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 2023/1
Operationelle Risiken und Resilienz – Banken

Management der operationellen Risiken und Sicherstellung der operationellen Resilienz

Referenz:	FINMA-RS 23/1 „Operationelle Risiken und Resilienz – Banken“
Erlass:	7. Dezember 2022
Inkraftsetzung:	1. Januar 2024
Konkordanz:	vormals FINMA-RS 08/21 „Operationelle Risiken – Banken“ vom 20. November 2008
Rechtliche Grundlagen:	FINMAG Art. 7 Abs. 1 Bst. b und 29 Abs. 1 BankG Art. 1*b* Abs. 3 Bst. b, Art. 3 Abs. 2 Bst. a und 3f BankV Art. 12 und 14*e* FINIG Art. 9 und 49 FINIV Art. 12 und 68
Anhang 1:	Erläuternde Graphik zur operationellen Resilienz

Adressaten																												
BankG				VAG			FINIG						FinfraG						KAG						GwG		Andere	
Banken	Finanzgruppen und -kongl.	Personen nach Art. 1*b* BankG	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	X																

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

Inhaltsverzeichnis

I.	**Gegenstand und Geltungsbereich**	Rz 1-2
II.	**Begriffe**	Rz 3-18
III.	**Proportionalitätsprinzip**	Rz 19-21
IV.	**Management der operationellen Risiken**	Rz 22-100
A.	Übergreifendes Management der operationellen Risiken	Rz 22-46
B.	Management der IKT-Risiken	Rz 47-60
a)	IKT-Strategie und Governance	Rz 47-49
b)	Änderungsmanagement (*Change Management*)	Rz 50-52
c)	IKT-Betrieb (*Run*, *Maintenance*)	Rz 53-57
d)	Vorfallmanagement (*Incident Management*)	Rz 58-60
C.	Management der Cyber-Risiken	Rz 61-70
D.	Management der Risiken kritischer Daten	Rz 71-82
E.	*Business Continuity Management* (BCM)	Rz 83-96
F.	Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft	Rz 97-100
V.	**Sicherstellung der operationellen Resilienz**	Rz 101-111
VI.	**Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken**	Rz 112
VII.	**Übergangsbestimmungen**	Rz 113-114
A.	Betreffend die Sicherstellung der operationellen Resilienz	Rz 113
B.	Betreffend die Eigenmittelanforderungen für operationelle Risiken	Rz 114

I. Gegenstand und Geltungsbereich

Dieses Rundschreiben bezieht sich auf die Vorschriften über die Funktionentrennung, das Risikomanagement und die interne Kontrolle der Bankenverordnung (Art. 12 und 14*e* BankV; SR 952.02) und der Finanzinstitutsverordnung (Art. 12 und 68 FINIV; SR 954.11) und konkretisiert die entsprechende Aufsichtspraxis. Es berücksichtigt die Basler Grundsätze zum einwandfreien Management der operationellen 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, Personen nach Art. 1*b* BankG, Wertpapierhäuser, Finanzgruppen und Finanzkonglomerate unter dem Begriff „Institute“ zusammengefasst. 2

II. Begriffe

Operationelle Risiken sind in Art. 89 ERV definiert. Es handelt sich um die Gefahr von finanziellen Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Prozessen oder Systemen, des unangemessenen Handelns von Menschen oder durch sie begangene Fehler, oder in Folge von externen Ereignissen eintreten. Dies beinhaltet die finanziellen Verluste, die aus Rechts- oder Compliance-Risiken entstehen können. Das Management der operationellen Risiken berücksichtigt typischerweise auch andere Schadensdimensionen[3], sofern diese letztendlich auch in finanziellen Verlusten resultieren können. Dabei ausgeschlossen sind die strategischen Risiken. 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 in Anbetracht der Grösse, der Komplexität, der Struktur, des Risikoprofils sowie des Geschäftsmodells des Instituts von so wesentlicher Bedeutung sind, dass sie einen erhöhten Sicherheitsanspruch erfordern. Dabei handelt es sich um Daten, die für die erfolgreiche und nachhaltige Erbringung der Dienstleistungen des Instituts oder für regulatorische Zwecke wesentlich sind. Bei der Beurteilung und Festlegung der Kritikalität von Daten sind sowohl die Vertraulichkeit als auch die Integrität und 7

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

[2] BCBS Principles for Operational Resilience (31 March 2021)

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

Verfügbarkeit zu berücksichtigen. Jeder dieser drei Aspekte kann ausschlaggebend dafür sein, dass Daten als kritisch klassifiziert werden.

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

Das *Business Continuity Management (BCM)* bezeichnet den institutsweiten Ansatz, um im Falle einer über das Vorfallmanagement hinausgehenden, bedeutenden Störung oder Unterbrechung den Betrieb der kritischen Prozesse wiederherzustellen. Es definiert die Reaktion auf bedeutende Störungen oder Unterbrechungen. Ein effektives BCM vermindert die residualen Risiken im Zusammenhang mit bedeutenden Störungen oder Unterbrechungen. 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 einer Zerstörung der IKT und unter Berücksichtigung des möglichen Ausfalls von Schlüsselpersonen, die Wiederherstellungsziele zu erreichen. 12

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

Kritische Funktionen beinhalten: 14

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

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

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. 17

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 18

Unterbrechungen auf die Erbringung der kritischen Funktionen zu minimieren. Ein operationell resilientes Institut hat sein Betriebsmodell so aufgebaut[4], dass es in Bezug auf seine kritischen Funktionen dem Risiko von Unterbrechungen weniger ausgesetzt ist. Die operationelle Resilienz verringert somit nicht nur die residualen Risiken von Unterbrechungen, sondern auch das inhärente Risiko, dass es zu Unterbrechungen kommt. Ein effektives Management der operationellen Risiken trägt dazu bei, die operationelle Resilienz des Instituts zu stärken.

III. Proportionalitätsprinzip

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

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

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

IV. Management der operationellen Risiken

A. Übergreifendes Management der operationellen Risiken

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

Das Oberleitungsorgan genehmigt die Grundzüge des Managements der operationellen Risiken, die für das Institut relevant sind, und überwacht deren Einhaltung. Darunter fallen unter anderem die IKT-Risiken, die Cyber-Risiken, die Risiken hinsichtlich kritischer Daten, die Risiken aus der Ausgestaltung und Implementierung des BCM und gegebenenfalls die Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft. Es genehmigt mindestens jährlich die Risikotoleranz für operationelle Risiken nach Massgabe der Risikopolitik in Anbetracht der strategischen und finanziellen Ziele des Instituts. Dabei berücksichtigt es die Ergebnisse aus den Risiko- und Kontrollbeurteilungen nach Rz 30. Es akzeptiert entweder das Ausmass, in dem das Institut den operationellen Risiken ausgesetzt ist, oder entscheidet über eine Anpassung der Risikotoleranz und die dafür notwendigen, strategischen Änderungen[5]. 23

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

[4] Häufig auch *Resilience by Design* genannt.

[5] Zum Beispiel eine Änderung des Geschäftsmodells

Die Geschäftsleitung stellt nachvollziehbar sicher, dass die operationellen Risiken identifiziert, beurteilt, begrenzt und überwacht werden, und dass die Effektivität sowohl der Ausgestaltung als auch der Implementierung dieses Managements der operationellen Risiken regelmässig überprüft wird. Für die Begrenzung der als wesentlich beurteilten, inhärenten Risiken[6] ergreift sie situativ risikospezifische ergänzende oder verschärfende Massnahmen. 25

Zur Stärkung des Bewusstseins der Mitarbeitenden zur Reduktion von relevanten operationellen Risiken, insbesondere der IKT-Risiken, der Cyber-Risiken, der Risiken hinsichtlich kritischer Daten und der Risiken aus der Ausgestaltung und Implementierung des BCM, sind unter Berücksichtigung ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) Massnahmen zu implementieren[7]. 26

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. 27

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

Für die Identifikation der operationellen Risiken werden interne[8] und externe[9] Faktoren berücksichtigt. Die identifizierten operationellen Risiken werden sowohl aus Sicht der inhärenten als auch der residualen Risiken nachvollziehbar beurteilt. 29

Die Identifikation und Beurteilung der operationellen Risiken stützt sich mindestens auf Prüfergebnisse[10] 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. 30

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

---

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

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

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

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

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

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

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

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

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

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

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. 37

Die Risikotoleranz für operationelle Risiken berücksichtigt sowohl die Toleranz in Bezug auf inhärente[11] als auch auf residuale operationelle Risiken und wird anhand von Risiko- oder Kontrollindikatoren überwacht. 38

Die Risikokontrolle erstattet dem Oberleitungsorgan mindestens jährlich und der Geschäftsleitung mindestens halbjährlich nach Rz 75–76 FINMA-RS 17/1 Bericht über die operationellen Risiken entlang der obersten Stufe[12] der nach Rz 28 definierten Kategorisierung, über deren Vergleich mit der festgelegten Risikotoleranz, sowie über Einzelheiten zu wesentlichen internen Verlusten. 39

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

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

- relevante, externe Faktoren nach Fussnote 9, 42
- zusammenfassende Gesamtübersicht über die Effektivität der Schlüsselkontrollen nach Rz 31, 43
- neu aufkommende operationelle Risiken, 44

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

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

- Ergebnisse aus der Anwendung zusätzlicher Instrumente und Methoden nach Rz 33. 45

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

B. Management der IKT-Risiken

a) IKT-Strategie und Governance

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

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

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

b) Änderungsmanagement (*Change Management*)

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

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

Bei Entwicklung und Beschaffung von IKT werden funktionale und nicht-funktionale Anforderungen[13] klar definiert und genehmigt und gemäss ihrer Kritikalität getestet und validiert. 52

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

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

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

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

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

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

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

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 AKV zur Behandlung dieser Vorfälle sind zu definieren. 58

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

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. 60

C. Management der Cyber-Risiken

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

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

a. Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken[14] und Beurteilung der möglichen Auswirkungen der Ausnützung von Schwachstellen bezüglich der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten (gemäss Rz 53, 54 und 7); 63

b. Schutz der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten vor Cyber-Attacken durch die Implementierung angemessener Schutzmassnahmen, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit; 64

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

c. Zeitnahe Aufzeichnung und Erkennung von Cyber-Attacken auf Basis eines Prozesses zur systematischen und durchgängigen Überwachung der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten; 65

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 66

e. Sicherstellung einer zeitnahen Wiederherstellung des ordentlichen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen. 67

Das Management der Cyber-Risiken hat sicherzustellen, dass eine erfolgreiche oder teilweise erfolgreiche Cyber-Attacke nach seiner Wesentlichkeit für kritische inventarisierte IKT-Bestandteile bzw. elektronische kritische Daten sowie kritische Prozesse (inkl. ausgelagerte Dienstleistungen und Funktionen) analysiert wird und die Meldepflicht nach FINMAG eingehalten wird. Nach erfolgter Erstbeurteilung und der Vororientierung an die zuständige Stelle bei der FINMA innerhalb von 24 Stunden ist die Meldung gemäss dem Anforderungskatalog der Erhebungsplattform EHP (Pflichtfelder) innerhalb von 72 Stunden zu übermitteln. Nach Abschluss der institutsseitigen Fallbearbeitung ist ein dem Schweregrad entsprechender abschliessender Ursachenbericht an die zuständige Stelle bei der FINMA einzureichen. 68

Die Geschäftsleitung lässt regelmässig Verwundbarkeitsanalysen[15] und Penetrationstests[16] durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen ausgeführt werden. Dabei sind alle inventarisierten Bestandteile der IKT, die über das Internet erreichbar sind, zu berücksichtigen. Zudem sind inventarisierte Bestandteile der IKT, welche nicht über das Internet erreichbar, aber für die Erbringung von kritischen Prozessen notwendig sind, oder welche elektronische kritische Daten beinhalten, zu berücksichtigen. 69

Auf Basis der institutsspezifischen Bedrohungspotenziale müssen risikobasiert szenariobezogene Cyber-Übungen[17] durchgeführt werden. Das Ergebnis der Übungen ist in geeigneter Form zu dokumentieren und zu rapportieren. 70

D. Management der Risiken kritischer Daten

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

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

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

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

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

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

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

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

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

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

Der Zugriff auf kritische Daten und verarbeitende Funktionalitäten ist auf Personen beschränkt, welche diesen zur Erfüllung ihrer Aufgaben benötigen[18]. Dabei muss das Institut über ein Autorisierungssystem verfügen. Der Zugang zu diesem Autorisierungssystem ist besonders zu schützen und regelmässig zu überprüfen. Die im Autorisierungssystem enthaltenen Berechtigungen sind regelmässig zu überprüfen. 78

Falls kritische Daten ausserhalb der Schweiz gespeichert werden[19] oder vom Ausland aus auf sie zugegriffen werden kann, sind die damit verbundenen erhöhten Risiken angemessen zu begrenzen und mit geeigneten Massnahmen zu überwachen sowie die Daten besonders zu schützen. 79

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[20] und regelmässig im Umgang mit diesen Daten zu schulen. Für Personen mit erhöhten Privilegien[21] gelten erhöhte Sicherheitsanforderungen. Es ist zudem eine Liste aller Personen mit erhöhten Privilegien zu führen und laufend zu aktualisieren. 80

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

Bei der Auswahl von Dienstleistern, die kritische Daten bearbeiten[22] oder einsehen können, ist der Sorgfaltsprüfung (*Due Diligence*) eine hohe Bedeutung beizumessen. Es sind klare Kriterien für die Beurteilung des Umgangs der Dienstleister mit kritischen Daten zu definieren und vor Vertragsvereinbarung zu prüfen. Die Dienstleister sind im Rahmen des internen Kontrollsystems des Instituts risikoorientiert periodisch zu überwachen und zu kontrollieren. 82

[18] Bspw. *Need-to-know*- und *Least Privilege*-Prinzip

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

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

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

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

E. *Business Continuity Management* (BCM)

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

Jeder relevante Geschäfts- und Organisationsbereich hat im Rahmen der *Business Impact Analyse* (BIA) seine kritischen Prozesse und die dafür benötigten Ressourcen[23] zu identifizieren. 84

Für die kritischen Prozesse definiert das Institut die RTO und RPO nach Rz 10. Diese sind mit den dafür erforderlichen Leistungserbringern[24] 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. 85

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

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

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

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

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

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

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

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

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

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

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

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. 95

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

F. 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. 97

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. 98

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. 99

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

V. Sicherstellung der operationellen Resilienz

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

Das Institut trifft Massnahmen zur Sicherstellung der operationellen Resilienz unter Berücksichtigung schwerwiegender, aber plausibler Szenarien[25]. 102

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

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

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

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. 106

Das Institut führt ein Inventar seiner kritischen Funktionen, das mindestens jährlich überprüft und aktualisiert wird. Dieses Inventar beinhaltet die Unterbrechungstoleranzen der kritischen Funktionen, sowie die Verbindungen und Abhängigkeiten zwischen den benötigten kritischen Prozessen und deren Ressourcen[26] zur Erbringung der kritischen Funktionen. 107

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

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

Die Fähigkeit, kritische Funktionen innerhalb ihrer Unterbrechungstoleranz unter schwerwiegenden, aber plausiblen Szenarien erbringen zu können, wird regelmässig getestet oder geübt. Dazu gehören auch Szenarien, die sich von kürzeren und eher begrenzt wirkenden Unterbrechungen unterscheiden und sich durch eine längere Zeitdauer (bspw. über Monate hinweg) und einen Ausfall grundlegender Ressourcen auszeichnen[27]. Die Tests bzw. Übungen werden dabei so gestaltet sein, dass sie das Institut nicht grundlegend gefährden. 110

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

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

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

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

VI. 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. 112

VII. Übergangsbestimmungen

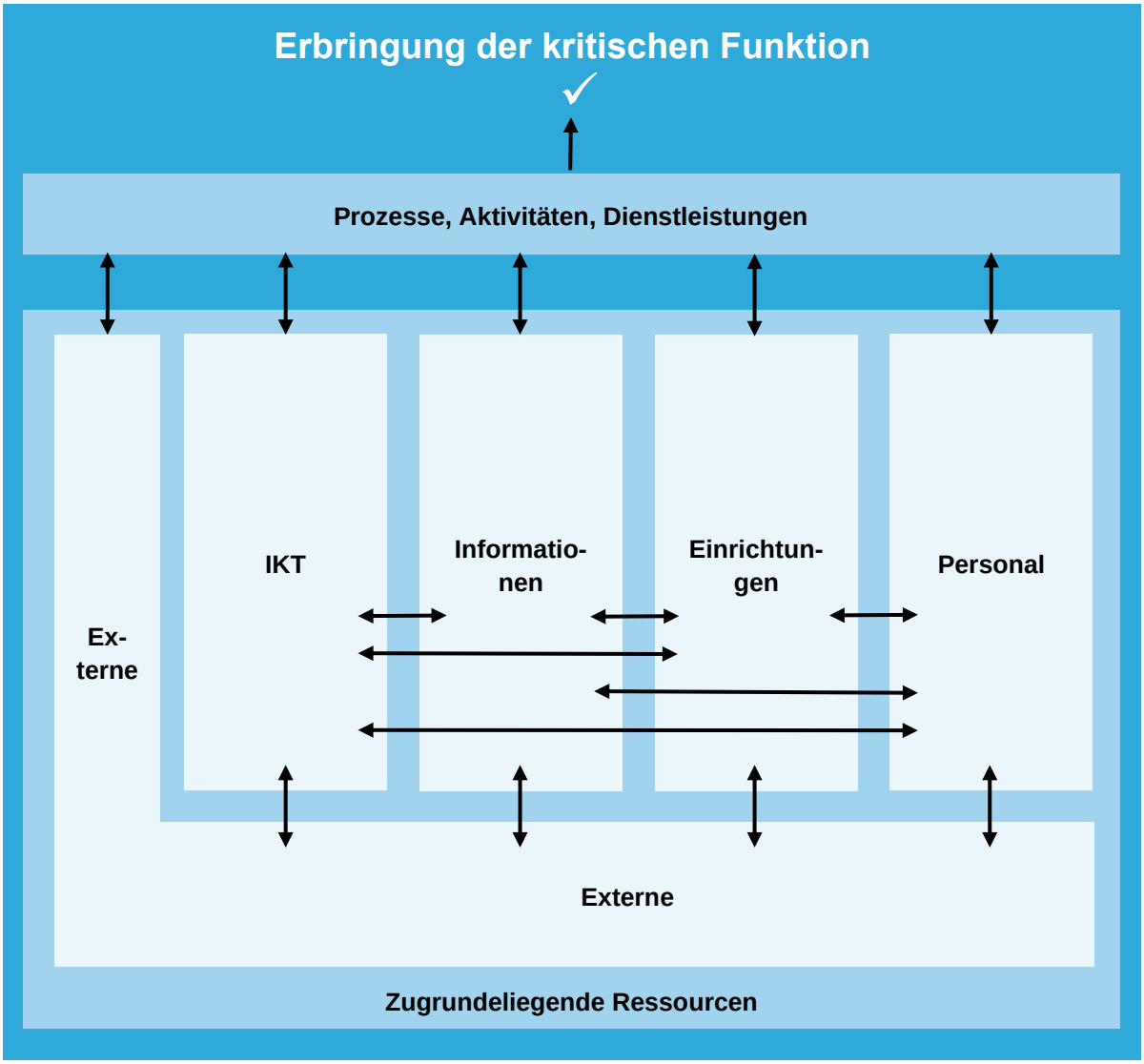
A. Betreffend die Sicherstellung der operationellen Resilienz

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

B. Betreffend die Eigenmittelanforderungen für operationelle Risiken

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

Anhang 1

Erläuternde Graphik zur operationellen Resilienz

Komponenten für die Erbringung der kritischen Funktion