FINMA-Rundschreiben 2023/1

«Operationelle Risiken und Resilienz – Banken»
Konkrete Umsetzungsherausforderungen für den Verwaltungsrat

Board Leadership News
Ausgabe 01/2023

Im Dezember 2022 veröffentlichte die FINMA das totalrevidierte Rundschreiben zu operationellen Risiken und Resilienz, welches am 1. Januar 2024 in Kraft tritt und das bisherige Rundschreiben ersetzt. Dabei werden auch die Anforderungen an den Verwaltungsrat konkretisiert und ausgeweitet. Banken müssen nun rechtzeitig allfällige Lücken in ihrer Organisationsstruktur, in den Risikoprozessen und im Kontrollsystem identifizieren, um das Rundschreiben fristgerecht zu erfüllen. Neben dem hohen Umsetzungsaufwand bieten die Vorgaben zur operationellen Resilienz auch Chancen für die Banken.

Ausgangslage und wichtigste Inhaltspunkte

Das aktuell gültige Rundschreiben 2008/21 zu operationellen Risiken trat 2009 in Kraft. Mit dem neuen Rundschreiben trägt die FINMA der gesteigerten Risikolage und den rapiden Entwicklungen in der Digitalisierung und der Informations- und Kommunikationstechnologie (IKT) Rechnung. Gleichzeitig setzt sie die revidierten Vorgaben des Basel Committee on Banking Supervision (BCBS) zum Management operationeller Risiken und die neuen Basler Grundsätze zur Sicherstellung der operationellen Resilienz um.

Die neuen FINMA-Anforderungen widerspiegeln drei Aspekte. Erstens wurde die bisherige Aufsichtspraxis in den Bereichen Risikogovernance und -strategie, Cyberrisiken und Krisenmanagement konkretisiert. Zweitens wurden die Anforderungen im Umgang mit kritischen Daten und IKT-Risiken wesentlich ausgeweitet und drittens, um Vorgaben zur operationellen Resilienz ergänzt.

«Die Umsetzung der neuen FINMA-Anforderungen sind mit einem hohen Aufwand verbunden.»

Mit operationeller Resilienz bezeichnet die FINMA die Fähigkeit eines Instituts, sein Betriebsmodell so aufzubauen, dass es sich präventiv vor Bedrohungen und Ausfällen schützt und im Ereignisfall seine kritischen Funktionen innerhalb vordefinierter Unterbrechungstoleranzen wiederherstellen kann. Kritische Funktionen sind für die FINMA-Aktivitäten, Prozesse und Dienstleistungen, deren Unterbrechung die Weiterführung des Instituts oder dessen Rolle im Finanzmarkt gefährden würden. Zum Schutz der kritischen Funktionen muss die Bank dabei eine «End-to-end»-Sicht auf die gesamte Wertschöpfungskette, inklusive der Abhängigkeiten zu Ressourcen, Systemen und externen Dienstleistern, einnehmen.

Die neuen Anforderungen gelten grundsätzlich für alle Banken, wobei die FINMA unter Anwendung des Proportionalitätsprinzips weitgehende Erleichterungen für kleinere Banken vorsieht.

Mit dem neuen Rundschreiben werden auch die Rolle und Aufgaben des Verwaltungsrats in Bezug auf das strategische Risikomanagement und die Überwachung konkretisiert und ausgeweitet.

Rolle und Verantwortlichkeiten des Verwaltungsrats unter dem neuen Rundschreiben

Als Oberleitungsorgan ist der Verwaltungsrat vor allem in Bezug auf den ersten und dritten Aspekt gefordert. So muss der Verwaltungsrat die Leitplanken in Form von internen Vorgaben zum operationellen Risikomanagement und Strategien im Umgang mit der IKT, den Cyberrisiken, den kritischen Daten und dem Business Continuity Management (BCM) genehmigen und die Einhaltung dieser Vorgaben überwachen.

Auf risikostrategischer Ebene muss der Verwaltungsrat mindestens jährlich die Risikotoleranz für operationelle Risiken unter Berücksichtigung der Wirksamkeit von Risiko- und Kontrollmassnahmen sowie von strategischen und finanziellen Zielen genehmigen. Die Risikotoleranz muss dabei nicht nur für die residualen Risiken, d.h. Risiken nach risikomindernden Massnahmen und Kontrollen, sondern auch für die inhärenten Risiken festgelegt werden. Hierzu muss der Verwaltungsrat strategische Entscheidungen in Bezug auf das Geschäfts- oder Betriebsmodell berücksichtigen, z.B. ob gewisse Kundensegmente oder Länder überhaupt bedient werden sollen oder ob bestimmte Produkte angeboten werden sollen. Je nach Risikotoleranz muss der Verwaltungsrat anschliessend die notwendigen strategischen Anpassungen vornehmen, z.B. eine Änderung im Geschäftsmodell.

Im Bereich Business Continuity Management wurden die als Selbstregulierung anerkannten Empfehlungen für das BCM von der Schweizerischen Bankiervereinigung (SBVg) in das neue Rundschreiben integriert und aktualisiert. Einige bisherige SBVg Empfehlungen in Bezug auf den Verwaltungsrat, welche nicht Mindeststandard waren, sind neu im Rundschreiben vorgegeben, u. a. die Erreichbarkeit der Verantwortungsträger in Krisensituationen sowie die regelmässige Berichterstattung an den Verwaltungsrat über die BCM Aktivitäten.

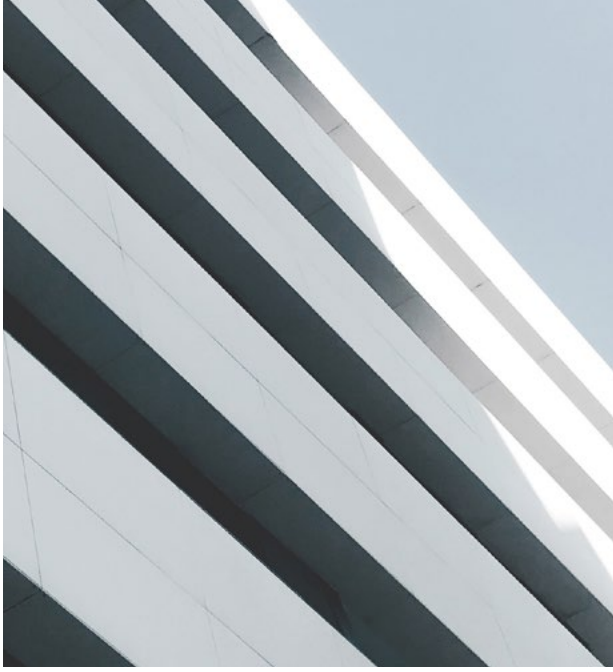
Der Verwaltungsrat wird auch in Bezug auf den dritten Aspekt, die operationelle Resilienz, eingebunden. Bei der Bestimmung der kritischen Funktionen erwartet die FINMA eine Top-down-Sicht auf die strategisch wichtigen Operationen und Leistungserbringungen, d.h. kritische Funktionen. Dementsprechend muss der Verwaltungsrat mindestens jährlich die kritischen Funktionen der Bank und deren Unterbrechungstoleranzen genehmigen. Dabei kann davon ausgegangen werden, dass eine Bank typischerweise nur sehr wenige kritische Funktionen hat, bei jeder Bank aber mindestens eine Funktion, z.B. der Zahlungsverkehr, als kritisch gilt. Der Verwaltungsrat muss zudem das Vorgehen zur Sicherstellung der operationellen Resilienz überwachen. Dazu muss ihm mindestens jährlich – oder aber bei Vorfällen – Bericht erstattet werden.

Herausforderungen für den Verwaltungsrat

Die Herausforderungen für den Verwaltungsrat bestehen vor allem auf der risikostrategischen und organisatorischen Ebene.

Damit der Verwaltungsrat in Bezug auf die Risikostrategie die an ihn gestellten Anforderungen erfüllen kann, muss er als Gremium über entsprechendes Know-how in den Bereichen operationelles Risikomanagement, internes Kontrollsystem, IKT- und Cyberrisiken sowie Krisenmanagement verfügen und ein gutes Verständnis der kritischen Funktionen und der damit verbundenen Abhängigkeiten haben. In vielen Banken, gibt es dabei eine signifikante Know-how- und Informationsasymmetrie zwischen dem Verwaltungsrat und der operativen Bankleitung.

Erschwerend kommt hinzu, dass bei vielen Banken das operationelle Risikomanagement eine tiefere Maturität hat als das finanzielle Risikomanagement. Dabei sind der Prozess zur Identifikation und Beurteilung operationeller Risiken sowie die Kriterien zur Festlegung von Toleranzen für inhärente und residuale Risiken oftmals weniger formalisiert – gerade in den Bereichen IKT, Cyberrisiken und Umgang mit kritischen Daten. Dies wiederum erschwert dem operativen Risikomanagement die Definition von risikomindernden Massnamen und wirksamen Kontrollen, was sich in einer fragmentierten und wenig stufengerechten Berichterstattung zu operationellen Risiken äussern kann. Dadurch fehlt dem Verwaltungsrat eine ganzheitliche Sicht auf die Risikosituation, die kritischen Funktionen und Ressourcen sowie deren Abhängigkeiten zu externen Partnern – Informationen, die er braucht, um den von der FINMA geforderten Abgleich der Risikolage mit der Geschäftsstrategie vornehmen zu können.



Als zusätzliche Herausforderung muss neu eine End-to-end-Sicht auf die kritischen Funktionen eingenommen und als integrales Element in die gesamte Organisation und über alle Verteidigungslinien hinweg implementiert werden. Dazu braucht es eine solide Verankerung im Risiko- und Krisenmanagement und eine bankweite Harmonisierung der für das Management der operationellen Ressourcen zuständigen Funktionen. Dies wird dadurch erschwert, dass bei vielen Banken die Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) im Bereich der operationellen Risiken oftmals historisch gewachsen sind und die Trennung zwischen den operativen Einheiten und der Risikokontrolle nicht immer eindeutig ist.

Die bisherige Erfahrung zeigt, dass die Umsetzung der neuen FINMA-Anforderungen mit einem hohen Aufwand verbunden ist – insbesondere in den Bereichen Risikokontrolle, IKT, Umgang mit kritischen Daten, operationelle Resilienz, Krisenübungen und interne Berichterstattung. Die fristgerechte Implementierung und der zu erwartende Mehraufwand im operativen Betrieb stellen somit eine grosse Herausforderung für Organisationseinheiten wie die IT und die Risikokontrolle dar.

Auf der organisatorischen Ebene sind der Verwaltungsrat und die Geschäftsleitung somit gefordert, für eine klare Risikogovernance im Bereich der operationellen Risiken zu sorgen, welche eine End-to-end-Risikosteuerung und -kontrolle ermöglicht. Parallel dazu müssen die die notwendigen finanziellen und personellen Ressourcen für die Implementation und den Betrieb bereitgestellt werden.

Handlungsempfehlungen

Der Verwaltungsrat muss sich aktiv mit den Themena operationelles Risikomanagement und operationelle Resilienz auseinandersetzen. Dazu wird empfohlen, regelmässig Schulungen zu diesen Themen durchzuführen.

Auf der risikostrategischen Ebene müssen der Verwaltungsrat und die Geschäftsleitung rechtzeitig allfällige Lücken und Verbesserungspotenzial in der Governance, im bankweiten Risikoprozess und im Kontrollsystem identifizieren, um das Rundschreiben fristgerecht zu erfüllen.

Der Verwaltungsrat soll dabei auch überprüfen und kritisch hinterfragen, ob er für seine Überwachungsfunktion und die risikostrategischen Entscheide zeitnah über die richtigen Informationen verfügt. Falls nicht, empfiehlt es sich, die Risikoberichterstattung anzupassen und insbesondere eine Integration mit der restlichen Risikoberichterstattung anzustreben, um eine ganzheitliche Sicht auf das Risikoprofil und dessen Abgleich mit der Risikotoleranz zu erhalten. Oftmals können dabei Synergien im Reportingprozess realisiert und über die Jahre gewachsene Berichte entschlackt werden.

In Bezug auf die organisatorischen Herausforderungen soll die Geschäftsleitung dem Verwaltungsrat die Vorgehensplanung zur Umsetzung des FINMA-Rundschreibens darlegen. Insbesondere soll dabei aufgezeigt werden, welche finanziellen und personellen Ressourcen für die Implementation und den anschliessenden Betrieb benötigt werden. Im Rahmen der Umsetzung oder spätestens im laufenden Betrieb empfiehlt es sich, regelmässig zu prüfen, ob mittels Systemunterstützungen (z.B. die Einführung einer Governance, Risk and Compliance Lösung), Anpassungen im Betriebsmodell (Digitalisierungsstrategie, Automatisierungen) oder Auslagerungen Effizienzsteigerungen realisiert werden können.

In Bezug auf die operationelle Resilienz ist es nötig, dass der Verwaltungsrat früh mit der Geschäftsleitung einen aktiven Dialog zur Bestimmung der kritischen Funktionen führt und dazu Transparenz hinsichtlich Unterbrechungstoleranzen und möglicher Ausfallszenarien einfordert. Dabei muss er bei seiner Beurteilung die wesentlichen Abhängigkeiten zu Drittparteien verstehen und die Auswirkungen auf die Reputation und andere Risiken, wie z.B. Liquiditätsrisiken, berücksichtigen.

Chancen des neuen FINMA-Rundschreibens

Die Vorgaben zur operationellen Resilienz bieten auch Chancen. Das Konzept der operationellen Resilienz ist keine neue Erfindung, sondern wird seit Langem von Unternehmen mit einer hohen Anforderung an die betriebliche Stabilität eingesetzt, z.B. in Spitälern, Kraftwerken und Flugsicherungen.

Damit ein Unternehmen operationell resilient wird, muss es auf der technischen Seite seine Prozesse, Systeme, Ressourcen und die damit verbundenen Abhängigkeiten sehr gut kennen, beherrschen und fortlaufend optimieren. Parallel dazu können Unternehmen ihre Widerstandskraft erhöhen, indem sie eine Resilienzkultur etablieren. Dazu gehören u.a. eine ausgeprägte Risiko- und Fehlerkultur, eine hohe Achtsamkeit in Bezug auf operative Abläufe («Sensitivity to operations») sowie der Wille zur operationellen Exzellenz.

Resiliente Unternehmen reagieren nicht nur im Krisenfall besser, sondern arbeiten oftmals auch im Normalbetrieb effizienter und damit kostengünstiger. Die Sicherstellung der operationellen Resilienz ist somit auch eine Chance, um Verbesserungen und Exzellenz im Betrieb voranzutreiben und Wettbewerbsvorteile zu generieren.

Dr. Hans Ulrich Bacher
Director, Financial Services,
KPMG Schweiz

+41 58 249 51 63
hbacher@kpmg.com

Hanna Read
Manager, Financial Services,
KPMG Schweiz

+41 58 249 28 33
hannaread@kpmg.com