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

Anpassung des FINMA-Rundschreibens 2013/3 „Prüfwesen“ vom 6. Dezember 2012, Anhörung vom 10. Mai bis 11. Juli 2022

Folgende Prüfgebiete bzw. -felder weichen von der Anwendung gemäss Rz 87.2–90 ab:	91*
• Interne Organisation und internes Kontrollsystem~~, Informatik (IT)~~: Graduelle Abdeckung der Themen über sechs Jahre mit einer im Ermessen der Prüfgesellschaft liegenden Prüftiefe.	97*
• Management der Informations- und Kommunikationstechnologie-Risiken (IKT-Risiken): Graduelle Abdeckung der Themen über vier Jahre mit einer im Ermessen der Prüfgesellschaft liegenden Prüftiefe.	97.1
~~Anträge an die FINMA für eine reduzierte Prüfkadenz im Sinne von Rz 113.2 können frühestens ab Zeitpunkt des Inkrafttretens von Art. 63 Abs. 2 FINIG (Finanzinstitutsgesetz, BBl 2018 3557; für Beaufsichtigte nach dem Finanzinstitutsgesetz) bzw. nach Aufhebung der jährlichen aufsichtsrechtlichen Prüfpflichten gemäss Art. 110 Abs. 1 und 2 KKV-FINMA (für Beaufsichtigte nach dem Kollektivanlagegesetz) gestellt werden.~~ Aufgehoben	150*

1. Anhang 2 „Standardprüfstrategie - Banken / Wertpapierhäuser“

ID	Prüfgebiete / Prüffelder / Themen	Prüftiefe / Periodizität (gemäss Standardprüfstrategie)
PS.IOK.~~INF~~IKT	Management der Informations- und Kommunikationstechnologie (IKT)-Risiken~~Informatik (IT)~~	Graduelle Abdeckung der Elemente über ~~6~~ 4 Jahre (Prüftiefe nach Ermessen der Prüfgesellschaft)
PS.IOK.CYB	Management der Cyber-Risiken	Keine Intervention falls Nettorisiko tief; Prüfung alle 6 Jahre falls Nettorisiko mittel; Intervention alle 3 Jahre falls Nettorisiko hoch (abwechselnd kritische Beurteilung - Prüfung); Jährliche Prüfung falls Nettorisiko sehr hoch

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

PS.IOK.~~EKD~~DAT	Management der Risiken kritischer Daten-~~Umgang mit elektronischen Kundendaten~~	Keine Intervention falls Nettorisiko tief; Prüfung alle 6 Jahre falls Nettorisiko mittel; Intervention alle 3 Jahre falls Nettorisiko hoch (abwechselnd kritische Beurteilung - Prüfung); Jährliche Prüfung falls Nettorisiko sehr hoch
PS.IOK.RES	Operationelle Resilienz	Keine Intervention falls Nettorisiko tief; Prüfung alle 6 Jahre falls Nettorisiko mittel; Intervention alle 3 Jahre falls Nettorisiko hoch (abwechselnd kritische Beurteilung - Prüfung); Jährliche Prüfung falls Nettorisiko sehr hoch
PS.IOK.~~QOR~~ORM	~~Qualitative~~ Generelle Anforderungen an das Management der operationelle~~n~~ Risiken	Keine Intervention falls Nettorisiko tief; Prüfung alle 6 Jahre falls Nettorisiko mittel; Intervention alle 3 Jahre falls Nettorisiko hoch (abwechselnd kritische Beurteilung - Prüfung); Jährliche Prüfung falls Nettorisiko sehr hoch

2. Anhang 13 „Risikoanalyse Banken und Wertpapierhäuser“

ID	Prüfgebiete / Prüffelder / Themen
RA.IOK.~~INF~~IKT	Management der Informations- und Kommunikationstechnologie (IKT)-Risiken~~Informatik (IT)~~
RA.IOK.CYB	Management der Cyber-Risiken
RA.IOK.~~EKD~~DAT	Management der Risiken kritischer Daten~~Umgang mit elektronischen Kundendaten~~
RA.IOK.RES	Operationelle Resilienz
RA.IOK.~~QOR~~ORM	Generelle ~~Qualitative~~ Anforderungen an das Management operationeller Risiken