EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Eidgenössische Finanzmarktaufsicht FINMA
Anne Feidt
Laupenstrasse 27
CH-3003 Bern

Zustellung per E-Mail an: anne.feidt@finma.ch

Zürich, 5. Juli 2022

Position von EXPERTsuisse zum revidierten FINMA-RS 2008/21 «Operationelle Risiken und Resilienz – Banken»

Sehr geehrte Frau Feidt

Am 10. Mai 2022 hat die FINMA bekannt gegeben, das FINMA-RS 2008/21 «Operationelle Risiken – Banken» einer Totalrevision zu unterziehen, um damit den neusten Prinzipien der Basler Standards zu entsprechen sowie den Entwicklungen im Bereich der Digitalisierung und der Informations- und Kommunikationstechnologie gerecht zu werden. Gleichzeitig wird das FINMA-RS 2013/3 «Prüfwesen» angepasst. Als Branchenverband EXPERTsuisse nutzen wir deshalb die Gelegenheit, zur Vorlage Stellung zu nehmen.

EXPERTsuisse zählt über 10'000 Einzelmitglieder und rund 800 Mitgliedunternehmen. Gleichzeitig gehören 90% der grössten 100 Prüfungs- und Beratungsgesellschaften sowie 100% all jener Gesellschaften, welche börsenkotierte Unternehmen prüfen, zu den Mitgliedern von EXPERTsuisse.

Änderungen

Für EXPERTsuisse ist nachvollziehbar, dass das Rundschreiben aufgrund der Anpassungen der Principles for the Sound Management of Operational Risk und Principles for Operational Resilience (POR) des Basel Committee on Banking Supervision (BCBS) totalrevidiert und umbenannt wird. Es erscheint uns zudem sinnvoll, die aktuell gültigen Empfehlungen für das Business Continuity Management (BCM) der Schweizerischen Bankiervereinigungen (SBVg) in das neue Rundschreiben zu überführen.

Auswirkungen

Neben den bekannten Anforderungen zum Umgang mit operationellen Risiken sind neu auch Vorgaben im Zusammenhang mit der operationellen Resilienz zu erfüllen. Damit dürfte die Überlebensfähigkeit der Banken bei schwerwiegenden, komplexen, systemischen oder länger andauernden operationellen Problemen gestärkt werden. Der Implementierungsaufwand bei den Finanzinstituten darf unseres Erachtens jedoch nicht unterschätzt werden.

Je nach Ausgestaltung und Maturität der bestehenden Dokumente, Prozesse und Verfahren eines Finanzinstituts kann ein unterschiedlicher Handlungsbedarf resultieren. Die Änderungen können weitreichende Auswirkungen auf das institutsweite Risikomanagement, die internen Corporate Governance-Regeln oder das Outsourcing haben. Gemäss Ziffer 8 des Erläuterungsberichts (Seite 33) ist die Verabschiedung des FINMA-Rundschreibens „Operationelle Risiken und Resilienz – Banken“ im Dezember 2022 und das Inkrafttreten per 1. Januar 2023 vorgesehen. Lediglich zum Grundsatz 7 «Operationelle Resilienz» werden gewisse Übergangsfristen vorgesehen. Eine derart kurzfristige Implementierung dieses Rundschreibens innerhalb rund eines Monats nach voraussichtlichem Vorliegen der definitiven Fassung scheint uns unrealistisch, da es sich unseres Erachtens nicht lediglich um eine geringfügige Überarbeitung der Regelungen handelt, sondern einen nicht zu unterschätzenden Anpassungsbedarf bei den Instituten hervorruft. Das Datum des Inkrafttretens resp. die Gewährung von Übergangsfristen sollte deshalb nochmals neu beurteilt werden.

Weitere Anmerkungen und Änderungsvorschläge haben wir in der Beilage zusammengefasst. Wir bedanken uns für die Prüfung und Berücksichtigung unserer Kommentare und Anliegen, welche diesem Schreiben beigelegt sind.

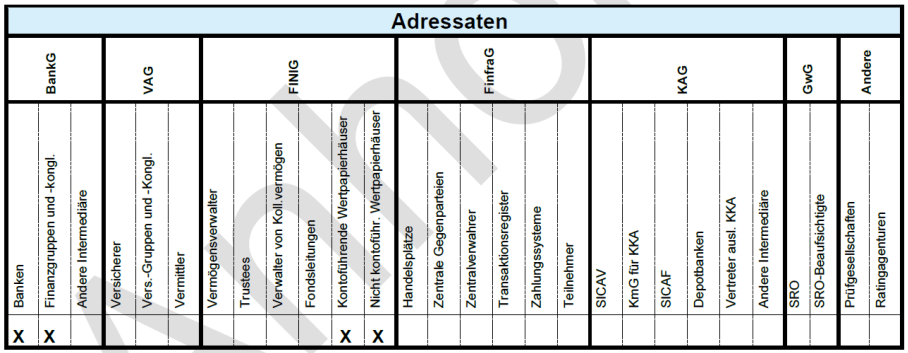
Für allfällige Rückfragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Freundliche Grüsse
EXPERTsuisse

Bruno Gmür
Fachkommissionspräsident
Bankenprüfung

Sergio Ceresola
Mitglied der Geschäftsleitung
Ressortleitung Regulatorisches & Fachliches

Anhörung – Rundschreiben «Operationelle Risiken und Resilienz – Banken»

Rz	Änderungsvorschlag Regulierungstext	Begründung / Kommentar
Titel-seite		Auf der Titelseite des Rundschreibens führt die FINMA die von den Bestimmungen des Rundschreibens betroffenen Institute auf. Die Personen nach Art. 1b BankG werden jedoch nicht aufgeführt und sollten bei neuen oder angepassten Rundschreiben ergänzt werden, da diese ebenfalls von diesen Regelungen betroffen sind.
1	Fussnoten 1 und 2	Wir gehen davon aus, dass die Fussnoten 1 und 2 vertauscht sind. Wir empfehlen, dies zu überprüfen.
2	Das Rundschreiben richtet sich an Banken nach Art. 1a und Personen nach Art. 1b Bankengesetz (BankG; SR 952.0), Wertpapierhäuser nach Art. 2 Abs. 1 Bst. e und Art. 41 des Finanzinstitutsgesetzes (FINIG; SR 954.1) sowie an Finanzgruppen und Finanzkonglomerate nach Art. 3c BankG und Art. 49 FINIG. Im Folgenden werden Banken, **Personen nach Art. 1b Bankengesetz,** Wertpapierhäuser, Finanzgruppen und Finanzkonglomerat unter dem Begriff „Institute“ zusammengefasst.	Zur Klarstellung sollten im Begriff «Institut» zusätzlich Personen nach Art. 1b BankG erfasst werden. In zahlreiche Randziffern (z.B. Rz 32, 36, 45, 47 etc.) wird der Begriff «Institut» verwendet. Wenn Personen nach Art. 1b nicht unter den Begriff «Institut» fallen, besteht die Unklarheit, ob die entsprechende Regel anwendbar ist oder nicht, obwohl die Regel unter Umständen nicht unter die Ausnahmen gemäss Rz 18 und 19 fällt.
3	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. **Dazu gehören insbesondere Compliance-Risiken (z. B. Geldwäschereirisiken, Risiken aus den Anforderungen über Suitability & Appropriateness), das Risiko von Betrug, Cyber-Attacken oder Unterbrechungen oder Rechtsrisiken wie das Risiko von Rechtsfällen.**	Die Definition des Begriffs «operationelle Risiken» entspricht Art. 89 ERV. Eine blosse Wiederholung des gleichen Wortlauts erachten wir als wenig zielführend. Insbesondere sollte die für die Praxis relevante Präzisierung im Erläuterungsbericht (Ziff. 4.1.2, Seite 11) hinzugefügt werden.
7	*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 Vertrau-	Die Einbindung der C.I.A. Prinzip sollte mit der Rückverfolgbarkeit erweitert werden. Ein Front-to-back Prinzip sollte bei kritischen Daten angewendet werden, um die Sicherstellung von Schnittstellen und allfälligen Manipulationen sicherzustellen.

Rz	Änderungsvorschlag Regulierungstext	Begründung / Kommentar
	lichkeit, als auch Integrität**, Rückverfolgbarkeit** 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).	
12	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.~~ **und Abhängigkeiten von Technologieinfrastruktur, Schlüsselpersonen, Drittparteien und kritischen Daten, um im Fall eines Unterbruchs eines kritischen Prozesses die Wiederherstellungsziele zu erreichen.**	Die DRPs sollten sich nicht nur auf Abhängigkeiten zu Technologieinfrastruktur und Schlüsselpersonen beschränken, sondern auch Drittparteien und kritische Daten berücksichtigen, die zur Erreichung der Wiederherstellungsziele benötigt werden. Dies wäre auch mit Sicht auf die Grundsätze 4, 6 und 7 sowie auf das Outsourcing RS schlüssiger.
Neu	**Neue RZ unter "Begriffe"** **Der Risikoappetit definiert das Risiko, das das Institut bewusst zu tragen bereit ist. Der Risikoappetit liegt dabei innerhalb der Risikokapazität, d.h. dem maximal tragbaren Risiko.**	Unsere Erfahrung aus Prüfungen in diesem Bereich hat gezeigt, dass bei vielen Instituten Unklarheit darüber herrscht, was unter «Risikotoleranz» und was unter «Risikoappetit» zu verstehen ist. Zudem verwenden die meisten Institute ausschliesslich den Begriff «Risikoappetit». Wir empfehlen deshalb, den Begriff «Risikotoleranz» generell mit «Risikoappetit» zu ersetzen und in einer zusätzlichen Rz unter dem Kapitel «Begriffe» zu definieren. Unser Vorschlag für die Definition richtet sich nach den Vorgaben der BCBS.
19	Institute nach Art. 47a–47e ERV, Personen gemäss Art. 1b BankG, sowie nicht-kontoführende Wertpapierhäuser sind zusätzlich von der Erfüllung der Rz 60, 63, 67, ~~**69–**~~70 und 92–96 ausgenommen.	Kleinbanken, Personen gemäss Art. 1b BankG sowie nicht-kontoführende Wertpapierhäuser sind von der Erfüllung der Rz 69 (Meldepflicht für Vorfälle, die kritische Daten wesentlich beeinträchtigen) ausgenommen. Dies erachten wir grundsätzlich als fragwürdig, da derartige Vorfälle insbesondere auch für Kleinbanken bedeutende Auswirkungen haben können. Zudem stellen sich Abgrenzungsprobleme in Bezug auf die Meldepflicht gemäss Rz 52 (wesentliche Störung durch IKT-Vorfälle bei der Erbringung kritischer Prozesse) sowie Rz 56 (Cyber-Attacke). Die aufgeführten Institute (Kleinbanken, Personen gemäss Art. 1b BankG sowie nicht-kontoführende Wertpapierhäuser) sind von der Anwendung der Rz 52 und 56 sowie der entsprechenden Meldepflicht nicht befreit. Wesentliche Vorfälle mit kritischen Daten dürften oft auch kritische Prozesse stören, weshalb auf die Befreiung zur Anwendung der Rz 69 verzichtet werden sollte, damit Abgrenzungsprobleme zu den anderen Meldepflichten vermieden werden können.
21	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**~~**7** behandelt werden	Risiken aus BCM und Operationeller Resilienz sollten ebenfalls im qualitativen Management von Operationellen Risiken berücksichtigt werden, wie dies für Risiken aus IKT, Cyber und Datenmanagement der Fall ist.

Rz	Änderungsvorschlag Regulierungstext	Begründung / Kommentar
22	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]. **Dabei sind jeweils auch diejenigen Risiken neu zu beurteilen, welche bei früheren Risikoanalysen nicht von Bedeutung waren.**	Als Teil des Managements von Risiken sollte nebst bestehenden Risiken, auch explizit die jährliche Evaluation neuer sowie die Reevaluation von Risiken, die bis anhin nicht relevant waren, genannt werden.
23	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**. Die Beurteilung der Angemessenheit und allfällige Anpassung bestehender Massnahmen sollte regelmässig wiederholt werden.**	Die kritische Beurteilung der Angemessenheit bestehender Massnahmen zur Reduktion identifizierter Risiken sollte regelmässig erfolgen.
26	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 **formell und nachvollziehbar** beurteilt. **Fussnote 5:** Externe Faktoren sind beispielsweise erkannte Verlustereignisse anderer Institute, Änderungen in der Sicherheitslage (bspw. durch Umwelteinflüsse**, Cyber-Angriffe** oder Terrorismus) oder Änderungen in den regulatorischen Anforderungen.	Ohne ausdrückliche Formerfordernis, wird dieser Punkt kaum prüfbar sein. Fussnote 5: Die Sicherheitslage ist zudem durch Cyber-Angriffe bedroht, was explizit erwähnt und berücksichtigt werden sollte.
28	Für die Beurteilung der bestehenden Kontroll- und Minderungsmassnahmen wird insbesondere eine regelmässige, unabhängige und **formale** 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. **Allfällig identifizierte Schwachstellen sind zeitnah zu adressieren.** Auch wird die Trennung der Aufgaben, Verantwortungen und Kompetenzen zur Sicherstellung der Unabhängigkeit und Vorbeugung vor Interessenskonflikten regelmässig beurteilt. **Unabhängig ist eine Beurteilung dann, wenn sie zur Vermeidung von Interessenkonflikten von einer anderen Organisationseinheit durchgeführt wird als von der die Kontrolle regelmässig durchführenden Stelle.**	Die Ergebnisse der unabhängigen Beurteilung sollen nachvollziehbar dokumentiert und allfällig identifizierte Schwachstellen zeitnah adressiert werden. Aus Prüfungssicht ist es zudem wichtig zu verstehen, wie der Begriff «unabhängig» ausgelegt werden soll, damit sich eine konsistente Beurteilung durch die verschiedenen Prüfgesellschaften ergibt.
29	**Vor der Vornahme** ~~**Für**~~ wesentliche**r** Änderungen in den Produkten, Aktivitäten, Prozessen und Systemen sind **ad hoc** Risiko- und Kontrollbeurteilungen durchzuführen. Diese berücksichtigen die mit dem Änderungsprozess einhergehenden operationellen	Es sollte klargestellt werden, dass Risiko- und Kontrollbeurteilungen vor der Vornahme der Veränderungen vorgenommen werden, damit zu hohe Risiken rechtzeitig erkannt und adressiert werden können. Um Missverständnisse zu vermeiden, sollte deshalb ausdrücklich auf «ad-hoc» Beurteilungen verwiesen werden.

Rz	Änderungsvorschlag Regulierungstext	Begründung / Kommentar
	Risiken und die operationellen Risiken des Zielzustands. Bei Bedarf wird die Risikotoleranz angepasst **sowie neue Kontroll- und Minderungsmassnahmen implementiert.**	Zudem hat eine Änderung in der Risikotoleranz auch Auswirkungen auf den Massnahmenkatalog sowie auf die entsprechenden Kontrollen.
30.b.	Risiko- und Kontrollindikatoren für die Überwachung der operationellen Risiken und zeitnahe Identifikation ~~von~~ **einer Risikoerhöhung** ~~einer relevanten Anstiegen im Ausmass~~, in dem das Institut den Risiken ausgesetzt ist;	Vorschlag einer sprachlichen Vereinfachung
31	**Der Risikoappetit** ~~**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. **Vorschlag Fusszeile: *Der inhärente Risikoappetit in Bezug auf operationelle Risiken kann z.B. durch die bestimmte Bedienung gewisser Kundensegmente oder Länder, oder dem Angebot/Vertrieb bestimmter Produkte festgelegt und überwacht werden.**	Da wir eine gewisse Unsicherheit bezüglich Umsetzung von inhärentem Appetit (siehe Kommentar zu Risikotoleranz vs. -appetit oben) beobachten, erachten wir eine zusätzliche Erklärung dazu als empfehlenswert.
35	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. **Die Geschäftsleitung stellt zudem sicher, dass ausreichende Ressourcen sowie interne oder externe IKT-Fachkräfte vorhanden sind, um die definierte IKT-Strategie sowie das vorgesehene Schutzniveau zu erreichen.**	Die IKT-Strategie soll so definiert werden, dass sie mit vorhandenen Ressourcen erreicht werden kann und ansonsten eine Allokation zusätzlicher Ressourcen vorsehen.
36	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.**~~ **Es trägt dazu bei, dass die Wirksamkeit des Kontrollsystems unabhängig und regelmässig überprüft wird**.	Die Wirksamkeit des Kontrollsystems in Bezug auf IT-Risiken wird in der Regel nicht umfassend und systematisch überprüft. Dies führt zu teilweise unwirksamen Kontrollen. Daher empfehlen wir hier eine präzisere Aussage.
37	Bei der Erstellung des Managements der IKT-Risiken sind relevante international anerkannte Standards **(bspw. COSO, COBIT)** und Best Practices zu berücksichtigen, sowie neue technologische Entwicklungen.	Die Erwähnung von anerkannten internationalen Standards unterstützt die Vergleichbarkeit und Best Practices.
40	Das Management der IKT-Risiken beinhaltet eine regelmässige Berichterstattung an die Geschäftsleitung hinsichtlich der Entwicklung der IKT-Risiken, **-Massnahmen, und** ~~-~~Kontrollen und -Ereignissen.	Eine Berichterstattung sollte alle Aspekte enthalten, inkl. der zu treffenden resp. getroffenen Massnahmen.
42	Dabei stehen insbesondere auch die **Anforderungen** ~~Ziele~~ hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit im Fokus.	Sprachliche Vereinfachung/Verbesserung
42	~~**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.**~~	Mit jeder Veränderung in der IKT können neue Risiken entstehen, so dass eine Schnittstelle zum IKT-Risikomanagement erforderlich ist, um eine dynamische Risikobewertung zu ermöglichen.

Rz	Änderungsvorschlag Regulierungstext	Begründung / Kommentar
	Das Änderungsmanagement definiert eine Schnittstelle zum IKT-Risikomanagement für alle Phasen der Entwicklung und Beschaffung, die eine dynamische und zeitnahe Beurteilung der Auswirkungen und Änderungen auf IKT-Risiken gewährleistet. Dabei stehen insbesondere auch die **Anforderungen ~~Ziele~~** hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit im Fokus. **Die Auswirkungen der durch einen Change Request beantragten Veränderungen müssen ermittelt und die Veränderungen klassifiziert und priorisiert werden.**	Sprachliche Vereinfachung Der Erläuterungsbericht enthält auf Seite 13 eine Vorgabe, die im Interesse der Klarheit direkt im Rundschreiben aufgeführt werden sollte.
43	Es ist eine Trennung zwischen den IKT-Umgebungen für die Entwicklung **oder ~~und~~** das Testen und denjenigen für die IKT-Produktion sicherzustellen. Dies umfasst**, soweit möglich,** auch eine eindeutige Zuweisung von Aufgaben, Funktionen und Verantwortlichkeiten und eine Regelung der damit einhergehenden Zugangsberechtigungen.	Um technische Entwicklungsmethoden wie DevOps zu berücksichtigen, empfehlen wir die Erwartung von drei auf zwei Umgebungen (Entwicklung/Testen und Produktion) zu ändern. Zudem gehen wir davon aus, dass die eindeutige Zuweisung Aufgaben, Funktionen und Verantwortlichkeiten nicht immer möglich ist.
45	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 **innerhalb des Instituts sowie** zu wesentlichen externen Dienstleistern berücksichtigt.	Der Begriff «interne Abhängigkeiten» ist eher schwer verständlich. Im Weiteren sollten bei Software-Komponenten auch Abhängigkeiten zu wesentlichen Dienstleistern dokumentiert werden (z.B. zu Providern einer SaaS Lösung).
46	**Das Inventar ~~Die Inventarisierung~~** ist **~~zeitnah~~** verfügbar und wird regelmässig **hinsichtlich Vollständigkeit und Richtigkeit** überprüft und aktualisiert.	Sprachliche Vereinfachung. Die Inventarisierung bezieht sich auf die Aktivität, was in diesem Zusammenhang nicht passt. «Zeitnah» wird als unnötig erachtet, da die Erwartung ist, dass das Inventar immer verfügbar ist. Zudem empfehlen wir zu präzisieren, was zu überprüfen ist.
48	**Das Institut stellt mit Hilfe seiner BCM- und DRP-Prozesse sicher, dass ein reibungsloser Übergang zwischen Krisensituation und Betriebsmanagement vorhanden ist.** **~~Das Institut stellt konsistente Übergänge vom IKT-Betriebsmanagement in seine BCM- und DRP-Prozesse sicher.~~**	Der Satz wurde umformuliert, um den Übergang zwischen BCM und Normalbetrieb zu erläutern.
55a	Identifikation der institutsspezifischen **~~Bedrohungspotenziale~~ Risiken** durch Cyber-Attacken[8] und Beurteilung der möglichen Auswirkungen der Ausnützung von Schwachstellen bezüglich der inventarisierten Bestandteile der IKT. Fussnote 8: Angriffe aus dem internen Netzwerk, dem Internet und ver-gleichbaren Netzen auf die Vertraulichkeit, Integrität und Verfügbarkeit der IKT sowie kritischen Daten.	Bedrohungen sind u.E. allgemeiner Natur und nicht institutsspezifisch. Es geht in diesem Absatz gemäss unserem Verständnis primär um die Identifikation von institutsspezifischen Cyberrisiken («Risiken durch Cyber-Attacken»). Nur wenn ein Institut ein Asset mit entsprechender Verwundbarkeit besitzt, wird die allgemeine Bedrohung zum institutsspezifischen Risiko. In der Fussnote 8 sollte zudem klar ausgewiesen werden, ob damit auch Angriffe aus dem internen Netzwerk durch eigene Mitarbeitende zu verstehen sind (d.h. Angriff wird bewusst durch eigene Mitarbeitende initiiert und nicht von externen Angreifern, welche lediglich interne Mitarbeitende für den Angriff «missbrauchen»).

Rz	Änderungsvorschlag Regulierungstext	Begründung / Kommentar
55b	Schutz der kritischen **Systeme, Daten und** Prozesse vor Cyber-Attacken durch die Implementierung angemessener Schutzmassnahmen, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen Daten und IT-Systeme.	Aus unserer Sicht geht nicht nur um den Schutz der kritischen Prozesse, sondern auch um die Systeme und die Daten. Wir empfehlen deshalb, dies zu präzisieren.
58	Die Geschäftsleitung lässt regelmässig Verwundbarkeitsanalysen[9], Penetrationstests und auf Basis der institutsspezifischen ~~**Bedrohungspotenziale**~~ **Risiken** szenariobasierte Cyber-Übungen 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.	Bedrohungen sind u.E. allgemeiner Natur und nicht institutsspezifisch. Es geht in diesem Absatz gemäss unserem Verständnis primär um die Identifikation von institutsspezifischen Cyberrisiken («Risiken durch Cyber-Attacken»). Nur wenn ein Institut ein Asset mit entsprechender Verwundbarkeit besitzt, wird die allgemeine Bedrohung zum institutsspezifischen Risiko. Die mit dem Wort «darüberhinaus» verbundene Absicht der FINMA ist uns unklar. Grundsätzlich sollen die Anforderungen gemäss unserem Verständnis für alle Systeme gelten, welche über das Internet erreichbar sind.
59	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.	Im Erläuterungsbericht (Ziff. 4.1.5, Seite 17: «Die Pflichten und Verantwortlichkeiten des Oberleitungsorgans und der Geschäftsleitung (Rz 59–60)») weist die FINMA auf die Pflichten und Verantwortlichkeiten des Oberleitungsorgans hin durch einen Verweis auf die Rz 59-60. Dieser Verweis scheint zu implizieren, dass die Datenstrategie durch den Verwaltungsrat zu erlassen sei. Falls dies die Absicht der FINMA ist, sollte im Interesse der Klarheit die Verantwortlichkeit für die Datenstrategie im Rundschreiben selber aufgeführt und klargestellt werden.
64	Kritische Daten sind **nebst dem operativen Betrieb auch** 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	Es soll ersichtlich sein, dass dies als Ergänzung zu den ohnehin bereits bestehenden Massnahmen zu verstehen ist.
70	Bei der Auswahl von Dienstleistern, die ~~**auf**~~ kritische Daten ~~**zugreifen können oder solche verwalten**~~**bearbeiten* 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 auslagernden Instituts risikoorientiert periodisch zu überwachen und zu kontrollieren. *** Vorschlag Fussnote: Bearbeiten: jeder Umgang mit kritischen Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.**	Der Begriff “Daten bearbeiten” ist im Datenschutzgesetz geregelt (Art. 3 Bst. e Datenschutzgesetz). Wir empfehlen, den Begriff in einer Fussnote in Anlehnung an Art. 3 Bst. e DSG zu definieren. Zudem sind gemäss Rz 19 Kleinbanken, Personen gemäss Art. 1b BankG sowie nicht-kontoführende Wertpapierhäuser sind von der Erfüllung der Rz 70 ausgenommen. Gleichzeitig verlangt jedoch das FINMA-RS 18/3 «Outsourcing» in Rz 24 trotzdem eine Überwachung von Dienstleistern: «Bei sicherheitsrelevanten Auslagerungen (namentlich im Bereich IT) legen das Unternehmen und der Dienstleister vertraglich Sicherheitsanforderungen fest. Deren Einhaltungen sind vom Unternehmen zu überwachen.» Falls ein externer Dienstleister auf kritische Daten zugreift oder diese verwaltet, dürfte die Wahrscheinlichkeit hoch sein, dass es sich um ein wesentliches Outsourcing im Sinne des RS 18/3 handelt und somit die Erleichterung nicht greift. Diese Regelungen widersprechen und sollten aufeinander abgestimmt werden.

Rz	Änderungsvorschlag Regulierungstext	Begründung / Kommentar
79	Die BIA und BCP werden einer institutsweiten Vorgabe folgend auf konsistente Art erstellt und dokumentiert. Sie sind **mindestens** jährlich sowie im Falle wesentlicher Änderungen im Geschäftsbetrieb (Reorganisationen, Aufbau eines neuen Geschäftsfelds usw.) **ad hoc** zu ~~**überprüfen**~~ **aktualisieren**.	Präzisierung der Periodizität
80	Das Institut definiert als Teil des BCP einen DRP. Wenn ~~**Teile der Technologieinfrastruktur ausgelagert sind**~~ **kritische Prozesse 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	Analog zum Kommentar zu Rz 12 sollten die DRP nicht nur Technologieinfrastruktur und Schlüsselpersonen abdecken.
91	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"), **das Management von IKT und Cyber Risiken** 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.	Wir erachten es als sinnvoll, bei einer Aufzählung der Bestandteile von Operationeller Resilienz auch die IKT und Cyber Risiken explizit zu erwähnen. Dies unter dem Gesichtspunkt, dass bereits alle anderen wichtigen Elemente aufgezählt werden und sonst der Eindruck entsteht, dass IKT und Cyber Risikomanagement weniger wichtig sind.
92	Zur operationellen Resilienz hat eine Berichterstattung an die Geschäftsleitung und das Oberleitungsorgan regelmässig zu erfolgen, sowie bei wesentlichen Kontrollschwächen, **wesentlichen Änderungen im Geschäftsbetrieb** oder Vorfällen, die die operationelle Resilienz gefährden.	Änderungen im Geschäftsbetrieb können auch einen direkten Einfluss auf die operationelle Resilienz haben.
100	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	Gemäss Ziffer 8 des Erläuterungsberichts (Seite 33) ist die Verabschiedung des FINMA-Rundschreibens „Operationelle Risiken und Resilienz – Banken" im Dezember 2022 und das Inkrafttreten per 1. Januar 2023 vorgesehen. Lediglich zum Grundsatz 7 «Operationelle Resilienz» werden gewisse Übergangsfristen vorgesehen. Eine derart kurzfristige Implementierung dieses Rundschreibens innerhalb rund eines Monats nach voraussichtlichem Vorliegen der definitiven Fassung ist unrealistisch, da es sich unseres Erachtens nicht lediglich um eine geringfügige Überarbeitung der Regelungen handelt, sondern einen nicht zu unterschätzenden Anpassungsbedarf bei den Instituten hervorruft.