Grant Thornton

Neues FINMA-Rundschreiben «Operationelle Risiken und Resilienz»

Am 1. Januar 2024 tritt das FINMA-Rundschreiben 2023/1 «Operationelle Risiken und Resilienz – Banken» in Kraft. Mit dem Inkrafttreten des überarbeiteten FINMA-Rundschreibens erfolgen wesentliche Anpassungen in den Bereichen Management der Informations- und Kommunikationstechnologie-Risiken (IKT-Risiken) und Management der Risiken kritischer Daten. Zudem gilt es neue Vorgaben zur Sicherstellung der operationellen Resilienz zu beachten. Was sind die wichtigsten Aspekte des Rundschreibens und welche Bedeutung hat es für FINIG-Institute?

Einordnung[1]

	Banken / Wertpapierhäuser	**Asset Management-Institute** (Fondsleitungen, Verwalter von Kollektivvermögen)	**Vermögensverwalter / Trustees**	**Übrige Finanzintermediäre** (SRO[2]-Beaufsichtigte)
Anwendbarkeit	Ja	Indirekt	Indirekt	Nein
Relevanz	Hoch	Teilweise	Teilweise	Gering

[1] Es handelt sich um eine stark vereinfachte Darstellung, welche eine rasche erste Einordnung der Thematik ermöglichen soll. Jedes Institut sollte die Relevanz und den konkreten Handlungsbedarf individuell-konkret bestimmen.
[2] Selbstregulierungsorganisation (SRO)

Hintergrund

Das neue Rundschreiben legt den Fokus auf die Bedeutung der operationellen Risiken und die Resilienz für Finanzinstitute. Es soll dem Strukturwandel und einer steigenden Bedrohungslage in Bezug auf die IKT-Risiken Rechnung tragen. Dies umfasst unter anderem technische Entwicklungen wie Fortschritt der Digitalisierung, Steigerung der Komplexität der Lieferketten und Abhängigkeiten sowie die Zunahme von Cyber-Attacken. Weitere Treiber für die Überarbeitung des Rundschreibens waren internationale regulatorische Entwicklungen.

Neuerungen im Bereich operationelles Riskmanagement

Die Vorgaben des Rundschreibens zum Management der operationellen Risiken werden nach den folgenden Bereichen unterteilt:

- Übergreifendes Management der operationellen Risiken
- Management der IKT-Risiken (Informations- und Kommunikationstechnologie)
- Management der Cyber-Risiken
- Management der Risiken kritischer Daten
- Business Continuity Management (BCM)
- Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft (Cross-Border)

Inhaltlich wurden diese Bereiche des FINMA-Rundschreibens in unterschiedlichem Ausmass überarbeitet oder erneuert. Einzelne blieben inhaltlich komplett unverändert, andere erfuhren bedeutende Neuerungen.

Ein bereits bekannter Schwerpunkt des FINMA-Rundschreibens liegt beim Management von operationellen Risiken. Die FINMA hat neu das übergreifende Management der operationellen Risiken in einem Kapitel zusammengefasst, um die Aufsichtserwartungen transparenter zu machen. Dabei blieb der inhaltliche Aspekt unverändert.

Im Bereich Management der IKT-Risiken erfolgten wesentliche Anpassungen aufgrund der vom Basler Ausschuss für Bankenaufsicht erarbeiteten Prinzipien der Operational Resilienz (POR) und der überarbeiteten Prinzipien für ein solides Management operationeller Risiken (PSMOR).

Weitere wesentliche Anpassungen erfolgten bei der Regulierung des Managements der Risiken kritischer Daten. Neu enthält das Rundschreiben eine Definition des Begriffs «kritische Daten». Dabei wurde der Begriff erweitert und umfasst alle Daten, die für das Institut von so wesentlicher Bedeutung sind, dass ein erhöhter Sicherheitsanspruch erforderlich ist.

Das neue Kapitel zum Business Continuity Management (BMC) im Rundschreiben ersetzt die bisherige SBVg-Selbstregulierung. Die Regulierung zu BCM wurde bei der Übernahme ins Rundschreiben aktualisiert. Geringe Anpassungen erfolgten beim Kapitel Management der Cyber-Risiken. Unverändert blieben das Management der Risiken aus dem grenzüberschreitenden Dienstleistungsgeschäft wie auch die Weiterführung von kritischen Dienstleistungen bei der Abwicklung und Sanierung von systemrelevanten Banken in Kapitel VI.

Operationelle Resilienz

Das Rundschreiben legt neu einen Fokus auf die Sicherstellung der operationellen Resilienz und enthält diesbezügliche Vorgaben im separaten Kapitel V. Operationelle Resilienz bezeichnet die Fähigkeit eines Instituts, seine kritischen Funktionen bei Unterbrechungen innerhalb der Unterbrechungstoleranz wiederherstellen zu können. Erwartet wird ein ganzheitlicher Ansatz, welcher sowohl präventive als auch reaktive Massnahmen in ihrer Gesamtheit erfasst, überwacht und darüber rapportiert.

Erwartungen der FINMA aufgrund von durchgeführten Vor-Ort-Kontrollen

Während Vor-Ort-Kontrollen im Vorfeld des Inkrafttretens des FINMA Rundschreibens hat die FINMA bei vielen Instituten Bereiche identifiziert, in denen Verbesserungspotential besteht, so beispielsweise beim IKT-Inventar hinsichtlich Aktualität und Vollständigkeit. Ferner haben einige Institute nach Ansicht der FINMA ihre technologische Infrastruktur nicht rechtzeitig und systematisch überwacht. Weiter stellte die FINMA fest, dass der Fokus bei der Identifikation der kritischen Daten teilweise sehr beschränkt auf Client Identifying Data (CID) liegt, wogegen im Hinblick auf das neue Rundschreiben bei der Beurteilung und Festlegung der Kritikalität von Daten ein breiterer Approach erwartet wird.

Anwendbarkeit und Bedeutung für FINIG Institute

Direkt anwendbar ist das Rundschreiben nur für Banken, Finanzgruppen und -konglomerate sowie Wertpapierhäuser. Die Anforderungen werden durch die FINMA eingeschränkt, indem Banken und Wertpapierhäuser der Aufsichtskategorien 4 und 5 von der Pflicht zur Erfüllung zahlreicher Randziffern ausgenommen werden. Die Umsetzung des FINMA-Rundschreibens hängt zudem im Einzelfall von verschiedenen Faktoren ab, wie beispielsweise der Grösse, Komplexität, Struktur und dem Risikoprofil der jeweiligen Bank. Je nach Situation kann die FINMA Erleichterungen oder strengere Massnahmen anordnen. Für das neue Kapitel zur operationellen Resilienz gelten teilweise Übergangsbestimmungen von bis zu zwei Jahren. Die übrigen Bereiche des Rundschreibens treten ohne Übergangsbestimmungen per 1. Januar 2024 in Kraft.

Das Rundschreiben richtet sich neben Banken und Wertpapierhäuser grundsätzlich nicht an übrige FINIG-Institute, daher ist es für diese nicht unmittelbar anwendbar. Dennoch enthält das Rundschreiben zahlreiche Erwartungen der FINMA, welche in geringerem Umfang und je nach Grösse, Komplexität, Struktur und Risikoprofil des Instituts auch für tiefer regulierte Institute gelten dürften. So beispielsweise viele allgemeine Vorgaben zum operationellen Risikomanagement oder Vorgaben im Bereich Crossborder. Auch die Randziffern zum Management der Cyber-Risiken und im Bereich BCM sollten von FINIG-Instituten nicht ausser Acht gelassen werden.

Fazit und Ausblick

Das FINMA-Rundschreiben 2023/1 enthält wichtige neue und höhere Anforderungen in Bezug auf das Management der operationellen Risiken und die operationelle Resilienz bei Finanzinstituten. Banken und Wertpapierhäuser dürften aufgrund der angemessenen Vorlaufzeit die meisten aus dem FINMA-Rundschreiben hervorgehenden Anpassungen vorbereitet und implementiert haben, um für das Inkrafttreten des FINMA-Rundschreibens bereit zu sein. Die nächste Herausforderung wird für sie die konkrete Umsetzung in der Praxis, insbesondere der Verfahren, Prozesse und Kontrollen, sein. Übrige FINIG-Institute sind zwar nicht unmittelbar betroffen, sie sollten aber je nach Grösse, Komplexität, Struktur und Risikoprofil ihres Instituts abklären, inwiefern das Rundschreiben für sie relevant oder hilfreich ist.

Fabian Schmid
Partner, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 50
E fabian.schmid@ch.gt.com

Christopher Oehri
Partner, Advisory IT & Digitalisation
Grant Thornton AG
T +423 237 42 10
E christopher.oehri@ch.gt.com

Nina Helbling
Senior Accountant, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 58
E nina.helbling@ch.gt.com