seiner kritischen Funktionen, das mindestens jährlich überprüft und aktualisiert wird. Dieses Inventar beinhaltet die Unterbrechungstoleranzen der 94

kritischen Funktionen, sowie die Verbindungen und Abhängigkeiten zwischen den benötigten kritischen Prozessen und deren Ressourcen[18] zur Erbringung der kritischen Funktionen.

Für die kritischen Funktionen werden die operationellen Risiken und die Schlüsselkontrollen dokumentiert. 95

Die kritischen Funktionen und die dafür benötigten kritischen Prozesse und Ressourcen sind durch BCPs nach Grundsatz 6 abgedeckt. 96

Die Fähigkeit, kritische Funktionen innerhalb ihrer Unterbrechungstoleranz unter schwerwiegenden, aber plausiblen Szenarien erbringen zu können, wird regelmässig getestet. 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 auszeichnen[19]. 97

Für systemrelevante Banken sind die für die Weiterführung der kritischen Funktionen nach Rz 14 relevanten BCP, DRP und Krisenorganisation nach Grundsatz 6 mit der Notfallplanung nach Grundsatz 8 abzustimmen. 98

H. Grundsatz 8: Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken

Systemrelevante Banken treffen im Rahmen ihrer Notfallplanung die für die unterbruchsfreie Weiterführung von systemrelevanten Funktionen nötigen Massnahmen (Art. 9 Abs. 2 Bst. d BankG i.V.m. Art. 60 ff. BankV). Sie identifizieren die zur Fortführung der systemrelevanten Funktionen im Fall der Abwicklung, Sanierung oder Restrukturierung notwendigen Dienstleistungen ("kritische Dienstleistungen") und ergreifen die für deren Weiterführung nötigen Massnahmen. Dabei berücksichtigen sie die in diesem Zusammenhang von internationalen Standardsettern erlassenen Vorgaben. 99

V. Übergangsbestimmungen

A. Betreffend den Grundsatz 7 „Operationelle Resilienz“

Die Identifikation der kritischen Funktionen und die Definition der Unterbrechungstoleranzen hat innert einer Übergangsfrist von einem Jahr ab Inkrafttreten zu erfolgen. Für die Erstellung des Inventars der kritischen Funktionen und erste Tests jeder kritischen Funktion ist eine Übergangsfrist von zwei Jahren ab Inkrafttreten gegeben. Die Sicherstellung der operationellen Resilienz wird innerhalb einer Übergangsfrist von drei Jahren ab Inkrafttreten erwartet. 100

B. Betreffend die Eigenmittelanforderungen

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 101

[18] Inklusive die für die kritischen Funktionen relevanten Bestandteile des Inventars nach Rz 45.

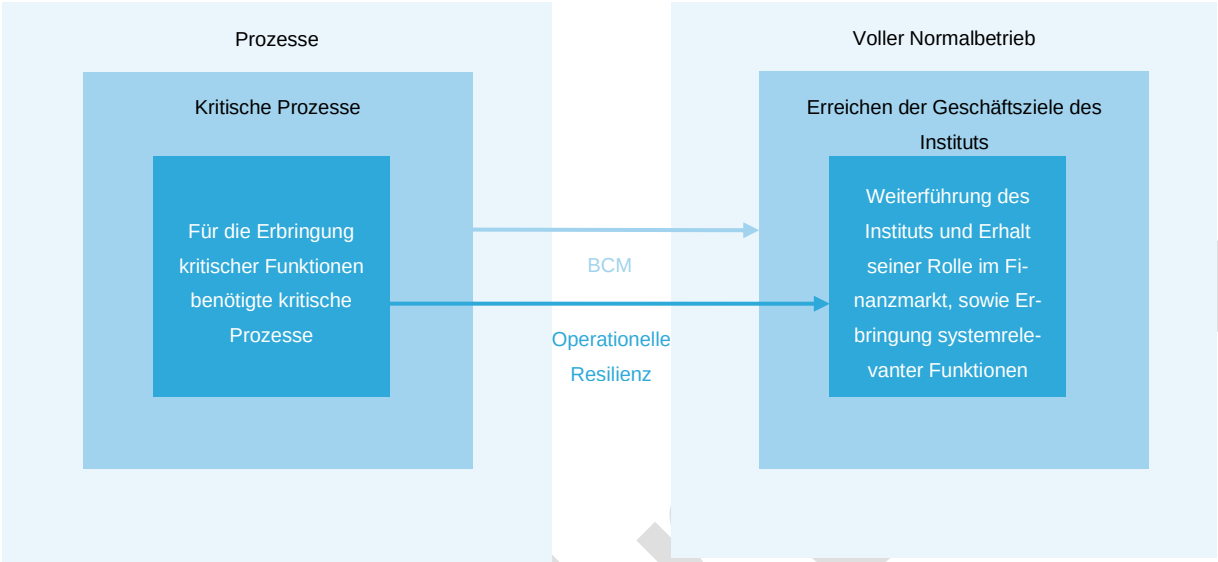
[19] Beispiele sind eine Pandemie oder eine Strommangellage.

und der ausführenden FINMA-Verordnung dazu am 1. Juli 2024 nach den Rz 3–116 des FINMA-Rundschreibens 2008/21 „Operationelle Risiken – Banken“.

Anhang 1

Erläuternde Graphiken zur operationellen Resilienz

I. Überlappung der Schutzziele des BCM und der operationellen Resilienz



II. Komponenten für die Erbringung der kritischen Funktion