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