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 04/2024

Management der operationellen Risiken von Fondsleitungen und Verwaltern von Kollektivvermögen

12. Juni 2024

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

Inhaltsverzeichnis

1 Einleitung

Für einen wirkungsvollen Schutz der Anlegerinnen und Anleger müssen Fondsleitungen und Verwalter von Kollektivvermögen (nachfolgend Institute) über ein gut funktionierendes Risikomanagement verfügen.

Das Risikomanagement umfasst alle wesentlichen Risiken, denen das Institut mit seiner Geschäftstätigkeit sowie die von ihm verwalteten Kollektivvermögen und weiteren verwalteten Vermögen ausgesetzt sind oder sein könnten (vgl. Art. 9 und 26 Finanzinstitutsgesetz [FINIG; SR *954.1*], Art. 12 Abs. 4, Art. 41 bzw. 57 Finanzinstitutsverordnung [FINIV; SR *954.11*] und Art. 8 ff. bzw. 18 Finanzinstitutsverordnung FINMA [FINIV-FINMA; SR *954.111*).

Die operationellen Risiken gehören zu diesen wesentlichen Risiken. Wie bei anderen FINMA-Beaufsichtigten nehmen die operationellen Risiken von Fondsleitungen und Verwaltern von Kollektivvermögen zu, wie insbesondere die Meldungen über Cyber-Angriffe zeigen. Zugleich stellt die FINMA in Bewilligungsverfahren und im Rahmen der Aufsichtstätigkeit vermehrt Mängel und Schwachstellen im Management der operationellen Risiken von Fondsleitungen und Verwaltern von Kollektivvermögen fest.

Die Aufsichtsmitteilung richtet sich deshalb an diese Institute, um sie an die Wichtigkeit eines angemessenen Managements der operationellen Risiken zu erinnern und ihnen mögliche Massnahmen aufzuzeigen.

Analog zum FINMA-Rundschreiben 2023/1 „Operationelle Risiken und Resilienz – Banken“[1] ist als operationelles Risiko die Gefahr von finanziellen Verlusten zu verstehen, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren oder Systemen, des unangemessenen Handelns von Menschen oder durch sie begangene Fehler, oder in Folge von externen Ereignissen eintreten. Dies beinhaltet auch finanzielle Verluste, die aus Rechts- oder Compliance-Risiken entstehen können. Dabei hat das Management der operationellen Risiken auch andere Schadensdimensionen[2] zu berücksichtigen, sofern diese ebenfalls in finanziellen Verlusten resultieren können. Der Begriff umfasst jedoch nicht die strategischen Risiken.

[1] s. www.finma.ch > Dokumentation > Rundschreiben

[2] z.B. negative Auswirkungen auf die Reputation, möglicher Vertrauensverlust, Verlust von Kundinnen und Kunden, negative Auswirkungen auf den Markt, negative regulatorische Auswirkungen (z. Bsp. möglicher Verlust der Lizenz)

2 Beispiele festgestellter Mängel und Schwachstellen

Nachfolgend werden einige Beispiele von kürzlich festgestellten Mängeln und Schwachstellen im Bereich des Managements operationeller Risiken aufgeführt.

2.1 Im Bereich der Prozesse und Verfahren allgemein

Fehlerhafte Erfassungen von Transaktionen oder Transaktionsabrechnungen wurden aufgrund fehlender oder nicht zeitgerechter Kontrollen erst nach Eintritt eines Schadens entdeckt.

2.2 Im Bereich der Informations- und Kommunikationstechnologie sowie Datensicherheit

Bei der Einführung von Cloud-Lösungen zur Speicherung von Kunden- und Unternehmensdaten wurden den Aspekten Auswahl und vor allem Kontrolle der Anbieter der Cloud-Dienstleistungen, Zugriffsrechte, Datensicherheit und Einbezug in das *Business Continuity Management* bzw. in die Business Continuity Pläne nicht oder ungenügend Rechnung getragen.

Die Identifikation der wesentlichen Infrastruktur, insbesondere der Informations- und Kommunikationstechnologie, zur Ausübung der wesentlichen Tätigkeiten des Instituts wurde nicht oder mangelhaft durchgeführt, weshalb für diese Infrastruktur kein angemessener Schutz vorgesehen war und keine angemessene Berücksichtigung in den Business Continuity Plänen erfolgte.

2.3 Im Bereich Cyber-Risiken

Aufgrund erfolgreicher Phishing-Angriffe gelangten unberechtigte Dritte an kritische Daten von Instituten einschliesslich Zugangsdaten für wesentliche Applikationen. Mit diesen entwendeten Daten wurde insbesondere versucht, unberechtigte Transaktionen vorzunehmen.

Institute, die ihre Buchführung an einen externen Dienstleister ausgelagert hatten, verloren nach erfolgreichen Cyber-Angriffen auf den Dienstleister vor-übergehend die Übersicht und Kontrolle über ihre finanzielle Situation und damit namentlich die Fähigkeit, ihre Eigenmittelsituation zu überwachen.

Institute waren zwar in der Lage, Cyber-Attacken zeitnah festzustellen, sie verfügten jedoch nicht über Pläne, wie auf diese Attacken zu reagieren ist und wie die Zuständigkeiten für diesen Fall geregelt sind.

Instituten war schliesslich nicht bewusst, dass sie, wie in der FINMA-Aufsichtsmitteilung 05/2020 „Meldepflicht von Cyber-Attacken gemäss Art. 29

Abs. 2 FINMAG“[3] beschrieben, Cyber-Angriffe der FINMA zu melden haben. Zudem war ihnen ebenfalls nicht bewusst, dass sie bei Verletzungen der Datensicherheit zudem dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten eine Meldung erstatten müssen.[4]

2.4 Im Bereich *Business Continuity Management*

Die im Rahmen des *Business Continuity Management* erstellten Pläne (sogenannte Business Continuity Pläne) erfassten nicht die gesamten für das Erbringen der aktuellen wesentlichen Tätigkeiten erforderlichen wesentlichen Ressourcen, insbesondere in personeller und technischer Hinsicht. Die Aufrechterhaltung bzw. die rasche Wiederaufnahme der wesentlichen Tätigkeiten der Institute in einem Krisenfall war damit nicht gewährleistet.

Business Continuity Pläne wurden nicht oder nicht regelmässig getestet, was zu erheblichen Verzögerungen bei der Behebung von eingetretenen Schäden führte oder führen könnte.

2.5 Im Bereich von Rechts- und Compliance-Risiken

Institute setzten in der individuellen Vermögensverwaltung Finanzinstrumente ein oder wendeten Anlagetechniken an, die für die betroffenen Kunden und Kundinnen ungeeignet waren oder nicht den Vereinbarungen entsprachen.

Institute, die u.a. Vermögensverwaltungsdienstleistungen für individuelle Kunden erbringen, berücksichtigten bei den gemäss Geldwäschereigesetzgebung vorgeschriebenen Risikoanalysen den Wohnsitz der Zielkunden ungenügend.

Institute verfügten wohl über eine interne Richtlinie für *Cross-Border*-Tätigkeiten und entsprechende Länderhandbücher. Allerdings wurden die in diesen Dokumenten vorgesehenen Kontrollen und Zuständigkeiten nicht oder nur mangelhaft durchgeführt und eingehalten.

2.6 Im Bereich ausgelagerter wesentlicher Tätigkeiten

Bei der Auswahl der Dienstleister, an die das operative Risikomanagement ausgelagert werden sollte, wurde zu wenig Gewicht auf die Kenntnisse und Erfahrungen dieser Dienstleister im Bereich des Managements operationel-

[3] s. www.finma.ch > Dokumentation > FINMA-Aufsichtsmitteilungen

[4] vgl. Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bei Verletzungen der Datensicherheit gemäss Art. 24 Datenschutzgesetz (DSG), s. Online-Dienst zur Meldung von Datensicherheitsverletzungen (Art. 24 DSG)

ler Risiken gelegt (vgl. Rz 16–21 FINMA-Rundschreiben 2018/3 „Outsourcing“[5] zu den Anforderungen an die Auswahl, Instruktion und Kontrolle von Dienstleistern).

Ausgelagerte Tätigkeiten wurden nicht oder nicht korrekt erfasst (vgl. Rz 14–15.1 FINMA-RS 18/3 zur Inventarisierung der ausgelagerten Funktionen). Dadurch entstanden Kontrolllücken, oder diese ausgelagerten Tätigkeiten wurden ungenügend in das Management der operationellen Risiken einbezogen.

3 Allgemeine Anforderungen an das Risikomanagement

3.1 Risikomanagement allgemein

Zur Vermeidung der vorgenannten und ähnlichen Schwachstellen und Mängel ruft die FINMA den Fondsleitungen und den Verwaltern von Kollektivvermögen deshalb die allgemeinen Anforderungen an ein angemessenes Risikomanagement in Erinnerung.

Das Organ für Oberleitung, Aufsicht und Kontrolle legt die Grundsätze des Managements aller wesentlichen Risiken, denen das Institut mit seiner Geschäftstätigkeit sowie die von ihm verwalteten Vermögen ausgesetzt sind, in internen Richtlinien fest. Es hat auch die Risikotoleranz zu bestimmen.

Basierend auf den Vorgaben des Organs für die Oberleitung, Aufsicht und Kontrolle hat das Organ für die Geschäftsführung geeignete Richtlinien, Verfahren sowie Prozesse für die Identifikation, die Beurteilung, die Steuerung und die Kontrolle der Risiken zu entwickeln. Es muss weiter die dafür zuständigen und verantwortlichen Funktionen oder Personen bezeichnen sowie eine angemessene periodische Berichterstattung an das Organ für die Oberleitung, Aufsicht und Kontrolle sicherstellen.

Die Organe für die Oberleitung, Aufsicht und Kontrolle und für die Geschäftsführung haben ihre Grundsätze, die Risikotoleranz, die Richtlinien, Verfahren und Prozesse für das Risikomanagement regelmässig auf Angemessenheit und Wirksamkeit zu überprüfen, insbesondere jedoch bei Änderungen der Geschäftstätigkeit oder der Organisation.

[5] s. www.finma.ch > Dokumentation > Rundschreiben

3.2 Management der operationellen Risiken als Teil des Risikomanagements

Die operationellen Risiken gehören zu den wesentlichen Risiken von Fondsleitungen und Verwaltern von Kollektivvermögen sowie der von ihnen verwalteten Vermögen. Entsprechend gelten die vorstehend genannten Anforderungen auch für das Management der operationellen Risiken. Insbesondere in personeller Hinsicht bedeutet das, dass die mit dem Management der operationellen Risiken betrauten Personen über die dafür erforderlichen Kenntnisse und Erfahrungen verfügen müssen.

4 Management der operationellen Risiken

4.1 Allgemeine Grundsätze für das Management der operationellen Risiken und seine Organisation

Voraussetzung für ein effektives institutsweites Management der operationellen Risiken ist die Berücksichtigung der tatsächlichen Geschäftstätigkeit und Organisation des Instituts. Zu beachten sind dabei insbesondere die für die Erbringung dieser Geschäftstätigkeit angewendeten Verfahren und Prozesse sowie die eingesetzten personellen und technischen Ressourcen und erforderlichen Daten.

Bei der Ausgestaltung der operativen Prozesse und Verfahren hat das Institut angemessene Massnahmen und Kontrollen vorzusehen (z.B. durch Anwendung des Vier-Augen-Prinzips), um deren Effektivität und Zuverlässigkeit sicherzustellen.

4.2 Spezifische Elemente des Managements der operationellen Risiken

4.2.1 Risiken der Informations- und Kommunikationstechnologie

Basis für ein effektives Management der Risiken der Informations- und Kommunikationstechnologie ist ein Inventar der wesentlichen Hardware- und Software-Komponenten, die vom Institut in den Prozessen und Verfahren zur Erbringung seiner wesentlichen Tätigkeiten verwendet werden.

Für diese wesentlichen Hardware- und Software-Komponenten legt das Institut die Risikotoleranz fest und ergreift die für die Sicherstellung der definierten Verfügbarkeit, Vertraulichkeit und Integrität nötigen Massnahmen.

4.2.2 Risiken hinsichtlich kritischer Daten

Die Daten, die besonders schutzwürdig (z.B. Kundendaten) oder für die Tätigkeit des Instituts kritisch sind, sind zu identifizieren und zur Wahrung ihrer Verfügbarkeit, Vertraulichkeit und Integrität sind angemessene Schutzmassnahmen zu treffen.

Dazu gehört auch, dass die Aufgaben, Zuständigkeiten und Verantwortlichkeiten wie auch die Kontrollen im Umgang mit den kritischen Daten klar festzulegen sind.

4.2.3 Cyber-Risiken

Ausgehend von seinen Geschäftstätigkeiten und seiner Organisation hat ein Institut zu analysieren und identifizieren, welches die möglichen Bedrohungen durch Cyber-Angriffe sind. Entsprechend ergreift es geeignete Schutzmassnahmen und stellt die Überwachung seiner Informations- und Kommunikations-Infrastruktur sicher.

Regelmässige Schulungen und Sensibilisierungen der Mitarbeitenden über den Umgang mit Cyber-Risiken werden erwartet.

Für den Fall eines erfolgreichen oder zumindest teilweise erfolgreichen Cyber-Angriffs hat das Institut Massnahmen vorzusehen, um den ordentlichen Geschäftsbetrieb zeitnah wieder aufnehmen zu können. Zudem hat es sicherzustellen, dass es seinen Meldepflichten für Cyber-Attacken ordnungsgemäss nachkommt.[6]

Wichtig ist gerade auch im Umgang mit Cyber-Risiken, dass das Institut die Aufgaben, Zuständigkeiten und Verantwortlichkeiten klar geregelt hat und dabei auch die allfällige Kommunikation insbesondere mit betroffenen Kundinnen und Kunden, Geschäftspartnern sowie gegebenenfalls weiteren Personen berücksichtigt.

4.2.4 *Business Continuity Management*

Ein Institut hat einen seinen Geschäftstätigkeiten und seiner Organisation entsprechenden Business Continuity Plan zur Aufrechterhaltung und Wiederherstellung der für den Geschäftsbetrieb wesentlichen Prozesse und Verfahren in Krisenfällen zu erstellen.

Wichtig ist, dass der Business Continuity Plan periodisch überprüft und gegebenenfalls aktualisiert wird. Eine Überprüfung und allfällige Aktualisierung

[6] Vgl. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG und FINMA-Aufsichtsmitteilung 05/2020 (s. Fn 3) sowie Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bei Verletzungen der Datensicherheit gemäss Art. 24 Datenschutzgesetz (DSG; SR **235.1**) (s. Fn 4).

des Business Continuity Plans ist zudem immer dann angezeigt, wenn Änderungen der Geschäftstätigkeiten und der Organisation vorgenommen werden.

Business Continuity Pläne sind periodisch zu testen, insbesondere bei Instituten mit umfangreichen oder komplexen Geschäftstätigkeiten.

Es ist schliesslich wichtig, dass ein Institut über eine klare Kommunikationsstrategie für Notfälle verfügt und klare Aufgaben und Zuständigkeiten bestimmt hat.

4.2.5 Management der Rechts- und Compliance-Risiken insbesondere aus dem *Cross-Border*-Geschäft

Falls ein Institut Dienstleistungen grenzüberschreitend erbringen oder Finanzinstrumente grenzüberschreitend vertreibt, muss es sicherstellen, dass es die sich daraus ergebenden Risiken angemessen erfasst, begrenzt und kontrolliert.

Das Institut muss sein grenzüberschreitendes Dienstleistungsgeschäft sowie den grenzüberschreitenden Vertrieb von Finanzinstrumenten einer Analyse der rechtlichen Rahmenbedingungen und der damit verbundenen Risiken unterziehen und die nötigen Massnahmen zur Risikominderung treffen.

Die relevante Rechtslage in den entsprechenden Ländern ist dauernd zu verfolgen, und die erfolgten Massnahmen zur Risikominderung sind bei Bedarf anzupassen.

4.2.6 Management der operationellen Risiken bei Auslagerungen

4.2.6.1 Auslagerung des Risikomanagements und der Compliance

Die Massnahmen zum Management der operationellen Risiken hat das Institut auch bei einer allfälligen Auslagerung des Risikomanagements und der Compliance an Dritte sicherzustellen. Entsprechend hat das Institut bei der Auswahl der mit dem Risikomanagement zu beauftragenden Dritten auch auf deren Kenntnisse und Erfahrung im Bereich des Managements der operationellen Risiken zu achten.

4.2.6.2 Auslagerung wesentlicher Tätigkeiten

Lagert das Institut andere für seine Geschäftstätigkeiten wesentliche Tätigkeiten an Dritte aus oder bezieht es von Dritten Ressourcen, die für wesentliche Verfahren und Systeme erforderlich sind, muss es die Anforderungen

gemäss FINMA-RS 18/3[7] sicherstellen (insbesondere hinsichtlich Inventarisierung der ausgelagerten Funktionen, Auswahl, Instruktion und Kontrolle des Dienstleisters). Das Institut hat auch dafür zu sorgen, dass die ausgelagerten Funktionen in das Management der operationellen Risiken einbezogen werden.

[7] s. Fn 5