Swiss Financial Market Supervisory Authority
FINMA
Anne Feidt
Laupenstrasse 27
CH-3003 Bern

Via e-mail: anne.feidt@finma.ch

8 July 2022

AMAZON WEB SERVICES (AWS) RESPONSE TO FINMA'S NEW DRAFT CIRCULAR "OPERATIONAL RISKS AND RESILIENCE – BANKS"

Dear Madame/Sir,

Amazon Web Services ("AWS") welcomes the opportunity to offer comments on FINMA's Circular 22/ "Operational Risks and Resilience - Banks". Our response provides views from the perspective of a Cloud Service Provider ("CSP") and reflects our experiences providing cloud services to a Swiss and global customer base and adhering to the highest international resiliency and security standards, including compliance within existing financial services regulations, certifications and accreditations, such as the FINMA ISAE 3000 Type 2 Report.

AWS provides highly reliable, secure, scalable, and low-cost cloud infrastructure that powers a wide range of businesses and public sector entities around the world. In particular, AWS financial services customers vary in size from fintech startups to global systemically important banks (or G-SIBs) and operate in every industry segment including asset management, banking, capital markets, and insurance. The AWS cloud enables these customers to innovate faster, improve their security posture and operational resilience, while minimizing the environmental impacts of running cloud workloads[1]. Our infrastructure technologies encompass compute, storage, databases, and networking, and we also offer technology services such as machine learning.

We welcome the FINMA's efforts to implement the globally agreed Basel Committee on Banking Supervision (BCBS) principles for sound management of operational risk and operational resilience. Given the global nature of both finance and technology, regulatory coordination across jurisdictions is critical in order to secure a harmonized set of requirements that facilitates financial institutions' adoption of technology in a way that enhances operational resilience. AWS is committed to supporting international

[1] The sustainability pillar of the AWS Well-Architected Framework provides recommendations and strategies to use when designing cloud architectures with sustainability in mind. By adopting the practices in this paper, customers can build architectures that maximize efficiency and reduce waste.

regulatory discussions in support of the establishment of a consistent and fair regulatory framework for the use of cloud services by the financial services sector globally.

In addition, given the rapid level of technological innovation, we welcome FINMA's principles-based approach and believe any regulatory initiatives should remain flexible enough to handle increasingly dynamic complexities in the financial and technology spaces. Further, we believe regulatory and supervisory practices should consider the evolving technology landscape, for example by requesting financial institutions to periodically reassess their technology risk and security methods in consideration of both emerging risks as well as technological advances that can improve the effectiveness by which these risks are mitigated.

In the Annex, you will find comments on specific sections of the consultation that echo the points previously made in our response to the BCBS's Consultation on the Principles for Operational Resilience.

We would appreciate the opportunity to discuss the comments included in the submission.

Kind regards,

Maria E. Tsani
Head of Financial Services Public Policy & Regulatory Affairs – EMEA
AWS

tsanim@amazon.com

Annex: Comments on Proposed Principles

i) Principle 2: Management of ICT risks

We welcome's FINMA's proposal related to the use of "*relevant internationally recognized standards and best practices…as well as new technological developments*" when managing ICT risks. Indeed, modern technology such as cloud services can be used to overcome traditional challenges associated with ICT risks and technology failure. Financial institutions can leverage globally distributed infrastructure to build redundancy in all components of the ecosystem and modernize, standardize and automate antiquated, manual disaster recovery processes. Further, the AWS cloud enables financial firms of all sizes to adopt state-of-the-art security services and capabilities such as fine-grained control of identity and access management, cryptography, managed Distributed Denial of Service (DDoS) protection, and threat detection. The robustness of AWS' cloud services and infrastructure, together with our security, services and tools help customers to ensure continuity of their services, which is a key prerequisite for resilience and, more widely, financial stability.

Financial institutions also get access to AWS' third party certifications proving their compliance with international security standards. AWS operates thousands of controls that meet the highest standards of operational resilience in the industry. To understand these controls and how we operate them, FIs can access security standards and compliance certifications issued by third parties. For example, our System and Organization Control (SOC) 2 Type II report, reflecting examination by our independent third-party auditor, provides an overview of the AWS Resiliency Program. In addition, AWS aligns with the ISO 27001, the ISO 27017 guidance on information security in the cloud and ISO 27018 code of practice on protection of personal data in the cloud and other standards.

We fully appreciate the importance of business continuity and disaster recovery in the context of operational resilience. As demonstrated by our response to the COVID-19 pandemic, by proactively preparing for potential disruptions, we have been able to scale servers and network capacity in order to respond to additional load resulting from changing work patterns, while protecting our customers from short-term supply disruptions. By doing this, our financial services customers, and also our non-financial services customers, are able to scale up when needed. Our Business Continuity Policy lays out the guidelines used to implement procedures to respond to a serious incident or degradation of AWS services, including the recovery model and its implications on the business continuity plan. This is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. AWS' comprehensive approach to business continuity planning is designed to mitigate risks to people, facilities, equipment, and technology. These efforts are intended to protect the safety and well-being of our employees and maintain continuity of our business operations.

Additionally, although the likelihood of such incidents is very low, AWS is prepared to manage large-scale events that affect our infrastructure and services. AWS becomes aware of incidents or degradations in service based on continuous monitoring through metrics and alarms, high-severity tickets, customer reports, and the 24x7x365 service and technical support hotlines. The AWS core infrastructure also provides financial institutions with the ability to monitor their resources 24/7 to help ensure the confidentiality, integrity, and availability of their customer data.

At the financial institution level, to most effectively manage operational risks (including technology risk), AWS encourages financial institutions to establish an enterprise-wide, holistic understanding of their

business activities in order of priority (e.g., mission critical, business critical, operational) along with the associated people, processes, and technologies that enable FIs to meet their desired business outcomes. This comprehensive approach enables FIs to effectively manage and mitigate risk utilizing key performance indicators and key risk indicators to appropriately escalate, as necessary. This also aligns with an Enterprise Risk Management (ERM) approach, which evaluates Operational Risk Management (ORM) risks together with all other risk areas that may impede or impair a financial institution from achieving its business objectives (e.g., governance, financial, human resources, reputational, operational, technology).

ii) Principle 3: Cyber risk management

AWS concurs with FINMA on the importance of cyber security and supports the FINMA's guidance on resilient ICT. In that regard, AWS maintains a very high bar for security. It is applicable to all our customers, who trust us to operate over 200 fully featured services for compute, storage, databases, networking, analytics, robotics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development and deployment. In the financial services sector, as part of our continuous engagement with finance ministries, central banks, and regulators, we continue to discuss how AWS's services are designed and built to allow all of our customers to operate and innovate securely. We would welcome to opportunity to present our security framework in further detail to FINMA.

When our customers use AWS services, they are operating in an environment of shared responsibility. In the context of security, shared responsibility means that the secure functioning of an application on AWS requires action on the part of both customers and AWS. In this model, customers are responsible for their security "in" the cloud. They control and manage the security of their content, applications, systems, and networks. AWS manages security "of" the cloud to protect our infrastructure and services, maintain our operational performance, and meet relevant legal and regulatory requirements. We design and manage AWS's global infrastructure according to security best practices, as well as a variety of compliance standards.

AWS has implemented a continuous security improvement model where we constantly examine the environment for threats, and make adjustments to our security protocols in an ongoing manner. We encourage financial institutions and their customers to explore the ways in which AWS provides assurance about the security of our environment. To understand our security controls and how we operate them, customers can access our third-party audit reports; financial services customers regularly review our System and Organization Controls (SOC) 2 Type II report prepared by our independent, third-party auditor.

Further, AWS has also satisfactorily completed the FINMA ISAE 3000 Type 2 Report. The International Standard on Assurance Engagements (ISAE) 3000 is a standard which is applied for audits of internal controls, sustainability, and compliance with laws and regulations. Completion of the ISAE 3000 Type 2 Report verifies that AWS's control environment is appropriately designed and implemented to align with FINMA requirements applicable to regulated financial services customers under Circulars 2018/03, 2008/21, 2008/21, 2013/03 and the Business Continuity Management (BCM) minimum standards proposed by the Swiss Insurance Association (01.06.2015) and Swiss Bankers Association (29.08.2013).

Clientis
Ihre Bank

Anhörung zur Revision des Rundschreibens zu operationellen Risiken bei Banken
(Daniel Heiniger/Nando Gasser, 25.05.2022)

Ziffer II. Begriffe

Wir empfehlen am Anfang des Dokuments nur jene Begriffe zu definieren, welche im Rundschreiben häufig verwendet werden. Fachbegriffe, welche nur in einem einzigen Kapitel zur Anwendung kommen, sollten im entsprechenden Kapitel definiert werden. Dies erleichtert die Übersicht im betreffenden Thema.

Ziffer III. Proportionalitätsprinzip

Für die Anwendung des Proportionalitätsprinzips braucht es nicht nur eine Unterscheidung zu den Kategorie 4 und 5 Banken, sondern auch entsprechende Erleichterungen für Kategorie 3 Banken. Wir empfehlen für Kategorie 3 Banken explizit zu definieren, welche Randziffern nicht zur Anwendung gebracht werden müssen, sofern die Komplexität und die Risiken dies zulassen.

Generell eignet sich das Regelwerk für grosse und komplexe Banken mit hohen Risiken für die Finanzmarktstabilität. Wir Regionalbanken wünschen uns daher eine differenziertere Regelung in den einzelnen Themengebieten.

Deshalb empfehlen wir, die einzelnen Themenbereiche so aufzubauen, dass zu Beginn jene Aspekte aufgeführt sind, welche alle Banken einhalten müssen. Die danach folgenden Abschnitte kommen nur dann zur Anwendung, wenn die Komplexität und das Risiko dies rechtfertigen. Auf diese Weise könnte auch die Dichte der Vorgaben variiert werden. Während die ersten Abschnitte nur grundlegende Aspekte enthalten und offen formuliert sind, enthalten die folgenden Abschnitte mit zunehmendem Risiko und zunehmender Komplexität eine immer höher werdende Regelungsdichte. Beispiel: Kleine Banken mit wenig Komplexität und tiefen Risiken setzen nur die ersten Abschnitte um. Je grösser die Bank, die Komplexität und das Risiko werden, desto mehr Abschnitte müssen umgesetzt werden.

IV. Grundsätze

Die Organisation des Dokuments in verschiedene Grundsätze erscheint uns nicht zweckmässig. Letztlich werden einzelne Fachgebiete und nicht Grundsätze geregelt. Wir empfehlen, auf die Bezeichnung «Grundsätze» zu verzichten und mit aussagekräftigen Kapitelüberschriften zu arbeiten.

B. Grundsatz 2: Management der IKT-Risiken

Dieses Kapitel ist bezüglich Governance und Prozesse zu detailliert geregelt. Ein derartiger Eingriff in die Organisation der Banken rechtfertigt sich nur bei hoher Komplexität und hohen Risiken für die Finanzmarktstabilität. Wir empfehlen hier mit Prinzipen zu arbeiten und nicht detaillierte Vorgaben zur Konzeption und zu Prozessen zu machen. Siehe hierzu auch die Empfehlung im Abschnitt «Ziffer III. Proportionalitätsprinzip».

C. Grundsatz 3: Management der Cyber-Risiken

Wir empfehlen dieses Kapitel mit dem Kapitel B. Grundsatz 2: Management der IKT-Risiken zu verschmelzen und Überschneidungen zu beseitigen. Das Management der IKT-Risiken und jenes der Cyber-Risiken lassen sich in der Praxis kaum trennen, weil die Cyber-Risiken einen wesentlichen Bestandteil der IKT bilden. Auf

diese Weise werden Redundanzen u.a. bezüglich Awareness von Mitarbeitenden, Regelung Meldungen von Cyber-Angriffen usw. vermieden.

D. Grundsatz 4: Management der Risiken kritischer Daten

Dieses Kapitel soll bezüglich Begrifflichkeiten und Regelungsgehalt konsequent auf die neue Datenschutzgesetzgebung ausgerichtet werden. Wenn immer möglich soll die FINMA keine Regelungen erlassen, sondern auf das revDSG verweisen. Dies gilt insbesondere für die dortigen Vorgaben bezüglich Datensicherheit (vgl. revDSG Art. 8 und E-VDSG Art. 8 f.). Damit soll vermieden werden, dass sich Banken an mehreren regulatorischen Vorgaben orientieren müssen, die nicht deckungsgleich sind.

G. Grundsatz 7: Operationelle Resilienz

Wir empfehlen dieses Kapitel mit dem Kapitel F. Grundsatz 6: Business Continuity Management (BCM) zu verschmelzen und Überschneidungen zu beseitigen. Beides lässt sich in der Praxis nur schwer trennen.

Ebenfalls kann das Kapitel H Grundsatz 8: Weiterführung von kritischen Dienstleistungen (...) ebenfalls ins Kapitel F. integriert werden.

Dieses Kapitel ist bezüglich Governance und Prozesse zu detailliert geregelt. Ein derartiger Eingriff in die Organisation der Banken rechtfertigt sich nur bei hoher Komplexität und hohen Risiken für die Finanzmarktstabilität. Wir empfehlen hier mit Prinzipen zu arbeiten und nicht detaillierte Vorgaben zur Konzeption und zu Prozessen zu machen. Siehe hierzu auch die Empfehlung im Abschnitt «Ziffer III. Proportionalitätsprinzip».

F. Grundsatz 6: Business Continuity Management (BCM)

Dieses Kapitel ist bezüglich Governance und Prozesse zu detailliert geregelt. Ein derartiger Eingriff in die Organisation der Banken rechtfertigt sich nur bei hoher Komplexität und hohen Risiken für die Finanzmarktstabilität. Wir empfehlen hier mit Prinzipen zu arbeiten und nicht detaillierte Vorgaben zur Konzeption und zu Prozessen zu machen. Siehe hierzu auch die Empfehlung im Abschnitt «Ziffer III. Proportionalitätsprinzip».

Dieses Fachthema soll bezüglich Begrifflichkeiten und Regelungsgehalt konsequent dem FINMA-RS Outsourcing angeglichen werden. Wenn immer möglich, soll die FINMA hier keine zusätzlichen Regelungen erlassen, sondern auf das erwähnte Rundschreiben verweisen. Dies gilt insbesondere für die Randziffer 80 (Auslagerung von Infrastruktur).

Das Kapitel 6 soll der Tatsache Rechnung tragen, dass Banken der Kategorien 3 bis 5 heute die überwiegende Mehrheit ihrer Infrastrukturen und damit einhergehend zahlreiche kritische Prozesse an externe Dienstleister ausgelagert haben.

V. Übergangsbestimmungen

Für das gesamte Rundschreiben empfehlen wir eine Übergangsfrist von zwei Jahren. Regionalbanken sind auf eine genügend lange Frist angewiesen, um eine korrekte Umsetzung zu gewährleisten. Dies ist unserer Ansicht nach vertretbar, weil Banken die heute geltenden Rundschreiben einhalten.

Anhang 1

Die Grafiken sind unklar und daher wenig aussagekräftig. Wir schlagen vor, allfällige regulatorische Vorgaben in den entsprechenden Kapiteln zu platzieren und auf die Grafiken zu verzichten.

Credit Suisse Group AG
Paradeplatz 8
P.O. Box
8070 Zurich

By email
Swiss Financial Market Supervisory Authority
FINMA
Anne Feidt
Laupenstrasse 27
CH- 3003 Bern

Credit Suisse Group AG
Nancy Licul
Non-Financial Risk
Group Chief Risk Officer

Stefan Vogt
Cyber & Technology Risk
Group Chief Risk Officer

June 30, 2022

Invitation to comment: Draft Circular "Operational risks and resilience – banks"

Dear Ms. Feidt,

We take note of the full revision of FINMA Circular 2008/21 "Operational risks – banks" and welcome and thank for the opportunity to provide comments to the Draft Circular "Operational risks and resilience – banks".

Credit Suisse is involved in drafting the Swiss Bankers' Association's (SBA) comment letter for the industry, which FINMA receives from SBA directly.

In addition to SBA's industry-wide perspective, we would like to draw your attention to points, which are relevant from our point of view. Specifically, the further definition and clarification of terms would reduce potential different interpretations by banks, and the consequential development and roll out of diverse approaches towards compliance with the Circular.

You will find detailed feedback in the next pages.

We look forward to our continued dialogue on the subject and remain at your disposal for further information as required.

Yours sincerely,

Credit Suisse Group AG

Sig. Nancy Licul
Non-Financial Risk
Group Chief Risk Officer

Sig. Stefan Vogt
Cyber & Technology Risk
Group Chief Risk Officer

Detailed Feedback:
FINMA Draft Circular "Operational risks and resilience – banks"

Kapitel II. Begriffe (Terms)	
Rz 7	"die "besonders" ... geschützt werden müssen" ("….that requires "particular" protection…"): "besonders" ("particular") is unclear. We suggest instead the use of the term "angemessen" ("appropriate"). According to the principle of proportionality, a measure should be suitable, necessary and proportionate in the narrow sense ("appropriate") and with regard to the achievement of the objective. The choice of the term "angemessen" ("appropriate") instead of "besonders" ("particular") would be consistent with the explanatory report, refer page 17: "Kritische Daten in Bezug auf Integrität und Verfügbarkeit sind vom Institut risikobasiert zu definieren" ("Critical data with regard to integrity and availability must be defined by the institution on a risk basis"). "Personendaten" ("Personal data"): we suggest FINMA specifies the term according to the applicable Federal Act on Data Protection (currently Art. 3 lit. a Federal Act on Data Protection of June 19, 1992 - Status as of March 1, 2019). "Geschäftsgeheimnisse" ("Trade secrets"): we suggest that FINMA specifies the term according to the applicable Swiss Criminal Code (currently Art. 162 Swiss Criminal Code of December 21, 1937 – Status as of January 1, 2022).
Rz 13	We propose FINMA aligns the definition of "Krisensituationen" ("crisis situation") with the more detailed definition in "SBA's Recommendations for Business Continuity Management", to avoid different interpretations, specifically from vendors.
Rz 14	Where FINMA states "kritische Funktionen" ("critical functions"), CS understands this definition to align to the existing FINMA definition within the recovery and resolution planning expectations i.e. "services and functions that are indispensable to the operation of the Swiss economy and cannot be re-placed at short notice ….. those services whose immediate discontinuation without transitional arrangements would cause serious damage to the overall financial system". We advise FINMA to clarify expectations and understanding.

IV. Grundsätze (Principles)	
Grundsatz 1: Generelle Anforderungen an das Management der operationellen Risiken (General requirements for the management of operational risks)	
Rz 28	We advise FINMA to specify the meaning of the term "unabhängige Beurteilung" ("independent appraisal") in relation to control assessments, e.g. is independent appraisal covered through an independent Audit Function.
Rz 31	Regarding the monitoring of the risk tolerance through risk and control indicators it should be noted that the inherent exposure can only be measured through risk indicators, and not through risk and control indicators.

Grundsatz 4: Management der Risiken kritischer Daten (Management of critical data risks)	
Rz 60	We assume that the setup and the positioning of the independent unit as a control function is at banks' discretion. Please indicate if FINMA has a different understanding.
Rz 61	We propose FINMA clearly defines the term "critical data" in line with Rz 7 as moving away from terms like "Kundenidentifikationsdaten" "Client Identification Data (CID)" or "Kundendaten" ("client data") is a paradigm shift.
Rz 64	We suggest FINMA uses the term "angemessen" ("appropriate") protected", instead of "protected". Refer Rz 7.
Rz 66	We advise FINMA to refer to principles to be applied (e.g., need-to-know or least privileges), instead of defining systems banks should have "ein rollen- und funktionsspezifisches Autorisierungssystem" ("a role-specific and function specific authorization system").
Rz 67	We recommend FINMA specifies the term "erhöhte Risiken" ("heightened risks"). We suggest FINMA uses the term "angemessen" ("appropriate") protection", instead of "particular protection". Refer Rz 7 and Rz 64.
Rz 69	We suggest FINMA specifies the term "wesentlich" ("significantly").

Grundsatz 5: Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft (Management of the risks arising from the cross-border services business)	
Rz 72	We suggest FINMA uses the term "angemessen" ("appropriate") analysis, instead of "vertieft" ("in-depth") analysis. Refer Rz 7, Rz 64 and Rz 67.

Grundsatz 7: Operationelle Resilienz (Operational Resilience)	
Rz 95	Where FINMA states "die operationellen Risiken und die Schlüsselkontrollen" ("operational risks and key controls"), is this in relation to all operational risks and key controls or specific for the risks in relation to Operational Resilience and the controls which ensure continuity of service provision? We advise FINMA to clarify scope and expectations.

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.

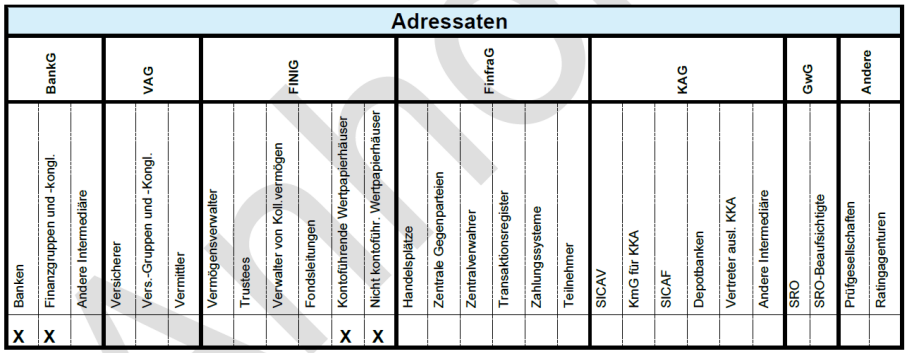
Für allfällige Rückfragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

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.

Adressaten

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

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.

Switzerland

Institute of Internal Auditing Switzerland
Vulkanstrasse 120
CH-8048 Zürich
+41 44 298 34 34
info@iias.ch
www.iias.ch

Autorité fédérale de surveillance des marchés financiers FINMA
Madame Anne Feidt
Laupenstrasse 27
CH-3003 Bern

Zurich, le 7 juillet 2022

Révision totale de la Circulaire FINMA 2008/21 "Risques opérationnels – banques"

Chère Madame Feidt,
Mesdames et Messieurs,

Nous nous référons à l'audition publiée le 10 mai dernier, et nous transmettons par la présente les commentaires de notre association, formulés sur la base de la lecture du texte aux yeux de ceux qui jouent le rôle de troisième ligne de défense.

L'IIA Suisse se félicite de la nouvelle version du document, qui s'aligne sur les développements internationaux, souligne et élargit le concept de données critiques et introduit la question de la résilience opérationnelle.

	II. Définitions
Cm 7	L'approche proportionnée et respectueuse de la réglementation proposée mérite d'être saluée. Pour autant, à des fins notamment «d'auditabilité» et de surveillance transverse des assujettis, la définition des données critiques devrait être précisée par le Régulateur, ou mieux explicitée. Nous suggérons de développer la définition telle que proposée en l'état au sein du projet.
Cm 8	L'approche proportionnée et respectueuse de la réglementation proposée mérite d'être saluée. A ce chiffre marginal également, à des fins notamment «d'auditabilité» et de surveillance transverse des assujettis, la définition des processus critiques devrait être précisée par le Régulateur, ou mieux explicitée. Nous suggérons de développer la définition telle que proposée en l'état au sein du projet.

Cm 9	L'importance de la Business Impact Analysis dans le contexte plus général du Business Continuity Management mérite qu'elle soit définie. Nous suggérons d'ajouter la définition de la «BIA».
	IV. Principes **Principe 1: exigences générales en matière de gestion des risques opérationnels**
Cm 28	Control testing: nous interprétons l'exigence d'un «examen régulier indépendant de l'efficacité des contrôles clés (*design effectiveness* et *operating effectiveness testing*)» comme une tâche de la 2ème ligne de défense, étant donné la nature «périodique» et «systématique» notamment relevée dans le Rapport explicatif (page 12/33). Ce dernier précise pourtant que cette activité peut être exécutée par «une unité organisationnelle indépendante telle que le contrôle des risques ou la révision interne». Afin d'éviter tout biais conceptuel (circ. FINMA 2017/01 Gouvernance d'entreprise – banques), nous suggérons de supprimer la référence à la révision interne, laissant à cette fonction de 3ème ligne de défense l'autonomie de définir, au travers de son appréciation périodique desdits risques, l'exécution ponctuelle de tels contrôles dans la fixation puis la réalisation indépendante de son plan d'audit, voire en coordination des efforts avec la 2ème ligne de défense.
	Principe 3: gestion des cyberrisques
Cm 53 à 55	L'organe préposé à la haute direction et à la surveillance est ignoré dans le projet et n'apparaît pas en charge de la responsabilité ultime dans ce domaine majeur de risques, alors qu'il l'est fort à propos en ce qui concerne la gestion des risques TIC, le BCM de même que pour la résilience opérationnelle. Nous relevons de surcroît qu'il ne l'est pas expressément pour les données critiques, ni pour les risques liés aux activités transfrontières, ce qui devrait être corrigé par souci de clarté. Nous suggérons de mieux intégrer les rôles et responsabilités de l'Organe préposé à la haute direction en ce qui concerne les cyberrisques, les données critiques et les activités transfrontières.

	Principe 4: gestion des données critiques
Cm 60	Du point de vue de la gouvernance, la disposition fait du sens et souligne la nécessité de disposer d'un «Chief Data Officer» (ou fonction similaire) au titre de 2ème ligne de défense. Pour autant, bien que la FINMA mentionne dans son Rapport explicatif ne pas vouloir entrer dans les détails des séparations de fonction entre 1ère et 2ème ligne, cette unité indépendante à titre de fonction de contrôle devrait être explicitée par souci de clarté au sein des Définitions, clarifiant ainsi la distinction entre instances de niveau 1, de niveau 2 respectivement de niveau 3. Nous suggérons de compléter les Définitions et d'étendre cette exigence aux autres risques technologiques.
Cm 70	Third party risk management: au chapitre 2 (page 7-8/33) du Rapport explicatif, la FINMA relève à juste titre que «[...] les chaînes d'approvisionnement ont en général gagné en complexité, impliquant de nouvelles problématiques». En matière de gestion du risque des parties tierces, respectivement des prestataires/fournisseurs tiers, seul ce cm 70 aborde timidement cette thématique-clé; quant à elle, la circ. FINMA 2018/03 demeure bien en-deçà de réglementations comparables, en abordant par ailleurs que les seuls outsourcers soumis à la circulaire FINMA 2018/03 «outsourcings essentiels», notion de surcroît abstraite dont la définition est à «géométrie variable» au sein des assujettis. La responsabilité des Organes (comprenant le SCI et la gestion et le contrôle des risques [notamment opérationnels] des activités déléguées) en ce qui concerne les activités déléguées (essentielles ou non essentielles) reste ainsi le «Parent pauvre» de ce projet de circulaire, et aurait mérité par cohérence que le présent projet intègre plus globalement la thématique de la gestion des risques des parties tierces ou, à tout le moins, entraîne une refonte majeure de la circ. FINMA 2018/03. Si tant est que cela soit faisable, nous suggérons de procéder, de concert à ce projet ou dans un proche avenir, à la refonte de la circulaire FINMA 2018/03 afin de mieux intégrer la gestion de la gestion/contrôle du risque des parties tierces.

	Principe 5: gestion des risques liés aux activités de service transfrontières
Cm 71 à 74	Tel que relevé ci-avant pour le Principe 3, l'Organe préposé à la haute direction et la surveillance ne figure pas comme ultime garant du respect du droit étranger applicable. L'analyse initiale des risques, sa revue périodique, la fixation du périmètre géographique d'activités, les reportings périodiques de la Direction au Conseil d'administration, notamment, mériteraient de trouver place dans cette réglementation sur les principes. Nous suggérons de compléter le projet de circulaire.
	Principe 6: Business Continuity Management (BCM)
Cm 75, 84 et 87	L'Organe responsable de la haute direction approuve à intervalles réguliers la stratégie BCM et surveille son respect [...]. Les principales mesures au sens du BCP et du DRP ainsi que l'organisation de crise sont testées au moins une fois par année. Des comptes rendus réguliers informent l'Organe responsable de la haute direction [...]. Nous suggérons de définir aussi la fréquence minimale des activités prévues au Cm 75 et 87.
	Principe 7: résilience opérationnelle
Cm 97	La capacité à exécuter des fonctions critiques dans les limites de leur tolérance aux interruptions en cas de scenarii graves mais plausibles est régulièrement testée. A l'image des cm 75, 84 et 87 ci-avant, et par souci de cohérence et d'alignement, nous suggérons que la périodicité minimale requise soit précisée.
	V. Dispositions transitoires
Cm 100	La cascade de 1-2-3 ans fait du sens et nous apparaît comme pragmatique. Par contre, nous suggérons l'ajout d'un délai transitoire de 1 an, voire de 2 ans, pour «définir, identifier, formaliser et mettre en place» le dispositif, nouveau, du Principe 4, soit la gestion des données critiques.

	Adaptation de la circ. FINMA 2013/03 «Activités d'audit»
Cm 97.1 Annexe 2	La proposition d'une approche graduelle sur 4 ans avec une étendue d'audit laissée à la libre appréciation de la société d'audit n'est pas optimale, et n'est pas cohérente du point de vue du risque avec les thèmes associés que sont i. le BCM et ii. les cyberrisques. Nous suggérons de ramener l'approche TIC sur celle applicable pour les autres domaines.

Nous vous remercions de nous avoir donné l'occasion de formuler nos observations et, restant à votre disposition pour toute information complémentaire, nous vous adressons nos plus cordiales salutations.

Gabrielle Rudolf von Rohr
Présidente du Comité

Gabriele Guglielmini
Membre du Comité

Revision of Circular 2008/21 "Operational risks – banks"

NCC Group's response to FINMA's consultation, July 2022

Introduction

NCC Group is delighted to offer its observations in response to FINMA's consultation.

We fully support FINMA's objectives to update its circular on operational risks to reflect the changing risk landscape, and bring it in line with the Basel Committee on Banking Supervision's revised principles for operational resilience. **The evolving risks facing financial services** – including those associated with the shift to remote working, cyber security risk, increased reliance on IT systems, new and emerging technologies, and the increasing use of third parties – **requires sound risk management and improved business continuity**. To this end, we believe that FINMA could strengthen and future-proof its guidance by **adopting more explicitly a 'Resilience by Design'** approach, providing financial institutions with additional guidance on the practical steps they can take to implement the required sound risk management of third-party technologies and services.

About NCC Group

With **over 30 years' experience protecting business critical software, data and information through escrow, secure verification testing, and cloud hosted software continuity services**, NCC Group has followed regulatory developments regarding supply chain risks and third-party arrangements closely, not least to ensure that we, too, are able to meet our customers' evolving demands as regulatory requirements change. We work with customers operating across financial services who understand how cyber security and software resilience can add value and represent a competitive advantage both in their own business as well as across their portfolios. We hold a unique position where we see compliance from the end-user's perspective as well as from the viewpoint of the IT provider, and try to assist both in achieving their aims.

NCC Group is a global cyber security business headquartered in the UK, but, through its $220m acquisition of Iron Mountain's Intellectual Property Management division (IPM), has an **established and significant footprint in North America, alongside our existing presence in Europe, the Middle East and Asia Pacific**. This means we are able to take an international perspective to regulatory approaches to cyber security and third-party risk management. The IPM business has been operating in the North America regulatory market for over 30 years. We believe strongly in the potential of appropriate regulatory measures to unleash the innovative ingenuity of adjacent services sectors to develop practical solutions that allow organisations to meet regulatory requirements in the most effective way.

Embedding a 'Resilience by Design' approach

We are passionate in our advocacy for a greater regulatory-driven focus on the adoption of cloud, software and technology escrow solutions as the baseline implementation of what we're calling 'Resilience by Design', to meet the financial sector's increased demand for third-party risk management, business continuity and operational resilience.

The feasibility of exhaustively identifying supplier risk is questionable. A supplier's overall risk profile is generally the result of a combination of a multitude of factors. Identifying all possible scenarios is

likely disproportionate to its potential benefits, and risks increasing costs, creating barriers to innovation, and subsequently reducing access to financial services.

For that reason, no less, we do believe that cloud, software and technology escrow solutions can offer legal, technical and proportional assurance to financial institutions in dealing with their third-party suppliers, particularly where they embrace the concept of 'Resilience by Design'. This would **assume supplier failure / compromise by default, regardless of their risk profile, and encourage or mandate using cloud, software and technology escrow agreements, as a proportionate and cost-effective solution for regulated entities to mitigate against this**, by offering a minimum level of resilience through the legal and technical means to ensure continuity of services while a service is being restored and/or alternative options are being implemented. In this sense, escrow agreements and verification services act as a technical insurance policy and business continuity strategy, safeguarding the long-term availability of business-critical technologies and applications while protecting intellectual property.

Establishing cloud, software and technology escrow agreements with supporting verification services will create a baseline to:

- Grant organisations access to the source code and the right to access the cloud environment where it is hosted, where: an application is material to the organisation's operational continuity, if the service is deployed in the cloud; or if the application presents a concentration risk. For example, the role of escrow agreements is reflected in CISA's guidance on ransomware[1] which states that, in being prepared for a ransomware incident, organisations should ensure the availability of source code through backups or escrow agreements. The details of any access rights and conditions will be set out in individual agreements, offering a legal basis with full transparency for all involved parties over when any such rights can be invoked.

- Specify how the agreement and access rights are to be used in the event of supplier compromise / failure. This goes beyond cyber risk, taking a broader view which includes non-technical risks such as bankruptcy / liquidation / insolvency, failure to maintain / inability to fix the service, transfer of ownership of intellectual property rights to the software, or the supplier company as a whole, unless the new owners agree to keep in place the agreement. Principally, financial entities rely on failed services continuing to operate while full recovery plans are being implemented. That means that continuity and exit planning needs to take account of implementation, testing and training times that impact on the ability to exchange or replace products and services expediently, safely and compliantly.

- Advance capabilities to automate risk tolerance at the application programable interface (API) gateways level to permit control to gracefully failsafe services or providers who may go out of compliance, removing exposure latency in a real-time digital economy.

Many financial services firms already use escrow solutions as part of their comprehensive business continuity planning when mitigating supplier risk, and some third-party service providers themselves have opted to build these solutions into their offer to support their customers' compliance with regulatory requirements.

By way of example, NCC Group has worked with banking technology provider Mambu on developing a cloud escrow solution. Built within Amazon Web Services (AWS) infrastructure, Mambu's cloud hosted digital banking software-as-a-service (SaaS) solutions supports more than 6000 loan and deposit products serving over 14 million end customers worldwide. Working with NCC Group,

[1] Ransomware Guide | CISA

Mambu adopted a cloud escrow solution to establish a robust approach to its customers' regulatory compliance, offering business continuity assurance by ensuring that financial institutions deploying Mambu's solution would have access to their application and specific cloud environment as well as support for the ongoing maintenance and management of their application.

However, we believe that there is still insufficiently widespread awareness of the benefits of software and technology escrow solutions, and the role they can play in addressing regulatory requirements on outsourcing and third-party risk management. To address this lack of awareness, **we believe that there is a role for FINMA – working with other regulators globally – to do more to promote and educate financial firms on the benefits of cloud, software and technology escrow solutions** as a practical means, and a baseline Resilience by Design solution, to meet outsourcing and risk management requirements - be that through explicitly encouraging the mandating of escrow solutions or by encouraging much greater inclusion of it in implementation guidance. This would align with approaches taken by other regulators, particularly those in the financial services sector[2].

Additional Resilience by Design elements could include:

- **Ensuring the development and regular testing requirements of business continuity and exit plans forms part of licensing or contractual agreements** between regulated entities and their third-party suppliers, particularly through the release lifecycle of critical applications.

- **Broadening business continuity and stressed exit plan requirements** so that:

    - Cloud providers should advise their software vendors initiate stressed exit plans where the latter provide services to critical financial service providers.

    - Software contained within other solutions, as well as the internal infrastructure of third parties supplying software and technology solutions, should also be subject to stressed exit plans.

In addition, **we advocate for greater information sharing to improve shared and contextualised understanding of concentration and cyber risk** through elements including:

- Anonymous outsourcing arrangement audits to gain early insights and intelligence on emerging dependencies and criticalities.

- Firms' assessments of non-material outsourcing arrangements from the outset so as to be able to track trends over time, for example, where non-material services are supplied by a single provider to a large number of financial organisations.

- Failed business continuity and stressed exit plans, particularly where these plans relate to larger suppliers.

Conclusion

NCC Group very much welcomes the opportunity to contribute to FINMA's consultation. We have positively contributed to other regulatory authorities' consideration of cyber security, operational

[2] For example, the Prudential Regulatory Authority (PRA) in the UK which considers escrow solutions as one of a number of relevant resiliency options for firms to consider when undertaking business continuity and exit planning: SS2/21 'Outsourcing and third party risk management' (bankofengland.co.uk).

resilience and third-party risk management and would welcome the opportunity to engage in more proactive dialogue with FINMA to support its objectives. NCC Group is able to offer interactive dialogue with its IT technical experts, solutions architects and qualified legal advisers each of which have years of experience in navigating the mitigation of risks for clients.

RAIFFEISEN

Raiffeisen Schweiz

Raiffeisenplatz 4
Postfach
9001 St. Gallen
Telefon 071 225 49 98
www.raiffeisen.ch
finma-office@raiffeisen.ch

via E-Mail
Eidgenössische Finanzmarktaufsicht FINMA
Anne Feidt
Laupenstrasse 27
3003 Bern
anne.feidt@finma.ch

Für Sie zuständig:
Gabriela Glaus, RA – 071 225 49 98

St. Gallen, 11. Juli 2022

Totalrevision FINMA-Rundschreiben «Operationelle Risiken und Resilienz - Banken» und «Prüfwesen»

Sehr geehrte Frau Feidt

Wir beziehen uns auf die Publikation der Anhörung vom 10. Mai 2022 in der rubrizierten Angelegenheit und danken Ihnen für die Möglichkeit, uns dazu zu äussern. Gerne nehmen wir zu den geplanten Änderungen wie folgt Stellung:

I. FINMA-Rundschreiben «Operationelle Risiken und Resilienz - Banken»

a. Generelle Vorbemerkungen: Definitionen, Abgrenzungen, Klärung von Schnittstellen

Einleitend möchten wir folgende allgemeine Anregungen zur Optimierung des Rundschreibens einbringen, da sich auch in den bestehenden Rundschreiben dazu keine weitergehenden Ausführungen befinden:

- Die Definition der operationellen Risiken wie auch der Rechts- und Compliance-Risiken sowie der strategischen Risiken und der Reputationsrisiken ist unseres Erachtens zu schärfen sowie eine gegenseitige Abgrenzung untereinander vorzunehmen.
- Zudem fehlt auch die Definition der Tax-Risiken. Wir empfehlen, diese Lücke zu schliessen.
- Die Ausführungen zu den grenzüberschreitenden Dienstleistungen in Rz. 71 ff. zeigen exemplarisch, dass die Definitionen und Abgrenzungen unvollständig sind. Diese Ausführungen wirken an der jetzigen Stelle wie ein Fremdkörper und sollten richtig eingebettet werden. Innerhalb dieser Spezialbestimmungen sind zudem weitere Ausführungen betreffend die Abgrenzung und das Zusammenspiel nötig.
- Ferner wäre es hilfreich, wenn die geschärften Definitionen der operationellen, Rechts- und Compliance-, strategischer und Reputationsrisiken mit einer exemplarischen Aufzählung von (weiteren) Beispielen ausgebaut würden.
- Als Nebenbemerkung erlauben wir uns den Hinweis, dass auch die Definition der Compliance-Funktion sowie der Risikokontrolle, deren Aufgaben und Verantwortlichkeiten sowie deren Abgrenzungen untereinander (vgl. dazu Finma RS 2017/1 Rz. 69 ff.) im vorliegenden Rundschreiben unklar bleiben. Die Schnittstellen und Abgrenzungen dieser beiden Funktionen sollten unseres Erachtens ebenfalls geklärt werden.

Für Finanzinstitute sind diese Optimierungen von erheblicher Bedeutung, um die Vorgaben korrekt umsetzen zu können. Im jetzigen Entwurf wird nur punktuell auf die einzelnen Risiken eingegangen.

Detaillierung der Definitionen der operationellen Risiken sowie weiterer Risiken / Abgrenzungen und beispielhafte Aufzählung sämtlicher Risiken: Im Erläuterungsbericht wird unter Ziff. 4.1.1 ausgeführt, dass das neue Rundschreiben nicht den Anspruch hat, jede Art von operationellen Risiken umfassend und im Detail zu behandeln. Im Rundschreiben wird unter Rz. 3 (lediglich) erwähnt, dass Rechtsrisiken bei den operationellen Risiken eingeschlossen sind. Speziell in Bezug auf die Rechtsrisiken wird darauf hingewiesen, dass das geltende Recht in jedem Fall zu identifizieren und einzuhalten sei, bspw. in Bezug auf das Risiko der Geldwäscherei oder den Datenschutz. Ergänzend gehören aber etwa nachteilige Änderungen der Gesetzeslage oder der Rechtsprechung (beispielsweise im Konsumenten-

schutz-, Steuer- oder Aufsichtsrecht), Folgen unklarer oder gar mangelhafter Gesetze oder Verordnungen sowie behördliche Fehlentscheidungen unseres Erachtens ebenfalls zu den Rechtsrisiken.

Zu den operationellen Rechtsrisiken gehören gemäss Erläuterungsbericht Ziff. 4.1.2 weiter 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.

In der Definition der operationellen Risiken nicht eingeschlossen sind sodann gemäss Rz. 3 des Rundschreibens die strategischen Risiken (z.B. das Risiko, dass das Anbieten eines neuen Produktes nicht zu den gewünschten und erwarteten Erträgen führt). Auch Reputationsrisiken sind ausgeschlossen, obwohl sie mit den operationellen Risiken eng verwandt sind und selten eine scharfe Trennung möglich ist. Dies wird im Erläuterungsbericht mit dem Beispiel eines Fehlverhaltens sowie dem Beispiel einer Cyber-Attacke unterlegt.

Hierzu sind nach unserem Dafürhalten weitere Präzisierungen notwendig. Wir erachten die Abgrenzung sämtlicher Begriffe in einem einzigen Rundschreiben (nicht teilweise verteilt auf mehrere) sowie entsprechende ergänzende Ausführungen für sinnvoll und notwendig, damit die Risiken durch Finanzinstitute korrekt erfasst und zugeordnet werden können. Das Zusammenspiel der einzelnen Risiken untereinander sollte geklärt werden, da es in der Praxis aus den beschriebenen Gründen immer wieder zu Interpretationsschwierigkeiten kommt. Dies vor dem Hintergrund, dass auch die Finanzinstitute über ein übergeordnetes, institutsweites Risiko-Framework verfügen müssen.

Die Definition der operationellen Risiken lehnt sich an Art. 89 der Eigenmittelverordnung (ERV) an.

Art. 89 ERV:
Mit operationellen Risiken wird die Gefahr von Verlusten bezeichnet, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen oder Systemen oder in Folge von externen Ereignissen eintreten. Eingeschlossen sind Rechtsrisiken, nicht aber strategische Risiken und Reputationsrisiken.

Diese Definition führt nicht näher aus, wie prozessual mit Fällen umzugehen ist, welche sowohl ein Rechts- oder Compliance-Risiko zum Inhalt haben, dessen Folgen aber auch ein wesentliches Reputationsrisiko darstellen. Sie sollte deshalb geschärft werden. Ist in diesen Fällen ein bloss teilweiser Ausschluss die Folge (in welcher Grössenordnung?) oder hat eine Einschätzung als blosse Reputationsrisiken, welche gänzlich ausgeschlossen sind, zu erfolgen? Ein klassisches Beispiel hierzu wäre etwa das Fehlverhalten eines Organes im privaten Umfeld.

Fehlende Definition der Compliance-Risiken: Im Finma RS 2017/1 wird in Rz. 7 lediglich festgehalten, dass als Compliance die Einhaltung von gesetzlichen, regulatorischen und internen Vorschriften sowie die Beachtung von marktüblichen Standards und Standesregeln gilt. Die Compliance-Risiken stellen zudem nach unserer Auffassung keine blosse Teilmenge der operationellen Risiken dar, weil diese teilweise keine quantifizierbaren Verluste, sondern wesentliche Reputationsrisiken als Folge haben. Dieser beschränkte Teilmengencharakter der Compliance-Risiken zeigt sich unseres Erachtens deutlich an der Trennung zwischen Risikokontrolle (operationelle Risiken) und Compliance-Funktion (Compliance-Risiken) gemäss FINMA-RS 2017/1 Rz. 69 ff., welche demnach zwei verschiedene Kontrollinstanzen sind (vgl. nachfolgende Ausführungen). Zudem werden Tax-Risiken an keiner Stelle angesprochen. Sie sollten nach unserem Dafürhalten zusätzlich beschrieben werden.

Ausführungen zu den grenzüberschreitenden Dienstleistungen: Die betreffenden Ausführungen werden im Entwurf unverändert aus dem bestehenden Rundschreiben 2008/21 Rz. 136.2 ff. übernommen. Da es sich hierbei um Compliance-Risiken handelt, sollten diese Ausführungen auch in die Beschreibung der Compliance-Risiken eingebettet werden. Im jetzigen Entwurf werden Risiken im grenzüberschreitenden Dienstleistungsverkehr inmitten der Grundsätze zu den Cyber-Risiken sowie den Business-Continuity-Grundsätzen präzisiert, was sachlich nicht korrekt erscheint und den fragmentarischen Eindruck des Rundschreibens unterlegt.

Exemplarische beispielhafte Aufzählung: Unseres Erachtens wäre es zudem sehr hilfreich, wenn diese Ausführungen mit einer beispielhaften Darlegung sämtlicher Risiken, d.h. von Rechts- und Compliance-Risiken, Tax-Risiken, übrigen operationellen Risiken sowie weiteren Beispielen von strategischen Risiken und Reputationsrisiken ausgebaut würden.

Nebenbemerkung: Abgrenzung der Aufgaben und Verantwortlichkeiten der Kontrollfunktionen sowie Klärung von Schnittstellen: Gemäss Rz. 20 des Rundschreibens gelten die Anforderungen an die organisatorischen Strukturen, die Risikopolitik und die Grundzüge des institutsweiten Risikomanagements nach FINMA-Rundschreiben 2017/1 „Corporate Governance – Banken" insbesondere auch für das Management der operationellen Risiken. Aus der Perspektive der Compliance bestehen jedoch Überschneidungen in Bezug auf Rechts-, Compliance- und Reputationsrisiken, welche geklärt werden sollten (vgl. auch Art. 12 Abs. 2 BankV). Gemäss Finma RS 2017/1 werden in Rz. 69 ff. die Aufgaben und Verantwortlichkeiten der Risikokontrolle beschrieben. Diese hat insbesondere die systematische Überwachung und Berichterstattung von einzelnen wie auch aggregierten Risikopositionen sicherzustellen. In Rz. 77 ff. wiederum werden die Aufgaben und Verantwortlichkeiten der Compliance-Funktion beschrieben, wozu die jährliche Einschätzung des Compliance-Risikos gehört.

Im aktuellen Entwurf des Rundschreibens werden die beiden Funktionen vermischt und nicht klar abgegrenzt. Bei den unter Rz. 71 ff. des Rundschreibens erwähnten Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft handelt es sich wie erwähnt beispielsweise um klassische Compliance-Risiken, deren Überwachung und Kontrolle regelmässig der Compliance-Funktion obliegt. Bezüglich der Handhabung von Compliance-Risiken erachten wir deshalb ebenfalls eine Klärung der Schnittstellen für sinnvoll. Konkret sollte definiert werden, welche Risiken in diesem Zusammenhang bei Finanzinstituten mit zwei unabhängigen Kontrollinstanzen durch die Risikokontrolle und welche durch die Compliance-Funktion zu überwachen sind.

b. Stellungnahme zu den einzelnen Bestimmungen

Ergänzend zu den einleitenden, generellen Vorbemerkungen nehmen wir nachfolgend zu den einzelnen Bestimmungen des FINMA-Rundschreibens «Operationelle Risiken und Resilienz - Banken» Stellung.

Rz. 7 – Definition «Kritische Daten»

Die Definition der kritischen Daten umfasst neben Daten, die ein Institut für eine erfolgreiche und nachhaltige Erbringung seiner Dienstleistungen als wesentlich erachtet, alle «Daten, die für regulatorische Zwecke aufbewahrt werden müssen». Letztere Bestimmung ist sehr weitgehend und umfasst regelmässig auch Daten, deren besonderer Schutzzweck nicht per se aufgrund der regulatorischen Relevanz ersichtlich ist. Das Prinzip der Wesentlichkeit respektive des besonderen Schutzes (z.B. Personendaten, Kundendaten oder Geschäftsgeheimnisse) sollte auch bei diesen Daten gegeben sein müssen, um als «kritische Daten» zu gelten. Derart «wesentliche, für regulatorische Zwecke aufzubewahrende Daten» sind grundsätzlich Teil einer «erfolgreichen und nachhaltigen Erbringung der Dienstleistungen», weshalb eine separate Auflistung unseres Erachtens nicht nötig erscheint.

Formulierungsvorschlag:
«Kritische Daten sind Daten, die ein Institut für eine erfolgreiche und nachhaltige Erbringung seiner Dienstleistungen oder für regulatorische Zwecke als wesentlich erachtet ~~oder Daten, die für regulatorische Zwecke aufbewahrt werden müssen~~.»

Rz. 37 – «Best Practices»

Im Rundschreiben ist mehrfach die Rede davon, dass «relevante international anerkannte Standards und Best Practices» einzuhalten sind (z.B. Rz. 37 und 55). Die Anforderung, «Best Practices» branchenweit für Kat. 1-3 Institute anzuwenden, erscheint dabei unklar und widersprüchlich. Zum einen dürfte kaum ein einheitliches Verständnis vorhanden sein, was «Best Practices» sind. Zum anderen ist es gerade das Wesensmerkmal von «Best Practices», dass diese nur von einem Teil aller Institute – nämlich den besten – umgesetzt werden. Folgerichtig redet der Erläuterungsbericht denn auch nur noch von «Good Practices» (S. 16, wobei er auf eben die gleiche Rz. 55 verweist, in welcher «Best Practices» vermerkt ist), was sinnvoller ist, da es sich bei «Good Practices» im allgemeinen Verständnis um einen «guten Branchenstandard» handelt, was für eine branchenweite Vorgabe als der sinnvollere Massstab erscheint. Zudem hat die FINMA immer die Möglichkeit, bei besonderen Risikoexpositionen einzelner Institute weitergehende Massnahmen im Sinne eines «Best Practice»-Ansatzes einzufordern.

Formulierungsvorschlag:
Rz. 37 und 55: Ersatz *«Best Practices»* durch *«Good Practices»*.

Rz. 24 – Weitergehende Anforderungen der FINMA

Rz. 24 gibt der FINMA weitgehende Kompetenzen, zusätzliche Anforderungen im Rahmen der laufenden Aufsicht zu stellen. Zwar mahnt das Rundschreiben die FINMA zu einer zurückhaltenden Anwendung; das im Erläuterungsbericht auf Seite 8 erwähnte Prinzip, dass das Rundschreiben ausschliesslich der Rechtsanwendung dient und keine rechtsetzenden Bestimmungen enthält, sollte auch in diesem Kontext explizit gelten.

Formulierungsvorschlag:
«Dies geschieht zurückhaltend, auf Basis bestehender gesetzlicher oder regulatorischer Anforderungen und unter Anwendung des Proportionalitätsprinzips.»

Rz. 27 – Prüfergebnisse vs. Risiko- und Kontrollbeurteilungen

Es ist unklar, was der Unterschied zwischen «Prüfergebnissen» sowie insbesondere «Kontrollbeurteilungen» sein soll. Prüfergebnisse sind im Regelfall nichts anderes als eine Kontrollbeurteilung, da es ja gerade das Ziel einer Prüfung ist, die Angemessenheit und Wirksamkeit einer Kontrolle zu beurteilen. Es ist zudem unklar, ob durch die Trennung impliziert wird, dass diese «Risiko- und Kontrollbeurteilungen» durch eine andere Einheit als die gemäss Fussnote 6 bezeichneten Kontrolleinheiten durchzuführen ist. Entsprechend schlagen wir vor, diese zwei Begriffe zusammenzufassen.

Formulierungsvorschlag: (ersetzt Rz. 27)
«Die Identifikation und Beurteilung der operationellen Risiken stützt sich auf regelmässig durchzuführende Risiko- und Kontrollbeurteilungen auf der Basis von Prüfergebnissen[6].»

Rz. 34 – Berichterstattungspflicht auf Stufe Geschäfts- oder Organisationsbereichen

Die regulatorischen Berichterstattungspflichten sollten auf Ebene Oberleitungsorgan und Geschäftsleitung gemäss Rz. 32/33 beschränkt bleiben und keine weitergehenden Berichterstattungspflichten auf Ebene einzelner Geschäfts- oder Organisationsbereiche festgelegt werden. Es sollte dem Institut überlassen bleiben, inwieweit es die Steuerung und Überwachung auf Ebene Geschäftsleitung wahrnimmt oder es an die untergeordneten Einheiten delegiert respektive aufteilt. Da die Verantwortlichkeiten korrekterweise auf Stufe Geschäftsleitung festgelegt werden (und dort auch die relevanten / wesentlichen operationellen Risiken enthalten sein müssen), sollte die regulatorisch geforderte Berichterstattung auch mit dieser Ebene kongruent sein und keine weitere Berichterstattungsebene regulatorisch gefordert werden.

Formulierungsvorschlag:
Streichung der Rz. 34.

Rz. 35ff. – Notwendige Vereinfachung bei weitgehenden Outsourcing-Verhältnissen

Zwar sind Outsourcing-Verhältnisse in einem separaten Rundschreiben geregelt und die FINMA verweist im Erläuterungsbericht explizit darauf, dass diese Vorgaben auch anwendbar sind (vgl. Ziff.4.1.3). Jedoch bleibt unklar, inwieweit bei einem weitgehenden Outsourcing der gesamten IKT-Prozesse an einen Drittdienstleister zusätzliche Vorgaben an die operative Überwachung und insbesondere die Berichterstattung zu beachten wären, welche sich aus Rz. 35 – 52 ergeben. Zahlreiche Anforderungen müssen in diesem Fall durch den Outsourcer sichergestellt werden und die auslagernde Bank müsste sich auf die generellen Pflichten zur Auswahl, Instruktion und Überwachung beschränken können. In diesem Sinne wäre eine klärende Bestimmung hilfreich, dass sich im Falle von Outsourcings der IKT-Prozesse die Pflichten der auslagernden Bank nach den Outsourcing-Vorgaben richten.

Dieselben Überlegungen sollten ebenfalls zum Management von Cyber-Risiken (Rz. 53ff.) berücksichtigt werden.

Formulierungsvorschlag: (zusätzlicher Absatz)

*«**e) Outsourcing***
Im Falle der Auslagerung wesentlicher Risiken bemessen sich die Pflichten des auslagernden Instituts gemäss Rz. 41-52 inklusive der notwendigen Berichterstattung gemäss Rz. 40 nach den Vorgaben des FINMA-RS 2018/3 Outsourcing.»

Rz. 58 – Umfang der Cyber-Übungen

Es ist unklar, worauf sich im zweiten Satz das Wort «diese» bezieht. Wenn es sich einzig auf Cyber-Übungen beziehen sollte, ist der Mindestumfang an IT-Systemen zu gross («die kritische Daten beinhalten», «die über das Internet erreichbar sind»). Dies sollte vielmehr ebenfalls risikobasiert und über einen definierten (Mehrjahres-)Rhythmus erfolgen.

Alternativer Formulierungsvorschlag:
«*mindestens*» streichen oder Absatz ersetzen durch *«[…] mit angemessenen Ressourcen und risikobasiert durchgeführt werden. Die Massnahmen sind so zu planen, dass über einen definierten Rhythmus alle IT-Systeme abgedeckt werden, welche für die Erbringung von kritischen Prozessen notwendig sind, beziehungsweise kritische Daten beinhalten.»*

II. FINMA-Rundschreiben 2013/3 «Prüfwesen»

Wir haben keine Bemerkungen zu den Folgeanpassungen am FINMA-Rundschreiben 2013/3 «Prüfwesen».

Für die Gelegenheit zur Stellungnahme bedanken wir uns noch einmal bestens. Wir bitten um Berücksichtigung der Anliegen von Raiffeisen und stehen Ihnen bei Fragen gerne zur Verfügung. Gerne sind wir auch bereit, Ihnen unsere Anliegen mündlich näher darzulegen.

Freundliche Grüsse

Raiffeisen Schweiz

Gabriela Glaus
FINMA-Office

Christian Bopp
Head Regulatory Affairs

Kopie an:
- EY via E-Mail (eych.raiffeisen.audit@ch.ey.com)

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

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association
Aeschenplatz 7
Postfach 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch

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.

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.ch

[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

	Grundsatz 1: Generelle Anforderungen an das Management der operationellen Risiken
[Rz 21]	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.~~

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association
Aeschenplatz 7
Postfach 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch

	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).

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.ch

[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 Regulierung

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.ch

Per E-Mail an anne.feidt@finma.ch

Eidgenössische Finanzmarktaufsicht
Frau Dr. Anne Feidt
Laupenstrasse 27
3003 Bern

SIX Group AG
Pfingstweidstrasse 110
CH-8005 Zürich

Postanschrift:
Postfach
CH-8021 Zürich

T +41 58 399 4260
www.six-group.com

Kontaktperson:
Bernhard Hurschler
bernhard.hurschler@six-group.com

Zürich, 8. Juli 2022

Stellungnahme zur Vernehmlassung betreffend Entwurf des neuen Rundschreibens „Operationelle Risiken und Resilienz – Banken“

Sehr geehrte Frau Dr. Feidt,
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die von der Eidgenössischen Finanzmarktaufsicht am 10. Mai 2022 eröffnete Vernehmlassung zum Entwurf des neuen Rundschreibens „Operationelle Risiken und Resilienz – Banken“ und bedanken uns für die Möglichkeit zur Konsultation in dieser für SIX als Betreiberin verschiedener Finanzmarktinfrastrukturen wesentlichen Angelegenheit. Gerne nehmen wir die Gelegenheit wahr und stellen Ihnen nachfolgend unsere Stellungnahme zu.

Generelle Bemerkungen

SIX begrüsst die inhaltlichen Anpassungen und Konkretisierungen der qualitativen Anforderungen des ehemaligen FINMA-Rundschreibens 2008/21, insbesondere dass das neue Rundschreiben „Operationelle Risiken und Resilienz – Banken“ technologieneutral und nach den Grundsätzen der Prinzipienbasierung und Proportionalität ausformuliert worden ist.

SIX hat sich aktiv an der Eingabe der Schweizer Bankiervereinigung (SBVg) vom 29. Juni 2022 beteiligt und befürwortet diese entsprechend. Darüber hinaus möchten wir vorliegend einige ergänzende Anmerkungen tätigen, welche mitunter unserer spezifischen Stellung als Finanzmarktinfrastruktur geschuldet sind, für welche das Rundschreiben bekanntlich nur teilweise und indirekt im Rahmen der konsolidierten Aufsicht Anwendung finden wird.

Eingabe im Rahmen der Ämterkonsultation

Seitens SIX hatten wir bereits die Gelegenheit, Anmerkungen im Rahmen der Ämterkonsultation anzubringen und verweisen auf unsere entsprechende Eingabe vom 15. März 2022. Mit Blick auf die

nun vorliegende Entwurfsfassung stellen wir fest, dass unsere bei dieser Gelegenheit eingereichten Kommentare und Fragestellungen nur marginale Berücksichtigung resp. Klärung erfahren haben. So bedürfen unseres Erachtens verschiedene Definitionen von Begrifflichkeiten einer weiteren Klärung, da sie teilweise zu einer mutmasslich ungewollten Ausweitung der damit verbundenen Pflichten führen. Die Verwendung des Begriffes "kritisch" etwa ist sehr weit gefasst. Wir ersuchen Sie entsprechend, unsere im Zuge der Ämterkonsultation getätigten Ausführungen gesamthaft nochmals in Betracht zu ziehen.

Ergänzende Kommentare

In der nachstehenden Übersicht findet sich eine die SBVg-Eingabe ergänzende Kommentierung einzelner Bestimmungen und Begriffe:

Randziffer	Bestimmung	Kommentar
54	"mindestens jährliche Berichterstattung an die Geschäftsleitung"	Sollte unseres Erachtens mindestens quartalsweise erfolgen
55	Bst. b. "insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen Daten und IT-Systeme"	Ergänzung um das Kriterium der Verbindlichkeit/Nichtabstreitbarkeit (sog. Non-repudiation)
55	Bst. c. "Zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken	Umkehrung: Erst nach erfolgter Aufzeichnung (sog. Logging) ist eine Erkennung möglich
65 und 67	"besonders zu schützen"	Allenfalls zu präzisieren, inwiefern diesbezüglich über den reinen Zugriff hinaus Anforderungen stipuliert werden sollen

***

Wir danken Ihnen für Ihre Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen im Zuge der anstehenden Arbeiten. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung.

Freundliche Grüsse

Bernhard Hurschler
Head Crisis, BCM & Physical Security

Simon Pabst
Senior Specialist Market Structure

Verband Schweizerischer Kantonalbanken
Wallstrasse 8
Postfach
CH-4002 Basel

Kantonalbanken
Banques Cantonales
Banche Cantonali

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

Per E-Mail an: anne.feidt@finma.ch

Datum 30. Juni 2022
Kontaktperson Michael Engeloch
Direktwahl 061 206 66 21
E-Mail m.engeloch@vskb.ch

Stellungnahme der Kantonalbanken zur Totalrevision des FINMA-Rundschreibens 2008/21 «Operationelle Risiken – Banken»

Sehr geehrte Frau Feidt
Sehr geehrte Damen und Herren

Am 10. Mai 2022 hat die Eidgenössische Finanzmarktaufsicht FINMA die Vernehmlassung über die Totalrevision des FINMA-Rundschreibens 2008/21 «Operationelle Risiken – Banken» eröffnet und die Kantonalbanken zu einer Stellungnahme eingeladen. Die Kantonalbanken danken Ihnen für diese Gelegenheit.

Die Kantonalbanken begrüssen das Regulierungsziel der Totalrevision des Rundschreibens zur Schaffung von mehr Transparenz und Klarheit über die qualitativen Anforderungen an das Management der operationellen Risiken. Zudem befürworten die Kantonalbanken, dass die Risiken nun umfassender definiert werden.

Die Anliegen der Kantonalbanken sind in die Stellungnahme der Schweizerischen Bankiervereinigung (SBVg) eingeflossen. Die Kantonalbanken können die Stellungnahme der SBVg daher unterstützen und sich den darin zum Ausdruck gebrachten Anliegen und Forderungen anschliessen.

Bei dieser Gelegenheit möchten die Kantonalbanken auf folgende Punkte hinweisen:

Grundsätzliches
Die Totalrevision des Rundschreibens wurde u.a. aufgrund der Finalisierung von Basel III nötig. Die Basler Standards richten sich allerdings nur an sehr grosse, internationale Banken. In der Schweiz gehören dazu höchstens die beiden Grossbanken. Dennoch sollen die internationalen Standards für alle Schweizer Banken umgesetzt werden. Hierzu fehlt aus

Sicht der Kantonalbanken die Legitimation. Entsprechend ist eine proportionale und prinzipienbasierte Umsetzung umso wichtiger.

Der vorliegende Entwurf wird diesen Anforderungen allerdings nicht genügend gerecht. So sind die Anforderungen teilweise regel- statt prinzipienbasiert und es fehlt eine angemessene Abstufung nach den fünf Aufsichtskategorien.

Weiter ist der Zeitplan zu ambitioniert. Die Publikation des revidierten Rundschreibens ist für Ende 2022 avisiert. Die Erwartung, dass ein Grossteil der Vorgaben bereits kurze Zeit später, am 1. Januar 2023, umgesetzt werden muss, erscheint wenig realistisch. Die Konzeption und Umsetzung der neuen Datenstrategie (kritische Daten) etwa, bedeutet einen grossen Eingriff in das bisherige Setup. Die Überführung der Anpassungen in das interne Regelwerk (Fachkonzepte, Reglemente und Weisungen) sowie deren Vernehmlassung in den entsprechenden Gremien benötigen deutlich mehr Zeit.

Zu einzelnen Randziffern bemerken die Kantonalbanken Folgendes:

Rz	Bemerkung
7	Die Definition von «kritischen Daten» ist derart weit gefasst, dass letztlich alle von einem Institut bearbeiteten Daten darunterfallen. Da «kritische Daten» allerdings die Ausnahme darstellen sollten, für welche eine erhöhte Schutzwürdigkeit besteht, macht eine derart weit gefasste Definition keinen Sinn. Verschiedene «kritische Daten» sind zudem bereits durch das Datenschutzgesetz, das Bankkundengeheimnis oder das Strafgesetzbuch umfassend geschützt und bedürfen somit keiner aufsichtsrechtlichen Zusatzregulierung. Die Bundesgesetze regeln den Schutz dieser Daten bereits abschliessend, weshalb der Aufsichtsbehörde eine weitergehende Regulierungskompetenz fehlt. 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. Formulierungsvorschlag: *Kritische Daten* sind Daten, die ein Institut für eine erfolgreiche und nachhaltige Erbringung seiner Dienstleistungen als derart wesentlich erachtet, um sie einem schärferen Schutz zu unterstellen, oder Daten, die für regulatorische Zwecke aufbewahrt werden müssen. Dies unter Würdigung von Grösse, Struktur, Geschäftsmodell und Risiken des Instituts. Daten können sowohl hinsichtlich der Vertraulichkeit als auch Integrität oder Verfügbarkeit kritisch sein. Daten, die hinsichtlich der Vertraulichkeit kritisch sind (vertrauliche Daten), sind ~~dabei~~ solche, die besonders vor unautorisierter Offenlegung geschützt werden müssen (bspw. Personendaten, Kundendaten, Geschäftsgeheimnisse).

8 Im Sinne der Konsistenz zu Rz 3 schlagen die Kantonalbanken folgende neue Formulierung vor:

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

13 Die derzeitige Formulierung berücksichtigt nur die Definition aus dem Glossar der SBVg-Empfehlungen für BCM, 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 weniger umfassend umgesetzt. Meist verfügen die Partner zwar über ein Störungsmanagement, es fehlt aber ein Plan für den Umgang mit Krisen. Die Banken benötigen deshalb eine Anpassung der Formulierung, um ihre Lieferanten zu einem Krisenmanagement verpflichten zu können.

Formulierungsvorschlag:

Krisensituationen sind ~~Situationen~~ weitreichende, potenziell existenzbedrohende Ereignisse, welche nicht mit ordentlichen Massnahmen und Entscheidungskompetenzen bewältigt werden können.

17 ff. Wie in der Einleitung bereits ausgeführt, ist die Abstufung nach Aufsichtskategorien aus Sicht der Kantonalbanken ungenügend. Insbesondere fehlen Erleichterungen für Banken der Kategorie 3. Im Sinne der Proportionalität sollten auch für diese Banken die Bestimmungen einzelner Randziffern ausgenommen werden. So könnten die Ausnahmen aus Rz 18 vollumfänglich auf Banken der Kategorie 3 angewendet werden. Die FINMA hätte gemäss Rz 18 immer noch die Möglichkeit, für einzelne Banken Verschärfungen auszusprechen.

Die Kantonalbanken bitten Sie, mindestens folgende Rz für Banken der Kategorie 3 auszunehmen:
31, 33, 34, 61, 68, 84, 85, 88, 90, 91 und 97.

Details zu den Randziffern 84 und 90 folgen unter den entsprechenden Ziffern.

24 Die Formulierung ist zu allgemein gewählt und muss entsprechend eingegrenzt werden, um weitere Massnahmen auf sachlich klar ausgewiesene Fälle zu beschränken.

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.

28 Bei der Rz 28 wird die Unabhängigkeit der verschiedenen Instanzen gefordert, ohne die «Unabhängigkeit» weiter auszuführen. Dabei ist unklar, ob eine zweite Person aus

dem gleichen Team ausreicht, oder ob zwingend eine Überprüfung durch die «Second Line» nötig ist. Die Kantonalbanken fordern eine entsprechende Erläuterung.

29 Der Begriff «Aktivitäten» ist nicht weiter spezifiziert und es ist nicht nachvollziehbar, was damit alles gemeint ist. Entsprechend fordern die Kantonalbanken eine abschliessende Definition dieses Begriffs.

30 Der Begriff «Risikogehalt» ist nicht definiert, weshalb die Kantonalbanken folgende neue Formulierung vorschlagen:

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

32 Der Teilsatz «…und wesentlichen Prüfergebnissen nach Fussnote 6.» führt zu einer Meta-Berichterstattung, bei welcher die Risikokontrollfunktion über Audit, FINMA-Prüfungen und externe Revisionen an das Oberleitungsorgan zu rapportieren hat. Dies ist nicht angemessen und führt zusammen mit den Vorgaben aus FINMA RS 2017/1 «Corporate Governance – Banken», wo festgehalten ist, dass das Oberleitungsorgan die verschiedenen Revisionsberichte zu würdigen hat, zu einer doppelten Berichterstattung. Entsprechend empfehlen die Kantonalbanken die ausnahmslose Streichung des erwähnten Teilsatzes.

37 Die Formulierung ist unklar:

- Sollen neue technologische Entwicklungen für den Aufbau des IKT-Managements als Hilfsmittel genutzt werden oder
- sollen neue technologische Entwicklungen gemanagt werden?

Erstes ist aus Sicht der Kantonalbanken nicht nachvollziehbar, da diese Entscheide bei einer prinzipienbasierten Umsetzung den Instituten zu überlassen ist, weshalb die Kantonalbanken für die zweite Möglichkeit folgende neue Formulierung vorschlagen:

> ~~Bei der Erstellung des Managements~~ Beim Management der IKT-Risiken sind relevante international anerkannte Standards, ~~und~~ Best Practices ~~zu berücksichtigen~~, aber auch ~~sowie neue~~ technologische Entwicklungen zu berücksichtigen.

43 Die Formulierung von Rz 43 ist zu pauschal und muss risikoorientierter verfasst werden.

Formulierungsvorschlag:

> Es ist eine Trennung zwischen den kritischen[1] IKT-Umgebungen für die Entwicklung und das Testen und denjenigen für die IKT-Produktion sicherzustellen. Dies umfasst auch eine eindeutige Zuweisung von Aufgaben, Funktionen und Verantwortlichkeiten und eine Regelung der damit einhergehenden Zugangsberechtigungen.
>
> [1]Kritisch hinsichtlich Verfügbarkeit oder Integrität.

47 Den Kantonalbanken ist unklar, wie sich der Begriff «Schutzbedürfnis» gegenüber dem Begriff «Risikotoleranz» aus Rz 35 abgrenzt. Hier wären eine entsprechende Definition und Abgrenzung wünschenswert.

55 Fussnote 8:
Die Formulierung ist unklar. Es könnte der Eindruck entstehen, dass auch Insiderdelikte betroffen sind.

Formulierungsvorschlag:

Angriffe auf kritische Aktiven von Extern via Internet oder vergleichbare Netzwerke oder durch Überwinden des physischen Perimeters, ~~aus dem internen Netzwerk dem Internet und vergleichbaren Netzen~~ auf die Vertraulichkeit, Integrität und Verfügbarkeit der IKT sowie kritischen Daten.

Weiter wird in der Aufzählung unter Rz 55, Punkt c, die «vollumfängliche Überwachung der IKT» gefordert. Dies widerspricht dem Proportionalitäts- und dem Risikoansatz und ist zudem nicht praktikabel umsetzbar.

Formulierungsvorschlag:

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

56 Die Banken müssen Cyber-Attacken der FINMA, dem NCSC (National Cyber Security Center) und dem FS-CSC (Financial Sector Cyber Security Center) melden. Weitere künftige Meldevorschriften sind nicht auszuschliessen. Die Kantonalbanken wünschen sich deshalb eine zentrale Bundesstelle zur Meldung von Cyber-Attacken. Diese Stelle wäre dann auch für die Weiterleitung an weitere Behördenstellen zuständig.

61 Für die Kantonalbanken ist unklar, was mit «Kritikalitätsstufe» gemeint ist und ob kritische Daten noch in Subkategorien eingeteilt werden müssen. Die Kantonalbanken wünschen sich hierzu eine klarere Definition mit eindeutigen Abgrenzungen.

64 Hier wird der nicht weiter definierte Begriff «Echtdaten» eingeführt. Im Sinne der Konsistenz der Begriffe empfehlen die Kantonalbanken, von «kritischen Daten in Testumgebungen» zu sprechen. Eine weitergehende Präzisierung scheint unnötig. Der Anspruch, die Vertraulichkeit in Testumgebungen zu schützen, besteht zurecht. Hingegen müssen Daten in Testumgebungen verändert werden können, um deren Auswirkungen zu testen. Der Schutz der Verfügbarkeit und der Integrität sollte sich folglich nicht auf die Entwicklung, Veränderung und Migration von Daten beziehen.

Formulierungsvorschlag:

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

84 Die Kantonalbanken fordern die Rz 84 für Banken der Kategorie 3 (siehe auch Rz 17 ff.) auszunehmen oder wenigstens die jährliche Prüfung durch eine periodische, risikobasierte Prüfung zu ersetzen.

89 Der Begriff «operationelle Resilienz» sollte klarer von den Begriffen «BCM», «ITSCM» und «IT-Security» abgegrenzt werden. Eine Übersicht über das Zusammenspiel und die Abhängigkeiten wäre wünschenswert.
Die «Identifikation kritischer Funktionen» ist bereits in Rz 76 geregelt. Die Kantonalbanken regen an, dass man diese beiden Punkte konsolidiert und die gleichen Begriffe verwendet.

90 Die Einholung der Genehmigung der kritischen Funktionen und der damit verbundenen Unterbrechungstoleranzen durch das Oberleitungsorgan ist «*jährlich*» vorgesehen. Die Genehmigung des Managements der operationellen Risiken (Rz. 22), der BCM-Strategie (Rz. 75) sowie der Sicherstellung der operationellen Resilienz (Rz. 89) haben hingegen «*regelmässig*» bzw. «*in regelmässigen Abständen*» zu erfolgen. Diese Formulierung ermöglicht eine risikobasierte Vorgehensweise und ist proportional ausgestaltet. Die Kantonalbanken sprechen sich deshalb für eine entsprechende Anpassung der Genehmigungsfrist betreffend die kritischen Funktionen und die damit verbundenen Unterbrechungstoleranzen aus.

Weiter fordern die Kantonalbanken, die Rz 90 für Banken der Kategorie 3 (siehe auch Rz 17 ff.) auszunehmen oder wenigstens die jährliche Prüfung durch eine periodische Prüfung oder eine Prüfung bei wesentlichen Veränderungen zu ersetzen.

Formulierungsvorschlag:

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

93 Eine «Business Impact Analyse» (BIA) beinhaltet auch die Identifikation von Ereignissen, welche eine BIA auslösen können. Aus Sicht der Kantonalbanken sollte die Abgrenzung von Operationeller Resilienz zum BCM noch weiter konkretisiert werden (siehe auch Rz 89).

100 Die Totalrevision des Rundschreibens führt zu grossen Veränderungen bei der Risikosteuerung, weshalb die Kantonalbanken hierfür eine explizite Übergangsfrist für die Umsetzung fordern. Zudem führen die unter Rz 100 aufgeführten Anforderungen zu tiefgreifenden Anpassungen. Zusätzlich bestehen Abhängigkeiten von externen Partnern. Aus diesen Gründen schlagen die Kantonalbanken eine Verlängerung der vorgesehenen Übergangfristen um jeweils mindestens ein Jahr vor. Zudem wäre eine Auflistung der von der jeweiligen Frist betroffenen Randziffern wünschenswert, um Diskussionen mit Prüfgesellschaften und Behörden zu vermeiden.

Anhang 1
Ein erläuternder Text zu den Grafiken wäre hilfreich, um diese korrekt zu verstehen.

Erläuterungsbericht
Im Erläuterungsbericht auf Seite 10 werden Geldwäschereirisiken zunächst als «Rechtsrisiken» und auf Seite 11 als «Compliance-Risiken» bezeichnet, was widersprüchlich ist. Auf Seite 11 werden die «Rechtsrisiken» mitunter als das Risiko von Rechtsfällen bezeichnet. Die Kantonalbanken schlagen vor, die Abgrenzung zwischen den beiden Risikogruppen respektive ihre Definitionen zu konkretisieren.

Wir bedanken uns für die wohlwollende Prüfung und Berücksichtigung der erwähnten Stellungnahme und insbesondere der oben erwähnten Anliegen.

Für allfällige Rückfragen und weitere Erläuterungen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Michele Vono
Leiter Public Affairs