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

Übersicht

Prüfgebiet:	**Management der Cyber-Risiken**
Prüftiefe:	[Prüfung / Kritische Beurteilung][1]
Grundlagen: (Liste ist nicht abschliessend)	Art. 3 Abs. 2 Bst. a Bankengesetz (BankG) Art. 9 Finanzinstitutsgesetz (FINIG) Art. 12 Bankenverordnung (BankV) Art. 12, 67 und 68 Finanzinstitutsverordnung (FINIV) Rz 13, 50, 52, 53, 58, 59 FINMA-Rundschreiben 2017/1 „Corporate Governance – Banken“ Rz 23–26, 40, 61–70, 104 FINMA-Rundschreiben 2023/1 „Operationelle Risiken und Resilienz – Banken“
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 (Rz 28ff FINMA-Rundschreiben 2013/3 „Prüfwesen“) 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. Die mit einem Stern (*) markierten Prüfungshandlungen sind bei allen Banken der Aufsichtskategorien 4 und 5 nicht anwendbar.

[1] Rz 33 und 34 FINMA-RS 13/3

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>Bestätigung, dass der Bereich „Management der Cyber-Risiken“ angemessen ausgestaltet war.</td><td>Ja (Prüfung / kritische Beurteilung) / Nein</td></tr>
<tr><td>Bestätigung, dass der Beaufsichtigte die durch die FINMA angeordneten Verschärfungen 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.			
2	Beurteilung der 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. Risikopolitik, Grundzüge des institutsweiten Risikomanagements, operationelles Risikomanagement, Geschäfts-, IKT- bzw. Daten-Strategie).		
Integration in das übergreifende operationelle Risikomanagement bzw. Strategie, Governance und Bewusstsein (Rz 23–26, 30, 40, 61 FINMA-RS 23/1)				
3	Beurteilung, ob die Cyber-Risiken als eigenständige Taxonomie in das übergreifende operationelle Risikomanagement integriert sind und dadurch umfassend, d. h. im Rahmen der Identifikation, Beurteilung, Begrenzung und Überwachung von operationellen Risiken angemessen berücksichtigt werden.	Prüfung auf Basis einer angemessenen Stichprobe von Anwendungen der Risikosteuerungsinstrumente (bspw. Risikotoleranz, Prüfergebnisse sowie Risiko- und Kontrollbeurteilungen gemäss Rz 30) für den Bereich Cyber-Risiken.		
4	Beurteilung, ob das Oberleitungsorgan mindestens jährlich die Risikotoleranz für Cyber-Risiken nach Massgabe der Risikopolitik und in Anbetracht der strategischen und finanziellen Ziele des Instituts beurteilt und genehmigt.			
5	Beurteilung, ob das Oberleitungsorgan für den Umgang mit Cyber-Risiken regelmässig eine Strategie genehmigt und deren Einhaltung überwacht.			
6	Beurteilung, ob die Identifikation von wesentlichen, inhärenten Risiken in Bezug auf Cyber-Risiken angemessen ist, d. h., falls Cyber-Risiken nicht als wesentliche, inhärente Risiken identifiziert sind, ist die Nachvollziehbarkeit der Begründung hierfür zu beurteilen.	Prüfung auf Basis einer angemessenen Stichprobe von Elementen zur Identifikation von wesentlichen Cyber-Risiken und Beurteilung, ob potenzielle Risiken im Zusammenhang mit Cyber-Risiken erkannt und berücksichtigt werden, und ob die Beurteilung der Wesentlichkeit der inhärenten Risiken der Risikotoleranz entspricht.		
7	Beurteilung der organisatorischen und technischen Massnahmen zur Stärkung des Bewusstseins der Mitarbeitenden im Hinblick auf ihre Aufgaben, Kompetenz und Verantwortlichkeiten zur allgemeinen Reduktion von Cyber-Risiken.			

Nr.	Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:	Zusätzliche Prüfungshandlungen für Prüftiefe „Prüfung“:	Durchgeführte Prüfungshandlungen / Feststellungen	Arbeitspapiere Ref.:
8	Beurteilung der Angemessenheit der durchgeführten Schulungen zum Thema Cybersicherheit im Hinblick auf cyber- und/oder institutsspezifische Bedrohungslagen und angemessene zielgruppenspezifische Ausrichtung der Schulung (z.B. für Führungskräfte, Mitarbeitende mit privilegierten bzw. erhöhten Berechtigungen, Mitarbeitende mit Zugriff auf kritische Daten, externes Personal [inkl. Contractors] usw.).	Prüfung der operativen Wirksamkeit der Kontrollen zur (regelmässigen) Schulung der Mitarbeitenden sowie von Schlüsselmitarbeitenden und Dritten im Bereich Cyber-Sicherheit auf Basis einer angemessenen Stichprobe.		
9	Beurteilung der Angemessenheit der Berichterstattung an die Geschäftsleitung (bspw. Inhalt, Regelmässigkeit usw.) über die Entwicklung der Cyber-Risiken, die Wirksamkeit von Schlüsselkontrollen und die wesentlichen internen sowie externen Ereignissen.			
10	Beurteilung der Erkenntnisse aus den Prüfungen bzw. Kontrollen der Internen Revision und/oder anderer Kontrollfunktionen (bspw. unabhängige Risikokontrolle) im Zusammenhang mit der Ausgestaltung der Cyber-Sicherheit und Durchsicht der Sitzungsprotokolle von relevanten Ausschüssen bzw. Funktionen.			
Aufgaben, Kompetenzen und Verantwortlichkeiten (Rz 62 FINMA-RS 23/1):				
11	Beurteilung einer eindeutigen Festlegung der Aufgaben, Kompetenzen und Verantwortlichkeiten innerhalb der Cyber-Organisation (bspw. in Hinblick auf Rollenbeschreibung, der Organisation, Funktionsabgrenzung, Berichtslinien und Kommunikationswege).			
12	Beurteilung, ob Cyber-Risiken in der Planung sowie Prüfungsdurchführung im Rahmen der unabhängigen Risikokontrolle sowie der Internen Revision angemessen berücksichtigt werden. Insbesondere sind zu beachten: Risikoanalyse und -beurteilung, Mehrjahresplanung, verwendete internationale Standards.			
13	* Beurteilung der Unabhängigkeit (vgl. Rz 62 FINMA RS 17/1) der internen Funktionen im Zusammenhang mit der Bewertung der Cyber-Sicherheitsrisikolage.			
Verfahren, Prozesse und Kontrollen (inklusive kontinuierliche Weiterentwicklung und Verbesserung) (Rz 62 FINMA-RS 23/1):				
14	Beurteilung, ob das Konzept über den Umgang mit Cyber-Risiken nach einem international anerkannten Standard bzw. Practices erstellt worden ist und die institutsspezifische Risikolage und Bedürfnisse abdeckt.	Prüfung auf Basis einer angemessenen Stichprobe, ob das Konzept über den Umgang mit Cyber-Risiken kontinuierlich auf Basis von Erkenntnissen aus Überprüfungen und Erfahrungswerten weiterentwickelt und verbessert wird.		
Identifikation (Rz 63 FINMA-RS 23/1):				

Nr.	Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:	**Zusätzliche** Prüfungshandlungen für Prüftiefe „Prüfung“:	Durchgeführte Prüfungshandlungen / Feststellungen	Arbeitspapiere Ref.:
15	Beurteilung, ob die Bestandteile der IKT (vgl. Rz 53 und 54), 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), • Software-Komponenten: Endbenutzersoftware (inkl. Versionierung), • Bewertung der Kritikalität, • Ablageort kritischer Daten, • Schnittstellen zu wesentlichen externen Dienstleistern.		
16	Beurteilung, ob eine Definition der kritischen Daten vorhanden ist, und diese Daten entsprechend inventarisiert sind (vgl. Rz 7, 53, 54).			
17	Beurteilung, ob die Bestandteile der IKT (vgl. Rz 7, 53, 54) nach ihrer Kritikalität und ihrem Schutzbedürfnis in der Netzwerkinfrastruktur angemessen abgebildet sind.			
18	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen zur Identifikation von institutsspezifischen Bedrohungspotenzialen durch Cyber-Attacken sowie zur Beurteilung von möglichen Auswirkungen durch die Ausnützung von Schwachstellen in Bezug auf die inventarisierten Bestandteile der IKT, sowie die Schnittstellen mit Dritten, und kritischen Daten (vgl. Rz 7, 53, 54).	* Prüfung auf Basis einer angemessenen Stichprobe von bestehenden Elementen des Instituts zur Identifizierung und Bewertung der Cyber-Bedrohungslage, deren Beurteilung auf die Auswirkung, der Wahrscheinlichkeit des Auftretens sowie deren Risikobewertung.		
19	Beurteilung, ob die institutsspezifischen Bedrohungspotenziale sowie die Schwachstellen, und damit die Auswirkungen von Cyber-Attacken auf die inventarisierten Bestandteile der IKT, sowie die Schnittstellen mit Dritten, und die kritischen Daten (vgl. Rz 7, 53, 54), bekannt sind und angemessen im Rahmen der Risikobeurteilung berücksichtigt werden.			
Schutzdispositiv (Rz 64 FINMA-RS 23/1):				
20	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen zur Gewährung des logischen und/oder physischen Zugangs (standardisiert sowie privilegiert) zu den inventarisierten Bestandteilen der IKT, sowie Schnittstellen mit Dritten (vgl. Rz 53, 54).	Prüfung der operativen Wirksamkeit der Kontrollen zur Gewährung des logischen und/oder physischen Zugangs zu den inventarisierten kritischen Bestandteilen der IKT sowie kritischen Schnittstellen mit Dritten (vgl. Rz 53, 54) auf Basis einer angemessenen Stichprobe.		
21	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen zur (regelmässigen) Bestätigung des logischen und/oder physischen Zugangs (standardisiert sowie privilegiert) zu den inventarisierten Bestandteilen der IKT, sowie Schnittstellen mit Dritten (vgl. Rz 53, 54).	Prüfung der operativen Wirksamkeit der Kontrollen zur (regelmässigen) Bestätigung des logischen und/oder physischen Zugangs zu den inventarisierten kritischen Bestandteilen der IKT sowie kritischen Schnittstellen mit Dritten (vgl. Rz 7, 53, 54) auf Basis einer angemessenen Stichprobe.		
22	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen zur Identifikation, Steuerung und Überwachung des logischen und/oder physischen Zugangs (standardisiert sowie privilegiert) zu	Prüfung der operativen Wirksamkeit der Kontrollen zur Identifikation, Steuerung und Überwachung des logischen		

Nr.	Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:	<u>Zusätzliche</u> Prüfungshandlungen für Prüftiefe „Prüfung“:	Durchgeführte Prüfungshandlungen / Feststellungen	Arbeitspapiere Ref.:
	den inventarisierten Bestandteilen der IKT, sowie Schnittstellen mit Dritten (vgl. Rz 53, 54).	und/oder physischen Zugangs (standardisiert sowie privilegiert) zu den inventarisierten kritischen Bestandteilen der IKT, sowie kritischen Schnittstellen mit Dritten (vgl. Rz 53, 54) auf Basis einer angemessenen Stichprobe.		
23	Beurteilung der Angemessenheit der organisatorischen und technischen Massnahmen gegen den unautorisierten Abfluss von kritischen Daten (Data Loss Prevention).	Prüfung der operativen Wirksamkeit der organisatorischen und technischen Massnahmen gegen den unautorisierten Abfluss von kritischen Daten auf Basis einer angemessenen Stichprobe.		
24	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).	Prüfung der operativen Wirksamkeit der Massnahmen zur Steuerung der Netzwerksicherheit auf Basis einer angemessenen Stichprobe.		
25	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen zur Steuerung der Infrastruktursicherheit (z.B. Endpoint Detection & Response [bzw. XDR], Anti-Virus usw.).	Prüfung der operativen Wirksamkeit der Massnahmen zur Steuerung der kritischen Infrastruktur auf Basis einer angemessenen Stichprobe.		
26	Beurteilung der Angemessenheit der Verfahren, Prozesse und Kontrollen über die Sicherstellung der Standardkonfiguration und Systemhärtung (Baseline-Konfiguration und -Hardening) der inventarisierten Bestandteile der IKT sowie deren kontinuierlichen Einhaltung.	Prüfung der operativen Wirksamkeit der Massnahmen zur Standardkonfiguration und Systemhärtung bei kritischen Systemen auf Basis einer angemessenen Stichprobe.		
27	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.		
28	Beurteilung der Angemessenheit der Vorgaben für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von gespeicherten und übertragenen kritischen Daten.	Prüfung der operativen Wirksamkeit der Massnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von gespeicherten und übertragenen kritischen Daten, z.B. durch Verschlüsselung, auf Basis einer angemessenen Stichprobe.		
Aufzeichnung und Erkennung (Rz 65 FINMA-RS 23/1):				
29	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.			
30	Beurteilung, ob Standardwerte für zulässige Netzwerkoperationen und die zu erwartenden Datenflüsse (bspw. bezogen auf Datenflüsse zwischen unterschiedlichen Netzwerkzonierungen und Schnittstellen zwischen IKT-Systemen) für Anwender und Systeme			

Nr.	Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:	Zusätzliche Prüfungshandlungen für Prüftiefe „Prüfung“:	Durchgeführte Prüfungshandlungen / Feststellungen	Arbeitspapiere Ref.:
	technisch über SIEM Use-Cases definiert sind und Beurteilung des Prozesses wie diese auf dem neuesten Stand gehalten werden.			
31	Beurteilung, ob die inventarisierten kritischen Bestandteile der IKT und deren Nutzung von Mitarbeitenden und Dritten systematisch und durchgängig überwacht wird.	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.		
32	Beurteilung der Angemessenheit der technischen Massnahmen zur Erkennung von Cyber-Vorfällen aufgrund von definierten Cyberrisiko-Szenarien (sog. Use Cases).			
33	Beurteilung, ob die Prozesse sowie Handlungsanweisungen zur Detektion von Cyber-Vorfällen regelmässig aktualisiert und getestet werden.			
Reaktion (Rz 66, 68 FINMA-RS 23/1):				
34	Beurteilung der Angemessenheit des Reaktionsplans zur Adressierung erkannter Cyber-Vorfälle, insbesondere wie dieser mit internen und externen Anspruchsgruppen abgestimmt ist und welche Unterstützung von externen Stellen im Ereignisfall notwendig ist.	Prüfung auf Basis einer angemessenen Stichprobe von Elementen, ob der Reaktionsplan im Ereignisfall oder bei einem Test effizient und zeitgerecht ausgeführt wurde.		
35	Beurteilung der Angemessenheit der Prozesse zur zeitnahen Analyse, Dokumentation und Klassifizierung von Meldungen aus den Detektionssystemen (sog. Events).	Prüfung der operativen Wirksamkeit der Prozesse zur Analyse und Klassifizierung der Meldungen aus Detektionssystemen (sog. Events).		
36	Beurteilung der Angemessenheit der Prozesse und Massnahmen (z.B. sog. Playbooks) zur Eingrenzung und Schadensminderung bei Cyber-Attacken.			
37	Beurteilung, ob die Anforderungen aus der FINMA-Aufsichtsmitteilung 05/2020 "Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG" im Reaktionsplan berücksichtigt werden.	Prüfung der operativen Wirksamkeit auf Basis einer angemessenen Stichprobe von teilweise erfolgreichen bzw. erfolgreichen Cyber-Attacken und ob der Meldeprozess nach den Anforderungen der FINMA-Aufsichtsmitteilung 05/2020 "Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG" eingehalten wurde.		
Wiederherstellung (Rz 67 FINMA-RS 23/1):				
38	Beurteilung der Angemessenheit der periodischen Beurteilung und Verbesserung von Reaktions- und Wiederherstellungsprozessen.	Prüfung der operativen Wirksamkeit auf Basis einer angemessenen Stichprobe, ob bei vergangenen Vorfällen entsprechende Lehren dokumentiert und umgesetzt wurden.		
39	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 Elementen, ob die Wiederherstellungsprozesse nach einer Cyber-Attacke durch angemessene Tests (sog. Walk-Throughs, Table-Top-Übungen) verifiziert wurden.		

Nr.	Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:	Zusätzliche Prüfungshandlungen für Prüftiefe „Prüfung“:	Durchgeführte Prüfungshandlungen / Feststellungen	Arbeitspapiere Ref.:
Verwundbarkeitsanalysen, Penetrationtests und risikobasierte szenariobezogene Cyber-Übungen (Rz 69, 70 FINMA-RS 23/1):				
40	Beurteilung der Angemessenheit der Prozesse zur regelmässigen Durchführung von Verwundbarkeitsanalysen, Penetrationtests und szenariobasierten Cyber-Übungen auf Basis von institutsspezifischen Bedrohungspotenzialen.			
41	Beurteilung, ob Verwundbarkeitsanalysen und Penetrationtests regelmässig auf allen Bestandteilen der IKT, die über das Internet erreichbar sind, und mindestens bei Systemen, welche für die Erbringung von kritischen Prozessen notwendig sind bzw. kritische Daten beinhalten, durchgeführt werden.			
42	Beurteilung der Angemessenheit der institutsspezifischen Vorgaben und Prozesse zum Umgang mit erkannten Schwachstellen und deren risikobasierten Behebung.	Prüfung auf Basis einer angemessenen Stichprobe, ob hohe und kritische Schwachstellen aus Verwundbarkeitsanalysen und Penetrationtests innerhalb der definierten Vorgaben geschlossen wurden.		
43	Beurteilung der Angemessenheit der technischen und personellen Ressourcen, welche die Anordnung, Durchführung sowie die risikobasierte Durchführung von Verwundbarkeitsanalysen, Penetrationtests sowie die szenariobasierten Cyber-Übungen sicherstellen.			
44	Beurteilung, ob die Ergebnisse von Cyber-Übungen in geeigneter Form dokumentiert und rapportiert werden.			

****