Musterbericht

zur Aufsichtsprüfung für Sicherungseinrichtungen (Anhang K2)

Januar 2026

Inhalt

[1. Rahmenbedingungen der Aufsichtsprüfung 5](#_Toc216426568)

[2. Weitere Mandate der Revisionsstelle bei der beaufsichtigten Sicherungseinrichtung 5](#_Toc216426569)

[3. Zusammenfassung der Prüfresultate aus der Aufsichtsprüfung 5](#_Toc216426570)

[3.1 Beanstandungen 5](#_Toc216426571)

[3.2 Empfehlungen 5](#_Toc216426572)

[3.3 Beanstandungen des Vorjahres 6](#_Toc216426573)

[3.4 Empfehlungen des Vorjahres 6](#_Toc216426574)

[3.5 Bestätigung zu aufsichtsrechtlichen Vorgaben der FMA 6](#_Toc216426575)

[3.6 Wesentliche Feststellungen durch Dritte 6](#_Toc216426576)

[3.7 Zusammenfassung zu weiteren Prüferkenntnissen sowie Gesamteinschätzung 6](#_Toc216426577)

[4. Wesentliche Feststellungen ausserhalb der Aufsichtsprüfung 6](#_Toc216426578)

[5. Wichtige Informationen zu der geprüften Sicherungseinrichtung / Darstellung bedeutender Änderungen 6](#_Toc216426579)

[5.1 Mitgliederstruktur 7](#_Toc216426580)

[5.2 Beteiligungsverhältnisse / Beziehungen zu anderen Unternehmen 7](#_Toc216426581)

[5.3 Betriebs- und Aufbauorganisation 7](#_Toc216426582)

[5.4 Wesentliche Änderungen bei der beaufsichtigten Sicherungseinrichtung 7](#_Toc216426583)

[6. Prüfresultate 7](#_Toc216426584)

[6.1 Organisatorische Anforderungen 9](#_Toc216426585)

[6.1.1 Interne Organisation 9](#_Toc216426586)

[6.1.2 Meldewesen 10](#_Toc216426587)

[6.2 Governance 10](#_Toc216426588)

[6.2.1 Geschäftsleitung 10](#_Toc216426589)

[6.2.2 Stiftungsrat 11](#_Toc216426590)

[6.2.3 IKT-Sicherheit 12](#_Toc216426591)

[6.2.4 Auslagerungen 18](#_Toc216426592)

[6.2.5 Business Continuity Management 19](#_Toc216426593)

[6.3 Finanzierung 20](#_Toc216426594)

[6.3.1 Finanzierung des Einlagensicherungssystems 20](#_Toc216426595)

[6.3.2 Finanzierung des Anlegerentschädigungssystems 21](#_Toc216426596)

[6.4 Prüfresultate aus von der FMA Liechtenstein zusätzlich festgelegten Prüffelder 22](#_Toc216426597)

[7. Weitere Bemerkungen 22](#_Toc216426598)

[8. Unterschrift / Bestätigung der Revisionsstelle 22](#_Toc216426599)

[9. Anhang 22](#_Toc216426600)

***Beaufsichtigte Sicherungseinrichtung***

Bericht der Revisionsstelle gemäss dem Gesetz über die Einlagensicherung und Anlegerentschädigung bei Banken und Wertpapierfirmen (Einlagensicherungs- und Anlegerentschädigungsgesetz – EAG) über die Aufsichtsprüfung *Berichtsjahr*

*[Die im Dokument kursiv und grau gehaltenen Textteile sind als Anleitung, jene in kursiv und gelb als beispielshafte Vorgabe zu verstehen. Nicht kursiv gehaltene Textvorgaben sind zwingend einzuhalten. Die Vorlage ist ab 2026 anwendbar (aufsichtsrechtliche Berichterstattung für Prüfperioden beginnend am 01. Januar 2026]*

1. Rahmenbedingungen der Aufsichtsprüfung

*Unter diesem Abschnitt sind die Rahmenbedingungen der Prüfung aufzuführen, d.h. insbesondere*

* Angabe der Zeitspanne(-n), in der die Prüfungshandlungen und die Berichterstattung durchgeführt bzw. erstellt wurden
* Auflistung der bei der Prüfung wesentlich eingesetzten Personen inklusive Angabe der Hierarchie- bzw. Funktionsstufe (z.B. Partner, Manager, eingesetzte Spezialisten in den Bereichen Recht, Steuern, IT usw.)
* Ausmass der Abstützung auf bzw. Verwendung von Arbeiten Dritter, eines Experten oder eines anderen Wirtschaftsprüfers
* Hinweise auf Einschränkungen und Schwierigkeiten bei der Prüfung (z.B. Abwesenheit von Entscheidungsträgern; unvollständige/qualitativ mangelhafte Dokumentation durch die beaufsichtigte Sicherungseinrichtung; Restriktionen bei den Prüfungen z.B. reduzierter Prüfungsumfang infolge von durch die beaufsichtigte Sicherungseinrichtung reduziertem Budget; Sachverhalte, die dazu führen, dass die Würdigung des Tatbestands verunmöglicht wird etc.)
* Bestätigung, dass alle Informationen zeitgerecht und in der erforderlichen Qualität zur Verfügung gestellt wurden
* Bestätigung der Unabhängigkeit der Revisionsstelle gemäss Art. 127 BankG (vgl. Art. 25 Abs. 7 EAG).

1. Weitere Mandate der Revisionsstelle bei der beaufsichtigten Sicherungseinrichtung

*Die Revisionsstelle führt allfällige weitere Mandate (z.B. Abschlussprüfung, vereinbarte Prüfungshandlungen, Beratungsmandate, andere Prüfmandate und Dienstleistungen) im berichtsrelevanten Zeitraum bei der beaufsichtigten Sicherungseinrichtung auf. Diesbezüglich sind die Art und der Umfang der Mandate zu beschreiben.*

1. Zusammenfassung der Prüfresultate aus der Aufsichtsprüfung

*Die Revisionsstelle vermerkt alle Beanstandungen und Empfehlungen des Berichtsjahres sowie der vorangegangenen Prüfperiode (jeweils mit Fristansetzung und zu treffenden bzw. getroffenen Massnahmen sowie der Stand der Umsetzung). Der Zusammenzug aller Beanstandungen und Empfehlungen ist in tabellarischer Form vorzunehmen (für Beanstandungen oder Empfehlungen des Berichtsjahres mit Verweis auf die Seitenzahlen des Berichts für die entsprechende Detailausführung). Hat die Revisionsstelle keine Beanstandungen oder Empfehlungen zum Berichts- oder Vorjahr anzubringen bzw. angebracht, so hält sie dies fest. Beanstandungen, die wiederholt auftreten, sind speziell zu kennzeichnen. Werden Beanstandungen oder Empfehlungen identifiziert, deren Bereinigung bereits erledigt ist, sind diese dennoch im Bericht aufzuführen. Dabei soll ersichtlich dargestellt werden, weshalb sich ein Handlungsbedarf erübrigt.*

*Die Beanstandungen und Empfehlungen sind gemäss der in der Revisionsprüfungsrichtlinie festgelegten Klassifizierung auszuweisen. Stellungnahmen der Sicherungseinrichtung sind jeweils bei Beanstandungen/Empfehlungen sowie bei noch nicht erledigten Beanstandungen und Empfehlungen des Vorjahres einzuholen und im Bericht darzulegen.*

* 1. Beanstandungen

*Tabelle / Text*

* 1. Empfehlungen

*Tabelle / Text*

* 1. Beanstandungen des Vorjahres

*Tabelle / Text*

* 1. Empfehlungen des Vorjahres

*Tabelle / Text*

* 1. Bestätigung zu aufsichtsrechtlichen Vorgaben der FMA

*Die Revisionsstelle bestätigt an dieser Stelle die Einhaltung der im Berichtszeitraum anwendbaren aufsichtlichen Verwaltungsakte der FMA, die explizit und individuell für die zu prüfende Sicherungseinrichtung gelten. Zu berücksichtigen sind gegebenenfalls auch nicht-normative Akte (z.B. Empfehlungen), sofern diese die gegenständlichen aufsichtlichen Verwaltungsakte definieren oder näher umschreiben.*

* 1. Wesentliche Feststellungen durch Dritte

*Die Revisionsstelle beschreibt an dieser Stelle allfällige wesentliche, aufsichtsrechtlich relevante Feststellungen durch Dritte (z.B. andere Revisionsstellen oder ausländische Aufsichtsbehörden), zu denen sie innerhalb oder ausserhalb der Prüfungstätigkeit Kenntnis erlangt hat. Die Revisionsstelle hat die Feststellungen angemessen zu würdigen. Sofern die Feststellungen an anderer Stelle im Bericht dargestellt werden, ist eine entsprechende Referenz ausreichend.*

* 1. Zusammenfassung zu weiteren Prüferkenntnissen sowie Gesamteinschätzung

*Die Revisionsstelle nimmt basierend auf den Erkenntnissen aus ihren Prüfungshandlungen Stellung zur Gewähr für eine einwandfreie Geschäftsführung durch die Organe und qualifiziert Beteiligten.*

*Des Weiteren würdigt die Revisionsstelle unter diesem Titel summarisch die Gesamtsituation der Sicherungseinrichtung sowie aktuelle Entwicklungen und weist zukunftsgerichtet auf mögliche (u.a. regulatorische) Herausforderungen hin. Die Würdigung der Revisionsstelle hat zumindest eine Stellungnahme der Revisionsstelle zu der Einhaltung der gesetzlichen Fristen zur Erstattung der gedeckten Einlagen (gem. Art. 12 ff EAG) und der gedeckten Anlagen (gem. 40 EAG) der Sicherungseinrichtung zu beinhalten.*

1. Wesentliche Feststellungen ausserhalb der Aufsichtsprüfung

*Stellt die Revisionsstelle ausserhalb der Aufsichtsprüfung Auffälligkeiten fest, welche wesentliche Auswirkungen auf die Risikolage, Aufgaben oder Pflichten der Sicherungseinrichtung haben, so sind diese im Rahmen der Berichterstattung aufzuführen (z.B. Empfehlungen im Rahmen des Management Letters bei der Abschlussprüfung; Wahrscheinlichkeit des Eintritts eines Sicherungsfalls bei einem Mitgliedinstitut, etc.)*

1. Wichtige Informationen zu der geprüften Sicherungseinrichtung / Darstellung bedeutender Änderungen
   1. Mitgliederstruktur

*Die Revisionsstelle erläutert die Mitgliederstruktur sowie diesbezügliche Veränderungen während dem Berichtsjahr.*

* 1. Beteiligungsverhältnisse / Beziehungen zu anderen Unternehmen

*Die Revisionsstelle erläutert, sofern anwendbar, die qualifiziert Beteiligten sowie wesentliche Beziehungen und Abhängigkeiten zu anderen Unternehmen oder Anspruchsträgern (z.B. wirtschaftlich bedeutende Verträge; Zusammenarbeit). Diesbezügliche Veränderungen werden adressiert.*

* 1. Betriebs- und Aufbauorganisation

*Die Revisionsstelle erläutert kurz die generelle Organisation, bestehende Auslagerungen und allfällige entsprechende Veränderungen. Dabei kann sich die Revisionsstelle auf das Organigramm abstützen.*

* 1. Wesentliche Änderungen bei der beaufsichtigten Sicherungseinrichtung

*Die Revisionsstelle erläutert, sofern noch nicht in den weiteren Kapiteln des Berichts aufgeführt wurden, allfällige wesentliche Veränderungen während dem Berichtsjahr oder solche, die bei der beaufsichtigten Sicherungseinrichtung noch bevorstehen; insbesondere hinsichtlich:*

* *Wechsel bei den qualifiziert Beteiligten (sofern anwendbar)*
* *Organe*
* *Beziehungen zu anderen Unternehmen*
* *Reorganisationen, Restrukturierungen, Delegationen*

1. Prüfresultate

*Die Revisionsstelle bewertet die Prüfelemente in Prüfgebieten mit Intervention durch „Ja (Detailprüfung)“, „Ja (kritische Beurteilung)“ oder „Nein“. Die Prüfbestätigungen gelten für beide Arten von Prüftiefen (Detailprüfung oder kritische Beurteilung). Im Falle einer „kritischen Beurteilung“ sind die Bestätigungen unabhängig vom Wortlaut des Prüfelements, als „negative assurance“ zu verstehen.*

*Die Revisionsstelle bewertet die Prüfelemente in Einklang mit den Vorgaben der Revisionsprüfungsrichtlinie. Führt die Intervention zu einer Beanstandung (siehe Revisionsprüfungsrichtlinie allgemeiner Teil I Ziff. 10.2), so ist das Prüfresultat mit „Nein“ anzugeben und eine angemessene Erläuterung inklusive Risikoeinschätzung vorzunehmen. Führt die Intervention zu keiner Beanstandung, so ist „Ja“ anzugeben.*

*Liegen die Voraussetzungen für eine Empfehlung vor (siehe Revisionsprüfungsrichtlinie allgemeiner Teil I Ziff. 10.2), so hat die Revisionsstelle eine kurze Erläuterung inklusive Risikoeinschätzung vorzunehmen.*

*Die Erläuterungen bei Prüfgebieten mit Beanstandungen müssen mind. Folgendes enthalten: Nachvollziehbare Angaben zu Ist- und Soll-Sachverhalten mit Gesetzesreferenzierungen; genaue zeitliche Angabe zum Sachverhalt («Zeitraum»), Zuständigkeit innerhalb der Sicherungseinrichtung und zugrundeliegende Quellen für die resultierende Beanstandung (Nachweise).*

*In den nachfolgenden Kapiteln nimmt die Revisionsstelle Stellung zu den einzelnen Prüfgebieten gemäss der Prüfstrategie. Allfällige spezifische Vorgaben der FMA sind durch die Revisionsstelle zu berücksichtigen.*

*Sofern im Berichtsjahr in einem Prüffeld keine Intervention erfolgte, müssen diese nicht im Bericht aufgeführt werden, wobei die entsprechende Berichtsziffer inkl. den Formatvorlagen gelöscht werden kann.*

*Für Prüffelder, welche im Berichtsjahr mittels Detailprüfung geprüft wurden, sind zwingend aussagekräftige Erläuterungen aufzuführen. Jene Prüffelder, hinsichtlich welcher im Bericht eine kritische Beurteilung durchgeführt wurde und aus den durchgeführten Prüfungshandlungen keine Beanstandungen oder Empfehlungen resultierten, können ohne Erläuterungen aufgeführt werden.*

*Die Revisionsstelle hat den Umfang und Tiefe der Erläuterungen so auszugestalten, dass sich der Verwaltungsrat bzw. der Stiftungsrat sowie die FMA ein angemessenes Bild über das jeweilige mit der Prüftiefe „Detailprüfung“ abgedeckte Prüffeld bilden kann. Die Erläuterungen im Rahmen der Detailprüfung müssen aussagekräftig sein und Rückschlüsse auf die einzelnen Mindestprüfinhalte bzw. Prüfelemente geben. Zudem sind Erläuterungen zur Stichprobenauswahl und der Stichprobengrösse darzulegen.*

*Im Musterbericht sind pro Prüfelement die Mindestprüfinhalte (jeweils auslegbar auf das zugrundeliegende Prüffeld), welche durch die Prüfungshandlungen der Revisionsstelle für die Beurteilung und Abgabe der Prüfbestätigungen abzudecken sind, aufgeführt. Es liegt in der Verantwortung der Revisionsstelle die Mindestprüfinhalte an die spezifische Situation der zu prüfenden Sicherungseinrichtung anzupassen. Werden die Mindestprüfinhalte durch die durchgeführten Prüfungshandlungen nicht vollständig abgedeckt, ist im Bericht über die Aufsichtsprüfung darauf hinzuweisen und zu begründen.*

* 1. Organisatorische Anforderungen
     1. Interne Organisation

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / tief* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 4, 5, 33, 34 und 50 EAG | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Verschwiegenheitspflichten, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte, Eskalationsmechanismen) angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das interne Kontrollsystem (Monitoring der Mitgliedsinstitute, 4-Augen-Prinzip, Frühwarnmechanismus, Dokumentations- und Archivierungswesen, Berichterstattung) angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die Abwicklung eines Sicherungsfalls bzw. Anlegerentschädigungsfalls zeitnah und korrekt getätigt wird. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren eine angemessene Durchführung und Berichterstattung des Stresstestings gewährleisten. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Verschwiegenheitspflichten, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Die Verantwortlichkeiten und Kompetenzen sind durchgehend klar geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher;*   + *Die internen Verfahren stellen die Einhaltung der Verschwiegenheitspflichten sicher;*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen.* |
| *Interne Kontrollsystem*  *(Monitoring der Mitgliedsinstitute, 4-Augen-Prinzip, Frühwarnmechanismus, Dokumentations- und Archivierungswesen, Berichterstattung)* | * + *Die internen Verfahren stellen ein angemessenes Monitoring der Mitgliedinstitute sicher;*   + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips vor;*   + *Die internen Verfahren stellen eine rechtzeitige Information der Aufsichtsbehörde sicher (Frühwarnmechanismus);*   + *Die internen Verfahren garantieren ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher.* |
| *Abwicklung des Sicherungs- und Entschädigungsfalls* | * + *Die internen Verfahren stellen die zeitnahe und korrekte Abwicklung eines Sicherungsfalls bzw. Anlegerentschädigungsfalls sicher.* |
| *Stresstesting* | * + *Die internen Verfahren stellen sicher, dass ein Stresstesting (Funktionstüchtigkeit der Organisation und der Systeme) mindestens im Rahmen der gesetzlich festgelegten Periodizität angemessen durchgeführt wird;*   + *Die internen Verfahren stellen sicher, dass die Ergebnisse des Stresstestings der FMA weitergeleitet werden.* |

*Text*

* + 1. Meldewesen

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / tief* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 26, 27 und 43 EAG | | | |
|  | | | |
| Bestätigung, dass die internen Verfahren zum Meldewesen (Datenqualität, Validierung, Übermittlung an die Behörde) angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Meldewesen*  *(Datenqualität, Validierung, Übermittlung an die Behörde)* | * + *Die internen Verfahren stellen eine hohe Datenqualität im Meldewesen, inklusive der Überprüfbarkeit der Daten bei den liefernden Instituten, sicher;*   + *Die internen Verfahren stellen eine regelmässige Validierung der Datenqualität im Meldewesen sicher;*   + *Die internen Verfahren stellen eine richtige und zeitnahe Berechnung der gedeckten Einlagen bzw. gedeckten Anlagen sicher;*   + *Die internen Verfahren stellen eine unverzügliche Anzeige an die FMA gemäss Art. 27 EAG sicher;*   + *Die internen Verfahren stellen eine jederzeitige Übermittlung der Daten an die FMA sicher;*   + *Die internen Verfahren stellen eine vollständige und angemessene Weiterleitung der Daten gemäss Art. 26 EAG an die FMA sicher;*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen und Meldedaten sicher.* |

*Text*

* 1. Governance
     1. Geschäftsleitung

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / tief* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 4 EAG iVm Art. 63/64 BankG | | | |
|  | | | |
| Bestätigung, dass die die Verantwortlichkeiten und Kompetenzen der Geschäftsleitung angemessen ausgestaltet sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder der Geschäftsleitung sowohl individuell als auch kollektiv geeignet sind und ihre Eignung regelmässig intern überprüft wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder der Geschäftsleitung sich fortlaufend fachlich adäquat weiterbilden | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Verantwortlichkeiten / Kompetenzen* | *Es besteht eine klare und effektive Aufteilung von Verantwortlichkeiten und Kompetenzen innerhalb der Geschäftsleitung* |
| *Eignung / Weiterbildung* | * + *Die Mitglieder des Gremiums sind sowohl individuell als auch kollektiv geeignet*   + *Es besteht ein internes Verfahren zur regelmässigen Überprüfung der individuellen und kollektiven Eignung*   + *Die Mitglieder des Gremiums werden regelmässig fachlich einschlägig weitergebildet*   + *Die Mitglieder des Gremiums sind zuverlässig, kümmern sich ausnahmslos um das gesetzeskonforme Gebahren der Sicherungseinrichtung und haben einen guten Ruf.*   + *Die Mitglieder des Gremiums sind hinreichend unabhängig* |

*Text*

* + 1. Stiftungsrat

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / tief* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 4 EAG iVm Art. 63/64 BankG | | | |
|  | | | |
| Bestätigung, dass die Verantwortlichkeiten und Kompetenzen des Stiftungsrats angemessen ausgestaltet sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder des Stiftungsrats sowohl individuell als auch kollektiv geeignet sind und ihre Eignung regelmässig intern überprüft wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder des Stiftungsrats sich fortlaufend fachlich adäquat weiterbilden | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Verantwortlichkeiten / Kompetenzen* | *Es besteht eine klare und effektive Aufteilung von Verantwortlichkeiten und Kompetenzen innerhalb des Stiftungsrats, insbesondere hinsichtlich* |
| *Eignung / Weiterbildung* | * + *Die Mitglieder des Gremiums sind sowohl individuell als auch kollektiv geeignet*   + *Es besteht ein internes Verfahren zur regelmässigen Überprüfung der individuellen und kollektiven Eignung*   + *Die Mitglieder des Gremiums werden regelmässig fachlich einschlägig weitergebildet*   + *Die Mitglieder des Gremiums sind zuverlässig, kümmern sich ausnahmslos um das gesetzeskonforme Gebahren der Sicherungseinrichtung und haben einen guten Ruf.*   + *Die Mitglieder des Gremiums sind hinreichend unabhängig* |

*Text*

* + 1. IKT-Sicherheit

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Abzudeckende(-s) Prüfelement(-e) im Rahmen der graduellen Abdeckung im Berichtsjahr mit Angabe der Prüftiefe | | In den vorangegangenen fünf Jahren im Rahmen der graduellen Abdeckung abgedeckte Prüfelemente mit Angabe der jeweiligen Prüftiefe und des Prüfjahrs |
| *niedrig/ mittel / hoch* | Beispiel für Berichtsjahr 2026:   * + IT-Strategie, IKT-Organisation und IKT-Governance (Detailprüfung)   + IKT-Risikomanagementrahmen (Kritische Beurteilung) | | *Beispiel:*  *2025: Informationssicherheitsmanagement (Detailprüfung) und Benutzerberechtigungsmanagement (Kritische Beurteilung)*  *2024: IKT-Betriebsmanagement (Kritische Beurteilung) und Management des IKT-Drittparteienrisikos (Detailprüfung)* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 5 EAG, FMA-Richtlinie 2021/3 | | | |
|  | |  | |
| *[Prüfbestätigung je nach abzudeckendem Prüfelement aus der untenstehenden Tabelle aufzuführen]* | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| *[Prüfbestätigung je nach abzudeckendem Prüfelement aus der untenstehenden Tabelle aufzuführen]* | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| *[Prüfbestätigung je nach abzudeckendem Prüfelement aus der untenstehenden Tabelle aufzuführen]* | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| *etc.* | | |  |

|  |  |  |
| --- | --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** | ***Bestätigungen*** |
| *IKT-Strategie, IKT-Organisation, IKT-Governance* | * + *Die IKT-Strategie ist unter Berücksichtigung der spezifischen Situation des Finanzintermediärs (Grösse, Geschäftstätigkeit, IKT-Komplexität/-Risiken, Auslagerungen usw.) angemessen*   + *Die internen Verfahren stellen die regelmässige Festlegung, Aktualisierung, Validierung/Abstimmung, Genehmigung und Kommunikation der IKT-Strategie sicher*   + *Die internen Verfahren stellen die Erstellung von Massnahmenplänen zur Erreichung der Ziele der IKT-Strategie sowie deren Kommunikation und regelmässige Überprüfung sicher*   + *Die internen Verfahren stellen sicher, dass die Mitarbeiter regelmässig zu IKT- und Sicherheitsrisiken inkl. Informationssicherheit geschult werden.* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass die IKT-Strategie sowie deren Massnahmenpläne angemessen sind*   + *Bestätigung, dass die internen Verfahren die regelmässige Schulung der Mitarbeiter zu IKT-Risiken inkl. Informationssicherheit sicherstellen* |
| *IKT-Risikomanagementrahmen* | * + *Die internen Verfahren stellen sicher, dass ein angemessener IKT-Risikomanagementrahmen besteht und dieser angemessen in das Risikomanagementkonzept eingegliedert ist.*   + *Finanzintermediäre richten eine Funktion ein oder benennen ein Mitglied der Geschäftsleitung, das für die Überwachung der mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen sowie der damit verbundenen Risikoexposition und die einschlägige Dokumentation verantwortlich ist.*   + *Die internen Verfahren stellen sicher, dass der Rahmen für das IKT-Risikomanagement eingehalten, dokumentiert und mindestens einmal jährlich überprüft und genehmigt wird.*   + *Es bestehen angemessene Verfahren zur regelmässigen Ermittlung und Dokumentation von IKT-Assets, Geschäftsfunktionen und Unterstützungsprozesse sowie zur Beurteilung deren Kritikalität und Abhängigkeiten*   + *Es bestehen angemessene Verfahren zur regelmässigen Identifikation, Beurteilung, Adressierung und Akzeptanz von IKT-Risiken, die auf die identifizierten IKT-Assets, Geschäftsfunktionen und Unterstützungsprozesse Einfluss haben.*   + *Es bestehen angemessene interne Verfahren zur Festlegung und Überwachung der IKT-bezogenen Kontrollen, welche die relevanten IKT-Risiken reduzieren.*   + *Es bestehen angemessene interne Verfahren, welche sicherstellen, dass die zugewiesenen Aufgaben und Verantwortlichkeiten zur Steuerung von IKT-Risiken / IKT-Kontrollen an die betroffenen Abteilungen und deren Integration in andere interne Risikomanagement- / Risikokontrollfunktionen überwacht werden*   + *Die internen Verfahren stellen eine angemessene interne Berichterstattung bezüglich der IKT-Risiken und -Kontrollen sicher* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass ein angemessenes IKT-Risikomanagementrahmen besteht, welcher angemessen in das Risikomanagementkonzept eingegliedert ist, dokumentiert ist und mindestens jährlich überprüft und genehmigt wird.*   + *Bestätigung, dass ein Mitarbeiter oder Mitglied der Geschäftsleitung die Funktion für die Überwachung der mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen sowie der damit verbundenen Risikoexposition und die einschlägige Dokumentation innehat.*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die IKT-Assets, Geschäftsprozesse und Unterstützungsprozesse regelmässig ermittelt, auf Kritikalität und Abhängigkeiten beurteilt und dokumentiert werden*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die IKT-Risiken, die auf die identifizierten IKT-Assets, Geschäftsfunktionen und Unterstützungsprozesse Einfluss haben, angemessen identifiziert, beurteilt und adressiert werden*   + *Bestätigung, dass die internen Verfahren angemessene IKT–Kontrollen auf allen zur Reduzierung der relevanten IKT-Risiken sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die zugewiesenen Aufgaben und Verantwortlichkeiten zur Steuerung von IKT-Risiken / IKT-Kontrollen an die betroffenen Abteilungen und deren Integration in andere interne Risikomanagement- / Risikomanagementkontrollfunktionen überwacht werden*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass eine angemessene interne Berichterstattung bezüglich der IKT-Risiken und Kontrollen bestehen* |
| *Informationssicherheitsmanagement* | * + *Die internen Verfahren stellen die Erarbeitung, regelmässige Überprüfung, Genehmigung, Dokumentation und interne Kommunikation einer angemessenen Informationssicherheitsleitlinie (Sicherheitsleitlinie/Sicherheitsstrategie) sicher.*   + *Die internen Verfahren gewährleisten die laufende Überwachung der IKT- und Informationssicherheit um Sicherheitsbedrohungen (z.B. Erkennen/Meldung von physischem oder logischem Eindringen, Datenlecks, schädliche Codes, öffentlich bekannte Sicherheitslücken in Software/Hardware, Verstösse gegen Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Assets) zu erkennen, zu melden und diese zu beheben*   + *Die internen Verfahren stellen die Erarbeitung, regelmässige Überprüfung, Genehmigung, Dokumentation eines angemessenen Rahmenwerks für Informationssicherheitstests sicher, welches die Robustheit und Wirksamkeit der Informationssicherheitsmassnahmen und -tests bewertet und sicherstellt.*   + *Die internen Verfahren stellen die regelmässige Durchführung von Überprüfungen, Bewertungen und Tests anhand eines risikobasierten Ansatzes sicher (für kritische IKT-Systeme mind. jährliche Durchführung; unkritische Systeme mind. alle fünf Jahre), um Schwachstellen in den IKT-Systemen und IKT-Diensten , welche kritische oder wichtige Funktionen unterstützen, sicherzustellen (z.B. Gap-Analysen anhand von Informationssicherheitsstandards, Konformitätsprüfungen, physische Sicherheitsüberprüfungen, Quellcode-Überprüfungen, Schwachstellenmanagement, Penetrationtests, Verwundbarkeitsanalysen, Red-Team-Übungen)*   + *Die internen Verfahren stellen für IKT-Systeme, welche kritische oder wichtige Funktionen unterstützen, basierend auf der Risikoeinschätzung die unverzügliche Behebung der festgestellten Schwachstellen durch gezielte Massnahmen sicher*   + *Die internen Verfahren legen Kriterien fest, nach welchen Tests der Sicherheitsmassnahmen ausserhalb des normalen Durchführungszyklus (z.B. Veränderungen der IT-Infrastruktur, Prozesse; Änderungen aufgrund von Betriebs- und Sicherheitsvorfällen etc.) durchgeführt werden und stellen die zeitnahe Durchführung sicher* | * + *Bestätigung, dass die internen Verfahren die Erarbeitung, regelmässige Überprüfung, Genehmigung, Dokumentation und interne Kommunikation einer angemessenen Informationssicherheitsleitlinie (Sicherheitsleitlinie/Sicherheitsstrategie) sicherstellen*   + *Bestätigung, dass die internen Verfahren die laufende Überwachung der IKT- und Informationssicherheit zur Erkennung, Meldung und Behebung von Sicherheitsbedrohungen sicherstellen*   + *Bestätigung, dass die internen Verfahren die Erarbeitung, regelmässige Überprüfung, Genehmigung, Dokumentation eines angemessenen Rahmens für Informationssicherheitstests (Rahmenwerk) sicherstellen*   + *Bestätigung, dass die internen Verfahren die regelmässige Durchführung von Überprüfungen, Bewertungen und Tests zur Identifikation von Schwachstellen in den IKT-Systemen und IKT-Diensten, welche kritische oder wichtige Funktionen unterstützen, sicherstellen*   + *Bestätigung, dass die internen Verfahren die unverzügliche Behebung der festgestellten Schwachstellen für IKT-Systeme, welche kritische oder wichtige Funktionen unterstützen, sicherstellen*   + *Bestätigung, dass die internen Verfahren Kriterien für ad-hoc-Tests der Sicherheitsmassnahmen ausserhalb des normalen Durchführungszyklus und deren zeitnahe Durchführung sicherstellen* |
| *Benutzerberechtigungsmanagement* | * + *Es bestehen interne Prozesse und Kontrollen zur Gewährung, Änderung und zum Entzug des logischen/physischen Zugangs zu IT-Systemen/Applikationen/Räumlichkeiten für Mitarbeitende und Dritte auf einer Need-to-Know-Basis (Definition von Rollen, Genehmigungsprozesse, Funktionentrennung etc.), welcher die Eigentümer der Informationen involviert.*   + *Es bestehen interne Verfahren, die sicherstellen, dass zumindest alle Aktivitäten (u.a. Zugänge zu IT-Systemen/Applikationen/Räumlichkeiten) von privilegierten Benutzern protokolliert und überwacht werden.*   + *Es bestehen interne Verfahren, die sicherstellen, dass die Zugriffsprotokolle gegen unbefugte Änderung oder Löschung gesichert und für einen angemessenen Zeitraum gemäss Aufbewahrungspflichten sicher aufbewahrt werden.*   + *Es bestehen interne Verfahren, welche sicherstellen, dass logische und physische Zugangsrechte regelmässig überprüft werden*   + *Es werden angemessene Authentifizierungsmethoden bzgl. der Kritikalität von IKT-Systemen, IKT-Informationen und des jeweiligen Zugriffsprozesses eingesetzt.*   + *Die internen Verfahren stellen eine angemessene interne Berichterstattung im Zusammenhang mit der logischen und physischen Sicherheit / dem Informationsschutz sicher* | * + *Bestätigung, dass die internen Verfahren die Gewährung, Änderung und den Entzug der logischen und physischen Zugangsrechte auf einer Need-to-Know-Basis angemessen sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass zumindest alle Aktivitäten der privilegierten Benutzer (u.a. Zugänge zu IT-Systemen/Applikationen/Räumlichkeiten) protokolliert und überwacht werden*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass Zugriffsprotokolle sicher und gemäss den Aufbewahrungspflichten angemessen aufbewahrt werden*   + *Bestätigung, dass die internen Verfahren die regelmässige Überprüfung der logischen und physischen Zugriffsrechte sicherstellen*   + *Bestätigung, dass angemessene Authentifizierungsmethoden angewandt werden*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass eine angemessene interne Berichterstattung bezüglich der physischen und logischen Sicherheit und dem Informationsschutz bestehen* |
| *IKT-Betriebsmanagement* | * + *Die internen Verfahren stellen sicher, dass ein aktuelles Inventar der IKT-Assets (inkl. IKT-Systeme, Netzwerkgeräte, Datenbanken etc.) ausreichend detailliert (IKT-System, Standort, Sicherheitsklassifizierung, Eigentümerschaft etc.) geführt wird, welches u.a. Interdependenzen zwischen Systemen dokumentiert*   + *Es bestehen angemessene Back-up und Wiederherstellungsprozesse, die regelmässig getestet werden*   + *Die Daten- und IKT-Systemsicherungen werden sicher gespeichert.*   + *Es bestehen angemessene interne Verfahren, die das Auftreten von IKT-bezogenen Vorfällen helfen zu vermeiden sowie ihre Auswirkungen auf die Erbringung von IKT-Dienstenn minimieren (u.a. durch. Sicherheits-Patches, Implementierung sicherer Basiskonfiguration wesentlicher Netzwerkkomponenten/Server, Netzwerksegmentierung, Verschlüsselung des Netzwerkverkehrs, Schutz von Endpunkten, Mechanismen zur Überprüfung der Integrität von Software, Firmware, Daten; Verschlüsselung gespeicherter Daten und Daten während der Übertragung, Virenschutz, Firewalls).*   + *Die internen Verfahren stellen sicher, dass IKT-bezogene Vorfälle überwacht, protokolliert und zeitnah behoben werden.*   + *Die internen Verfahren stellen sicher, dass angemessene Kriterien und Schwellenwerte für die Klassifizierung von Ereignissen als IKT-bezogene Vorfälle sowie Frühwarnindikatoren definiert und implementiert werden*   + *Die internen Verfahren stellen eine angemessene interne und externe Berichterstattung im Zusammenhang mit Meldung von IKT-bezogenen Vorfällen und Eskalationsverfahren sicher* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass ein aktuelles Inventar der IKT-Assets geführt wird, welches ausreichend granulare Inhalte der IKT-Assets beinhaltet*   + *Bestätigung, dass angemessene Back-up- und Wiederherstellungsprozesse, die regelmässig getestet werden, bestehen, sowie die Daten- und IKT-Systemsicherungen sicher gespeichert werden*   + *Bestätigung, dass angemessene interne Verfahren bestehen, die Helfen das Auftreten von IKT-bezogenen Vorfällen zu verhindern sowie deren Auswirkungen auf die Erbringung von IKT-Diensten zu minimieren*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass IKT-bezogene Vorfälle angemessen klassifiziert, überwacht, protokolliert, gemeldet und zeitnah behoben werden* |
| *Management des IKT-Drittparteienrisikos* | * + *Die internen Verfahren stellen sicher, dass in Bezug auf IKT-Drittdienstleister eine eindeutige Zuweisung der Zuständigkeiten für Dokumentation, Management und Kontrolle der Vereinbarung samt den daraus resultierenden Risiken besteht, dass ausreichende Mittel zur Erfüllung aller rechtlichen und aufsichtlichen Anforderungen zugewiesen werden, und dass definiert wird, wie Abhängigkeiten von IKT-Drittdienstleistern auf ein akzeptables Mass reduziert werden können*   + *Die internen Verfahren haben sicherzustellen, dass vor dem Abschluss von Vereinbarungen mit IKT-Drittdienstleistern geprüft wird, ob eine kritische oder wichtige Funktion betroffen ist, alle damit zusammenhängenden, relevanten Risiken ermittelt und gesamthaft bewertet werden, eine angemessene Due-Diligence-Prüfung des IKT-Drittdienstleisters vorgenommen wird, alle geltenden aufsichtsrechtlichen Anforderungen erfüllt werden und allfällige Interessenkonflikte ermittelt und bewertet werden.*   + *Die internen Verfahren stellen sicher, dass angemessene Richtlinien zum IKT-Drittparteienrisiko bestehen, die insb. die zentralen Phasen des Lebenszyklus von Vereinbarungen mit IKT-Drittdienstleistern, Zuständigkeiten, Rollenbezeichnungen, Aufgaben und Prozesse bezüglich der Inanspruchnahme der IKT-Drittdienstleister, sowie die Kriterien für die Auswahl von IKT-Drittdienstleistern umfassen*   + *Die internen Verfahren stellen sicher, dass ein laufend aktualisiertes Register der vertraglichen Vereinbarungen mit IKT-Drittdienstleistern und – sofern diese wichtige und und die Vereinbarungen mit IKT-Drittdienstleistern sowie die Begleitdokumente mindestens 5 Jahre lang aufbewahrt werden*   + *Die internen Verfahren stellen sicher, dass geeignete IKT-Sicherheitsstandards eingehalten werden und ein angemessenes Schutzniveau für die Vertraulichkeit von Daten, die Verfügbarkeit ausgelagerter Funktionen und Daten sowie die Integrität und Rückverfolgbarkeit von Daten und Systemen im Einklang mit der Informationssicherheitsrichtlinie besteht*   + *Die internen Verfahren stellen sicher, dass Vereinbarungen mit IKT-Drittdienstleistern zumindest angemessene und verhältnismässige Ziele und Massnahmen im Zusammenhang mit der Informationssicherheit, Prozesse zur Behandlung von IKT-bezogenen Vorfällen, sowie Sicherungs- und Wiederherstellungsverfahren samt Verfahren zur Prüfung deren Wirksamkeit enthalten*   + *Die internen Verfahren stellen sicher, dass Vereinbarungen mit IKT-Drittdienstleistern und Unterauftragsnehmer in Bezug auf kritische oder wichtige Funktionen Zugangs-, Informations- und Prüfungsrechte für den Finanzintermediär, ihre interne und externe Revisionsstelle und die FMA gewähren, die zur Überwachung der Vereinbarung mit IKT-Drittdienstleistern und zur Einhaltung aller geltenden aufsichtsrechtlichen Anforderungen erforderlich sind*   + *Die internen Verfahren stellen sicher, dass die Ausführung der Tätigkeiten, die Sicherheitsmassnahmen und die Einhaltung der vereinbarten Dienstleistungsgüte durch IKT-Drittdienstleister überwacht wird*   + *Die internen Verfahren stellen sicher, dass für IKT-Dienstleistungen, welche kritische oder wichtige Funktionen unterstützen, und vom einem IKT-Drittdienstleister erbracht werden, ein geeignetes und ausreichendes Business Continuity Management besteht und die Business Continuity Pläne gepflegt und regelmässig getestet werden*   + *Die internen Verfahren stellen sicher, dass für ausgelagerte kritische oder wichtige Funktionen angemessene Ausstiegstrategien sowie Plänen bestehen, die mit der Richtlinie zum IKT-Drittparteienrisiko und den Business Continuity Plänen im Einklang stehen und die Kontinuität der ausgelagerten kritischen oder wichtigen Funktion sicherstellen* | * + *Bestätigung, dass in Bezug auf IKT-Drittdienstleiter eine eindeutige Zuweisung der Zuständigkeiten für Dokumentation, Management und Kontrolle der Vereinbarung samt den daraus resultierenden Risiken besteht, dass ausreichende Mittel zur Erfüllung aller rechtlichen und aufsichtlichen Anforderungen zugewiesen wurden, und dass definiert wurde, wie Abhängigkeiten von IKT-Drittdienstleistern auf ein akzeptables Mass reduziert werden können*   + *Bestätigung, dass vor dem Abschluss von Vereinbarungen mit IKT-Drittdienstleistern geprüft wurde, ob eine kritische oder wichtige Funktion betroffen ist, alle damit zusammenhängenden, relevanten Risiken ermittelt und gesamthaft bewertet wurden, eine angemessene Due-Diligence-Prüfung des IKT-Drittdienstleisters vorgenommen wurde, alle geltenden aufsichtsrechtlichen Anforderungen erfüllt wurden und allfällige Interessenkonflikte ermittelt und bewertet wurden*   + *Bestätigung, dass angemessene Richtlinien zum IKT-Drittparteienrisiko bestehen*   + *Bestätigung, dass ein angemessenes Register der vertraglichen Vereinbarungen mit IKT-Drittdienstleistern besteht*   + *Bestätigung, dass geeignete IKT-Sicherheitsstandards eingehalten werden und ein angemessenes Schutzniveau für die Vertraulichkeit von Daten, die Verfügbarkeit ausgelagerter Funktionen und Daten sowie die Integrität und Rückverfolgbarkeit von Daten und Systemen im Einklang mit der Informationssicherheitsrichtlinie besteht*   + *Bestätigung, dass Vereinbarungen mit IKT-Drittdienstleistern angemessene und verhältnismässige Ziele und Massnahmen im Zusammenhang mit der Informationssicherheit, Prozesse zur Behandlung von IKT-bezogenen Vorfällen, sowie Sicherungs- und Wiederherstellungsverfahren samt Verfahren zur Prüfung deren Wirksamkeit enthalten*   + *Bestätigung, dass der Finanzintermediär, die externe Revision sowie die FMA die nötigen Zugangs-, Informations- und Prüfungsrechte bei IKT-Drittdienstleistern haben*   + *Bestätigung, dass die Ausführung der Tätigkeiten, die Sicherheitsmassnahmen und die Einhaltung der vereinbarten Dienstleistungsgüte durch IKT-Drittdienstleister überwacht wird*   + *Bestätigung, dass IKT-Dienstleistungen, welche kritische oder wichtige Funktionen unterstützen und vom einem IKT-Drittdienstleister erbracht werden, ein angemessenes Business Continuity Management besteht und Business Continuity Pläne gepflegt und regelmässig getestet werden.*   + *Bestätigung, dass für ausgelagerte kritische oder wichtige Funktionen angemessene Ausstiegsstrategien sowie konkrete Pläne bestehen, welche sicherstellen, dass die Kontinuität der ausgelagerten kritischen oder wichtigen Funktion im Falle der Umsetzung der Ausstiegsstrategie gewahrt bleibt.* |
|  |  |  |

*Text*

* + 1. Auslagerungen

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / tief* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 5 EAG | | | |
|  | | | |
| Bestätigung, dass angemessene interne Verfahren und Auslagerungspolitik zu Auslagerungen von Dienstleistungen bestehen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass angemessene interne Verfahren zur Identifikation, Steuerung und Überwachung von Konzentrationsrisiken im Bereich der Auslagerungen bestehen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

Betreffen Aspekte des Prüffelds «Auslagerungen» IKT-Dienstleistungen, sind diese unter dem Prüfgebiet «IKT-Sicherheit» zu berücksichtigen.

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Auslagerungspolitik* | * + *Die Auslagerungspolitik steht in Einklang mit der Risikostrategie und dem IKS und inkludiert Schnittstellen zum Gesamtrisikomanagement*   + *Die Auslagerungspolitik lässt „Ketten-Auslagerungen“ (d.h. Weitergabe der ausgelagerten Tätigkeiten an weitere Subunternehmer) nicht oder nur unter klaren Bedingungen zu.*   + *Bei Auslagerung der Datenverarbeitung in Drittländer werden sowohl die nationalen als auch die ausländischen Vorschriften betreffend Buchführung, bankinterne Organisation, Geheimhaltung und Datenschutz eingehalten* |
| *Konzentrationsrisiken im Bereich der Auslagerungen* | * + *Es bestehen angemessene interne Verfahren, welche eine angemessene Identifikation, Steuerung und Überwachung von Konzentrationsrisiken im Bereich der Auslagerungen sicherstellen* |

*Text*

* + 1. Business Continuity Management

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / hoch* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 5 EAG | | | |
|  | | | |
| Bestätigung, dass Business Impact Analysen angemessen und regelmässig durchgeführt werden | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die Business Continuity Strategie und die enthaltenen Massnahmen angemessen ausgestaltet und dokumentiert sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die Business Continuity Strategie alle wichtigen Funktionen und Ressourcen (inkl. geschäftskritische ausgelagerte Funktionen) umfasst. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass angemessene Notfallpläne bestehen, welche sicherstellen, dass die Tätigkeit ohne Unterbruch aufrechterhalten werden können und sich die bei schwerwiegenden Betriebsstörungen auftretenden Verluste in Grenzen halten | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren ein regelmässiges Testing und Aktualisierung der Business Continuity Strategie und der Massnahmen sicherstellen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die internen Verfahren zum Business Continuity Management regelmässig einem Review unterliegen. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Business Impact Analysis* | * + *Die internen Verfahren stellen eine angemessene Quantifizierung der Auswirkungen durch schwerwiegende Betriebsstörungen sicher*   + *Die internen Verfahren stellen einen angemessenen Einbezug von qualitativen Auswirkungen durch schwerwiegende Betriebsstörungen sicher*   + *Die internen Verfahren stellen die angemessene Berücksichtigung von Szenario-Analysen und Prozessabhängigkeiten sicher*   + *Die internen Verfahren stellen sicher, dass die geschäftskritischen Funktionen und Prozesse inkl. ausgelagerter kritischer oder wesentlicher Funktionen in die Szenario-Analyse miteinbezogen werden*   + *Die internen Verfahren stellen die regelmässige und angemessene Durchführung von Business Impact Analysen sicher* |
| *Business Continuity Strategie und Massnahmen* | * + *Die internen Verfahren stellen sicher, dass sich die Business Continuity Strategie auf die Erkenntnisse aus der Business Continuity Analyse stützt.*   + *Die internen Verfahren stellen sicher, dass die Business Continuity Strategie angemessen dokumentiert und verfügbar ist*   + *Die internen Verfahren stellen sicher, dass Massnahmen (Reaktions- und Wiederherstellungspläne) für die Verfügbarkeit, Kontinuität und Wiederherstellung der für die gemäss Business Continuity Strategie geschäftskritischen Funktionen und Prozesse definiert sind.*   + *Die internen Verfahren gewährleisten, dass die Massnahmen das Vorgehen, die Mittel und die notwendigen Ressourcen zur Überbrückung und Wiederherstellung der geschäftskritischen Funktionen und Prozesse berücksichtigen.* |
| *Testing & Aktualisierung der Business Continuity Strategie und der Massnahmen* | * + *Die internen Verfahren stellen eine regelmässige Evaluierung der Business Continuity Strategie und der Massnahmen sicher*   + *Die internen Verfahren stellen die Dokumentation der Evaluierung und deren Ergebnisse sicher*   + *Die internen Verfahren stellen die Überarbeitung der Pläne bei existierenden Problemen oder Störungen sicher*   + *Die internen Verfahren stellen sicher, dass die überarbeiteten Pläne angemessen kommuniziert wurden.* |
| *Business Continuity Review* | * + *Die internen Verfahren stellen sicher, dass die Prüfung der internen Verfahren zum Business Continuity Management regelmässig durchgeführt werden.* |

*Text*

* 1. Finanzierung
     1. Finanzierung des Einlagensicherungssystems

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / tief* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 5, 17 bis 24 EAG | | | |
|  | | | |
| Bestätigung, dass die internen Verfahren die zeitgerechte Finanzierung eines Sicherungsfalls bzw. die Entschädigung der Einleger sicherstellen und die internen Verfahren zur Finanzierung eines Sicherungsfalls angemessen ausgestaltet sind. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die Verwendung der verfügbaren Mittel sich im Rahmen des Art. 24 EAG bewegen. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Finanzierung*  *(Finanzierung der Sicherungseinrichtung)* | * + *Die internen Verfahren stellen sicher, dass die Sicherungseinrichtung in der Lage ist, die Finanzierung eines Sicherungsfalls bzw. die Entschädigung der Einleger im Rahmen der gesetzlichen Fristen sicherzustellen;*   + *Die internen Verfahren stellen sicher, dass die gedeckten Einlagen jederzeit berechnet bzw. hochgerechnet werden können.*   + *Die internen Verfahren stellen sicher, dass die verfügbaren Finanzmittel in einem angemessenen Verhältnis zu den bestehenden und potentiellen Verbindlichkeiten der Sicherungseinrichtung stehen;*   + *Die internen Verfahren stellen sicher, dass die Methode der Berechnung nach Art 20 EAG korrekt und konsistent angewandt wird;*   + *Die internen Verfahren stellen eine korrekte Veranlagung des Einlagensicherungsfonds, dessen jederzeitige Verwertbarkeit sowie die korrekte und effektive Nutzung von Zahlungsverpflichtungen, sicher;*   + *Die internen Verfahren stellen eine jederzeitige und nachvollziehbare Berechnung des durch Sonderbeiträge maximal abrufbaren Betrags im Einlagensicherungssystem sicher;*   + *Die internen Verfahren stellen eine bestmögliche Ausschöpfung der gesetzlichen Möglichkeiten zur Refinanzierung der Sicherungseinrichtung, insbesondere zur laufenden Rückversicherung und zur Inanspruchnahme von Kreditoperationen im Sicherungsfall, sicher.* |
| *Verwendung* | * + *Die internen Verfahren stellen sicher, dass sich die Verwendung der verfügbaren Mittel im Rahmen des Art. 24 EAG bewegt.* |

* + 1. Finanzierung des Anlegerentschädigungssystems

|  |  |  |  |
| --- | --- | --- | --- |
| Nettorisiko | Intervention Berichtsjahr: | Angabe des Jahres mit letzter Intervention mit folgender Prüftiefe (vor dem Berichtsjahr) | |
| *niedrig/ mittel / tief* | *Detailprüfung / Kritische Beurteilung* | Detailprüfung: *Jahr* | Kritische Beurteilung:  *Jahr* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 34 und 40 EAG | | | |
|  | | | |
| Bestätigung, dass die die internen Verfahren sicherstellen, dass die Finanzierung eines Anlegerentschädigungsfalls bzw. die Entschädigung der Anleger jederzeit sichergestellt ist und die internen Verfahren zur Finanzierung eines Entschädigungsfalls angemessen ausgestaltet sind. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Finanzierung*  *(Finanzierung der Sicherungseinrichtung)* | * + *Die internen Verfahren stellen sicher, dass die Sicherungseinrichtung die Finanzierung eines Anlegerentschädigungsfalls bzw. die Entschädigung der Anleger im Rahmen der gesetzlichen Fristen sicherstellen kann.*   + *Die internen Verfahren stellen sicher, dass die gedeckten Anlagen jederzeit berechnet bzw. hochgerechnet werden können.*   + *Die internen Verfahren stellen sicher, dass die verfügbaren Finanzmittel in einem angemessenen Verhältnis zu den bestehenden und potentiellen Verbindlichkeiten der Sicherungseinrichtung stehen.* |

* 1. Prüfresultate aus von der FMA Liechtenstein zusätzlich festgelegten Prüffelder

*Unter diesem Abschnitt sind die Prüfresultate sämtlicher, von der FMA Liechtenstein vorgängig kommunizierte, zusätzlich festgelegte Prüffelder, welche im Rahmen der Aufsichtsprüfung abzudecken sind, aufzuführen.*

1. Weitere Bemerkungen

*Die weiteren Bemerkungen/Hinweise dienen der Ergänzung der vorgehend aufgeführten Sachverhalte. Sie sollen, wo es die Revisionsstelle für erforderlich hält, dazu dienen, das Gesamtbild des Berichts über die Aufsichtsprüfung abzurunden. Sie dürfen nicht so formuliert werden, dass sie die im vorliegenden Bericht eindeutig getroffenen Prüfbestätigungen der Revisionsstelle relativieren.*

1. Unterschrift / Bestätigung der Revisionsstelle

*Der Bericht über die Aufsichtsprüfung ist vom leitenden Revisor sowie einer weiteren Person mit Zeichnungsberechtigung zu unterzeichnen.*

1. Anhang

*Folgende Unterlagen sind mit dem Bericht über die Aufsichtsprüfung einzureichen:*

1. Aktuelle Organigramme (im Minimum mit Angabe der verantwortlichen Personen pro Geschäftsbereich bzw. Abteilung)
2. Darstellung des Mitgliederkreises der Sicherungseinrichtung