Swiss Banking

Eidgenössische Finanzmarktaufsicht FINMA
Frau Dr. Anne Feidt
Laupenstrasse 27
CH-3003 Bern

Per Mail zugestellt an: anne.feidt@finma.ch

Basel, 29. Juni 2022
MHU / +41 58 330 62 54

Totalrevision des FINMA-Rundschreibens 2008/21 «Operationelle Risiken – Banken»

Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 10. Mai 2022 eröffnete Anhörung der Eidgenössischen Finanzmarktaufsicht (FINMA) zur Totalrevision des FINMA-Rundschreibens 2008/21 «Operationelle Risiken – Banken» (nachfolgend «Rundschreiben»).

Die SBVg bedankt sich für die Gelegenheit zur Stellungnahme zum referenzierten Rundschreiben und für die vorgängige Vorkonsultation. Gerne nehmen wir diese Gelegenheit wahr und führen nachfolgend unsere Anliegen aus.

- Wir befürworten die Konzeption der FINMA, die entsprechenden Standards des Basler Ausschusses für Bankenaufsicht, die Aufsichtspraxis der FINMA sowie die Inhalte der Selbstregulierung der SBVg im Bereich des Business Continuity Management (BCM) konsolidiert und integral zu berücksichtigen.
- Wir begrüssen die vereinfachte Struktur, welche durch die Integration des ehemaligen Anhangs 3 des Rundschreibens sowie der Selbstregulierung der SBVg ermöglicht wurde.
- Ebenfalls unterstützen wir, dass das Rundschreiben technologieneutral und nach den Grundsätzen der Prinzipienbasierung und Proportionalität ausformuliert wurde. Gleichwohl gehen gewisse Änderungen den kleineren, vorwiegend in der Schweiz tätigen Instituten zu weit. Insbesondere sind Vereinfachungen auch für Banken der Aufsichtskategorie 3 wünschenswert.
- Die gewählten Definitionen mehrerer Begrifflichkeiten bedürfen einer weiteren Klärung, da sie zu einer unnötigen und teilweise ungewollten Ausweitung der damit verbundenen Pflichten führen. So ist bspw. die Verwendung des Begriffes "kritisch" sehr weit gefasst. Wir

anerkennen, dass die Begriffserklärungen und die Anwendung im Rundschreiben verbessert wurden, es besteht jedoch unseres Erachtens nach wie vor ein zu grosser Interpretationsspielraum.
- Im Rundschreiben werden Aufgaben und Kompetenzen an die Geschäftsleitung und das Oberaufsichtsorgan übertragen, welche teilweise als zu detailliert erscheinen und dadurch nicht stufengerecht sind.
- Das Rundschreiben fordert eine Vorbereitung auf den Wegfall grundlegender Ressourcen über Monate. Die Bewältigung eines solchen Szenarios, unter den dort vorgeschlagenen Vorgaben, ist nur mit Vorarbeit und Garantien von Seiten des Staates möglich. Dementsprechend erscheint eine verpflichtende Vorbereitung und damit einhergehende Übung solcher Szenarien ohne diese notwendige Grundbedingung als nicht zielführend.
- Für das gesamte Rundschreiben empfehlen wir, die Übergangsfristen jeweils um ein Jahr zu erweitern und für die Risiko-Steuerung ebenfalls eine spezifische Übergangsfrist von einem Jahr vorzusehen.

1. Allgemeine Betrachtungen

Umsetzung Basler Standards

Die Anpassungen basieren auf den Revisions to the Principles for the Sound Management of Operational Risk (PSMOR) und den neuen Principles for Operational Resilience (POR) des Basler Ausschusses für Bankenaufsicht (BCBS) vom März 2021.

Bei einer Umsetzung der Basler Standards ist zu beachten, dass diese allgemeine, prinzipien- und risikobasiert formulierte Grundsätze darstellen und bei der Überführung ins nationale Recht dessen Usanzen und bewährte Mechanismen zu berücksichtigen sind. Die FINMA hat bei der Umsetzung einen grossen Ermessensspielraum, insbesondere wenn es darum geht, welche Vorgaben aus welchen Gründen auch auf national tätige bzw. kleinere Banken Anwendung finden sollen. Dabei sind stets auch Wettbewerbsfähigkeit und Verhältnismässigkeit zu berücksichtigen. Ein Teil unserer Vorschläge ist insbesondere vor diesem Hintergrund zu verstehen.

Im Erläuterungsbericht wird der Handlungsbedarf dieser Umsetzung und die Einbettung in das nationale und internationale Umfeld thematisiert (S. 8 f.). Bei den Ausführungen wird jedoch nicht ganz klar, wie sich das Verhältnis zu anderen bestehenden Regelwerken präsentiert, wie z.B. zum Standard Nummer 239 «Principles for effective risk data aggregation and risk reporting» des Basler Ausschusses.

Prinzipienbasierte Regulierung

Wir anerkennen, dass der vorliegende Entwurf bereits zu einem grossen Teil dem Leitprinzip der Prinzipienbasierung genügt. Allerdings geht diese Prinzipenbasierung in einigen Teilen noch zu wenig weit.

Richtig verstandene prinzipienbasierte Regulierung definiert das konkrete Regulierungsziel, belässt aber für den Weg ins Ziel ein grosses Ermessen bzw. Handlungsfreiheit. Die Institute haben dieses Ermessen vernünftig auszuüben und die Umsetzung aufgrund der konkreten Verhältnisse wie namentlich Grösse,

Struktur, Komplexität, Risiken und Geschäftsmodell, angemessen vorzunehmen. Entgegen diesen Grundsätzen erscheint es nun in Teilen zu einer Verschärfung zu kommen, bspw. indem der Anwendungsbereich kritischer Daten generalisiert wird (z.B. Abkehr von der bisherigen Eingrenzung auf «Client Identifying Data» (CID)).

Technologieneutrale Regulierung

Wir begrüssen es, dass der Entwurf des Rundschreibens technologieneutral ausformuliert wurde und es keine differenzierende Behandlung unterschiedlicher Technologien unterhalb des Regulierungsziels gibt. Damit kann verhindert werden, dass bestimmte Prozesse oder aktuelle Technologien erwähnt werden, die in einigen Jahren überholt sein könnten und eine erneute Überprüfung erfordern würden.

Verhältnismässige Regulierung (Proportionalitätsprinzip)

Entsprechend den Ausführungen im Erläuterungsbericht (vgl. S. 1, Ziff. 1) wurde auf eine proportionale Umsetzung der Basler Vorgaben geachtet. Grundsätzlich begrüssen wir, dass die FINMA bereits im Rahmen der Vorkonsultation bereit war, die Grundsätze der Verhältnismässigkeit im Rundschreiben zu verankern. Die SBVg erachtet es als von entscheidender Bedeutung, dass die Umsetzung der im Rundschreiben enthaltenen Anforderungen entsprechend der Grösse, der Komplexität, der Struktur und dem Risikoprofil des Instituts erfolgen kann.

Nach diesen Grundsätzen sollen bei Vorliegen von sachlich überzeugenden Kriterien die rechtlichen Pflichten auch zwischen unterschiedlichen Gruppen von rechtsunterworfenen Instituten vernünftig und angemessen abgestuft werden. Dies drängt sich namentlich bei Organisationspflichten sowie bei den Anforderungen ans Risikomanagement auf. Nur schon unter dem Aspekt der Grösse ist es naheliegend, dass bei kleineren Instituten nicht dieselbe Komplexität von bankinterner Organisation und Kompetenzverteilung sinnvoll ist, wie dies bei grossen Instituten allenfalls angezeigt ist.

Entsprechend ist zu überlegen, unter welchen Voraussetzungen und bei welchen Randziffern die Kategorie 3 Banken noch weiter entlastet werden sollen.

2. Anmerkungen zu den Begriffen

Grundsätzlich scheint es einige Begrifflichkeiten zu geben, bei welchen Klärungsbedarf besteht. Der teils sehr hohe Detaillierungsgrad führt dazu, dass bei der Umsetzung grosse Sorgfalt angewendet werden muss, was auch bei der Fristensetzung zur Umsetzung berücksichtigt werden sollte. Zusätzlich bitten wir um Schärfung verschiedener Definitionen.

	II. Begriffe
[Rz 3]	Bei der Definition zu «**Operationellen Risiken»** werden Begrifflichkeiten verwendet, welche einer weiteren Spezifizierung bedürfen. So ist bspw. nicht klar, wie sich «**Verlust»** definiert; beschränkt sich der Begriff auf den finanziellen Verlust, oder sind eventuell Auswirkungen gemeint in den Dimensionen, wie sie

	in Rz 8 des Rundschreibens beschrieben werden (finanziell, operationell, rechtlich und reputationell)? Bei der Betrachtung des zweiten Teilsatzes scheint die Systematik nicht ganz stimmig zu sein. So stellt sich die Frage, ob **«Rechtsrisiken»** und **«Reputationsrisiken»** als eigenständige Risikokategorien (also auf der gleichen Ebene wie **strategische Risiken**, wie in Rz 3 impliziert) oder als Schadensdimensionen («Auswirkungen»), wie in Rz 8 definiert, zu betrachten sind (vgl. auch Kommentar zu Rz 8). Es scheint zudem widersprüchlich, dass die Reputationsrisiken hier ausgeschlossen werden, während hingegen bei den kritischen Prozessen (Rz 8) auch die reputationellen Auswirkungen beachtet werden. Selbstverständlich sind aber auch wir der Ansicht, dass Reputationsrisiken nicht Bestandteil des operationellen Risikos sind. Falls Rechtsverletzungen als eigenständige Risikokategorie angesehen werden, bedürfte es einer Abgrenzung zur Definition von Compliance(-Risiken) nach dem FINMA-RS 17/1 «Corporate Governance – Banken», Rz 7. Eine Abgrenzung zu ESG-Risiken wäre zusätzlich wünschenswert, speziell zu den Klimarisiken. Ein Beispiel einer Abgrenzungs-Schwierigkeit könnte wie folgt lauten: Ist die Beschädigung eines Bankgebäudes durch Erdrutsch als «Folge von externen Ereignissen» und damit als operationelles Risiko zu qualifizieren, oder als Folge der klimatischen Veränderung und damit als ein ESG ─ Risiko?
[Rz 7]	Der neu verwendete Begriff **«Kritische Daten»** scheint sehr weit gefasst zu sein. So ist es unklar, ob mit «Daten» jeweils (wie im bisherigen Rundschreiben) elektronische Daten oder auch physisch vorliegende Daten gemeint sind (wird nicht explizit aufgeführt). Dies kann dazu führen, dass sämtliche von einem Institut bearbeiteten Daten unter vorliegende Umschreibung fallen. Das lässt sich nur schon systematisch nicht begründen. Rz 7 ist eine Ausnahmebestimmung für Daten, die eines besonderen Schutzes bedürfen und auf welche deshalb verschärfte Pflichten anwendbar sein sollen. Solche Ausnahmebestimmungen dürfen nicht derart weit gefasst werden, dass sie dadurch zur Regel werden. Dies würde nämlich zur sachlich falschen Folge führen, dass praktisch sämtliche von einem Institut bearbeiteten Daten im Ergebnis dem höchstmöglichen Schutzniveau zu unterstellen wären, womit auch unnötige Mehrkosten in massivem Umfang anfallen würden. Ferner sind verschiedene im Rundschreiben erwähnte Datensätze bereits durch spezialgesetzliche Regelungen geschützt**.** Dies trifft namentlich auf im Datenschutzgesetz (DSG) einlässlich geregelte «Personendaten» und auf gemäss Strafgesetzbuch (StGB) geregelte «Geschäftsgeheimnisse» zu. Regelverstösse sind sowohl gemäss DSG als auch gemäss StGB sogar strafbewehrt. Die Institute haben auch diese Spezialgesetze einzuhalten, weshalb eine zusätzliche Regulierung durch die FINMA in solchen Bereichen weder sinnvoll noch nötig ist. Nunmehr generalisiert die FINMA den Anwendungsbereich, was sich sachlich nicht begründen lässt. Zudem werden dadurch strikte Pflichtenhefte undifferenziert generalisiert, womit jedes Ermessen des einzelnen Instituts verunmöglicht wird.

	Das Bankkundengeheimnis (Art. 47 BankG) sieht für Personendaten, sofern es sich um Kundendaten handelt, einen viel strikteren und schärferen Schutz vor als die Regeln des DSG. Selbst innerhalb der vom Bankkundengeheimnis geschützten Kundendaten kann es unterschiedlich sensible Kundensegmente geben, weshalb eine sinnvolle Abstufung mit unterschiedlichen Schutzniveaus angezeigt ist. Dies festzulegen, muss dem einzelnen Institut obliegen. Personendaten ausserhalb des Kundenstammes stellen per se keine kritischen Daten dar. Deshalb ist auch aufsichtsrechtlich keine Zusatzregulierung angezeigt. Im Bereich des strafrechtlich geschützten Geschäftsgeheimnisschutzes kann ein Geheimnisträger aus verschiedenen Gründen legitimerweise auf seinen Geheimnisschutz verzichten. Auch ein aufsichtsrechtlich weitergehender Schutz von Geschäftsgeheimnissen macht aus diesem Blickwinkel keinen Sinn. Somit wird auch klar, dass der FINMA für eine solche zusätzliche aufsichtsrechtliche Regulierung von Spezialgesetzen wie DSG oder StGB nur schon die Regulierungskompetenz fehlt, da es sich um abschliessend geregelte Bundesgesetze handelt. Richtigerweise hat jedes Institut selbst in Anwendung von vernünftigem Ermessen unter Würdigung seiner konkreten Verhältnisse zu entscheiden, zwischen welchen Datensätzen risikoadäquat wie zu unterscheiden ist. Dabei sind – entsprechend der von der FINMA selbst geprägten Formel – namentlich Grösse, Struktur, Komplexität, Geschäftsmodell und Risiken des einzelnen Instituts massgebend. Da der Begriff für wichtige Pflichten von zentraler Bedeutung ist (z.B. erhöhter Schutz der Daten im Ausland, erhöhte Anforderungen an Mitarbeitende und Dienstleister mit Zugriff auf kritische Daten), ist es notwendig, den Begriff schärfer zu umreissen und vorgehende Überlegungen miteinzubeziehen.
	Formulierungsvorschlag Kritische Daten sind Daten, die ein Institut unter vernünftiger Würdigung der konkreten Verhältnisse wie namentlich Grösse, Struktur, Komplexität, Geschäftsmodell und Risiken als derart wesentlich und kritisch erachtet, um sie einem schärferen Schutz zu unterstellen. Dies werden typischerweise bestimmte besonders wichtige Daten in Zusammenhang mit der ~~für eine~~ erfolgreichen und nachhaltigen Erbringung von ~~seiner~~ Dienstleistungen ~~als wesentlich erachtet,~~ oder ~~Daten, die~~ für regulatorische Zwecke sein ~~aufbewahrt werden müssen~~. Solche Daten können sowohl hinsichtlich der Vertraulichkeit als auch Integrität oder Verfügbarkeit besonders kritisch sein. Daten, die hinsichtlich der Vertraulichkeit besonders kritisch sind ~~(vertrauliche Daten)~~, sind dabei solche, die besonders vor unautorisierter Offenlegung geschützt werden müssen. Dies sind namentlich ~~(bspw. Personendaten,~~ Kundendaten, ~~Geschäftsgeheimnisse)~~, wobei typischerweise eine Differenzierung zwischen Kundendaten von unterschiedlich sensiblen Kundensegmenten angezeigt ist.
[Rz 8]	Betrachtet man die Definitionen aus Rz 8 und Rz 14, kann daraus abgeleitet werden, dass die **kritischen Prozesse** eine Teilmenge der **kritischen Funktionen** sind. Der Erläuterungsbericht hält fest, dass zwar die für die Erbringung kritischer Funktionen notwendigen

	Prozesse immer kritische Prozesse, umgekehrt jedoch nicht alle kritischen Prozesse auch für kritische Funktionen relevant seien (S. 22). Auch dieser Hinweis vermag letztlich keine genügende Klarheit zu schaffen. Darüber hinaus heisst es unter Rz 96: «Die kritischen Funktionen und die dafür erforderlichen kritischen Prozesse und Ressourcen werden abgedeckt durch...». Stattdessen sollte es heissen: «Die hierfür erforderlichen kritischen Funktionen (einschliesslich der kritischen Prozesse und der zugrunde liegenden Ressourcen) ...». Das Dokument sollte unserer Meinung nach den Unterschied und die Beziehung zwischen diesen beiden Schlüsselbegriffen deutlicher machen, um Mehrdeutigkeiten sowie Fehlinterpretationen zu vermeiden. Um eine klare Abgrenzung zum FINMA RS 2018/3 zu erreichen, regen wir zudem an, die Formulierung **«wesentlich gefährdet»** durch «signifikant gefährdet» zu ersetzen. Wir möchten hier ergänzend anmerken, dass der Begriff «Geschäftsziele» zu weit gefasst ist, da «Geschäftsziele» vom Management definiert sind, oft wirtschaftliche Wachstumsziele beinhalten, welche nicht in jedem Fall für den weiteren Betrieb des Unternehmens entscheidend sind. Wir würden es begrüssen, wenn die Definition von «kritischen Prozesse» entsprechend angepasst wird.
[Rz 9]	Im Zusammenhang mit dem Business Continuity Management (BCM) gehörte der Begriff **«wesentliche Unterbrechung»** bisher nicht zu den gebräuchlichen Ausdrücken. Das bisherige Wording aus den BCM-Empfehlungen der SBVg sah vor: «… dass kritische Geschäftsprozesse im Falle von massiven, einschneidenden internen oder externen Ereignissen aufrechterhalten werden können.» Das Rundschreiben lässt die Lesart zu, dass im Falle einer wesentlichen Unterbrechung der Betrieb der kritischen Prozesse wiederherzustellen, die Institute neu im operativen Modus (Notfallstufe) und nicht im klassisch definierten BCM-Umfeld (strategisch, Krisenstufe) agieren müssen. Diese Abkehr von einer strategischen Ebene führt zu einer Änderung in der BCM-Definition und kann grosse Auswirkungen auf die bisherigen und dokumentierten Aufgaben, Kompetenzen und Verantwortlichkeiten (Änderungen von Vorgabe-Dokumenten, Not- und Krisendokumentation; Änderungen von Eskalations-Definitionen, Prozessen und Verantwortlichkeiten etc.) nach sich ziehen. Im gleichen Zusammenhang wäre ebenfalls zu klären, wie «wesentlich» definiert ist. Siehe dazu auch die Auskunfts- und Meldepflicht nach Art. 29 Finanzmarktaufsichtsgesetz (FINMAG), welche folgendes besagt: «die Beaufsichtigten und die Prüfgesellschaften, die bei ihnen Prüfungen durchführen, müssen der FINMA zudem unverzüglich Vorkommnisse melden, die für die Aufsicht von wesentlicher Bedeutung sind.» Diese Definition lässt der FINMA sehr viel Spielraum, ist jedoch für das einzelne Institut schwierig zu interpretieren. Reicht bspw. der Ausfall des E-Bankings für 24 Stunden, oder

	ist dazu eine höhere Intensität erforderlich? Wir möchten beliebt machen, hier eine risikogerechte Abgrenzung vorzugeben.
[Rz 10]	Die **«Recovery Time Objective» (RTO)** und «**Impact Tolerance»** sind nicht widerspruchsfrei definiert (insbesondere aufgrund der Feststellung in den Erläuterungen, dass die Impact Tolerance «ähnlich dem RTO aus dem BCM» sei). Der im BCM gebräuchliche Wert «**Maximum Period of Downtime» (MPDT)** wird im Rundschreiben und in den Erläuterungen nicht definiert. Mit der Einführung der Unterbrechungstoleranz stellt sich allerdings die Frage nach der Abgrenzung der verschiedenen Werte, z.B. zwischen RTO und Unterbrechungstoleranz und MPDT. Wir bitten um Klärung der entsprechenden Abhängigkeiten.
[Rz 13]	Die derzeitige Formulierung von **«Krisensituationen»** berücksichtigt nur die Definition aus dem Glossar der BCM-Empfehlungen der SBVg, nicht jedoch den dazugehörigen Anhang B. Während Banken die Abgrenzung von Krisen von bedeutenden Störungen aufgrund der SBVg-Empfehlungen bereits gut implementiert haben, ist dies bei «Outsourcing»-Partnern und Lieferanten alles andere als selbstverständlich. Langjährige Erfahrungen bei Vertragsverhandlungen mit Outsourcings und kritischen Lieferanten zeigen, dass diese jeweils ihr Incident-/Störungs-Management als Krisenmanagement «verkaufen» wollen und Banken diese Lieferanten mittels schwierigen Verhandlungen dazu zwingen müssen, ein Krisenmanagement aufzubauen, welches nicht nur Incidents, sondern auch Krisen regelt. Da bei den meisten Unternehmen bereits auf Stufe «bedeutende Störung» spezielle Gremien und Taskforces zum Einsatz kommen (d.h. Bewältigung der Situation mittels ausserordentlicher Massnahmen und Entscheidungsgremien), regeln diese Unternehmen faktisch nur das Vorgehen bei «bedeutenden Störungen» - nicht aber bei echten Krisensituationen (wo eine Taskforce für Incidents nicht mehr ausreicht). Sofern die Rz 13 nicht angepasst wird, können Banken künftig nicht mehr auf das FINMA-Rundschreiben verweisen, um ihre Lieferanten zu einem Krisenmanagement (statt nur einem Incident-Management) zu verpflichten. Um die Ausserordentlichkeit der Situation herauszuheben und damit die Voraussetzungen von den Mitteln abzuheben, schlagen wir nachfolgende Formulierung vor. Zudem soll die Definition von Krisensituationen nicht von der Wahl der Mittel abhängig gemacht werden, sondern vielmehr von der Art der Bedrohung. Die Definition muss entsprechend geschärft werden. **Formulierungsvorschlag** Krisensituationen sind ausserordentliche, potenziell existenzbedrohende Situationen, welche das Institut oder kritische Geschäftsprozesse des Unternehmens bedrohen oder stören und welche nicht mit ordentlichen Massnahmen und Entscheidungskompetenzen bewältigt werden können.

[Rz 14 / 96]	Die hier vorliegende Definition der «**Kritischen Funktionen»** ist aus unserer Sicht unklar, weil neben «Aktivitäten, Prozessen, Dienstleistungen» die «zugrundeliegenden Ressourcen» mit einer «und»-Verknüpfung aufgezählt werden: Eine «kritische Funktion» sollte nur der erste Teil sein, während die dafür benötigten Ressourcen kein integrales Element einer «kritischen Funktion» sind, sondern nur zu deren Erbringung benötigt werden. Wir schlagen darum vor, die «und»-Verknüpfung zu ersetzen durch eine «inklusive»-Verknüpfung.
	Formulierungsvorschlag Kritische Funktionen beinhalten: a. die Aktivitäten, Prozesse, Dienstleistungen ~~und~~ 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 […]
[Rz 15]	Die Aussage zur «**Unterbrechungstoleranz»** (**Impact Tolerance)** in den Erläuterungen («eine maximal tolerierbare Zeitspanne der Unterbrechung (ähnlich dem RTO aus dem BCM)») suggeriert, dass die Zeitspanne ähnlich lang wie der RTO sein könnte, was in der Praxis nicht der Fall sein dürfte ─ es ist mit erheblichen Abweichungen zwischen RTO und Impact Tolerance zu rechnen. Auf die entsprechende Klammerbemerkung («ähnlich dem RTO aus dem BCM») sollte aus diesen Gründen verzichtet werden.
[Rz 16]	Die Definition zur «**Operationellen Resilienz»** sollte klarer zu den folgenden Begriffen abgegrenzt werden: BCM, ITSCM, IT-Security. Ebenso sollten das Zusammenspiel bzw. die Abhängigkeiten aufgezeigt werden. So scheint nicht klar zu sein, wie bei der Operationellen Resilienz die «schwerwiegenden, aber plausiblen Szenarien» hineinspielen (vgl. dazu Rz 83). Die Ausführungen im Erläuterungsbericht sind ausführlicher (vgl. S. 24 f.) und sollten besser in der Definition bzw. im Rundschreiben selbst berücksichtigt werden. Wichtig scheint uns auch, dass die verschiedenen Regulierungsbehörden eine gleiche Vorstellung der Definitionen haben. So sollten bspw. die «schwerwiegenden, aber plausiblen Szenarien» bzw. «severe but plausible scenarios» bei der FINMA und der SNB abgestimmt sein.

3. Anmerkungen zum Proportionalitätsprinzip

[Rz 17 f.]	Entsprechend den Ausführungen zur verhältnismässigen Regulierung (vgl. S. 3, vorstehend) sollen bei Vorliegen von sachlich überzeugenden Kriterien die rechtlichen Pflichten auch zwischen unterschiedlichen Gruppen von Rechtsunterworfenen **«**vernünftig**»** und

	«angemessen» abgestuft werden (Differenzierung bzw. Proportionalität). So ist es bspw. nur schon unter dem Aspekt der Grösse naheliegend, dass bei kleineren Instituten nicht dieselbe Komplexität von bankinterner Organisation und Kompetenzverteilung sinnvoll ist, wie dies bei grossen Instituten allenfalls angezeigt ist. Folgerichtig sind auch die Anforderungen an das Risikomanagement zwischen den 5 Aufsichtskategorien angemessen abzustufen. Entsprechend ist zu überlegen, unter welchen Anforderungen und bei welchen Randziffern neben den Aufsichtskategorien 4 und 5 die Aufsichtskategorie 3 noch weiter entlastet werden soll. Wir beurteilen insbesondere nachfolgende Randziffern als zu weitgehend für Banken der Aufsichtskategorie 3: • Rz 68: Die sorgfältige Auswahl von Personen mit Zugriff auf kritische Daten ist sinnvoll. Deren angemessene Überwachung ist hingegen fragwürdig, da beispielsweise die Ausarbeitung von Prozessen und deren Ausführung zu Auswertungen von Log-Dateien für Banken der Aufsichtskategorie 3 einen unverhältnismässigen Aufwand darstellen. • Rz 84 - 85: Jährliche Tests der wichtigsten Massnahmen unter Einbindung sämtlicher Fachbereiche, der IT und allfälliger Outsourcing-Provider können unverhältnismässigen Aufwand verursachen. Unseres Erachtens reichen periodische Tests in Abhängigkeit der Risiken (Mehrjahresplanung). Diese Bemerkung soll generell für alle Bankenkategorien gelten (vgl. dazu die Bemerkungen zu Rz 84). • Rz 97: Mindestens für Banken der Aufsichtskategorie 3 mit einem tiefen Risikoprofil sind Tests über eine längere Zeitdauer klar zu weitgehend.

4. Anmerkungen zu den Grundsätzen

[Rz 21]	**Grundsatz 1: Generelle Anforderungen an das Management der operationellen Risiken**
	In Rz 21 und 23 werden die Aufgaben an die **Geschäftsleitung** definiert. Wir haben generell Zweifel bezüglich der Stufengerechtheit gewisser Verantwortungsklauseln für die Geschäftsleitung und das Oberaufsichtsorgan (Verwaltungsrat). Wir schlagen vor, dass die Formulierung wie untenstehend abgeändert wird. (Der Wortlaut «implementieren» findet sich wiederholt in Bezug auf Geschäftsleitung wie auch Oberleitungsorgan (z.B. Rz 35) und sollte demensprechend auch bei diesen Stellen angepasst werden.)
	Formulierungsvorschlag Die Geschäftsleitung ~~implementiert~~ stellt sicher 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.
[Rz 22 / 39 / 89]	Grundsätzlich stellt sich die Frage, ob das **«Oberleitungsorgan»** bzw. der VR mit einem solch detaillierten Aufgabenkatalog betraut werden muss. Die Pflichten des Oberleitungsorgans sind sehr ausführlich geregelt (bspw. Rz 89), gleichzeitig wird jedoch nicht klar, was konkret verabschiedet werden muss: Handelt es sich um alle operationellen Risiken oder nur um **«Top-Risiken»**? Es ist zwar richtig, dass sich der VR mit diesen Themen befasst. Die spezifischen Anforderungen des RS gehen aber weit über das hinaus, was als sinnvoll erscheint, insbesondere wenn es sich nicht nur um die Top-Risiken handelt. Wir empfehlen deshalb, eine stärker prinzipienbasierte, generische und stufengerechtere Formulierung auszuarbeiten.
[Rz 23]	Die im Rundschreiben vorgegebenen Aufgaben der Geschäftsleitung lassen Interpretationsraum zu, wie die grundsätzliche Verantwortlichkeit aus dem Verfahren aussehen würde. Dementsprechend schlagen wir vor, mittels nachfolgendem Formulierungsvorschlag eine abschliessende Verantwortung eindeutig zuzuweisen.
	Formulierungsvorschlag Die Geschäftsleitung hat ~~für die~~ ~~Steuerung~~ über die Umsetzung von ~~und die~~ Kontrolle~~-~~ und Minderungsmassnahmen ~~der als wesentlich beurteilten, inhärenten Risiken ergänzende risikospezifische Massnahmen~~ oder ~~eine~~ die Verschärfung bestehender Massnahmen bezogen auf als wesentlich beurteilte inhärente Risiken ~~situativ~~ zu bestimmen ~~und umzusetzen~~.
[Rz 24]	Die vorliegende Definition ist sehr offen formuliert und lässt der FINMA – das Proportionalitätsprinzip vorbehalten – einen grossen Handlungsspielraum, im Rahmen der laufenden Aufsicht für spezifische Themen weitergehende Anforderungen an das Management der operationellen Risiken vorzusehen. Es bedarf unbedingt einer sachlichen, auf klar ausgewiesene Fälle eingrenzenden Definition, bei welcher es um Zusatzmassnahmen zur Steuerung einer für das betroffene Institut einschneidenden Risikolage geht. Andernfalls bestünde gestützt auf diese Rz 7 ein «Freipass», um nach Gutdünken im Einzelfall weitere Massnahmen anzuordnen. Im Ergebnis würden dadurch Aufwand und Kosten der Institute zusätzlich erhöht.
	Formulierungsvorschlag Falls zur Steuerung einer für das Institut einschneidenden Risikolage 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.

[Rz 25]	Die Pflicht, operationelle Risiken einheitlich zu **kategorisieren** und in einem «**Inventar»** aufzuführen, lässt Fragen offen bezüglich der Anforderungen aus der einheitlichen Kategorisierung sowie der konsistenten Anwendung in allen Bereichen des Instituts sowie Komponenten des OpRisk-Managements. Unklar bleibt, ob diese Kategorisierung bspw. eindeutig sein muss oder Risiken auch mehreren Kategorien zugeteilt werden dürfen (bspw. «ICT» und «Sourcing»). Zudem ist unklar, ob die Erwartung besteht, dass die Rapportierung entlang dieser Kategorisierung verläuft.
[Rz 28]	Die Umsetzung des Erfordernisses der **Unabhängigkeit** für die Beurteilung der Effektivität der Schlüsselkontrollen sollte präzisiert werden. So stellt sich die Frage, welche Kontrollinstanz ausreichend ist: Reicht ein Teamkollege in der «First Line of Defense», dessen Vorgesetzter oder würde eine separate Unit (oder gar die «Second Line of Defense») benötigt?
[Rz 31]	Die geforderte Überwachung der Risikotoleranz für operationelle Risiken im Bereich der inhärenten Risiken scheint insbesondere im Bereich der Cyber-Risiken sehr schwer umsetzbar zu sein. Wir empfehlen die Prüfung alternativer Ansätze, welche bspw. auf Strategien zum Umgang mit entsprechenden Risken abstellen.
[Rz 32] **Fussnote 6**	Die Anforderungen an die Risikokontrolle sehen auch eine Berichterstattung der wesentlichen Prüfergebnisse an das Oberleitungsorgan vor (nach **Fussnote 6**). Es kann jedoch nicht sein, dass die Risikokontrollfunktion über Audit Berichte, über Berichte der FINMA oder der externen Revision berichtet. Die entsprechenden Stellen (Audit, externer Review, FINMA) berichten separat. Die Risikokontrollfunktion kann keine Meta-Berichterstattung erstellen, zumal diese z.T. selbst Gegenstand der Berichte dieser drei Kontrollfunktionen ist. Aus diesen Gründen ist der letzte Teilsatz zu streichen. Zudem findet die Vorgabe einer Berichterstattung der wesentlichen Prüfergebnisse an das Oberleitungsorgan (Rz 32, Fussnote 6) keine Grundlage im «Rundschreiben 2017/1 Corporate Governance – Banken» (vgl. Rz 69 ff.).
	Formulierungsvorschlag 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.~~

	Grundsatz 2: Management der IKT-Risiken
[Rz 37]	Das im Rundschreiben festgelegte Erfordernis, «neue technologische Entwicklungen» bei der **Erstellung** des Managements zu berücksichtigen, kann missverständlich sein. Es kann dazu führen, dass das rechtsanwendende Institut sich gezwungen sieht, bspw. für die Überwachung bei der Erstellung des Managements die neusten technologischen Mittel anzuwenden. Es ist zu vermeiden, einen nicht technologieneutralen Grundsatz in das Rundschreiben aufzunehmen. Aus diesen Gründen bitten wir Sie darum, den nachfolgenden Formulierungsvorschlag zu berücksichtigen.
	Formulierungsvorschlag Beim Management ~~Bei der Erstellung des Managements~~ der IKT-Risiken sind relevante international anerkannte Standards und Best Practices ~~aber auch~~, sowie soweit möglich auch ~~neue~~ technologische Entwicklungen zu berücksichtigen.
[Rz 43]	Die gewählte Formulierung scheint etwas pauschal zu sein. Aus unserer Sicht sollte eine Einschränkung bezüglich Risikoorientierung eingebaut werden.
	Formulierungsvorschlag Es ist eine Trennung zwischen den kritischen[1] IKT-Systemen ~~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. 1 Kritisch hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit.
[Rz 47]	Im Rundschreiben wird neu der Ausdruck **«Schutzbedürfnis»** verwendet, im Unterschied zu vorherigen Versionen des Entwurfes. Dabei ist nicht klar, wie sich dieser Begriff von der Risikotoleranz (Rz 35) abgrenzt. Zudem stellt sich die Frage, ob die «Schutzmassnahmen» (vgl. Rz 55), welche wohl im Einklang mit dem hier referenzieren Schutzbedürfnis stehen, eine Definition kennen.

	Grundsatz 3: Management der Cyber-Risiken
[Rz 55] **Fussnote 8**	Die **Fussnote 8** sollte präzisiert werden, da nicht klar ist, wie «Angriffe aus dem internen Netzwerk» zu interpretieren sind. Wir werten diese als Teil eines Angriffs von extern, durch Überwinden des Perimeters, Eindringen und Ausnutzen des internen Netzwerks (klare Abgrenzung zu reinen Insider-Delikten, die internen Deliktrisiken zuzuordnen wären).

[Rz 58]	Bei «Cyber-Security» wird eher von Bedrohungen und Angriffspfaden (Cyber Kill Chain) gesprochen als von Szenarien. Ist es notwendig, dass ähnlich den BCM-Szenarien auch «**Cyber-Szenarien»** (z.B. Angriffsmuster) aufgezeigt werden? Die Krisensimulationen basieren bei Cyber-Vorfällen auf «Playbooks», «Security Incident Response» Plänen resp. Reaktionsplänen. Die Definition ist dahingehend zu schärfen bzw. präzisieren, dass klarer hervorgeht, ob und wie die Szenarien dargestellt werden müssen. Weiter wurde folgender Kritikpunkt aus der Vorkonsultation bisher nicht umgesetzt: Der Nebensatz «oder die darüber hinaus über das Internet erreichbar sind», ist missverständlich, da nicht klar ist, ob sämtliche vom Internet erreichbaren IT-Systeme gemeint sind oder nur solche, welche gleichzeitig für kritische Prozesse notwendig sind. Insbesondere in ersterem Fall wäre zu argumentieren, dass auch genutzte Services wie Twitter (die möglicherweise im Inventar als genutzte Applikationen hinterlegt sind) solchen Prüfungen unterzogen werden müssten, obwohl es geltenden Gesetzen, mindestens aber den Twitter-AGB, widersprechen könnte, diese mit Penetration-Testing-Tools zu traktieren. Letztlich ist unseres Erachtens die Formulierung zu spezifisch; so müssen Übungen nicht immer IT-Systeme umfassen. Wir schlagen darum vor, diese Randziffer wie folgt umzuformulieren.
	Formulierungsvorschlag Die Geschäftsleitung lässt regelmässig Verwundbarkeitsanalysen[9], Penetrationstests und auf Basis der institutsspezifischen Bedrohungspotenziale 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.~~ Cyber-Übungen müssen schwerwiegende und plausible Szenarien umfassen, die sich materiell auf kritische Systeme, Prozesse oder Daten auswirken.

	Grundsatz 4: Management der Risiken kritischer Daten
[Rz 59]	Der bisherige Fokus auf die Vertraulichkeit im Rahmen von Kundenidentifikationsdaten wird nun auch auf die Dimensionen der Integrität und Verfügbarkeit kritischer Daten allgemein erweitert. Kritische Daten in Bezug auf Integrität und Verfügbarkeit werden dadurch definiert, dass diese für das Funktionieren des Instituts notwendig bzw. «missionskritisch» sind und mit einem IT-Prozess verknüpft sind (BCP-Prozess oder Cybersicherheitsprozess). Die Verfügbarkeit und Integrität der Daten (Kontostand, Kreditbetrag) können demnach abhängig davon zu sein, ob sich diese Daten in einem kritischen Bereich der Bank (bspw. Kernbankensystem) oder nur in einem Ad-hoc-Kontrollsystem befinden. Demnach bestehen Daten, welche nur für einen Moment ihres Lebenszyklus als kritisch einzustufen sind. Dennoch

	sollten nach Rz 62 f. die erhöhten Anforderungen über die ganze Lebensdauer der Daten angewendet werden, was keinen Sinn macht. Wir beantragen eine klare und eingrenzende Definition. Es wird nicht klar, was die FINMA unter einer «vollständigen Datenstrategie» versteht. Da die derzeitige Formulierung einen grossen Interpretationsraum zulässt, sollte das Wort «vollständig» gestrichen werden.
	Formulierungsvorschlag 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.
[Rz 60]	Aus unserer Sicht sollte die unabhängige Kontrollfunktion nicht selbst dafür verantwortlich sein, die genannten Rahmenbedingungen zu schaffen und aufrecht zu erhalten. Das sollte ein Fachbereich in der «Second Line of Defense» sein, welcher auch die unabhängige Überwachung garantiert. Die «First Line of Defense» führt das operationelle Risikomanagement. Das Rundschreiben sollte zumindest die Option offenlassen, diese Zuständigkeits-Trennung vornehmen zu können. Zudem wäre es hilfreich, wenn im Rundschreiben eine Präzisierung erfolgen würde, um die Vorgabe klarer zu definieren: Muss die unabhängige Einheit einer der zwei Kontrollfunktionen gemäss RS 17/01 (Risk und Compliance) angehören?
[Rz 61]	Generell führen die vermeintlichen «Detailänderungen», bei denen einzelne, aber etablierte, Worte wie «CID», «Massen CID» oder «Kundendaten» durch andere bzw. grössere Mengen von Assets ersetzt wurden (z.B. in Rz 61, in der Datenverantwortliche nun für kritische Daten gemäss Vertraulichkeits- oder Kritikalitätsstufe definiert werden, während bisher gemäss RS 08/21 ein Datenverantwortlicher für «Kundendaten» nötig war) zu grossen Aufwänden in der Umsetzung. Diese Änderungen stellen einen grösseren Paradigmenwechsel dar, als man auf den ersten Blick vermuten würde und sorgen in unseren Augen für mehr Ungenauigkeit, da sie zwar ein potenziell grösseres Set an Daten erfassen, aber eine etwaige Einstufung den Instituten überlässt. Wir beantragen eine klare und eingrenzende Definition.
[Rz 64]	Es wird gegenüber der Version der Ämterkonsultation ein neuer Begriff («Echtdaten») eingeführt. Wir regen an, diesen Begriff im Rundschreiben abschliessend zu definieren oder alternativ von «kritischen Daten in Testumgebungen» zu sprechen. Eine Präzisierung oder Weiterentwicklung des letzten Satzes wäre empfehlenswert.

[Rz 66]	Die FINMA schreibt das Zugriffsmodell «Role Based Access Control» (RBAC) vor, das nicht unbedingt immer das optimale Modell für die Zugriffsverwaltung ist. Die FINMA sollte das «Need-to-know»- und «Least Privileges»-Prinzip vorschreiben und den Finanzinstituten aber Spielraum lassen, das für ihr Geschäftsmodell oder die Organisation am besten geeignete Zugriffsmodell (RBAC, «Discretionary Access Control» (DAC) usw.) zu implementieren.
[Rz 67]	Das Erfordernis, erhöhte Risiken angemessen zu begrenzen und die Daten besonders zu schützen, falls kritische Daten ausserhalb der Schweiz gespeichert werden, ist unseres Erachtens nicht ins Rundschreiben aufzunehmen. Zum einen ergeben sich die entsprechenden Pflichten für erhöhte Risiken bereits aus Rz 59 und Rz 63 des Rundschreibens und zum anderen kann auf das FINMA Rundschreiben «Outsourcing» verwiesen werden.
[Rz 68] **Fussnote 15**	Im Rundschreiben wird das Erfordernis aufgestellt, dass «eine Liste dieser Personen zu führen und laufend zu aktualisieren» ist. Dabei ist uns nicht klar, ob sich diese Liste nur auf Personen mit erhöhten Privilegien bezieht oder auf alle Personen, die auf kritische Daten zugreifen können. Im gleichen Zusammenhang stellt sich die Frage, wie das qualifizierende Element für Personen mit erhöhten Privilegien, Anwender mit funktionalem Zugriff auf eine grosse Menge an kritischen Daten zu sein, zu interpretieren ist.

	Grundsatz 5: Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft
[Rz 73]	Nach Ablauf der einschlägigen Übergangsfristen werden sowohl Banken als auch unabhängige Vermögensverwalter (UVV) jeweils als vollumfänglich lizenzierte und beaufsichtigte Finanzinstitute operieren (im Fall der Depotbanken durch die FINMA bzw. im Fall der UVV durch Aufsichtsorganisationen «AO» und die FINMA). Die Depotbanken fordern nach der aktuellen Praxis im Grundsatz und primär aus Risikoüberlegungen bei Aufnahme der Geschäftsbeziehungen bestimmte Informationen von den UVV ein (und verlangen in bestimmten Fällen eine Aktualisierung dieser Informationen). Die Depotbanken sehen grundsätzlich jeweils nur einen Teil der Aktivitäten der UVV. Infolgedessen haben die Depotbanken in gewissen Bereichen keine Möglichkeit, die Vollständigkeit und Plausibilität der gelieferten Informationen zu überprüfen. Vor diesem Hintergrund sind die Depotbanken darauf angewiesen, Informationen zu erhalten, welche Prüfungen die neuen Aufsichtsorganisationen bezüglich der Einhaltung der sich aus FIDLEG/FINIG ergebenden regulatorischen Verpflichtungen der UVV vornehmen werden. Diese Angaben werden in die künftige Ausgestaltung der Bewirtschaftung der Risiken aus den Geschäftsbeziehungen mit UVV einfliessen. Es wird erwartet, dass eine Abgrenzung der Verantwortlichkeiten der Depotbanken gegenüber denjenigen der UVV und ihren eigenen Aufsichtsorganisation und der FINMA gemacht wird. Diesbezüglich ist bekanntlich ein Austausch mit der FINMA bereits aufgegleist worden.

	Grundsatz 6: Business Continuity Management (BCM)
[Rz 79 f. / Rz 83 / 86]	Im Zusammenhang mit BCM bestehen seit Jahren stehende Begrifflichkeiten, die nach Möglichkeit einheitlich verwendet werden sollten. Aus diesem Grund sollen überall, wo Tests erwähnt werden, auch Übungen figurieren. Dies, da viele Überprüfungen nicht in Form von Tests stattfinden können, sondern nur als (bspw. Table-Top) Übungen möglich sind. Das Rundschreiben macht eine klare Unterscheidung zwischen BCM und operationeller Resilienz – warum wird dann hier vom BCM verlangt, dass schwerwiegende, aber plausible Szenarien getestet werden müssen? Nach unserem Verständnis sind diese Szenarien ein wichtiges Abgrenzungsmerkmal vom BCM zu operationeller Resilienz. Im Abschnitt zur Resilienz werden Tests ebenfalls verlangt. Die Anforderung, schwerwiegende, aber plausible Szenarien zu testen, sollte dort erfolgen, nicht aber hier für das BCM.
[Rz 80]	Das Rundschreiben beschreibt die Anforderung eines **«Disaster Recovery Plans»** (DRP). Für grössere Finanzinstitute ist es jedoch oft praktikabler, mehrere DRPs zu erstellen; dies sollte im Wortlaut entsprechend berücksichtigt werden.
[Rz 84]	Eine Testfrequenz im Jahresrhythmus scheint sehr hoch bemessen und führt zu grossen Umsetzungs-, wie auch Überprüfungsaufwendungen. Es wäre zudem sinnvoll, wenn das Erfordernis aus Rz 87, welches «eine regelmässige Berichterstattung an das Oberleitungsorgan und die Geschäftsleitung» vorsieht, mit der Testfrequenz abgestimmt wird. Generell wird empfohlen, hier ein grösseres Ermessen zu Gunsten der Institute vorzusehen.
	Formulierungsvorschlag Variante A Die gemäss BCP und DRP wichtigsten Massnahmen und die Krisenorganisation werden regelmässig getestet.» Variante B Die gemäss BCP und DRP wichtigsten Massnahmen und die Krisenorganisation werden mindestens einmal jährlich überprüft resp. getestet. *(gemäss Wording in BCM-Empfehlungen SBVg 2013)*

	Grundsatz 7: Operationelle Resilienz
[Rz 93]	Eine «Business Impact Analyse» (BIA) beinhaltet auch die Identifikation von Ereignissen, welche solche Pläne auslösen können. Aus unserer Sicht sollte die Abgrenzung von Operationeller Resilienz zum BCM noch weiter konkretisiert werden (vgl. Rz 16).

[Rz 94]	Es wird verlangt, ein **Inventar** der **kritischen Funktionen** zu führen, das die Unterbrechungstoleranzen der kritischen Funktionen beinhaltet sowie die Verbindungen und Abhängigkeiten zwischen den benötigten kritischen Prozessen und deren Ressourcen. Aus dem Rundschreiben geht nicht klar hervor, wie das ebenfalls neue Erfordernis der Inventarisierung kritischer Daten nach Rz 45 davon abzugrenzen ist. Es wäre wünschenswert, wenn das Verständnis des Inventars im obigen Sinne präzisiert werden könnte (entweder in einer Fussnote oder im separaten Erläuterungspapier).
[Rz 97]	Tritt ein schwerwiegendes und länger anhaltendes Szenario ein (z.B. eine Pandemie oder Strommangellage), liegt es nicht bei jedem Szenario in der Macht des einzelnen Finanzinstitutes, dieses aus eigener Kraft zu bewältigen. Es müssten ─ je nach Szenario ─ übergeordnete, branchen-, bzw. schweizweite Katastrophen-Pläne ausgelöst werden. So ist es bei einer Strommangellage für ein einzelnes Bankinstitut nicht möglich, die Services während der vierten Phase einer Strommangellage-Situation (periodische Netzabschaltungen) aus eigener Kraft zu erbringen. Es bestehen dabei sehr hohe Abhängigkeiten, u.a. von Bund, Stromanbietern, Telekommunikation und Detailhändlern (Offline-Funktion POS). Die Bewältigung eines solchen Szenarios, unter den dort vorgeschlagenen Vorgaben, ist nur mit Vorarbeit und Garantien von Seiten des Staates möglich. Hierzu zählen wir insbesondere die Analyse und den Erhalt bestimmter Internetverbindungen oder eine Sicherstellung der gesamthaften Funktion des Internets innerhalb der Schweiz, den Einsatz von staatlichen Sicherheitskräften sowie eine den Anforderungen angemessene Risikoabfederung. Dementsprechend erscheint eine verpflichtende Vorbereitung und damit einhergehende Übung solcher Szenarien derzeit als nicht zielführend. Das im Rundschreiben verankerte Erfordernis, längere Unterbrechungen (bspw. über Monate hinweg), die sich durch einen Ausfall grundlegender Ressourcen auszeichnen, zu testen, sehen wir als problematisch an. Solch aufwändige Tests bzw. Übungen (bspw. für eine Strommangellage) sind nicht praktikabel und nicht zielführend. Es sind niederschwelligere Sensibilisierungsmassnahmen zu wählen. So können bspw. Notfalldokumente, Checklisten, Arbeitsanleitungen und weitere vorbereitende Massnahmen (z.B. Blackout-Tests in Rechenzentren) erstellt, Aufgaben, Kompetenzen und Verantwortlichkeiten definiert und der Krisenstab entsprechend informiert, sensibilisiert und geschult werden (auch z.B. Walkthroughs). Vorliegend kann eine Abstimmung der Testfrequenz sinnvoll sein (vgl. dazu Rz 84 vorstehend).

5. Anmerkungen zu den Übergangsbestimmungen

	Betreffend den Grundsatz 7 «Operationelle Resilienz»
[Rz 100]	Im revidierten Rundschreiben werden einige Parameter der Vorgaben deutlich verändert, welche auch ausserhalb dieses Grundsatzes massive Veränderungen in der Steuerung der Risiken bedingen. Wir sehen deshalb die Abwesenheit einer spezifischen Übergangsfrist für die Umsetzung hier kritisch. Wir würden eine explizite Übergangsfrist für die Risiko-Steuerung im Interesse einer seriösen und strukturierten Angleichung an das revidierte Rundschreiben begrüssen, da Qualität und Nachhaltigkeit der Umsetzung sicherlich profitieren würden. Neben den kleineren Instituten können auch grössere Institute in Zeitnot für eine umsichtige Umsetzung geraten (insbesondere da auch Abhängigkeiten von Partnern bestehen). Aus diesem Grund sollten die Übergangsbestimmungen jeweils und zu allen Grundsätzen um mindestens ein Jahr verlängert werden. Zudem sollte eine explizite Übergangsfrist für die Risiko-Steuerung eingeführt werden.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen für die weiteren Arbeiten. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung.

Freundliche Grüsse
Schweizerische Bankiervereinigung

Oliver Buschan
Mitglied der Geschäftsleitung
Leiter Retail Banking & Capital Markets

Dr. Markus Staub
Mitglied der Direktion
Leiter Retail Banking und Prudenzielle Regulierung