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

Wegleitung

für **Prüfgesellschaften** von **Banken, Wertpapierhäusern und Finanzgruppen**
zur Durchführung der Aufsichtsprüfung

Ausgabe vom 2. Februar 2024

Zweck

Diese Wegleitung versteht sich als Hilfestellung für aufsichtsrechtliche Prüfgesellschaften von Banken, Wertpapierhäusern und Finanzgruppen zur Bearbeitung der folgenden in der Aufsichtsprüfung zu verwendenden Erhebungsformulare: Risikoanalyse, Standardprüfstrategie und aufsichtsrechtlicher Prüfbericht. Sie enthält ausserdem Hinweise zur Prüfungsdurchführung.

I. Allgemeine Ausführungen

- Die Ausgestaltung dieser Wegleitung sowie der vorgenannten Erhebungsformulare basieren auf dem FINMA-Rundschreiben 2013/3 „Prüfwesen“.
- Die FINMA stellt der Prüfgesellschaft für jedes zu prüfende Institut separate Erhebungsformulare auf der elektronischen Erhebungs- und Gesuchsplattform (nachfolgend „EHP“)[1] zur Verfügung. Somit erfasst die Prüfgesellschaft die Risikoanalyse, die Prüfstrategie und die aufsichtsrechtliche Berichterstattung direkt in den ihr elektronisch zugestellten Erhebungsformularen auf der EHP. Die Einreichung der Formulare erfolgt ebenfalls elektronisch via die entsprechende Funktion auf der EHP, wobei der aufsichtsrechtliche Prüfbericht unterzeichnet einzureichen ist (vgl. Ziff. IV Aufsichtsrechtliche Berichterstattung).
- Bei Instituten ohne Konzernaspekte wird nur der Teil „Einzelstufe“ ausgefüllt. Bei Vorliegen einer Stammhausstruktur wird der Teil „Konsolidierte Aufsicht“ auch ausgefüllt, wodurch grundsätzlich Einzel- und Konzernaspekte in einem Formular adressiert werden. Bei Vorliegen einer Holdingstruktur bzw. atypischen Struktur wird lediglich der Teil „Konsolidierte Aufsicht“ (Gruppenstufe) ausgefüllt, wodurch in solchen Fällen – unter Berücksichtigung der Aspekte für

[1] vgl. www.finma.ch > FINMA > Extranet > Erhebungs- und Gesuchsplattform;
Login: https://portal.finma.ch/auth-login/portal?lang=de

den Bewilligungsträger auf Einzelstufe – mindestens zwei Formulare einzureichen sind. Die auszufüllenden Teile der Formulare werden in Abhängigkeit der getroffenen Auswahl im Erhebungsformular (Stammdaten) angezeigt.

- Falls Anpassungen oder Ergänzungen in bereits eingereichten Formularen notwendig werden, kann dies der jeweiligen FINMA-Ansprechperson mitgeteilt werden. Die Formulare erhalten anschliessend den Status „in Korrektur“ und sind nach den Anpassungen/Ergänzungen erneut einzureichen.
- Allfällige in den einzelnen Erhebungsformularen aufgeführte Erläuterungen und Hinweise werden von der Prüfgesellschaft bei der Bearbeitung der entsprechenden Formulare ebenfalls berücksichtigt.
- Die mit Stern (*) gekennzeichneten Felder stellen Pflichtfelder dar und sind vor Einreichung der Erhebung zwingend auszufüllen.
- Ist im Erhebungsformular das Prüfjahr anzugeben, so bezieht sich diese vierstellige Jahreszahl auf den Beginn des Prüfjahres.
- Allgemeine Informationen zur EHP, beispielsweise betr. Bearbeitung und Einreichung eines Erhebungsformulars, Status einer Erhebung oder Berechtigungsverwaltung, finden sich auf der Internetseite der FINMA[2].

II. Risikoanalyse Banken und Wertpapierhäuser

- Die relevanten Risiken innerhalb eines Prüfgebietes bzw. Prüffeldes werden konkret, spezifisch auf das Institut bezogen und, falls möglich, unter Angaben von belegenden Daten beschrieben (**„Beschreibung des Risikos“**).
- Bei auf ein einzelnes Institut nicht anwendbaren Prüfaspekten sieht die Prüfgesellschaft mit der entsprechenden Begründung von der Behandlung dieses Prüfgebietes bzw. Prüffeldes ab. Die Begründung wird bei **„Beschreibung des Risikos“** angebracht und bei **„Ausmass / Umfang“** entsprechend „n / a“ gewählt.
- Bei **„Ausmass / Umfang**“ gibt die Prüfgesellschaft eine Einschätzung darüber ab, in welchem Ausmass bzw. Umfang der Bewilligungsträger bzw. die Gruppe betroffen wäre, wenn sich die identifizierten Risiken manifestieren. Bei **„Eintrittswahrscheinlichkeit“** gibt die Prüfgesellschaft eine subjektive Einschätzung pro identifiziertes Risiko ab.
- Die Verknüpfung zwischen Ausmass / Umfang und der Eintrittswahrscheinlichkeit des Risikos pro Prüfgebiet bzw. Prüffeld bestimmt das **„inhärente Risiko (brutto)“**.
- Bei **„Kontrollrisiko“** gibt die Prüfgesellschaft eine Einschätzung zur Angemessenheit und die Wirksamkeit der internen Kontrollen ab. Es gelten die Vorgaben nach Rz 80 ff. FINMA-RS 13/3.

[2] vgl. www.finma.ch > FINMA > Extranet > Erhebungs- und Gesuchsplattform > Support

- Aus der Verknüpfung von inhärentem Risiko (brutto) und dem Kontrollrisiko ergibt sich schliesslich das kombinierte Risiko (netto) bei **„Nettorisiko“**. Die Bestimmung des Nettorisikos erfolgt im Erhebungsformular automatisch gemäss der Systematik nach Rz 85 FINMA-RS 13/3.
- Die Prüfgesellschaft ordnet die Risiken nach dem inhärenten Risiko (**„Rangordnung der Risiken (brutto, Top 10)“**) bzw. nach dem Nettorisiko (**„Rangordnung der Risiken (netto, Top 10)“**). Dabei nummeriert sie die zehn grössten Risiken von 1 bis 10 (1 = schwerwiegendstes Risiko), wobei nur die Prüfgebiete bzw. Prüffelder auf Einzelstufe zu berücksichtigen sind.
- Im Teil „Konsolidierte Aufsicht“ unter **„Ergänzende Elemente“** erfolgt eine Adressierung in folgenden Fällen:

  Bei Vorliegen einer Stammhausstruktur werden Informationen erfasst, falls neben der in der Risikoanalyse auf Einzelstufe abgebildeten Gesellschaft weitere Gruppengesellschaften mit wesentlichen Geschäftsrisiken bestehen.

  Bei Vorliegen einer Holdingstruktur bzw. atypischen Struktur wird adressiert, aus welchen Gruppengesellschaften die wesentlichen Geschäftsrisiken stammen. Verweise auf separate Risikoanalysen auf Einzelstufe sind möglich.

III. Prüfstrategie Banken und Wertpapierhäuser

- Die Prüfgesellschaft nimmt gemäss Rz 106 FINMA-RS 13/3 im Rahmen der Prüfstrategie eine Schätzung der Prüfkosten vor. Diese erfolgt aufgeteilt in (i) direkt für die Prüfung der Prüfgebiete anfallende Kosten und (ii) allgemeine Kosten, welche nicht den Prüfgebieten zugeordnet werden können (bspw. für Prüfungsplanung, Berichterstattung, Qualitätssicherung). Bei Beaufsichtigten der Aufsichtskategorien 1 bis 3 erfolgt die Schätzung der den Prüfgebieten zuordenbaren Prüfkosten pro einzelnes Prüfgebiet bzw. Prüffeld.
- Prüfungen im Zusammenhang mit bewilligungspflichtigen, internen Modellansätzen für operationelle Risiken, Kredit-, Gegenparteikredit- und Marktrisiken sind zu unterscheiden in Prüfungshandlungen für Modellneubewilligungen (i), Modelländerungen (ii) und Modellüberwachung (iii). Im Rahmen des Erhebungsformulars Prüfstrategie sind einzig Prüfungshandlungen für die Modellüberwachung zu berücksichtigen. Diese sind als Teil der Basisprüfung im Prüfgebiet „Eigenmittelanforderungen aus und Bewilligungsvoraussetzungen für von der FINMA bewilligte interne Modellansätze“ zu planen. Die für die Modellüberwachung geschätzten Prüfkosten/-stunden sind zudem unter „Anteil Stunden/Kosten für ‚Modellüberwachung’ im Rahmen der Basisprüfung“ (als Davon-Zahl) detailliert auszuweisen.
- Für Institute der Aufsichtskategorien 3 bis 5 kommt grundsätzlich die Standardprüfstrategie gemäss Rz 87.1 ff. FINMA-RS 13/3 zur Anwendung. Weicht die **„Aktuelle / geplante Intervention“** von der Standardprüfstrategie ab, ist dies entsprechend anzugeben und dafür eine Begründung zu erfassen (**„Begründung Prüfstrategie“**).

- Bei **„Begründung Prüfstrategie / kurze Beschreibung der Prüfbereiche“** soll summarisch beschrieben werden, was in den Prüfgebieten bzw. Prüffeldern mit gradueller Abdeckung geplant ist und welche Prüfbereiche dort in den vorangegangenen drei Jahren abgedeckt wurden. Grundsätzlich stellt die Prüfgesellschaft die Einhaltung der Periodizität sicher.
- Im Falle von Nachprüfungen im Sinne von Rz 110 FINMA-RS 13/3 ist dies im Feld **„Nachprüfung“** des entsprechenden Prüfgebiets anzugeben und den betroffenen Mangel bei **„Begründung Prüfstrategie / kurze Beschreibung der Prüfbereiche“** aufzuführen. Falls die Nachprüfung in einem Prüfgebiet erfolgt, in dem gemäss Risikoanalyse und Prüfstrategie im entsprechenden Jahr keine Intervention erforderlich ist, ist bei „**Aktuelle / geplante Intervention**“ „Keine“ zu wählen.
- Bei einer erstmaligen Prüfung nach Übernahme des Mandates liegt die Festlegung der Prüftiefe und/oder Periodizität – wo angebracht und unter Berücksichtigung der vorhergehenden Bestimmungen – im Ermessen der Prüfgesellschaft (Angabe bei **„Begründung Prüfstrategie / kurze Beschreibung der Prüfbereiche“**).
- Die Prüfgesellschaft kann der FINMA Zusatzprüfungen vorschlagen, wenn bei einem Bewilligungsträger (inkl. konsolidierte Aufsicht) Risiken existieren, welche nicht durch die vorgegebenen Prüfgebiete bzw. Prüffelder der Basisprüfung abgedeckt sind (Angabe bei **„Zusatzprüfungen“**). Der Entscheid über die Durchführung und Modalitäten von Zusatzprüfungen obliegt der FINMA. Zudem kann die FINMA im Bedarfsfalle selber Zusatzprüfungen festlegen.

Interventionen nach dem 1. Januar 2024 (Inkrafttreten des FINMA-Rundschreibens 2023/1 „Operationelle Risiken und Resilienz – Banken“ und der Teilrevision vom 7. Dezember 2022 des FINMA-RS 13/3)

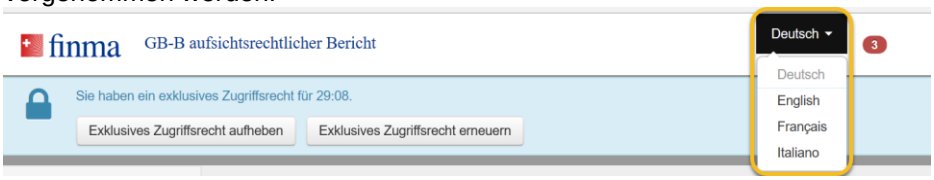
- Die ersten Interventionen mit Bezug auf das FINMA-RS 23/1 und das teilrevidierte FINMA-RS 13/3 finden ab dem **Prüfjahr 2024** statt.
- Die Prüfpunkte zur Informatik und die Prüfpunkte zum Umgang mit elektronischen Kundendaten wurden per Ende 2023 aufgehoben. Ab dem Prüfjahr 2024 bestehen neu **Prüfpunkte zum Management der Cyber-Risiken** und **Prüfpunkte zum Management der Risiken kritischer Daten**.
- Für die Erstellung der Risikoanalyse und der Prüfstrategie zum Prüffeld „**Übergreifendes Management der operationellen Risiken**“ (PS.IOK.ORM) können die bisherigen Interventionen zum Prüffeld „Qualitative Anforderungen an das Management operationeller Risiken“ (PS.IOK.QOR) berücksichtigt werden (bzgl. „Letzte Interventionen“ und „Kontrollrisiko“).
- Für die Erstellung der Risikoanalyse und der Prüfstrategie zum Prüffeld „**Management der Risiken kritischer Daten“** (PS.IOK.DAT) können die bisherigen Interventionen zum Prüffeld „Umgang mit elektronischen Kundendaten“ (PS.IOK.EKD) berücksichtigt werden (bzgl. „Letzte Interventionen“ und „Kontrollrisiko“). Das neue Prüfprogramm zum Management der Risiken kritischer Daten wird angewendet.

- Für die Erstellung der Risikoanalyse und der Prüfstrategie zum Prüffeld „**Management der Cyber-Risiken**“ (PS.IOK.CYB) können die bisherigen Interventionen zum Prüfprogramm-Element „IT-Risiken und -Kontrollen / Cyber-Risiken“ des Prüffelds „Informatik (IT)“ (PS.IOK.INF) berücksichtigt werden (bzgl. „Letzte Interventionen“ und „Kontrollrisiko“). Bei Instituten mit einem Nettorisiko „mittel“ liegt es danach im Ermessen der Prüfgesellschaft, die gemäss Standardprüfstrategie im Prüfjahr 2024 anfallenden Interventionen auf die Jahre 2024 bis 2026 zu verteilen. Bei Instituten mit einem Nettorisiko „hoch“ oder „sehr hoch“ ist grundsätzlich die Standardprüfstrategie anzuwenden. Das neue Prüfprogramm zum Management der Cyber-Risiken wird angewendet.
- Für die Erstellung der Risikoanalyse und der Prüfstrategie zum Prüffeld „**Management der Informations- und Kommunikationstechnologie (IKT)-Risiken**“ (mit den neuen Elementen: (a) IKT-Strategie und Governance, (b) Änderungsmanagement, (c) IKT-Betrieb sowie (d) Vorfallmanagement) im Jahr 2024 und den darauffolgenden Jahren, können die bisherigen Interventionen zum Prüffeld „Informatik (IT)“ (PS.IOK.INF) und den jeweiligen Prüfprogramm-Elementen aus den aufgehobenen Prüfpunkten zur Informatik wie folgt berücksichtigt werden (bzgl. „Letzte Interventionen“ und „Kontrollrisiko“):
  - Das neue Element „**IKT-Strategie und Governance“** bezieht sich auf die Historie der Interventionen zum vorherigen Prüfprogramm-Element „IT-Strategie, Organisation und Governance“.
  - Das neue Element „**Änderungsmanagement“** bezieht sich auf die Historie der Interventionen des Prüfprogramm-Elements „IT-Infrastruktur und IT-Leistungserbringung“.
  - Das neue Element „**IKT-Betrieb“** bezieht sich auf die Historie der Interventionen des Prüfprogramm-Elements „IT-Infrastruktur und IT-Leistungserbringung“.
  - Für das Element „**Vorfallmanagement“** steht keine Historie an Interventionen zur Verfügung.

  Die Abstützung auf die Historie der Interventionen wird möglicherweise einen Bedarf nach Interventionen zu mehreren der vier Elemente des Prüffelds „Management der IKT-Risiken“ im Jahr 2024 aufzeigen. Die Auswahl von einem der vier Elemente zur Intervention im Jahr 2024 wird anhand der Risikoanalyse im Ermessen der Prüfgesellschaft getroffen. Gleichermassen wird in den Folgejahren vorgegangen, bis sich der neue Zyklus der graduellen Abdeckung der vier Elemente über vier Jahre eingependelt hat. Bei Instituten mit reduzierter Prüfkadenz wird jeweils pro Zwischen- und Prüfjahr ein Element abgedeckt (drei Elemente pro Intervention bei Instituten mit einer reduzierten Prüfkadenz von drei Jahren).
- Für das neue Prüffeld „**Operationelle Resilienz“** (PS.IOK.RES) sieht das FINMA-RS 23/1 teilweise Übergangsbestimmungen von bis zu zwei Jahren vor. Eine erstmalige Intervention kann ab 2024 im Ermessen der Prüfgesellschaft und gestützt auf ihre Risikoanalyse stattfinden. Eine Intervention muss spätestens im Prüfjahr 2027 durchgeführt werden, d. h. im zweiten Jahr nach Ablauf der Übergangsfrist.

IV. Aufsichtsrechtliche Berichterstattung Banken und Wertpapierhäuser

- Gemäss Art. 9 Abs. 2 FINMA-PV wird der Prüfbericht in einer Amtssprache verfasst. Die Berichterstattung in englischer Sprache ist in Ausnahmefällen auf Gesuch der Prüfgesellschaft und nach Genehmigung der FINMA möglich. Die Umstellung der Berichtssprache kann in der Kopfzeile des Erhebungsformulars vorgenommen werden.



- Der aufsichtsrechtliche Prüfbericht muss die Resultate der Prüfung umfassend, eindeutig und objektiv darstellen. Die leitende Prüferin oder der leitende Prüfer sowie eine weitere Prüferin oder ein weiterer Prüfer mit Zeichnungsberechtigung bestätigen dies mit ihren Unterschriften (qualifiziert elektronische Signatur) auf dem Bericht (PDF), den sie als Anhang zur elektronischen Erhebung via Erhebungsplattform der FINMA einreichen. Besteht die Möglichkeit nicht, den Bericht qualifiziert elektronisch zu signieren, muss dieser, zusätzlich zur elektronischen Einreichung der Erhebung via Erhebungsplattform, ausgedruckt, handschriftlich unterzeichnet und auf dem Postweg der FINMA eingereicht werden.
- Beanstandungen sowie Empfehlungen gemäss Art. 11 Finanzmarktprüfverordnung (FINMA-PV; SR 956.161) werden vollzählig unter dem Kapitel **„Zusammenfassung der Prüfresultate“** wiedergegeben. Diese sind zu bewerten (Klassifizierung gemäss Rz 75.2 ff. FINMA-RS 13/3).
- Die Prüfgesellschaft stellt sicher, dass der Prüfbericht und eine allfällige ergänzende Berichterstattung an den Bewilligungsträger (z.B. im Sinne eines „Management Letters“) konsistent sind. Wesentliche Feststellungen aus weiteren Mandaten/Berichterstattungen werden auch im Prüfbericht wiedergegeben. Allfällige weitere Berichterstattungen an den Bewilligungsträger sind der FINMA grundsätzlich nicht unaufgefordert einzureichen.
- Zur aufsichtsrechtlichen Berichterstattung bei Banken und Wertpapierhäusern sowie deren Finanzgruppen, falls eine konsolidierte Überwachung angezeigt ist, werden mindestens folgende Dokumente als „**Anhang“** eingereicht[3]:
  - GwG-Erhebungsformular (als separate Erhebung);
  - Grafische Darstellung der Konzernstruktur inklusive Beteiligungsverhältnisse (unter Berücksichtigung zusätzlicher Angaben zur konsolidierten Aufsicht, vgl. Ziffer 6.10 des aufsichtsrechtlichen Berichts);

[3] Die jährliche Einreichung einer Kopie der umfassenden Berichterstattung zur Rechnungsprüfung gemäss Art. 728*b* Abs. 1 OR (vgl. Anhang 18 FINMA-RS 13/3) erfolgt als Anhang zur separaten „Erhebung Rechnungsprüfung“.

- Organigramm(e) (im Minimum mit Angabe der verantwortlichen Personen pro Geschäftsbereich bzw. Abteilung).

V. Hinweise zur Prüfungsdurchführung

- Die Beilage zu dieser Wegleitung führt die rechtlichen Grundlagen auf, welche im Rahmen der Basisprüfung abzudecken sind. Sie stellt keine abschliessende Aufzählung rechtlicher Bestimmungen dar. Weiter zeigt die Beilage in einer synoptischen Darstellung der Rz 87.1–102 FINMA-RS 13/3 auf, welche Prüfzyklen pro Prüfgebiet bzw. Prüffeld basierend auf den Nettorisiken anwendbar sind.
- Für einige Prüffelder bzw. Prüfgebiete sind standardisierte Prüfpunkte entwickelt worden. Diese sind bei jeder Intervention im entsprechenden Prüffeld bzw. Prüfgebiet anzuwenden. Sind einzelne Aspekte dieser Prüfpunkte nicht anwendbar, so sind die diesbezüglichen Überlegungen in den Prüfunterlagen für Dritte nachvollziehbar zu dokumentieren. Zu beachten ist, dass die Prüfpunkte möglicherweise keine abschliessende Grundlage für die Prüfungshandlungen bilden und vom Prüfer, wo notwendig, ergänzt werden müssen. Die durchgeführten Prüfungshandlungen und vorgenommenen Schlussfolgerungen sind für Dritte nachvollziehbar zu dokumentieren. Diese Dokumentation kann auch auf andere Weise als in den Musterdokumenten für die Prüfpunkte erfolgen, sofern sämtliche Angaben der Musterdokumente wiedergegeben werden.

Beilage: Rechtliche Grundlagen für die aufsichtsrechtliche Prüfung / Standardprüfstrategie