finma
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

Prüfpunkte zum Management der Cyber-Risiken Fondsleitungen und Verwalter Kollektivvermögen

Übersicht

Prüffeld:	**Management der Cyber-Risiken**
Prüftiefe:	[Prüfung / Kritische Beurteilung]
Grundlagen: (Liste ist nicht abschliessend[1])	Art. 9 Bundesgesetz vom 15. Juni 2018 über die Finanzinstitute (FINIG; SR *954.1*) Art. 20 Bundesgesetz vom 23. Juni 2006 über die kollektiven Kapitalanlagen (KAG; SR *951.31*) Art. 12, 41, 48, 57, 63 Finanzinstitutsverordnung vom 6. November 2019 (FINIV; SR *954.11*)
Sign-offs:	

Sign-offs:	**Name:**	**Funktion:**	**Datum:**
Prüfer:	[Name]	[Assistant / Senior / Manager / Senior Manager / Direktor / Partner]	[TT. MM JJJJ]
Reviewer:	[Name]	[Senior / Manager / Senior Manager / Direktor / Partner]	[TT. MM JJJJ]

Dies ist ein Standard-Prüfprogramm, welches bei jeder Intervention gemäss Prüfstrategie grundsätzlich anzuwenden ist. Es liegt in der Verantwortung des Prüfteams, das Standard-Prüfprogramm an die spezifische Situation (Grösse, Geschäftsmodell, Organisation, Prozesse, Risikoexposition usw.) des geprüften Instituts anzupassen. Werden die angegebenen Prüfungshandlungen nicht vollständig durchgeführt, ist in den Arbeitspapieren eine aussagekräftige Erläuterung dazu anzubringen.

Der Prüfpunkt 9* kann ausgeklammert werden, wenn das geprüfte Institut keine schützenswerten und/oder kritische Daten bearbeitet.[2]

Die Prüfhandlungen zu den Prüfpunkten 9–14 (Schutzdispositiv, Aufzeichnung und Erkennung, Reaktion) sind grundsätzlich nach den identifizierten Cyber-Bedrohungen in der spezifischen Situation auszurichten. Dies kann beispielsweise den Umfang der Bearbeitung von schützenswerten und/oder kritischen Daten, vorhandenen Schnittstellen und/oder den Betrieb kritischer Systeme (bspw. für die Fondsadministration oder das Portfolio

[1] Vgl. auch die FINMA-Aufsichtsmitteilungen 05/2020 „Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG“, 03/2024 „Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen“ und 04/2024 „Management der operationellen Risiken von Fondsleitungen und Verwaltern von Kollektivvermögen“.
[2] Vgl. Ziff. 4.2.2 Aufsichtsmitteilung 04/2024.

Management) im Einzelfall umfassen. Bei einer weitgehenden Delegation des IT Betriebs an Dienstleister ist insbesondere die Definition/Ausgestaltung, Sicherstellung und Überwachung der jeweiligen Inhalte durch das Institut im Fokus der Prüfhandlungen.

finma
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

Abschliessende Zusammenfassung

<table>
<tr><th>Thema:</th><th>Information / Beschreibung:</th></tr>
<tr><td>Zusammenfassende Gesamtbeurteilung</td><td>
<table>
<tr><th>Bestätigung im Prüfbericht:</th><th>Zusammenfassung:</th></tr>
<tr><td>Die Ausgestaltung der Prozesse und Massnahmen zur Erkennung und Minimierung von Cyber-Risiken sowie Meldung von Cyber-Attacken ist hinsichtlich Art und Umfang der Geschäftstätigkeit angemessen.</td><td>Ja (Prüfung / kritische Beurteilung) / Nein</td></tr>
<tr><td>Bestätigung, dass der Beaufsichtigte die durch die in Einzelfall spezifisch angeordneten Massnahmen der FINMA eingehalten hat.</td><td>Ja (Prüfung / kritische Beurteilung) / Nein</td></tr>
</table>
</td></tr>
<tr><td>Zusammenfassung der Prüfresultate / Beanstandungen und Empfehlungen (ausführliche Informationen nachstehend)</td><td>[Zusammenfassung der Prüfresultate / Beanstandungen und Empfehlungen]</td></tr>
<tr><td>Prüffelder, Prüfresultate und durchgeführte Prüfungshandlungen der internen Revision, auf die sich die Prüfgesellschaft gestützt hat (einschliesslich der Würdigung durch die Prüfgesellschaft)</td><td>[Beschreibung]</td></tr>
</table>

finma
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

Prüfprogramm: Management der Cyber-Risiken

Nr.	Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:	<u>Zusätzliche</u> Prüfungshandlungen für Prüftiefe „Prüfung“:	Durchgeführte Prüfungshandlungen / Feststellungen	Arbeitspapiere Ref.:
Management der Cyber-Risiken unter Berücksichtigung des Proportionalitätsprinzips, d. h. unter Berücksichtigung der Grösse, Komplexität (insbesondere hinsichtlich IKT und Outsourcing) sowie Struktur und Risikoprofil				
1	Aneignung grundlegender Kenntnisse über den übergreifenden Umgang des Instituts mit Cyber-Risiken unter Berücksichtigung des Proportionalitätsprinzips und den folgenden Prüfungshandlungen.			
Governance und Strategie				
2	Beurteilung der Konsistenz und Angemessenheit interner Vorgaben (bspw. Reglemente, Richtlinien, Weisungen) in Bezug auf das Management der Cyber-Risiken.	Prüfung der inhaltlichen Abstimmung der Strategie im Umgang mit Cyber-Risiken mit anderen internen Vorgaben (bspw. IT-Strategie, Cyber-Strategie, Risikopolitik).		
3	Beurteilung, ob das Oberleitungsorgan regelmässig die Risikotoleranz für Cyber-Risiken nach Massgabe der Risikopolitik und in Anbetracht der strategischen und finanziellen Ziele des Instituts beurteilt.			
4	Beurteilung der Angemessenheit der durchgeführten Schulungen zum Thema Cyber-Sicherheit im Hinblick auf cyber- und/oder institutsspezifische Bedrohungslagen und angemessene zielgruppenspezifische Ausrichtung der Schulung.			
5	Beurteilung der Angemessenheit der Berichterstattung an die Geschäftsleitung, sowie von der Geschäftsleitung an das Organ für die Oberleitung, Aufsicht und Kontrolle (bspw. Inhalt, Regelmässigkeit usw.) über die Entwicklung von Cyber-Risiken sowie die Wirksamkeit von relevanten Cyber-Kontrollen.			
Aufgaben, Kompetenzen und Verantwortlichkeiten				
6	Beurteilung einer eindeutigen Festlegung der Aufgaben, Zuständigkeiten und Verantwortlichkeiten innerhalb der Cyber-Organisation (bspw. in Hinblick auf Rollenbeschreibung, der Organisation, Funktionsabgrenzung, Berichtslinien und Kommunikationswege).			
Identifikation				
7	Beurteilung, ob die Bestandteile der IKT, sowie die Schnittstellen mit Dritten, identifiziert, katalogisiert und bewertet sind.	Prüfung auf Basis einer angemessenen Stichprobe von Schlüsselkontrollen zur Sicherstellung der Vollständigkeit und Richtigkeit der Inventare. Beispielsweise sind zu berücksichtigen: • Hardware-Komponenten, • Software-Komponenten: Applikationen (inkl. Abhängigkeiten),		
8	Beurteilung, ob die Bestandteile der IKT nach ihrer Kritikalität und ihrem Schutzbedürfnis in der Netzwerkinfrastruktur angemessen abgebildet sind.			

		• Software-Komponenten: Endbenutzersoftware (inkl. Versionierung), • Bewertung der Kritikalität, • Ablageort kritischer Daten, • Schnittstellen zu wesentlichen externen Dienstleistern.		
Schutzdispositiv				
9*	Beurteilung der Angemessenheit der organisatorischen und technischen Massnahmen gegen den unautorisierten Abfluss von kritischen und/oder schützenswerten Daten (*Data Loss Prevention*).			
10	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen zur Steuerung der Netzwerksicherheit (bspw. Zonierung, *Network Access Control* [NAC], *Firewall*, *Web Application Firewall* [WAF], Schutz vor DDoS, *Proxyserver*).			
11	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen zur Steuerung der Infrastruktursicherheit (z.B. *Endpoint Detection & Response* [bzw. XDR], Anti-Virus usw.).			
12	Beurteilung des risikoorientierten Ansatzes zur zeitnahen Schliessung von Sicherheitslücken (*Patching*) bzw. Adressierung von Fehlkonfigurationen (Konfigurationsänderung) in Systemen, Anwendungen oder zugrundeliegender Infrastruktur.	Prüfung der operativen Wirksamkeit der Massnahmen zur Schliessung von hohen oder kritischen Sicherheitslücken bei kritischen Systemen auf Basis einer angemessenen Stichprobe.		
Aufzeichnung und Erkennung				
13	Beurteilung, ob Auffälligkeiten (z.B. abnormes Verhalten) und sicherheitsrelevante Ereignisse zeitgerecht mit der Hilfe einer durchgängigen Überwachung der IKT erkannt werden und potenzielle Auswirkungen dieser Ereignisse angemessen beurteilt werden.	Prüfung auf Basis einer angemessenen Stichprobe, ob alle kritischen inventarisierten Bestandteile der IKT sowie Geschäftsapplikationen Log-Daten an ein zentrales System liefern und diese entsprechend analysiert werden, um Cyber-Vorfälle zu erkennen.		
Reaktion				
14	Beurteilung der Angemessenheit der Prozesse und Massnahmen zur Reaktion auf Cyber-Attacken (z.B. sog. *Playbooks*), deren Klassifizierung und Eskalation sowie Schadensminderung.			
15	Berücksichtigung der in den FINMA-Aufsichtsmitteilungen 05/2020 und 03/2024 wiedergegebenen Punkte	Prüfung der operativen Wirksamkeit auf Basis einer angemessenen Stichprobe von teilweise erfolgreichen bzw. erfolgreichen Cyber-Attacken und ob der Meldeprozess (vgl. FINMA-Aufsichtsmitteilung 05/2020) eingehalten wurde.		
Wiederherstellung				
16	Beurteilung der Angemessenheit der Wiederherstellungsprozesse, so dass eine zeitnahe Wiederherstellung der Systeme nach einer Cyber-Attacke gewährleistet werden kann.	*Prüfung auf Basis einer angemessenen Stichprobe von dokumentierten Massnahmen, ob die bei einer Cyber-Attacke durchzuführenden Wiederherstellungsprozesse mittels*		

		angemessener Tests (sog. Walk-Throughs, Table-Top-Übungen) verifiziert wurden.		

****