Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA-Aufsichtsmitteilung 05/2025

Operationelle Resilienz bei Banken, Personen nach Art.1*b* BankG, Wertpapierhäusern und Finanzmarktinfrastrukturen

10. November 2025

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Inhaltsverzeichnis

1 Einleitung

Banken, Personen nach Art. 1*b* des Bankengesetzes (BankG; SR *952.0*), Wertpapierhäuser und Finanzmarktinfrastrukturen haben im Rahmen ihrer Geschäftstätigkeiten ein angemessenes Risikomanagement vorzusehen. Das Risikomanagement muss dabei die gesamte Geschäftstätigkeit erfassen und so organisiert sein, dass sich alle wesentlichen Risiken feststellen, bewerten, steuern und überwachen lassen. Vor dem Hintergrund verschiedener zunehmender Risiken im Finanzmarkt und neuer operationeller Herausforderungen (u.a. Cyberattacken), legt die FINMA seit längerem einen stärkeren Aufsichtsfokus nicht nur auf operationelle Risiken allgemein, sondern insbesondere auch auf die operationelle Resilienz von Instituten.

Operationelle Resilienz bezeichnet in den verschiedenen aufsichtsrechtlichen Bestimmungen die Fähigkeit des Instituts, seine kritischen Funktionen bei Unterbrechungen innerhalb der Unterbrechungstoleranz wiederherstellen zu können. Es ist die Fähigkeit des Instituts, Bedrohungen und mögliche Ausfälle zu identifizieren, sich davor zu schützen und darauf zu reagieren, bei Unterbrechungen den ordentlichen Geschäftsbetrieb wiederherzustellen und die Auswirkungen von Unterbrechungen auf die Erbringung der kritischen Funktionen zu minimieren. Die operationelle Resilienz verringert somit nicht nur die residualen Risiken von Unterbrechungen, sondern auch das inhärente Risiko, dass es zu Unterbrechungen kommt.

Die Finanzbranche ist heute stark vernetzt und voneinander abhängig. Diese Vernetzung führt zu einer Konzentration von Risiken. Eine Störung in einem Bereich kann daher weitreichende Auswirkungen auf andere Teile des Finanzsystems haben. Operationelle Resilienz ist demzufolge von entscheidender Bedeutung für den Schutz der Funktionsfähigkeit der Finanzmärkte. Der Fokus der FINMA auf die operationelle Resilienz von Finanzinstituten stärkt dadurch nicht nur den Schutz der Gläubigerinnen und Gläubiger, sondern auch die Funktionsfähigkeit der Finanzmärkte als solche und ist damit elementar für ein starkes Finanzmarktsystem.

Die vorliegende Aufsichtsmitteilung beruht auf Erkenntnissen einer Datenerhebung, die die FINMA per 31. Dezember 2024 bei 267 Banken, Wertpapierhäusern, Finanzgruppen und Finanzmarktinfrastrukturen (nachstehend als „Institute“ bezeichnet) zum Thema Sicherstellung der operationellen Resilienz durchgeführt hat.

Die Aufsichtsmitteilung bezweckt die Sensibilisierung in Bezug auf das Thema operationelle Resilienz und damit die effektive Umsetzung der verschiedenen aufsichtsrechtlichen Anforderungen sowie die zielgerichtete Stärkung der operationellen Resilienz gegenüber wachsenden Bedrohungen und operationellen Schocks.

2 Rechtliche Grundlage

Für Banken und Personen nach Art. 1*b* BankG ergibt sich die Pflicht zur Erfassung, Begrenzung und Überwachung ihrer Risiken primär aus den organisatorischen Anforderungen gemäss Art. 1*a,* Art. 1*b,* Art. 3 Abs. 2 Bst. a und Art. 3*c* BankG i.V.m. Art. 12 Abs. 2 und Art. 14*e* der Bankenverordnung vom 30. April 2014 (BankV; SR *952.02*).

Für Wertpapierhäuser ergibt sich diese Pflicht im Wesentlichen aus den Art. 9 Abs. 2, 41 und 49 des Finanzinstitutsgesetzes vom 15. Juni 2018 (FINIG; SR *954.1*) sowie Art. 12 Abs. 4 und 68 der Finanzinstitutsverordnung vom 6. November 2019 (FINIV; SR *954.11*). Für Finanzmarktinfrastrukturen ergibt sich die Pflicht gestützt auf Art. 8 Abs. 3 des Finanzmarktinfrastrukturgesetzes vom 19. Juni 2015 (FinfraG; SR *958.1*) und Art. 9 Abs. 1 Bst. d der Finanzmarktinfrastrukturverordnung vom 25. November 2015 (FinfraV; SR *958.11*).

Die FINMA hat ihre diesbezügliche Aufsichtspraxis im Rundschreiben 2023/1 „Operationelle Risiken und Resilienz – Banken“ konkretisiert.

3 Erkenntnisse der Datenerhebung

Die 267 von der FINMA befragten Institute bewerteten die Maturität ihrer eigenen operationellen Resilienz auf einer Skala von 0–10[1] mit 7.5 (Mittelwert) und diejenige des Schweizer Finanzsektors insgesamt mit 6.7 (Mittelwert). Nachfolgend werden ausgewählte Erkenntnisse aus der Datenerhebung zur Sicherstellung der operationellen Resilienz dargestellt.

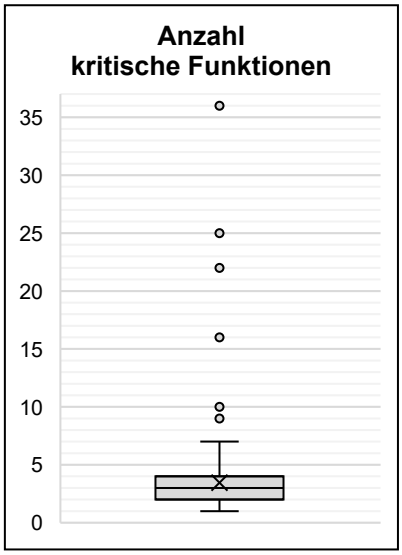
3.1 Kritische Funktionen[2]

Erkenntnisse

Die nachfolgende Grafik stellt aggregiert die Anzahl der durch die Institute definierten kritischen Funktionen dar. Dabei beobachtet die FINMA, dass die Anzahl der kritischen Funktionen zwischen 1 und 36 liegt, wobei die Hälfte der Institute nicht mehr als 3 kritische Funktionen (Median) definiert hat. Gleichzeitig liegt die mittlere Hälfte aller Nennungen zwischen 2 und 4 kritischen Funktionen. Das arithmetische Mittel liegt bei rund 3.5 kritischen Funktionen.

[1] Selbsteinschätzung durch die Institute auf einer Skala von 0 bis 10; wobei 0 = nicht resilient und 10 = absolut resilient.

[2] Vgl. dazu Rz 14–16 FINMA-RS 23/1.

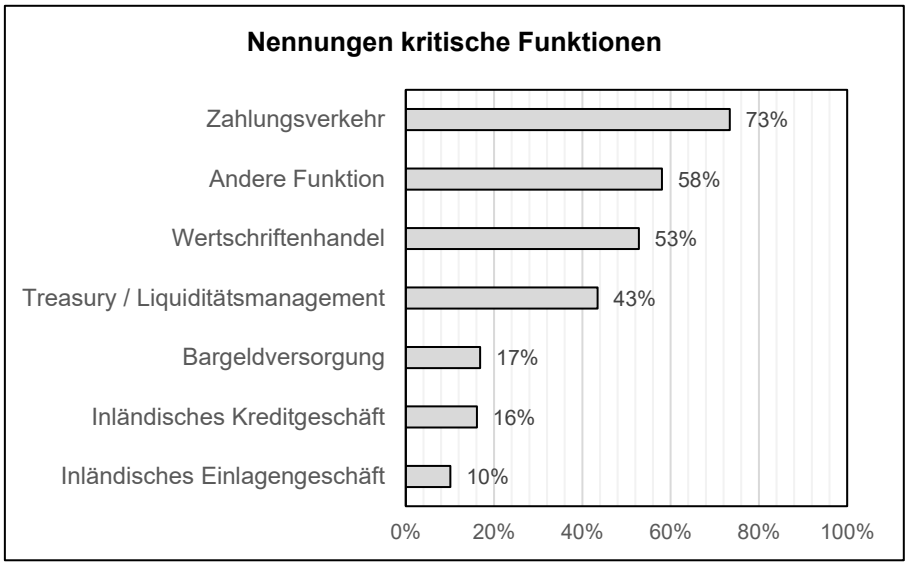


Im „Normalbereich“ identifizierten Institute mindestens eine einzige kritische Funktion, während die grösste beobachtete Anzahl bei 7 kritischen Funktionen liegt. Darüber hinaus zeigt der Boxplot mehrere Ausreisser von 9 bis 36 kritischen Funktionen.

Die zugrundeliegenden Daten erlauben eine Aussage zur Korrelation der Anzahl kritischer Funktionen mit der Grösse und Komplexität des Instituts. So kann geschlussfolgert werden, dass grosse, komplexe Institute eine höhere Anzahl kritischer Funktionen definiert haben und umgekehrt.

Zusammenfassend zeigte sich, dass die mittlere Hälfte der Institute zwischen 2 und 4 kritische Funktionen identifizierte und die Anzahl mit der Grösse und Komplexität des Instituts zunimmt.

Die Art der identifizierten kritischen Funktionen ist insbesondere vom jeweiligen Geschäftsmodell des Instituts abhängig. Das nachfolgende Balkendiagramm zeigt die Häufigkeit der Antworten auf die Umfrage zu der Art der kritischen Funktionen, wobei Mehrfachnennungen möglich waren.



Die FINMA stellt fest, dass die Institute in Bezug auf die vordefinierten Antwortmöglichkeiten am häufigsten den „Zahlungsverkehr“ als kritische Funktion identifizierten (73 %) und dass das „Inländische Einlagengeschäft“ am seltensten genannt wurde. Neben den vordefinierten Antwortmöglichkeiten erfassten die Institute unter „Andere Funktion“ rund 300 Nennungen in Frei-

textform. Bei rund zwei Dritteln dieser Nennungen (z.B. Postwesen, Telefonzentrale, IT-Betrieb, Backoffice) handelt es sich um keine kritischen Funktionen im Sinne des FINMA-RS 23/1, Rz 14–16, sondern um Prozesse, Aktivitäten oder zugrundeliegende Ressourcen.[3] Gleichzeitig sind 71 % aller genannten kritischen Funktionen direkt oder indirekt von Leistungen durch Dritte abhängig.

Hinweise

Die Mehrheit der Institute hat sich mit 1 bis 7 kritischen Funktionen auf eine geringe und leicht überschaubare Anzahl[4] an kritischen Funktionen beschränkt, was im Sinne der aufsichtsrechtlichen Bestimmungen ist. Bei den Instituten mit mehr als 7 kritischen Funktionen ist die Höhe der Anzahl derselben zu hinterfragen. Dabei stellt sich unter anderem die Frage, ob 25 oder 36 kritische Funktionen, wie dies einzelne Institute angegeben haben, überwacht und resilient betrieben werden können, resp. der Betrieb einer so hohen Anzahl von kritischen Funktionen betriebswirtschaftlich überhaupt Sinn macht. Aufgrund des hohen Anteils der von Dritten abhängigen kritischen Funktionen ist insbesondere eine *End-to-End* bzw. *Front-to-Back* Sicht auf die gesamte für ihre Erbringung erforderliche Lieferkette sowie der dazu benötigten Ressourcen wichtig.[5]

Die Art der kritischen Funktionen spiegelt das Geschäftsmodell eines Instituts wider und ist klar von Prozessen, Aktivitäten und zugrundeliegenden Ressourcen abzugrenzen. Die rund zwei Drittel der im Freitext genannten kritischen Funktionen sind vor dem Hintergrund des FINMA-RS 23/1 einer kritischen Überprüfung zu unterziehen. So stellen beispielsweise das regulatorische Reporting, die Sicherstellung der Sorgfaltspflichten im Bereich der Conduct-Themen, das Risikomanagement sowie die Risikokontrolle, die Kundenbewirtschaftung, die Buchhaltung, die Front- und Back-Office Aktivitäten sowie die Repräsentationstätigkeiten zwar zentrale Bestandteile der Geschäftstätigkeit dar. Es handelt sich aber um keine kritischen Funktionen im Sinne des FINMA-RS 23/1, sondern um Prozesse, die als solche entsprechend zu klassifizieren sind. Das Kernbankensystem beispielsweise, die IT-Infrastruktur und der IT-Betrieb sowie die Telefonie stellen ebenfalls keine kritischen Funktionen aus strategischer Sicht dar, sondern sind als zugrundeliegende Ressourcen zu qualifizieren. Weitere Nennungen, wie beispielsweise die Konnektivität, die Systemverfügbarkeit und die Erreichbarkeit sind lediglich Kenngrössen zur Überwachung des Inventars der kritischen Funktionen.

---

[3] Vgl. dazu auch die Erläuterungen vom 7. Dezember 2022 zum Rundschreiben 2008/21 „Operationelle Risiken – Banken“ – Totalrevision Rundschreiben 2013/3 „Prüfwesen“ – Teilrevision, Abschnitt 4.1.8 Operationelle Resilienz (Kapitel V), S. 20–25, abrufbar unter www.finma.ch > Dokumentation > Anhörungen und Evaluationen > Abgeschlossene Anhörungen > 2022 > FINMA-Rundschreiben 2008/21 „Operationelle Risiken – Banken“ – Totalrevision (10.05.2022–11.7.2022) (nachfolgend „Erläuterungen zum FINMA-RS 23/1“).

[4] Vgl. Erläuterungen zum FINMA-RS 23/1, S. 22.

[5] Vgl. Erläuterungen zum FINMA-RS 23/1, S. 22.

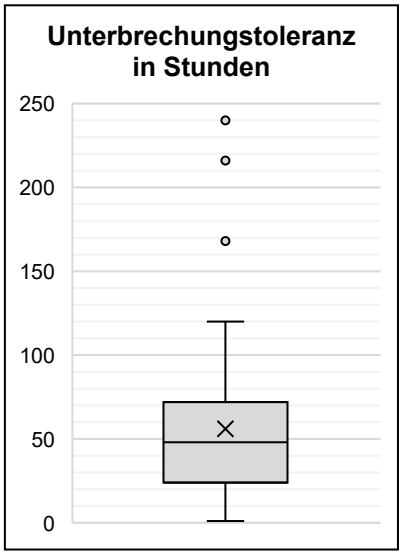
Die Prozesse und zugrundeliegenden Ressourcen dienen dem übergeordneten Zweck der Erbringung von kritischen Funktionen. Deshalb hat der Ausfall einer kritischen Funktion stets eine direkte und unmittelbare Auswirkung auf die Kundinnen und Kunden eines Instituts, auf das Institut selbst oder auf die Funktionsfähigkeit des Finanzmarktes insgesamt. So ist bei der Identifikation der kritischen Funktion eine strategische Sicht *Top-Down* einzunehmen und sind entsprechend lediglich die strategisch wichtigsten Operationen oder Leistungserbringungen als kritische Funktionen zu definieren.

Im Inventar der kritischen Funktionen sind neben den kritischen Funktionen unter anderem auch die darunterliegenden Prozesse, zugrundeliegenden Ressourcen und deren Interdependenzen darzustellen. Eine ausschliesslich tabellarische Darstellung ohne interne Abhängigkeiten stellt kein Inventar der kritischen Funktionen im Sinne der Rz 107 FINMA-RS 23/1 dar.

3.2 Unterbrechungstoleranzen

Erkenntnisse

Die nachfolgende Grafik stellt summarisch die Unterbrechungstoleranz aller kritischen Funktionen der befragten Institute in Stunden dar. Sie zeigt, dass die Mehrheit der Institute eine zeitliche Messgrösse für die Unterbrechungstoleranz gewählt haben. Nur vereinzelt wurde anstatt der Zeit die Storno- und Fehlerquote oder ein unterer Schwellenwert für beispielsweise die „Flüssigen Mittel“ als Toleranzgrösse definiert.



Die Unterbrechungstoleranzen liegen zwischen 1 und 8 736 Stunden (365 Tage)[6], wobei die Hälfte aller Institute nicht mehr als 48 Stunden (Median) Toleranz definieren. Gleichzeitig liegt die mittlere Hälfte aller Nennungen zwischen 24 und 72 Stunden. Das arithmetische Mittel liegt bei 56 Stunden.

Die zugrundeliegenden Daten zeigen keine Korrelation der Unterbrechungstoleranzen mit der Grösse und Komplexität des Instituts. Die Unterbrechungstoleranz wird – wie von den aufsichtsrechtlichen Bestimmungen

[6] Im Sinne des FINMA-RS 23/1 sind Funktionen mit einer Unterbrechungstoleranz mit mehr als 10 Tagen / 240 Stunden auf ihre Kritikalität hin zu überprüfen. Zu Auswertungszwecken sowie zur besseren Lesbarkeit wurden alle Werte über 10 Tage / 240 Stunden aus dieser Boxplot-Grafik entfernt und fliessen ebenfalls nicht in die Durchschnittsberechnungen ein.

vorgesehen – in Abhängigkeit zur Art der kritischen Funktion und der Auswirkungen auf ebendiese definiert.

Zusammenfassend zeigt sich, dass die mittlere Hälfte der Institute Unterbrechungstoleranzen zwischen 24 und 72 Stunden definierten und diese unabhängig von der Grösse oder Komplexität des Instituts sind.

Weiter hat die FINMA im Zuge ihrer Aufsichtstätigkeit und den *Horizontal Reviews Operational Resilience 2025*[7] bei den Instituten der Aufsichtskategorien 1 bis 3 festgestellt, dass die Unterbrechungstoleranzen teilweise anhand der Wiederherstellungsfähigkeiten des Instituts nach einem schwerwiegenden, aber plausiblen Szenario definiert wurden (sogenanntes *Reverse-Engineering*) und nicht anhand der Toleranzbereitschaft des Oberleitungsorgans.

Hinweise

Für die Definition der Unterbrechungstoleranzen können neben der zeitlichen Dimension auch andere Messgrössen wie finanzieller Schaden, Kundenverlust usw. verwendet werden. Dabei sind die zu erwartenden Auswirkungen auf die Kundenbeziehung, das Institut selbst und die Funktionsfähigkeit des Finanzmarktes insgesamt von zentraler Bedeutung.

Die aufsichtsrechtlichen Anforderungen sehen vor, dass die Unterbrechungstoleranzen die Toleranz des Oberleitungsorgans gegenüber Schocks – unabhängig von der Wiederherstellungsfähigkeit des Instituts – widerspiegeln.[8] Ein sogenanntes *Reverse-Engineering* ist nicht im Sinne der aufsichtsrechtlichen Bestimmungen.

Ausreisser mit weniger als 24 Stunden Unterbrechungstoleranzen sind zu hinterfragen. Einerseits ist zu prüfen, ob es sich tatsächlich um kritische Funktionen im Sinne des FINMA-RS 23/1 handelt (siehe Abschnitt 3.1) oder um kritische Prozesse, deren Toleranzen im *Business Continuity Management (BCM)* in Form von RTO/RPO[9] definiert werden. Andererseits ist zu prüfen, ob die Definition und Kalibrierung der Unterbrechungstoleranz angemessen ist und die Dimensionen Kundenbeziehung, Weiterführung des Instituts sowie Funktionsfähigkeit des Finanzmarktes angemessen berücksichtigt wurden.

Bei tief definierten Unterbrechungstoleranzen ist insbesondere die Abhängigkeit zu externen Dienstleistern sowie Lieferanten kritisch zu prüfen und eine transparente Kommunikation der Toleranzen in der gesamten Lieferkette sicherzustellen. So ist bei der Definition der Unterbrechungstoleranz

[7] Zum Zeitpunkt der Veröffentlichung dieser Aufsichtsmitteilung sind noch nicht alle *Horizontal Reviews Operational Resilience 2025* abgeschlossen.

[8] Vgl. Rz 101 FINMA-RS 23/1.

[9] RTO/RPO steht für *Recovery Time Objective* (RTO) / *Recovery Point Objective* (RPO), vgl. Rz 10 FINMA-RS 23/1.

eine *End-to-End* bzw. *Front-to-Back* Sicht der gesamten Lieferkette einzunehmen und die dazu benötigten Ressourcen sind zu berücksichtigen.[10]

Unterbrechungstoleranzen von über 240 Stunden (10 Tagen) sind hingegen sehr hoch. Eine Funktion, auf welche die Kundinnen und Kunden, das Institut sowie der Finanzmarkt mehr als 10 Tage verzichten können – ohne partielle Wiederherstellung, alternative Fallback-Systeme, *Workaround*, o.ä. – ist womöglich nicht kritisch für das Institut. Die FINMA regt an, diese hohen Unterbrechungstoleranzen bei der nächsten Genehmigung durch das Oberleitungsorgan zu überprüfen.

Unterbrechungstoleranzen von über 120 Stunden (5 Tage) sind ebenso zu hinterfragen. Hierbei stellt sich die Frage, ob eine Kundenbeziehung resp. das Institut selbst eine so hohe Toleranz überstehen würde. Bei der Definition der Unterbrechungstoleranzen ist es ebenfalls möglich, eine tiefere Unterbrechungstoleranz zu definieren als die derzeitige Wiederherstellungsfähigkeit des Instituts. In einem solchen Fall (*out-of tolerance*) sind Massnahmen zur Sicherstellung der operationellen Resilienz zu ergreifen, um in den Toleranzbereich zu gelangen.

3.3 Testing

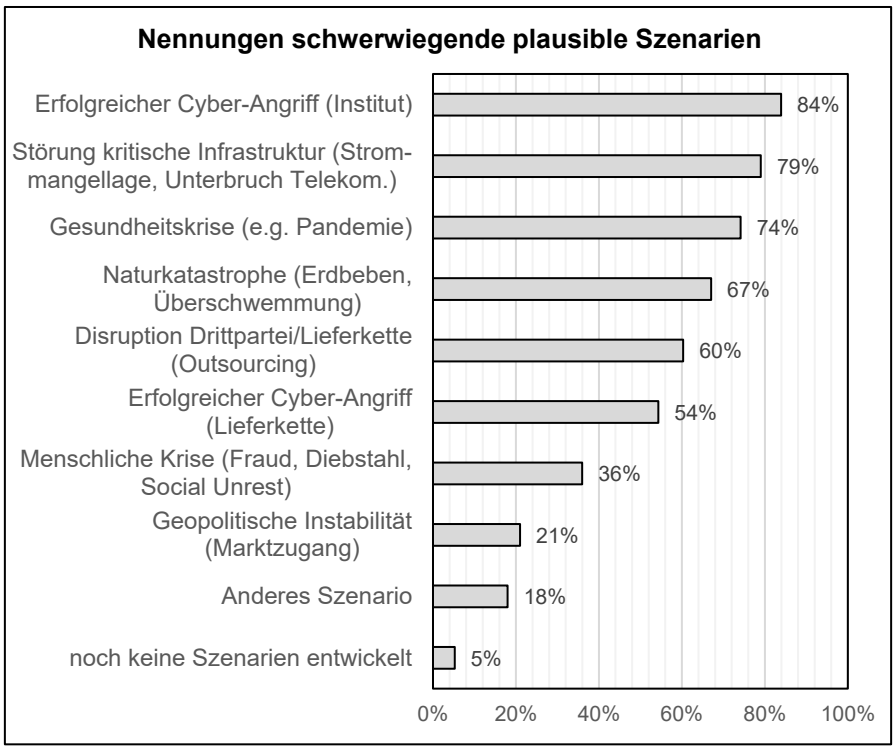
Erkenntnisse

Das *Testing* dient der Identifikation von Schwachstellen und damit der Verbesserung der operationellen Resilienz. Die FINMA beobachtet, dass zum Zeitpunkt der Datenerhebung 85 % der Institute der Aufsichtskategorien 1 bis 3 noch kein *Testing* durchgeführt haben.

10 % der Institute haben das *Testing* bereits eingeplant, wovon die deutliche Mehrheit (72 %) künftig jährliche *Testings* plant. Die restlichen rund 5 % der Institute hat weder getestet noch dieses in die künftigen Pläne aufgenommen.

Das nachfolgende Balkendiagramm zeigt die schwerwiegenden, aber plausiblen Szenarien, welche die Institute in den vorgegebenen Antwortmöglichkeiten für das *Testing* genannt haben.

[10] Vgl. Erläuterungen zum FINMA-RS 23/1, S. 22.



In der Datenerhebung nannten 84 % der Institute einen „Erfolgreichen Cyber-Angriff“ als schwerwiegendes, aber plausibles Szenario für ihr *Testing*. Mit 54 % wurde das Szenario „Erfolgreicher Cyber-Angriff (Lieferkette)“ angegeben. Ebenfalls mit einer Häufigkeit von 60 % wurde das Szenario „Disruption Drittpartei/Lieferkette (Outsourcing)“ aufgeführt. Von den Befragten definierten 18 % andere Szenarien; 5 % der Institute haben noch keine Szenarien entwickelt.

Hinweise

Institute der Aufsichtskategorien 1 bis 3 haben regelmässig *Testings* durchzuführen.[11] Dabei wird die Fähigkeit, kritische Funktionen innerhalb ihrer Unterbrechungstoleranzen unter schwerwiegenden, aber plausiblen Szenarien erbringen zu können, getestet.

Bei der Planung und Ausgestaltung des *Testings* ist insbesondere eine *End-to-End* bzw. *Front-to-Back* Sicht der gesamten Lieferkette und der dazu benötigten Ressourcen einzunehmen.[12] Dabei kann ein institutsübergreifender Test oder ein *Testing* im Verbund mit anderen Instituten Vorteile bieten. Darüber hinaus hat die Gesamtheit aller zu testenden Elemente für das Oberleitungsorgan ersichtlich zu sein, um eine unabhängige Beurteilung des Rahmenwerks der operationellen Resilienz zu ermöglichen.[13]

[11] Vgl. Rz 20 und 110 FINMA-RS 23/1.

[12] Vgl. Erläuterungen zum FINMA-RS 23/1, S. 22.

[13] Vgl. Rz 103 FINMA-RS 23/1.

Die FINMA weist darauf hin, dass die Beaufsichtigten die Entwicklung von schwerwiegenden, aber plausiblen Szenarien für das *Testing* auf der Basis der institutsspezifischen Bedrohungspotentiale zu erarbeiten haben.[14] Insbesondere ist die Bedrohungs- und Verwundbarkeitsanalyse aus *non-Cyber* Aktivitäten weiterzuentwickeln, da diese bei einigen Instituten noch nicht den erforderlichen Reifegrad aufweist.

3.4 Rahmenwerk der operationellen Resilienz

Erkenntnisse

Die FINMA stellt fest, dass die Koordination der bestehenden relevanten Bestandteile[15] zur Stärkung der operationellen Resilienz gemäss der Datenerhebung erst bei 12–15 %[16] der befragten Institute in den Aufsichtskategorien 1 bis 3 erfolgt und damit im Markt noch nicht vollständig implementiert ist.

Um die operationelle Resilienz sowie das damit implementierte Rahmenwerk zu überwachen, verwenden rund 60 % aller befragten Institute eigene Kenngrössen und Indikatoren.[17] Dabei variiert die Anzahl der Indikatoren pro Institut von einem Indikator bis zu 31 definierten Kenngrössen, um die operationelle Resilienz zu überwachen und zu steuern.

Hinweise

Institute der Aufsichtskategorien 1 bis 3 haben ab dem 1. Januar 2026 das Rahmenwerk zur Sicherstellung der operationellen Resilienz mit anderen relevanten Bestandteilen wie beispielsweise das Management der operationellen Risiken inklusive des Managements der IKT- und Cyber-Risiken, das *Business Continuity Management (BCM)*, das Management von Drittparteien sowie die Notfallplanung zu koordinieren, um langfristig ihre operationelle Resilienz zu stärken.[18]

Dies umfasst einen angemessenen Austausch relevanter Informationen zwischen den relevanten Bestandteilen. Dieser Informationsaustausch sowie die Definition von relevanten Kenngrössen stellen die Grundvoraussetzung

[14] Vgl. Rz 70 FINMA-RS 23/1 i.V.m. FINMA Aufsichtsmitteilung 03/2024.

[15] Management der operationellen Risiken, inklusive das Management der IKT- und Cyber-Risiken, das *Business Continuity Management (BCM)*, das Management von Drittparteien und die Notfallplanung.

[16] Abhängig von dem jeweiligen aufsichtsrechtlichen Bestandteil.

[17] z.B.: *End-of-Life Monitoring*, Systemverfügbarkeit Kernbankensystem, IT-Stabilität: Kumulierte Störungszeit / ungeplante Ausfälle, Anzahl kritische Verwundbarkeiten, Anteil überfällige Schwachstellenmanagement, Anzahl *SOC Incidents*, Anzahl *failed* Cyber Schlüsselkontrollen, Anzahl *DLP*-Ereignisse, Anzahl Fälle mit Überschreitung definierter *RTO/RPO*, Anzahl überfällige *Major Incidents*, Anzahl überfällige Audit Beanstandungen/Massnahmen, Anzahl Verlustereignisse, Anzahl aktivierte *BCP*-Pläne, Verletzungen *Service Level Agreements (SLAs)* für wesentliche Outsourcing, Anzahl Ausfall Schlüsselpersonen.

[18] Vgl. Rz 104 und 113 FINMA-RS 23/1.

für die Wirksamkeit der ergriffenen Massnahmen zur Sicherstellung der operationellen Resilienz dar.[19] Dadurch wird einerseits die Effektivität des Rahmenwerks überwacht, andererseits die operationelle Resilienz des Instituts durch unabhängige Indikatoren beurteilt.

4 Fazit und weiteres Vorgehen

Im Rahmen ihrer Aufsichtstätigkeit legt die FINMA gestützt auf das aufsichtsrechtliche Erfordernis eines angemessenen Risikomanagements Wert darauf, dass Institute operationell resilient sind. Dabei steht insbesondere die Widerstandsfähigkeit kritischer Funktionen, unabhängig von der Grösse und der Komplexität des jeweiligen Instituts, im Fokus.

Die Erkenntnisse aus der Datenerhebung, den regulären Aufsichtsgesprächen sowie den *Horizontal Reviews Operational Resilience 2025*[20] zeigen derzeit noch ein sehr heterogenes Bild bei der Auslegung der aufsichtsrechtlichen Anforderungen, dem Umsetzungsstand und dem Reifegrad der operationellen Resilienz bei den beaufsichtigten Instituten.

Ab dem 1. Januar 2026 haben Institute unabhängig von ihrer Aufsichtskategorie Massnahmen zur Sicherstellung der operationellen Resilienz unter Berücksichtigung schwerwiegender, aber plausibler Szenarien zu ergreifen.[21] Durch diese Massnahmen ist zu erwarten, dass sich die operationelle Resilienz der einzelnen Institute verbessert und dies zu einer Stärkung der operationellen Resilienz des gesamten Schweizer Finanzmarktes beiträgt.

Im Fokus der Institute sollten daher weiterhin Aktivitäten zur Sicherstellung der operationellen Resilienz mit präventivem Charakter und geeignete Massnahmen stehen, welche den Ausbau eines Betriebsmodells mit einem kontinuierlichen Verbesserungsprozess ermöglichen, um die kritischen Funktionen resilient zu betreiben (*Resilience by Design)*.

Gleichzeitig wird die FINMA ihre institutsspezifischen Aufsichtsaktivitäten zur Sicherstellung der operationellen Resilienz weiterführen und intensivieren. Insbesondere ist geplant, Szenarioanalysen vertieft auszubauen und langfristig die Voraussetzungen für ein sektorweites *Testing* zu schaffen. Des Weiteren beobachtet die FINMA internationale Entwicklungen, wie beispielsweise bei der IAIS[22], und prüft, ob eine Ausweitung der aufsichtsrechtlichen

[19] Vgl. Rz 102 und 113 FINMA-RS 23/1.

[20] Zum Zeitpunkt der Veröffentlichung dieser Aufsichtsmitteilung sind noch nicht alle *Horizontal Reviews Operational Resilience 2025* abgeschlossen.

[21] Vgl. Rz 102 und 113 FINMA-RS 23/1.

[22] IAIS bezeichnet die International Association of Insurance Supervisors.

Anforderungen zur Sicherstellung der operationellen Resilienz auf andere von der FINMA beaufsichtigte Institute angezeigt wäre.