Musterbericht

zur Aufsichtsprüfung für Zahlungsinstitute (Anhang E2)

Januar 2023

Inhalt

[1. Rahmenbedingungen der Aufsichtsprüfung 5](#_Toc122549717)

[2. Weitere Mandate der Revisionsstelle bei dem beaufsichtigten Zahlungsinstitut 5](#_Toc122549718)

[3. Zusammenfassung der Prüfresultate aus der Aufsichtsprüfung 5](#_Toc122549719)

[3.1 Beanstandungen 5](#_Toc122549720)

[3.2 Empfehlungen 5](#_Toc122549721)

[3.3 Beanstandungen des Vorjahres 6](#_Toc122549722)

[3.4 Empfehlungen des Vorjahres 6](#_Toc122549723)

[3.5 Bestätigung zu aufsichtsrechtlichen Vorgaben der FMA 6](#_Toc122549724)

[3.6 Wesentliche Feststellungen der Interne Revision 6](#_Toc122549725)

[3.7 Wesentliche Feststellungen durch Dritte 6](#_Toc122549726)

[3.8 Zusammenfassung zu weiteren Prüferkenntnissen sowie Gesamteinschätzung 6](#_Toc122549727)

[4. Wesentliche Feststellungen ausserhalb der Aufsichtsprüfung 7](#_Toc122549728)

[5. Wichtige Informationen zum geprüften Zahlungsinstitut / Darstellung bedeutender Änderungen 7](#_Toc122549729)

[5.1 Geschäftstätigkeit und Kundenstruktur 7](#_Toc122549730)

[5.2 Beteiligungsverhältnisse / Beziehungen zu anderen Unternehmen 7](#_Toc122549731)

[5.3 Betriebs- und Aufbauorganisation 7](#_Toc122549732)

[5.4 Wesentliche Änderungen beim beaufsichtigten Zahlungsinstitut 7](#_Toc122549733)

[6. Prüfresultate 8](#_Toc122549734)

[6.1 Geschäftsrisiken 9](#_Toc122549735)

[6.1.1 Kreditrisiken / Gegenparteiausfallrisiken im Zusammenhang mit Zahlungsgeschäften mit Kreditgewährung (GR-1) 9](#_Toc122549736)

[6.1.2 Operationelle Risiken im Zusammenhang mit der Erbringung von Zahlungsdiensten (GR-2) 10](#_Toc122549737)

[6.1.3 Operationelle Risiken im Zusammenhang mit der Erbringung von betrieblichen Dienstleistungen und damit eng verbundenen Nebendienstleistungen (GR-3) 11](#_Toc122549738)

[6.1.4 Operationelle Risiken im Zusammenhang mit dem Betrieb von Zahlungssystemen (GR-4) 12](#_Toc122549739)

[6.1.5 Operationelle Risiken im Zusammenhang mit anderen gewerbsmässigen Tätigkeiten (GR-5) 13](#_Toc122549740)

[6.1.6 Operationelle Risiken im Zusammenhang mit Cyberrisiken und neue Technologien (GR-6) 14](#_Toc122549741)

[6.1.7 Operationelle Risiken: Rechts- und Prozessrisiken inkl. Kundenbeschwerden (GR-7) 16](#_Toc122549742)

[6.1.8 [Weitere Operationelle Risiken von der Revisionsstelle selber zu definieren] (GR-8) 17](#_Toc122549743)

[6.1.9 Liquiditätsrisiken inkl. Refinanzierungsrisiken (GR-9) 18](#_Toc122549744)

[6.1.10 Risikokonzentrationen aus Kreditrisiken / Gegenparteiausfallrisiken (GR-10) 19](#_Toc122549745)

[6.1.11 Risikokonzentrationen aus operationellen Risiken (GR-11) 20](#_Toc122549746)

[6.1.12 [Weitere Risikokonzentrationen von der Revisionsstelle selber zu definieren] (GR-12) 21](#_Toc122549747)

[6.1.13 Sonstige Risiken im Zusammenhang mit grenzüberschreitenden Dienstleistungen (GR-13) 22](#_Toc122549748)

[6.1.14 Reputations- und Step-In-Risiken (GR-14) 23](#_Toc122549749)

[6.1.15 [Weitere sonstige Risiken von der Revisionsstelle selber zu definieren] (GR-15) 24](#_Toc122549750)

[6.2 Governance 25](#_Toc122549751)

[6.2.1 Geschäftsleitung (GOV-1) 25](#_Toc122549752)

[6.2.2 Verwaltungsrat (GOV-2) 26](#_Toc122549753)

[6.2.3 Interessenskonflikte (GOV-3) 27](#_Toc122549754)

[6.2.4 Interne Kontrollfunktion: Risikomanagementfunktion und Risikomanagement-Rahmenwerk (GOV-4) 28](#_Toc122549755)

[6.2.5 Interne Kontrollfunktion: Compliance (GOV-5) 29](#_Toc122549756)

[6.2.6 Interne Kontrollfunktion: Interne Revision (GOV-6) 30](#_Toc122549757)

[6.2.7 Auslagerungen (GOV-7) 31](#_Toc122549758)

[6.2.8 Business Continuity Management (Massnahmen zur Aufrechterhaltung des Geschäftsbetriebs) (GOV-8) 36](#_Toc122549759)

[6.2.9 IKT-Sicherheit (GOV-9) 38](#_Toc122549760)

[6.3 Anfangs- und Eigenkapital / Eigenmittel (EM-1) 44](#_Toc122549761)

[6.4 Sicherungsanforderungen (SA-1) 45](#_Toc122549762)

[6.5 Agenten, Vertreibern und Zweigstellen 46](#_Toc122549763)

[6.5.1 Inanspruchnahme von Agenten sowie Vertreibern (AVZ-1) 46](#_Toc122549764)

[6.5.2 Zweigstellen (AVZ-2) 47](#_Toc122549765)

[6.6 Andere Vorschriften / EBA/GL/2017/10 Schwerwiegende Betriebs- oder Sicherheitsvorfälle (EBA/GL/2017/10) und Starke Kundenauthentifizierung (DelVO (EU) Nr. 2018/389) (And-1) 48](#_Toc122549766)

[6.7 Periodisches Meldewesen (MW-1) 51](#_Toc122549767)

[6.8 Prüfresultate aus von der FMA Liechtenstein zusätzlich festgelegten Prüfgebieten / Risikoarten bzw. Prüffelder 57](#_Toc122549768)

[7. Weitere Bemerkungen 58](#_Toc122549769)

[8. Unterschrift / Bestätigung der Revisionsstelle 58](#_Toc122549770)

[9. Anhang 58](#_Toc122549771)

***Beaufsichtigtes Zahlungsinstitut***

Bericht der Revisionsstelle gemäss Zahlungsdienstegesetz 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 2023 anwendbar (aufsichtsrechtliche Berichterstattung für Prüfperioden beginnend am 01. Januar 2023]*

1. Rahmenbedingungen der Aufsichtsprüfung

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

* Bestätigung, dass die Prüfung gemäss der an die FMA vorab eingereichten Prüfstrategie durchgeführt wurden; Abweichungen sind zu begründen
* 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 das Zahlungsinstitut inkl. dessen Interne Revision; Restriktionen bei den Prüfungen z.B. reduzierter Prüfungsumfang infolge von durch das Zahlungsinstitut 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. 40a ZDG.

1. Weitere Mandate der Revisionsstelle bei dem beaufsichtigten Zahlungsinstitut

*Die Revisionsstelle führt allfällige weitere Mandate (z.B. Abschlussprüfung, vereinbarte Prüfungshandlungen, Beratungsmandate, andere Prüfmandate und Dienstleistungen) im berichtsrelevanten Zeitraum bei dem beaufsichtigten Zahlungsinstitut 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.*

* 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 das zu prüfende Zahlungsinstitut 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 der Interne Revision

*Die Revisionsstelle beschreibt an dieser Stelle allfällige wesentliche Feststellungen (v.a. Feststellungen mit hoher Gewichtung), durch die Interne Revision. Die Revisionsstelle hat die Feststellungen sowie deren Auswirkungen auf das Risikoprofil des Zahlungsinstituts angemessen zu würdigen. Die Revisionsstelle hat an dieser Stelle auch eine Auflistung sämtlicher Prüfthemen der Internen Revision im Berichtszeitraum darzustellen. Sofern die Feststellungen an anderer Stelle im Bericht dargestellt werden, ist eine entsprechende Referenz ausreichend.*

* 1. Wesentliche Feststellungen durch Dritte

*Die Revisionsstelle beschreibt an dieser Stelle allfällige wesentliche, aufsichtsrechtlich relevante Feststellungen durch Dritte (z.B. die für die konsolidierte Aufsicht zuständige ausländische Behörde; andere Revisionsstellen), zu denen sie innerhalb oder ausserhalb der Prüfungstätigkeit Kenntnis erlangt hat. Die Revisionsstelle hat die Feststellungen, sowie deren Auswirkungen auf das Risikoprofil des Zahlungsinstituts 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. Diesbezüglich hat die Revisionsstelle u.a. darzulegen, ob die finanzielle Solidität der qualifiziert Beteiligten des Zahlungsinstituts gegeben ist.*

*Des Weiteren hält die Revisionsstelle – basierend auf den Ergebnissen der durchgeführten Prüfungshandlungen – ein Prüfurteil fest, ob die internen Verfahren sicherstellen, dass die Bewilligungsvoraussetzungen (Art. 40b Abs. 1 Bst. b ZDG i.V.m. Art. 7 ff ZDG) eingehalten werden. Diesbezüglich erläutert die Revisionsstelle allfällige Vorkommnisse, welche die Einhaltung der Bewilligungsvoraussetzungen tangieren können. Die Revisionsstelle schlägt, falls notwendig, Massnahmen zur Wiederherstellung des ordnungsgemässen Zustands vor. Die Revisionsstelle beurteilt, inwiefern die Beanstandungen mit Fristansetzung im Berichtsjahr die Einhaltung der Bewilligungsvoraussetzungen in Frage stellen und hält fest, ob gemäss ihrer Einschätzung Massnahmen seitens der FMA notwendig sind oder nicht.*

*Die Revisionsstelle legt ein Prüfurteil - basierend auf den Ergebnissen der durchgeführten Prüfungshandlungen dar - ob die internen Verfahren sicherstellen, dass die Vorschriften über die Geschäftstätigkeit (Art. 40b Abs. 1 Bst. a ZDG i.V.m Art. 17 ff ZDG) eingehalten werden.*

*Zudem legt die Revisionsstelle ein Prüfurteil – basierend auf den Ergebnissen der durchgeführten Prüfungshandlungen im Rahmen der Abschlussprüfung dar - ob die internen Verfahren sicherstellen, dass der Geschäftsbericht und der konsolidierte Geschäftsbericht nach Form und Inhalt den gesetzlichen, statutarischen und reglementarischen Erfordernissen (Art. 41 Abs. 1 Bst. c ZDG) entsprechen.*

*Des Weiteren würdigt die Revisionsstelle unter diesem Titel summarisch die Gesamtsituation des Zahlungsinstituts sowie aktuelle Entwicklungen und weist zukunftsgerichtet auf mögliche (u.a. regulatorische) Herausforderungen hin.*

1. Wesentliche Feststellungen ausserhalb der Aufsichtsprüfung

*Stellt die Revisionsstelle ausserhalb der Aufsichtsprüfung Auffälligkeiten fest, welche wesentliche Auswirkungen auf die Risikolage des Finanzintermediärs haben und die in der Risikoanalyse zu berücksichtigen sind, so sind diese im Rahmen der Berichterstattung aufzuführen (z.B. Empfehlungen im Rahmen des Management Letters bei der Abschlussprüfung; steuerrechtliche Verfahren etc.)*

1. Wichtige Informationen zum geprüften Zahlungsinstitut / Darstellung bedeutender Änderungen
   1. Geschäftstätigkeit und Kundenstruktur

*Die Revisionsstelle erläutert kurz das Geschäftsmodell inkl. Beschreibung der Zahlungsdienste und Kundenstruktur des Zahlungsinstitut, die Kernmärkte unter Berücksichtigung der Notifikationen, der Vertrieb unter Berücksichtigung von Agenten und Vertreibern sowie diesbezügliche Veränderungen während dem Berichtsjahr.*

*Die Revisionsstelle nimmt zudem basierend auf den Erkenntnissen aus ihren Prüfungshandlungen Stellung dazu, ob die Geschäftstätigkeit bezogen auf die von der FMA bewilligten Tätigkeiten effektiv ausgeübt werden.*

* 1. Beteiligungsverhältnisse / Beziehungen zu anderen Unternehmen

*Die Revisionsstelle erläutert kurz die qualifiziert Beteiligten sowie wesentliche Beziehungen und Abhängigkeiten zu anderen Unternehmen oder Anspruchsträgern (z.B. wirtschaftlich bedeutende Verträge, konzerninterne Zusammenarbeit), sowie bestehende enge Verbindungen (gem. Art. 9 Abs. 1 lit. g ZDG). Diesbezügliche Veränderungen werden aufgeführt.*

* 1. Betriebs- und Aufbauorganisation

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

* 1. Wesentliche Änderungen beim beaufsichtigten Zahlungsinstitut

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

* *Organe*
* *Geschäftsmodell und Geschäftsstrategie*
* *Fusionen, Reorganisationen, Restrukturierungen, Delegationen*

1. Prüfresultate

*Die Revisionsstelle bewertet die Prüfelemente in Prüfgebieten mit Intervention durch „Ja (Detailprüfung)“, „Ja (kritische Beurteilung)“ oder „Nein“. Diese Prüfresultate gelten als Prüfbestätigungen 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 des Zahlungsinstituts und zugrundeliegende Quellen für die resultierende Beanstandung (Nachweise).*

*Eine Abstützung auf Ergebnisse der internen Revision ist im jeweiligen Prüfgebiet auszuweisen und selbstständig zu würdigen. Es ist anzugeben, in welchem Umfang die Interne Revision Prüfungshandlungen durchgeführt hat und zu welchem Ergebnis sie dabei gekommen ist.*

*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 Prüfgebiet bzw. -feld keine Intervention erfolgte, müssen diese nicht im Bericht aufgeführt werden, wobei die entsprechende Berichtsziffer inkl. der Formatvorlagen gelöscht werden kann.*

*Für Prüfgebiete bzw. -felder, welche im Berichtsjahr mittels Detailprüfung geprüft wurden, sind zwingend aussagekräftige Erläuterungen aufzuführen. Jene Prüfgebiete bzw. -felder, hinsichtlich welcher im Berichtjahr 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 des Zahlungsinstitut 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 im Verhältnis zum Gesamtvolumen 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 des Zahlungsinstituts bzw. an die Prüftiefe anzupassen. Werden die Mindestprüfinhalte durch die durchgeführten Prüfungshandlungen nicht vollständig abgedeckt, ist im Bericht über die Aufsichtsprüfung darauf hinzuweisen und zu begründen.*

* 1. Geschäftsrisiken
     1. Kreditrisiken / Gegenparteiausfallrisiken im Zusammenhang mit Zahlungsgeschäften mit Kreditgewährung (GR-1)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 2 Abs. 1 Bst. g und h ZDG i.V.m Art. 7 Abs. 7 ZDG; Art. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von Kreditrisiken im Zusammenhang mit Zahlungsgeschäften mit Kreditgewährung angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von Kreditrisiken im Zusammenhang mit Zahlungsgeschäften mit Kreditgewährung angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von Kreditrisiken im Zusammenhang mit Zahlungsgeschäften mit Kreditgewährung angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen Zahlungsinstitut;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. Operationelle Risiken im Zusammenhang mit der Erbringung von Zahlungsdiensten (GR-2)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 2 Abs. 2 Bst. a bis h ZDG; Art. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von operationellen Risiken im Zusammenhang mit der Erbringung von Zahlungsdiensten angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von operationellen Risiken im Zusammenhang mit der Erbringung von Zahlungsdiensten angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von operationellen Risiken im Zusammenhang mit der Erbringung von Zahlungsdiensten angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. Operationelle Risiken im Zusammenhang mit der Erbringung von betrieblichen Dienstleistungen und damit eng verbundenen Nebendienstleistungen (GR-3)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 7 Abs. 3 Bst. a ZDG; Art. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von operationellen Risiken im Zusammenhang mit der Erbringung von betrieblichen Dienstleistungen und damit eng verbundenen Nebendienstleistungen angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von operationellen Risiken im Zusammenhang mit der Erbringung von betrieblichen Dienstleistungen und damit eng verbundenen Nebendienstleistungen angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung operationellen Risiken im Zusammenhang mit der Erbringung von betrieblichen Dienstleistungen und damit eng verbundenen Nebendienstleistungen angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. Operationelle Risiken im Zusammenhang mit dem Betrieb von Zahlungssystemen (GR-4)

|  |  |  |  |
| --- | --- | --- | --- |
| 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 ZDG; Art. 7 Abs. 3 Bst. b ZDG; Art. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von operationellen Risiken im Zusammenhang mit dem Betrieb von Zahlungssystemen angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von operationellen Risiken im Zusammenhang mit dem Betrieb von Zahlungssystemen angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung operationellen Risiken im Zusammenhang mit dem Betrieb von Zahlungssystemen angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. Operationelle Risiken im Zusammenhang mit anderen gewerbsmässigen Tätigkeiten (GR-5)

|  |  |  |  |
| --- | --- | --- | --- |
| 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 ZDG; Art. 7 Abs. 3 Bst. c ZDG; EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von operationellen Risiken im Zusammenhang mit anderen gewerbsmässigen Tätigkeiten angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von operationellen Risiken im Zusammenhang mit anderen gewerbsmässigen Tätigkeiten angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von operationellen Risiken im Zusammenhang mit anderen gewerbsmässigen Tätigkeiten angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. Operationelle Risiken im Zusammenhang mit Cyberrisiken und neue Technologien (GR-6)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09; FMA-Mitteilung 2018/3 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von operationellen Risiken im Zusammenhang mit Cyberrisiken und neuen Technologien angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von operationellen Risiken im Zusammenhang mit Cyberrisiken und neuen Technologien angemessen ist. \* | | | *Ja (Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von operationellen Risiken im Zusammenhang mit Cyberrisiken und neuen Technologien angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken, insbesondere in Bezug auf kritische und/oder sensitive Daten und IKT-Systeme angemessen identifiziert werden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit von kritischen und/oder sensitiven Daten und IKT-Systemen durch angemessene Massnahmen geschützt sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass Cyberattacken durch eine systematische Überwachung der Technologieinfrastruktur zeitnah erkannt und aufgezeichnet werden\* | | | *Ja (Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass angemessene, zeitnahe Massnahmen als Reaktion auf Cyber-Attacken zur Aufrechterhaltung des normalen Geschäftsbetriebs in Abstimmung mit dem Business Continuity Management durchgeführt werden | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die zeitnahe Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken gewährleistet ist.\* | | | *Ja (Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren gewährleisten, dass die FMA innert 7 Tagen ab Kenntniserlangung über schwerwiegende oder betriebsstörende Cyber-Attacken informiert wird. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

*\*gekennzeichnete Bestätigungen sind mit eingeschränkter Prüfsicherheit («Kritische Beurteilung») zu bestätigen, unabhängig der Prüftiefe «Detailprüfung» gemäss Risikoanalyse*

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert* |
| *Cyberrisiken* | * + *Die internen Verfahren stellen sicher, dass die institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken, insbesondere in Bezug auf kritische und/oder sensitive Daten und IKT-Systeme angemessen identifiziert werden (u u.a. durch den Betrieb eines Security Operation Center (SOC) resp. die Zusammenarbeit mit einem externen SOC, die Durchführung von regelmässigen Verwundbarkeitsanalysen und Penetration Testings zur Überprüfung von Sicherheitslücken und zum Schutz kritischer und/oder sensitiver Daten und IT-Systeme)*   + *Die internen Verfahren stellen sicher, dass der Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen und/oder sensitiven Daten und IKT-Systeme gewährleistet ist*   + *Die internen Verfahren stellen sicher, dass Cyberattacken durch eine systematische Überwachung der Technologieinfrastruktur zeitnah erkannt und aufgezeichnet werden*   + *Die internen Verfahren stellen sicher, dass gezielte, zeitnahe Massnahmen als Reaktion auf Cyber-Attacken, insb. bei wesentlichen Cyberattacken zur Aufrechterhaltung des normalen Geschäftsbetriebs in Abstimmung mit dem Business Continuity Management, durchgeführt werden.*   + *Die internen Verfahren stellen sicher, dass die zeitnahe Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen gewährleistet ist.*   + *Die internen Verfahren gewährleisten, dass die FMA innert 7 Tagen ab Kenntniserlangung über schwerwiegende oder betriebsstörende Cyber-Attacken informiert wird* |

*Text*

* + 1. Operationelle Risiken: Rechts- und Prozessrisiken inkl. Kundenbeschwerden (GR-7)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 8 Bst. e ZDG; Art. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09; FMA-Mitteilung 2015/2 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von operationellen Risiken im Zusammenhang mit Rechts- und Prozessrisiken inkl. Kundenbeschwerden angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von operationellen Risiken im Zusammenhang mit Rechts- und Prozessrisiken inkl. Kundenbeschwerden angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von operationellen Risiken im Zusammenhang mit Rechts- und Prozessrisiken inkl. Kundenbeschwerden angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert* |

*Text*

* + 1. [Weitere Operationelle Risiken von der Revisionsstelle selber zu definieren] (GR-8)

|  |  |  |  |
| --- | --- | --- | --- |
| 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:  tbd | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von [weiteren operationellen Risiken - tbd] angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von [weiteren operationellen Risiken – tbd] angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von [weiteren operationellen Risiken – tbd] angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert* |

*Text*

* + 1. Liquiditätsrisiken inkl. Refinanzierungsrisiken (GR-9)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 8 Bst. e ZDG; Art. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von Liquiditätsrisiken\* inkl. Refinanzierungsrisiken angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von Liquiditätsrisiken inkl. Refinanzierungsrisiken angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von Liquiditätsrisiken inkl. Refinanzierungsrisiken angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert* |

\*Mit dem Liquiditätsrisiko wird das Risiko bezeichnet gegenwärtigen oder zukünftigen Zahlungsverpflichtungen nicht mehr vollständig oder nicht fristgerecht nachkommen zu können. Mit dem Refinanzierungsrisiko wird das Risiko bezeichnet die benötigten Zahlungsmittel nur zu erhöhten Refinanzierungskosten beschaffen zu können.

*Text*

* + 1. Risikokonzentrationen aus Kreditrisiken / Gegenparteiausfallrisiken (GR-10)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 2 Abs. 2 Bst. g und h ZDG i.V.m Art. 7 Abs. 7 ZDG; Art. 9 Abs. 1 Bst. g ZDG, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von Risikokonzentrationen aus Kreditrisiken angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von Risikokonzentrationen aus Kreditrisiken angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von Risikokonzentrationen aus Kreditrisiken angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher;* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenendes Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. Risikokonzentrationen aus operationellen Risiken (GR-11)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 8 Bst. e ZDG, Art. 9 Abs. 1 Bst. e ZDG, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von Risikokonzentrationen aus operationellen Risiken angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von Risikokonzentrationen aus operationellen Risiken angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von Risikokonzentrationen aus operationellen Risiken angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher;* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenendes Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. [Weitere Risikokonzentrationen von der Revisionsstelle selber zu definieren] (GR-12)

|  |  |  |  |
| --- | --- | --- | --- |
| 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:  tbd | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von [weiteren Risikokonzentrationen – tbd] angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von [weiteren Risikokonzentrationen – tbd]] angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von [weiteren Risikokonzentrationen – tbd] angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher;* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert;* |

*Text*

* + 1. Sonstige Risiken im Zusammenhang mit grenzüberschreitenden Dienstleistungen (GR-13)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 27 f ZDG; EBA/GL/2017/09; FMA-Mitteilung 2015/3 | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von sonstigen Risiken im Zusammenhang mit grenzüberschreitenden Dienstleistungen angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von sonstigen Risiken im Zusammenhang mit grenzüberschreitenden Dienstleistungen angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von sonstigen Risiken im Zusammenhang mit grenzüberschreitenden Dienstleistungen angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert* |

*Text*

* + 1. Reputations- und Step-In-Risiken (GR-14)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 9 Abs. 1 Bst. g ZDG; | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von Reputations- und Step-In-Risiken angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von Reputations- und Step-In-Risiken angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von Reputations- und Step-In-Risiken angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert* |

*Text*

* + 1. [Weitere sonstige Risiken von der Revisionsstelle selber zu definieren] (GR-15)

|  |  |  |  |
| --- | --- | --- | --- |
| 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:  tbd | | | |
|  | | | |
| Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das Management von [weiteren sonstigen Risiken – tbd] angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem für das Management von [weiteren sonstigen Risiken – tbd]] angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung und Steuerung von [weiteren sonstigen Risiken – tbd] angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Es bestehen wirksame interne Eskalationsmechanismen;*   + *Die Verantwortlichkeiten und Kompetenzen sind klar und angemessen geregelt;*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher* |
| *Internes Kontrollsystem* | * + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   + *Die internen Verfahren sehen die Anwendung des 4-Augen-Prinzips oder Funktionstrennung bei Schlüsselkontrollen vor;*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen;*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |
| *Risikomanagement* | * + *Die wesentlichen Risiken werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht und gesteuert;*   + *Die Annahmen und Parameter des Risikomanagements werden regelmässig validiert;*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert* |

*Text*

* 1. Governance
     1. Geschäftsleitung (GOV-1)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 8 ZDG, Art. 9 Abs. 1 Bst. d ZDG, FMA-Wegleitung 2019/8, EBA/GL/2017/09 | | | |
|  | | | |
| 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 fachliche Eignung regelmässig intern überprüft wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder der Geschäftsleitung die Struktur des Zahlungsinstituts sowie deren Geschäftsfelder und Risiken kennen | | | *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* |
| *Fachliche 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 kennen die Struktur, in denen sich das Zahlungsinstitut bewegt ("Know-Your-Structure")*   + *Die Mitglieder des Gremiums kennen sämtliche Geschäftsfelder und Risiken des Zahlungsinstituts ("Know Your Business and Risks")*   + *Die Mitglieder des Gremiums werden regelmässig fachlich einschlägig weitergebildet*   + *Die Mitglieder des Gremiums sind zuverlässig, kümmern sich ausnahmslos um das gesetzeskonforme Gebahren des Zahlungsinstituts und haben einen guten Ruf.* |

*Text*

* + 1. Verwaltungsrat (GOV-2)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 8 ZDG, Art. 9 Abs. 1 Bst. d ZDG, FMA-Wegleitung 2019/8, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die die Verantwortlichkeiten und Kompetenzen des Verwaltungsrats angemessen ausgestaltet sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder des Verwaltungsrats sowohl individuell als auch kollektiv geeignet sind und ihre fachliche Eignung regelmässig intern überprüft wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder des Verwaltungsrats die Struktur des Zahlungsinstituts sowie deren Geschäftsfelder und Risiken kennen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Mitglieder des Verwaltungsrats 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* |
| *Fachliche 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 kennen die Struktur, in denen sich das Zahlungsinstitut bewegt ("Know-Your-Structure")*   + *Die Mitglieder des Gremiums kennen sämtliche Geschäftsfelder und Risiken des Zahlungsinstituts ("Know Your Business and Risks")*   + *Die Mitglieder des Gremiums werden regelmässig fachlich einschlägig weitergebildet*   + *Die Mitglieder des Gremiums sind zuverlässig, kümmern sich ausnahmslos um das gesetzeskonforme Gebahren des Zahlungsinstituts und haben einen guten Ruf.* |

*Text*

* + 1. Interessenskonflikte (GOV-3)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 9 Abs. 1 Bst. e, g ZDG, FMA-Wegleitung 2019/8, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass adäquate Richtlinien und Verfahren für den Umgang mit Interessenskonflikten auf Ebene des Zahlungsinstituts bestehen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass adäquate Richtlinien und Verfahren für den Umgang mit Interessenskonflikten für Mitarbeiter bestehen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass adäquate Richtlinien und Verfahren für den Umgang mit Interessenskonflikten für den Verwaltungsrat bestehen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass adäquate Richtlinien und Verfahren für den Umgang mit Interessenskonflikten für die Geschäftsleitung bestehen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass adäquate Richtlinien und Verfahren für den Umgang mit Interessenskonflikten für natürliche und juristische Personen, die enge Verbindungen zum des Zahlungsinstituts aufweisen, bestehen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Richtlinien und Verfahren für den Umgang mit Interessenskonflikten*  *- auf Ebene Zahlungsinstituts*  *- für Mitarbeiter*  *- für den Verwaltungsrat*  *- für die Geschäftsleitung*  *- für natürliche und juristische Personen mit engen Verbindungen zum Zahlungsinstitut* | * + *Es besteht eine klare und effektive Aufteilung von Verantwortlichkeiten und Kompetenzen*   + *Es bestehen interne Richtlinien, welche den Umgang mit Interessenskonflikten auf Ebene des Zahlungsinstituts, für Mitarbeiter, für den Verwaltungsrat, die Geschäftsleitung, sowie für enge Verbindungen regeln*   + *Das beaufsichtigte Zahlungsinstitut hat Massnahmen zur Steuerung oder Minderung von Interessenskonflikten auf institutioneller Ebene implementiert (z.B. Aufgabentrennung, Einrichtung von Informationssperren; Festlegung geeigneter Verfahren für Transaktionen mit verbundenen Parteien etc.), welche dokumentiert sind*   + *Es besteht ein angemessenes Meldeverfahren für Interessenskonflikte z.B. für Beziehungen von Mitarbeitenden aus der Vergangenheit*   + *Es besteht ein Bewertungsverfahren von tatsächlichen und potenziellen Interessenskonflikten und ein Dokumentationsverfahren über die Entscheidung, wie mit den festgestellten Interessenskonflikten umgegangen wird*   + *Es besteht eine angemessene interne Berichterstattung und Kommunikation über identifizierte Interessenskonflikte* |

*Als enge Verbindung gelten insbesondere die in Art. 4 Abs. 1 Ziff. 38 Verordnung (EU) Nr. 575/2013.*

*Die unabhängigen Mitglieder des Verwaltungsrats sind – unabhängig der Prüftiefe (kritische Beurteilung/Detailprüfung) - jeweils im Text aufzulisten und zu kennzeichnen.*

*Text*

* + 1. Interne Kontrollfunktion: Risikomanagementfunktion und Risikomanagement-Rahmenwerk (GOV-4)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 9 Abs. 1 Bst. e ZDG, FMA-Wegleitung 2019/8, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die organisatorische Anordnung der Risikomanagementfunktion und das Entschädigungssystem dieser keine Zielkonflikte herbeiführen und deren Unabhängigkeit nicht negativ beeinflussen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Verantwortlichkeiten und Kompetenzen der Risikomanagementfunktion angemessen ausgestaltet sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die technischen und personellen Ressourcen angemessen sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren ein angemessenes Berichterstattungswesen sicherstellen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Verantwortlichen der Risikomanagementfunktion sich fortlaufend fachlich adäquat weiterbilden | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Risikomanagement-Rahmenwerk angemessen ausgestaltet ist. | | |  |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Ausgestaltung der Risikomanagementfunktion* | * + *Die Risikomanagementfunktion ist unabhängig ausgestaltet*   + *Es bestehen klare Verantwortlichkeiten und Kompetenzen*   + *Die Risikomanagementfunktion ist ressourcentechnisch (personelle und technische Ressourcen) angemessen*   + *Die Mitarbeiter im Risikomanagement werden regelmässig weitergebildet*   + *Die Risikomanagementfunktion kann ungefiltert an den Verwaltungsrat berichten* |
| *Ausgestaltung des Risikomanagement-Rahmenwerks* | * + *Das Rahmenwerk stellt die Identifizierung und Quantifizierung sämtlicher wesentlicher Risiken sicher inkl. den Risiken aus dem makroökonomischen Umfeld und geopolitische Risiken*   + *Das Rahmenwerk nutzt zur Quantifizierung u.a. risikoadjustierte Erfolgskennzahlen*   + *Das Rahmenwerk steht in Einklang mit dem Risikoappetit Zahlungsinstituts (konsistentes und validiertes Limitwesen)*   + *Das Rahmenwerk berücksichtigt die interne Budgetierung und Mehrjahresplanung*   + *Das Rahmenwerk wurde in die Gesamtsteuerung konsistent integriert*   + *Das Rahmenwerk gewährleistet die Etablierung angemessener Management-Puffer*   + *Das Rahmenwerk inkludiert ein unabhängiges und regelmässiges internes Überprüfungsverfahren des Risikomanagement-Rahmenwerks sowie Verfahren zur Weiterentwicklung*   + *Das Rahmenwerk stellt sicher, dass die Ergebnisse aus dem Risikomanagement tatsächlich zur Steuerung von Risiken verwendet werden* |

*Text*

* + 1. Interne Kontrollfunktion: Compliance (GOV-5)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 9 Abs. 1 Bst. e ZDG, FMA-Wegleitung 2019/8, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die organisatorische Anordnung der Compliance-Funktion und das Entschädigungssystem dieser keine Zielkonflikte herbeiführen und deren Unabhängigkeit nicht negativ beeinflussen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Verantwortlichkeiten und Kompetenzen der Compliance-Funktion angemessen ausgestaltet sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die technischen und personellen Ressourcen angemessen sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren ein angemessenes Berichterstattungswesen sicherstellen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass interne Verfahren bestehen, welche sicherstellen, dass die Compliance-Funktion die Gesetzeskonformität der Geschäftstätigkeit laufend beurteilt | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Ausgestaltung der Compliance-Funktion* | * + *Die Compliance-Funktion ist unabhängig ausgestaltet*   + *Es bestehen klare Verantwortlichkeiten und Kompetenzen*   + *Die Compliance-Funktion ist ressourcentechnisch (personell und technische Ressourcen) angemessen*   + *Die Mitarbeiter im Compliance werden regelmässig weitergebildet*   + *Die Compliance-Funktion kann ungefiltert an den Verwaltungsrat berichten*   + *Die Compliance-Funktion prüft die Gesetzeskonformität der Geschäftstätigkeit laufend* |

*Text*

* + 1. Interne Kontrollfunktion: Interne Revision (GOV-6)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 9 Abs. 1 Bst. e ZDG, FMA-Wegleitung 2019/8, EBA/GL/2017/09 | | | |
|  | | | |
| Bestätigung, dass die organisatorische Anordnung der Internen Revision und das Entschädigungssystem dieser keine Zielkonflikte herbeiführen und deren Unabhängigkeit nicht negativ beeinflussen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Verantwortlichkeiten und Kompetenzen der Internen Revision angemessen ausgestaltet sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die technischen und personellen Ressourcen angemessen sind | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren und die Organisationsstruktur ein angemessenes Berichterstattungswesen der Internen Revision sicherstellen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass der Prüfplan der Internen Revision auf einem angemessenen risikobasierenden Ansatz beruht, einen angemessenen Zeithorizont umfasst und die Risikobeurteilung und der Prüfplan durch den Verwaltungsrat genehmigt werden | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass ein angemessenes Mängelbeseitigungsverfahren (Audit Tracking) existiert und effektiv angewandt wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Ausgestaltung der Internen Revision* | * + *Die Funktion stellt sicher, dass keine Selbstprüfung stattfindet*   + *Es bestehen klare Verantwortlichkeiten und Kompetenzen*   + *Die Funktion ist ressourcentechnisch (personell und technisch) angemessen ausgestattet*   + *Die Mitarbeiter werden regelmässig weitergebildet*   + *Die Interne Revision kann ungefiltert an den Verwaltungsrat berichten*   + *Die Interne Revision erstattet dem Verwaltungsrat regelmässig, zumindest jährlich, objektiv, vollständig, klar und zeitnah über die Prüfungstätigkeiten zumindest durch Darlegung des Prüfungsgegenstands, der Prüfungsfeststellungen und der Massnahmen Bericht.*   + *Die interne Revision verfügt über ein umfassendes und uneingeschränktes Auskunfts-, Einsichts- und Prüfrecht für sämtliche Unterlagen, Arbeitspapiere und IT-Systeme.* |
| *Prüfplan* | * + *Der Prüfplan basiert auf einem risikobasierenden Ansatz (unter Berücksichtigung von IKS und Risikomanagement)*   + *Die Risikobeurteilung und Prüfungsplanung umfassen alle wesentlichen Geschäftsaktivitäten, Kontrollsysteme und Risiken der Bank.*   + *Die Risikobeurteilung und der Prüfplan werden vom Verwaltungsrat jährlich genehmigt*   + *Ad-hoc-Anpassungen des Prüfplans werden ebenfalls durch den Verwaltungsrat genehmigt* |
| *Audit Tracking* | * + *Es existiert ein angemessenes Mängelbeseitigungsverfahren*   + *Das Mängelbeseitigungsverfahren wird auch effektiv angewandt* |

*Text*

* + 1. Auslagerungen (GOV-7)

|  |  |  |  |
| --- | --- | --- | --- |
| 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 2019:   * + Auslagerungspolitik / -richtlinien (Kritische Beurteilung)   + Dokumentationsanforderungen / Registerführung (Detailprüfung) | | *Beispiel:*  *2014: Analyse vor Auslagerung / Auslagerungsvereinbarungen (Kritische Beurteilung)*  *2015: Identifikation von Auslagerungen i.V.m kritischer oder wesentlicher Funktionen (Kritische Beurteilung)*  *2016: Internes Kontrollsystem von Auslagerungen / Interne Revision der ausgelagerten Tätigkeiten (Detailprüfung)*  *2017: Risikomanagement von Auslagerungen (Kritische Beurteilung)*  *2018: Ausstiegsstrategien (Detailprüfung)* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 24 ZDG, Art. 5a ZDV, Art. 34b und 35 BankV, EBA/GL/2019/02, EBA/GL/2017/02 | | | |
|  | |  | |
| *[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* |

|  |  |  |
| --- | --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** | ***Bestätigungen*** |
| *Auslagerungspolitik / -richtlinien* | * + *Die Auslagerungspolitik sowie die internen Verfahren stellen die Einhaltung der regulatorischen Bestimmungen sicher*   + *Die Auslagerungsrichtlinien sind anagemessen ausgestaltet und decken zumindest folgende Gesichtspunkte ab:*     - *Zuständigkeiten von Verwaltungsrat und Geschäftsleitung*     - *Einbindung der Geschäftsbereiche und der internen Kontrollfunktionen*     - *Planung von Auslagerungsvereinbarungen*     - *Umsetzung, Überwachung und das Management von Auslagerungsvereinbarungen*     - *Dokumentation von Auslagerungsvereinbarungen*     - *Ausstiegsszenarien und Kündigungsverfahren inkl. eines dokumentierten Ausstiegsplans für jede auszulagernde kritische oder wesentliche Funktion*   + *Die Auslagerungsrichtlinien wurden vom Verwaltungsrat genehmigt*   + *Die Auslagerungsrichtlinien werden regelmässig überprüft und aktualisiert*   + *Die Auslagerungsrichtlinien werden angemessen umgesetzt* | * + *Bestätigung, dass eine angemessene Auslagerungspolitik zu Auslagerungen sowie interne Verfahren bestehen, die die Einhaltung der regulatorischen Bestimmungen zu Auslagerungen sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die internen Auslagerungsrichtlinien angemessen ausgestaltet sind, regelmässig überprüft und aktualisiert werden* |
| *Analyse vor der Auslagerung* | * + *Die internen Verfahren stellen sicher, dass vor der Auslagerung die aufsichtlichen Bedingungen für eine Auslagerung geprüft werden und erfüllt sind*   + *Die internen Verfahren stellen sicher, dass die wesentlichen Risiken der Auslagerungsvereinbarung im Vorfeld ermittelt und bewertet werden*   + *Die internen Verfahren stellen ein angemessenes Auswahl- und Bewertungsverfahren (Due-Diligence-Prüfung) des künftigen Dienstleisters sicher*   + *Das Auswahl- und Bewertungsverfahren für die Auslagerung von kritischen und wesentlichen Funktionen hat die Beurteilung der Reputation, der angemessenen und ausreichenden Fähigkeiten, Fachkenntnisse, Kapazitäten, personelle und finanzielle Mittel und eine angemessene Organisationsstruktur zu beinhalten*   + *Die internen Verfahren stellen sicher, dass Interessenskonflikte, die durch die Auslagerung entstehen könnten, im Vorfeld der Auslagerungsvereinbarung analysiert und bewertet werden* | * + *Bestätigung, dass angemessene interne Verfahren für die Analyse des Dienstleister und der auszulagernden Funktionen/Prozesse/Dienstleistungen vor der effektiven Auslagerung bestehen, die die Prüfung der aufsichtlichen Bedingungen, die Berücksichtigung wesentlicher Risiken, eine angemessene Due-Diligence-Prüfung und die Analyse von Interessenskonflikte berücksichtigen* |
| *Auslagerungsvereinbarungen* | * + *Die internen Verfahren stellen sicher, dass für sämtliche ausgelagerte Funktionen/Prozesse/Dienstleistungen schriftliche Auslagerungsvereinbarungen abgeschlossen werden*   + *Die internen Verfahren stellen sicher, dass die Auslagerungsvereinbarung die Rechte und Pflichten des Dienstleisters und des Zahlungsinstituts, die Ziele und Massnahmen bzgl. der Informationssicherheit (Cybersecurity, Datenlebenszyklus, Datenverschlüsselung, Standort, Rechenzentren etc.), die Prozesse zur Behandlung, Eskalations- und Berichterstattung von Betriebs- und Sicherheitsvorfällen eindeutig festlegt*   + *Die internen Verfahren stellen sicher, dass die Auslagerungsvereinbarung darlegt, ob Weiterverlagerungen von kritischen oder wesentlichen Funktionen zulässig sind oder nicht*   + *Die Auslagerungsvereinbarung beinhaltet Kündigungsrechte*   + *Die Auslagerungsvereinbarungen stellen sicher, dass das Zahlungsinstitut, die interne und externe Revisionsstelle sowie die FMA über uneingeschränkte Zugangs-, Informations- und Prüfungsrechte zu den ausgelagerten Diensten, Systemen und Cloud-Services verfügt (im Falle einer Weiterverlagerung auch gegenüber Subunternehmen).* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass die schriftlichen Auslagerungsvereinbarungen angemessen ausgestaltet sind* |
| *Identifikation von Auslagerungen i.V.m kritischer oder wesentlicher Funktionen* | * + *Die internen Verfahren stellen die vollständige und korrekte Identifikation der ausgelagerten Funktionen/Prozesse/Dienstleistungen an einen Dienstleister („Auslagerungen“) sicher*   + *Die internen Verfahren stellen die angemessene Identifikation der kritischen oder wesentlichen ausgelagerten Funktionen/Prozesse/Dienstleistungen des Zahlungsinstituts gemäss regulatorischen und internen Bestimmungen sicher*   + *Die internen Verfahren stellen bei Weiterverlagerung von kritischen oder wesentlichen Funktionen sicher, dass die Auslagerungsvereinbarung die vorgegebenen regulatorischen Mindestinhalte beinhaltet: Angaben von Tätigkeiten die von einer Weiterverlagerung ausgeschlossen sind; Bedingungen, die bei der Weiterverlagerung vom Dienstleister einzuhalten sind; die Überwachungspflichten des Dienstleisters; die Genehmigungs- und Informationspflichten des Dienstleisters, die Kündigungsrechte für Zahlungsinstitute im Falle einer unzulässigen Weiterverlagerung durch den Dienstleister* | * + *Bestätigung, dass die internen Verfahren gewährleisten, dass die ausgelagerten Funktionen/Prozesse/Dienstleistungen an einen Dienstleister vollständig und korrekt identifiziert werden.*   + *Bestätigung, dass die internen Verfahren die angemessene Definition der kritischen oder wesentlichen ausgelagerten Funktionen/Prozesse/Dienstleistungen des Zahlungsinstituts gemäss regulatorischen und internen Bestimmungen sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass bei der Weiterverlagerung von kritischen oder wesentlichen Funktionen die Auslagerungsvereinbarung die vorgegebenen regulatorischen Mindestinhalte beinhaltet* |
| *Internes Kontrollsystem von Auslagerungen* | * + *Die Verantwortlichkeiten und Kompetenzen für die Dokumentation, das Management und die Kontrolle von Auslagerungsvereinbarungen sind klar und angemessen geregelt;*   + *Die Verantwortlichkeiten und Kompetenzen zur Instruktion, Steuerung und Überwachung von Dienstleistern sind durch die angemessene Ausgestaltung der Auslagerungsfunktion klar geregelt.*   + *Es besteht eine angemessene Funktionentrennung zwischen dem Management und der Kontrolle von Auslagerungsvereinbarungen*   + *Es besteht ein angemessener Prozess zur ordnungsgemässen Überwachung und Bewertung von Dienstleistern (z.B. Service Reports, Bewertungsprogramm, KPIs etc.) und ihrer Leistungserbringung (Aufdeckung, Beurteilung und Behebung von Mängeln)*   + *Es bestehen angemessene Verfahren zur Beurteilung oder zur Gewährleistung von Schlüsselkontrollen, die an die Dienstleister ausgelagert wurden (z.B. unabhängige Beurteilungen, etc.)*   + *Es bestehen angemessene Verfahren zur Erkennung, Vermeidung, Bewertung, Reduzierung und Offenlegung von Interessenkonflikten hinsichtlich der Auslagerungsvereinbarungen*   + *Es bestehen jederzeit angemessene Personalressourcen (Anzahl, Eignung, Zuverlässigkeit) um ein angemessenes Management und die Überwachung der Auslagerungsvereinbarungen sicherzustellen*   + *Es bestehen angemessene interne Verfahren um sicherzustellen, dass die Auslagerung nicht zur Delegation der Aufgaben des Verwaltungsrats führt*   + *Es bestehen wirksame interne Eskalationsmechanismen in Bezug auf die Nicht-Einhaltung von Kontrollen zur Überwachung der Auslagerungen*   + *Die internen Verfahren gewährleisten ein angemessenes Dokumentations- und Archivierungswesen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* | * + *Bestätigung, dass das Interne Kontrollsystem für die Dokumentation, das Management und die Kontrolle von Auslagerungsvereinbarungen und Outsourcing-Dienstleistern/Drittanbietern angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.* |
| *Risikomanagement von Auslagerungen* | * + *Die wesentlichen Risiken, welche durch Vereinbarungen mit Dienstleistern verursacht werden, werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht, gesteuert und dokumentiert;*   + *Bei Weiterverlagerungen an einen anderen Dienstleister („Ketten-Auslagerungen“) sind die daraus entstehenden Risiken in der Risikobewertung zu berücksichtigen*   + *Die Risikobewertung hat zumindest Folgendes zu umfassen: Sensitivität der Daten und Systeme, Sicherheitsmassnahmen, Folgen des Standorts des Dienstleisters, politische Stabilität, Sicherheitslage der betreffenden Rechtsordnungen, Vertraulichkeit von Daten, Kontinuität ausgelagerter Tätigkeiten, Integrität und Rückverfolgbarkeit von Daten und Systemen*   + *Die Auslagerungsfunktion innerhalb der Risikomanagementfunktion ist angemessen ausgestaltet und unmittelbar dem Leitungsorgan unterstellt*   + *Die Auslagerungsfunktion dokumentiert sämtliche Auslagerungsvereinbarungen*   + *Die Auslagerungsfunktion ist für die Steuerung und Kontrolle des Risikos aus Auslagerungen verantwortlich*   + *Die Szenarien berücksichtigen mögliche Auswirkungen unterlassener oder unzureichender Dienstleistungen von Dienstleistern*   + *Die Annahmen, Parameter und Szenarien des Risikomanagements werden regelmässig validiert*   + *Die verwendeten Daten sind von hoher Aktualität und Qualität;*   + *Die Risiken werden transparent und angemessen quantifiziert*   + *Die Ergebnisse und Analysen werden angemessen dokumentiert* | * + *Bestätigung, dass die Methoden zur Identifikation, Bewertung, Messung, Begrenzung, Überwachung, Steuerung und Dokumentation von Risiken, welche durch Vereinbarungen mit Dienstleistern für Auslagerungen verursacht werden angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden* |
| *Interne Revision der ausgelagerten Tätigkeiten* | * + *Die Interne Revision verfügt über uneingeschränktes Zugangs-, Informations- und Prüfungsrecht zu den ausgelagerten Tätigkeiten*   + *Die internen Verfahren stellen sicher, dass der risikobasierte Prüfplan der internen Revision u.a. die Prüfung der Auslagerungsvereinbarungen für kritische oder wesentliche Funktionen umfasst*   + *Die Interne Revision prüft hinsichtlich des Auslagerungsprozess zumindest Folgendes: Rahmenwerk für Auslagerungen inkl. Auslagerungsrichtlinien; Bewertung der Kritikalität oder Wesentlichkeit von Funktionen; die Risikobewertung der Auslagerungsvereinbarungen, die angemessene Einbringung vom Verwaltungsrat, die angemessene Überwachung und das Management von Auslagerungsvereinbarungen* | * + *Bestätigung, dass die interne Revisionsfunktion für die Überprüfung der ausgelagerten Funktionen/Prozesse/Dienstleistungen angemessen ausgestaltet ist und die ausgelagerten Funktionen/Prozesse/Dienstleistungen im risikobasierten Prüfplan der Internen Revision angemessen adressiert und geprüft werden* |
| *Dokumentationsanforderungen / Registerführung* | * + *Die internen Verfahren stellen sicher, dass ein Register mit Informationen über alle Auslagerungsvereinbarungen geführt und laufend aktualisiert wird*   + *Die internen Verfahren stellen sicher, dass das Register vollständig und den Mindestinhalten der regulatorischen Vorschriften entspricht* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass ein Register mit Informationen über alle Auslagerungsvereinbarungen vollständig, gemäss den regulatorischen Mindestinhalten, geführt und laufend aktualisiert wird* |
| *Ausstiegsstrategien* | * + *Die Ausstiegsstrategie stimmt mit der Auslagerungspolitik und den Plänen zur Geschäftsfortführung (BCM) überein*   + *Die internen Verfahren stellen die Entwicklung von angemessenen Ausstiegspläne sicher*   + *Die Ausstiegspläne werden angemessen dokumentiert*   + *Die Ausstiegspläne sind ausreichend erprobt (z.B. Durchführung einer Analyse der potenziellen Kosten, Folgen, Mittel und zeitlicher Auswirkungen der Übertragung auf einen anderen Anbieter)*   + *Für Wiedereingliederungen von ausgelagerten Funktionen bestehen angemessene interne Verfahren*   + *Die internen Verfahren stellen sicher, dass ausgelagerte Tätigkeiten ohne wesentlichen Unterbruch der Geschäftstätigkeiten wieder in das Zahlungsinstitut eingegliedert werden können* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass angemessene Ausstiegsstrategien und –pläne existieren, die mit der Auslagerungspolitik und den Plänen zur Geschäftsfortführung (BCM) übereinstimmen und die regelmässig erprobt werden* |

\*Der Begriff „Dienstleister“ beinhaltet gruppeninterne Dienstleister als auch Dritte.

*Text*

* + 1. Business Continuity Management (Massnahmen zur Aufrechterhaltung des Geschäftsbetriebs) (GOV-8)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 8 Abs. 1 Bst. h ZDG; FMA-Wegleitung 2019/8; EBA/GL/2017/09; EBA/GL/2019/02, EBA/GL/2019/04, EBA/GL/2017/11; Art. 35 BankV | | | |
|  | | | |
| 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 (Notfallpläne) 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 (Notfallpläne) alle wichtigen Funktionen und Ressourcen (inkl. ausgelagerte kritische oder wesentliche Funktionen) umfasst. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Zahlungsinstitut über angemessene Notfallpläne verfügt, welche sicherstellen, dass das Zahlungsinstitut ihre Tätigkeit ohne Unterbruch aufrechterhalten kann 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 (Notfallpläne) und der Massnahmen sicherstellen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die internen Verfahren zum Business Continuity Management angemessen im Mehrjahresplan der internen Revision berücksichtigt und regelmässig geprüft werden | | | *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, Prozessabhängigkeiten und der Kritikalität der identifizierten und klassifizierten Geschäftsfunktionen, Unterstützungsprozesse, Drittparteien und IKT-Assets sicher*   + *Die internen Verfahren stellen sicher, dass die wesentlichen Geschäftsbereiche und interne Einheiten bzw. Prozesse inkl. ausgelagerter kritischer oder wesentlicher Funktionen in die Analyse miteinbezogen werden*   + *Die internen Verfahren stellen die regelmässige und angemessene Durchführung von Business Impact Analysen sicher*   + *Die internen Verfahren regeln Kriterien aufgrund welcher eine ad-hoc Business Impact Analyse ausserhalb des normalen Aktualisierungszyklus ausgelöst wird (z.B. neue Produkte / Geschäftsfelder, Veränderungen der IT Infrastruktur, etc.)* |
| *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 (Notfallpläne, Pläne zur Aufrechterhaltung des Geschäftsbetriebs und Pläne zur Wiederherstellung) angemessen dokumentiert und genehmigt ist*   + *Die internen Verfahren stellen die Verfügbarkeit einer aktuellen und angemessenen Business Continuity Strategie (Notfallpläne, Pläne zur Aufrechterhaltung des Geschäftsbetriebs und Pläne zur Wiederherstellung) sicher*   + *Die internen Verfahren stellen die Berücksichtigung von verschiedenen Szenarien (u.a. Cyber-Angriffsszenarien) im Business Continuity Plan sowie die Bewertung möglicher Auswirkungen sicher*   + *Die internen Verfahren stellen sicher, dass Massnahmen (Reaktions- und Wiederherstellungspläne) für die Verfügbarkeit, Kontinuität und Wiederherstellung der für die gemäss Business Continuity Strategie wichtigen und zeitkritischen Geschäftsfunktionen, Unterstützungsprozesse, IKT-Assets und deren gegenseitige Abhängigkeiten definiert sind.*   + *Die internen Verfahren gewährleisten, dass die Massnahmen das Vorgehen, die Mittel und die notwendigen Ressourcen zur Überbrückung und Wiederherstellung der wichtigen und zeitkritischen Geschäftsfunktionen, Unterstützungsprozesse, IKT-Assets und deren gegenseitige Abhängigkeiten berücksichtigen.*   + *Die internen Verfahren stellen die Schulung von Mitarbeitenden und die Kommunikation innerhalb des Zahlungsinstituts über die Massnahmen sicher* |
| *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 und Berichterstattung 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 innerhalb des Zahlungsinstituts angemessen kommuniziert wurden.* |
| *Business Continuity Review* | * + *Die internen Verfahren stellen sicher, dass die Prüfung der internen Verfahren zum Business Continuity Management angemessen in der Mehrjahresplanung der Internen Revision berücksichtigt und regelmässig geprüft werden.* |

*Text*

* + 1. IKT-Sicherheit (GOV-9)

|  |  |  |  |
| --- | --- | --- | --- |
| 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 2019:   * + IKT-Strategie, IKT-Organisation und IKT-Governance (Detailprüfung)   + IKT- und Informationssicherheitsrisikomanagement (Kritische Beurteilung) | | *Beispiel:*  *2014: Cloud (Detailprüfung)*  *2015: IKT-Projekte und Änderungsmanagement (Kritische Beurteilung)*  *2016: Informationssicherheitsmanagement (Kritische Beurteilung)*  *2017: Benutzerberechtigungsmanagement (Detailprüfung)*  *2018: IKT-Betriebsmanagement (Detailprüfung)* |
| Referenzen (demonstrativ; nicht abschliessend):  Art. 8 Bst. b ZDG; Art. 24 ZDG, Art. 101 ZDG, Art. 34b und Art. 35 BankV, EBA/GL/2017/09; EBA/GL/2019/02; EBA/GL/2019/04 | | | |
|  | |  | |
| *[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 Zahlungsinstituts (Grösse, Geschäftstätigkeit, IKT-Komplexität/-Risiken, Auslagerungen usw.) angemessen*   + *Die IKT-Strategie stimmt mit der Geschäftsstrategie und dem IKT-Risikomanagementkonzept überein*   + *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*   + *Es bestehen klare Rollen und Verantwortlichkeiten innerhalb der IKT-Organisation*   + *Die internen Verfahren stellen eine angemessene Unterstellung und Trennung der IKT-bezogenen Abteilungen/Funktionen (IKT-Entwicklung, IKT-Betrieb, IKT-Sicherheit etc.) inkl. der verbundenen Kontrollen sicher*   + *Die internen Verfahren stellen sicher, dass die Ressourcenausstattung und das Fachwissen der IKT-Mitarbeiter angemessen sind*   + *Die internen Verfahren stellen sicher, dass die Mitarbeiter regelmässig zu IKT- und Sicherheitsrisiken inkl. Informationssicherheit geschult werden.*   + *Die internen Verfahren stellen sicher, dass die Prüfung der IKT- und Sicherheitsrisiken angemessen in der Mehrjahresplanung der Internen Revision berücksichtigt und regelmässig geprüft werden.* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass die IKT-Strategie sowie deren Massnahmenpläne angemessen sind*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die IKT-Organisation und IKT-Governance angemessen ist*   + *Bestätigung, dass die internen Verfahren eine angemessene Ressourcenausstattung und Know-How der IKT Mitarbeiter sicherstellen*   + *Bestätigung, dass die internen Verfahren die regelmässige Schulung der Mitarbeiter zu IKT- und Sicherheitsrisiken inkl. Informationssicherheit sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die Prüfung der IKT- und Sicherheitsrisiken in der Mehrjahresplanung der Internen Revision berücksichtigt und regelmässig geprüft werden* |
| *IKT- und Informationssicherheitsrisikomanagement* | * + *Die internen Verfahren stellen sicher, dass ein angemessenes IKT-Risikomanagementkonzept besteht und dieses angemessen in das Risikomanagementkonzept des Zahlungsinstituts eingegliedert ist*   + *Die internen Verfahren stellen sicher, dass der Rahmen für das IKT- und Informationssicherheitsrisikomanagement 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- und Sicherheitsrisiken, 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- und Sicherheitsrisiken reduzieren.*   + *Es bestehen angemessene interne Verfahren, welche sicherstellen, dass die zugewiesenen Aufgaben und Verantwortlichkeiten zur Steuerung von IKT- und Sicherheitsrisiken / 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- und Sicherheitsrisiken und Kontrollen sicher* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass ein angemessenes IKT-Risikomanagement-Konzept besteht, welches angemessen in das Risikomanagementkonzept des Zahlungsinstituts eingegliedert ist, dokumentiert ist und mindestens jährlich überprüft und genehmigt wird.*   + *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- und Sicherheitsrisiken, 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 Ebenen des Zahlungsinstitut zur Reduzierung der relevanten IKT- und Sicherheitsrisiken sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die zugewiesenen Aufgaben und Verantwortlichkeiten zur Steuerung von IKT- und Sicherheitsrisiken / 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- und Sicherheitsrisiken 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 sicherzustellen (z.B. Gap-Analysen anhand von Informationssicherheitsstandards, Konformitätsprüfungen, physische Sicherheitsüberprüfungen, Quellcode-Überprüfungen, Schwachstellenmanagement, Penetrationtests, Verwundbarkeitsanalysen, Red-Team-Übungen)*   + *Die internen Verfahren stellen für kritische IKT-Systeme 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 sicherstellen*   + *Bestätigung, dass die internen Verfahren die unverzügliche Behebung der festgestellten Schwachstellen für kritische IKT-Systeme 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 Entzugs 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 die logische und physische Zugangsrechte regelmässig überprüft wird*   + *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 der 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 die IKT-Infrastruktur und die IKT-Leistungserbringung angemessen (Grösse, Geschäftstätigkeit, IKT-Komplexität/-Risiken, Auslagerungen) sind*   + *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*   + *Die internen Verfahren gewährleisten eine angemessene Zuweisung von Aufgaben und Verantwortlichkeiten zur Steuerung und Überwachung der IKT-Systeme und der Aufgaben betreffend der IKT-Leistungserbringung (Lebenszyklusmanagement der IKT-Systeme, Überwachung, Service Level Management, Änderungsmanagement der Programme usw.) sowie der Behandlung und Nachverfolgung von Betriebs- und Sicherheitsvorfällen (u.a. Identifikation der Hauptursachen und Bereinigung)*   + *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 Sicherheitsproblemen bei IKT-Systemen/IKT-Diensten helfen zu vermeiden sowie ihre Auswirkungen auf die Erbringung von IKT-Diensten minimieren (u.a. durch. Sicherheits-Patches, Implementierung sicherer Basiskonfiguration wesentlicher Netzwerkkomponenten/Server, Netzwerksegmentierung, Verschlüsselung 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 betriebliche und sicherheitsrelevante IKT-Vorfälle überwacht, protokolliert und zeitnah behoben werden.*   + *Die internen Verfahren stellen sicher, dass angemessene Kriterien und Schwellenwerte für die Klassifizierung von Ereignissen als Betriebs- und Sicherheitsvorfälle sowie Frühwarnindikatoren definiert und implementiert werden*   + *Die internen Verfahren stellen eine angemessene interne und externe Berichterstattung im Zusammenhang mit Meldung von Vorfällen und Eskalationsverfahren sicher* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass die IKT-Infrastruktur und die IKT-Leistungserbringung angemessen sind*   + *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 die internen Verfahren sicherstellen, dass eine angemessene Zuweisung von Aufgaben und Verantwortlichkeiten zur Steuerung und Überwachung der IKT-Systeme und der Aufgaben betreffend der IKT-Leistungserbringung sowie der Behandlung und Nachverfolgung von Betriebs- und Sicherheitsvorfällen besteht*   + *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 Sicherheitsproblemen bei IKT-Systemen/IKT-Diensten zu verhindern sowie deren Auswirkungen auf die Erbringung von IKT-Diensten zu minimieren*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass betriebliche und sicherheitsrelevante IKT-Vorfälle angemessen klassifiziert, überwacht, protokolliert, gemeldet und zeitnah behoben werden* |
| *IKT-Projekte und Änderungsmanagement* | * + *Die internen Verfahren stellen sicher, dass für IKT-Projekte ein angemessenes IKT-Projektmanagement gemäss IKT-Projektmanagementrichtlinie (Projektziele, Rollen und Verantwortlichkeiten / IKT-Projektteam, Projektrisikobewertung, Projektplan/Zeitrahmen und Projektschritte, Meilensteine, Anforderungen an das Änderungsmanagement) implementiert ist*   + *Die internen Verfahren stellen sicher, dass im IKT-Projektteam alle von einem IKT-Projekt betroffenen Bereiche vertreten sind und diese über die erforderlichen Kenntnisse (inkl. die entsprechenden Funktionen für Veränderungen an IKT-Systemen und Diensten) verfügt, um eine sichere und erfolgreiche Projektumsetzung sicherzustellen.*   + *Die internen Verfahren stellen die regelmässige oder anlassbezogene Berichterstattung über die IKT-Projekte (Fortschritt, Risiken etc.) an die Geschäftsleitung sicher*   + *Die internen Verfahren stellen sicher, dass vor Erwerb und Entwicklung von IKT-Systemen die funktionalen/nichtfunktionalen Anforderungen (inkl. Anforderungen an die Informationssicherheit) klar definiert und genehmigt werden*   + *Die internen Verfahren stellen sicher, dass die Anforderungen an die Informationssicherheit von einer von der Entwicklungsfunktion unabhängigen Funktion analysiert und freigegeben werden*   + *Die internen Verfahren stellen die Implementierung von Risikominderungsmassnahmen vor unbeabsichtigter/beabsichtigter Änderung/Manipulation der IKT-Systeme während der Entwicklung und Implementierung in die Produktionsumgebung sicher*   + *Die internen Verfahren stellen sicher, dass Testings der IKT-Systeme/IKT-Dienste vor ihrer ersten Anwendung auf Testumgebungen, die die Produktionsumgebung angemessen widerspiegeln, angemessen - gemäss ihrer Kritikalität - durchgeführt und genehmigt werden*   + *Die internen Verfahren stellen die Trennung der Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht-Produktivumgebungen sicher*   + *Die internen Verfahren gewährleisten die umfangreiche Dokumentation der Entwicklung, Implementierung, den Betrieb u/o die Konfiguration der IKT-Systeme (v.a. Benutzerdokumentation, technische Systemdokumentation, Beschreibung der Betriebsabläufe)*   + *Die internen Verfahren stellen sicher, dass alle Änderungen an IKT-Systemen aufgezeichnet, getestet, bewertet, genehmigt, umgesetzt und überprüft werden.* | * + *Bestätigung, dass die internen Verfahren ein angemessenes IKT-Projektmanagement gemäss IKT-Projektmanagementrichtlinie sicherstellen*   + *Bestätigung, dass die internen Verfahren die regelmässige oder anlassbezogene Berichterstattung über die IKT-Projekte an die Geschäftsleitung sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass vor Erwerb und Entwicklung von IKT-Systemen die funktionalen/nichtfunktionalen Anforderungen (inkl. Anforderungen an die Informationssicherheit) klar definiert, durch eine von der Entwicklungsfunktion unabhängigen Funktion analysiert und genehmigt werden*   + *Bestätigung, dass die internen Verfahren die Implementierung von Risikominderungsmassnahmen vor unbeabsichtigter/beabsichtigter Änderung/Manipulation der IKT-Systeme während der Entwicklung und Implementierung in die Produktionsumgebung sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass Testings der IKT-Systeme/IKT-Dienste vor ihrer ersten Anwendung auf Testumgebungen, die die Produktionsumgebung angemessen widerspiegeln und von diesen getrennt sind, angemessen - gemäss ihrer Kritikalität - durchgeführt und genehmigt werden*   + *Bestätigung, dass die internen Verfahren eine umfangreiche Dokumentation der Entwicklung, Implementierung, den Betrieb u/o die Konfiguration der IKT-Systeme gewährleisten*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass alle Änderungen an IKT-Systemen aufgezeichnet, getestet, bewertet, genehmigt, umgesetzt und überprüft werden* |
| *Cloud* | * + *Die internen Verfahren stellen sicher, dass eine angemessene Risikoanalyse bei der Verwendung von Cloud Anbietern durchgeführt wird, welche u.a. Folgendes beinhaltet; Ausgestaltung des Cloud-Dienstes, Kritikalität, Einfluss auf BCM, Bewertung der Risiken durch Cloud-Auslagerung, Standort der Datenspeicherung/Datenverarbeitung, Eignung Cloud-Anbieter*   + *Die internen Verfahren stellen sicher, dass die Risikoanalyse bei der Verwendung von Cloud Anbietern regelmässig überprüft und neu durchgeführt wird.*   + *Die internen Verfahren stellen sicher, dass ein angemessenes Schutzniveau und Massnahmen für die Vertraulichkeit von Daten, die Kontinuität ausgelagerter Tätigkeiten sowie die Integrität und Rückverfolgbarkeit von Daten und Systeme bei Cloud-Auslagerungen festgelegt werden.*   + *Die internen Verfahren stellen sicher, dass die Rückführung und Verwendung der beim Cloud-Anbieter gespeicherten Daten uneingeschränkt gewährleistet werden kann* | * + *Bestätigung, dass die internen Verfahren die Durchführung einer angemessenen Risikoanalyse bei der Verwendung von Cloud Anbietern sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die Risikoanalyse bei der Verwendung von Cloud Anbietern regelmässig überprüft und neu durchgeführt wird*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass ein angemessenes Schutzniveau und Massnahmen für die Vertraulichkeit von Daten, die Kontinuität ausgelagerter Tätigkeiten sowie die Integrität und Rückverfolgbarkeit von Daten und Systeme bei Cloud-Auslagerungen festgelegt werden.*   + *Bestätigung, dass die internen Verfahren die Rückführung und Verwendung der beim Cloud-Anbieter gespeicherten Daten uneingeschränkt gewährleisten* |

*Text*

* 1. Anfangs- und Eigenkapital / Eigenmittel (EM-1)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 10 ZDG; Art. 18 f ZDG; Art. 5 Abs. 1 Bst. a ZDV | | | |
|  | | | |
| **Anfangs- und Eigenkapital** | | |  |
| Bestätigung, dass die internen Verfahren die dauerhafte Einhaltung des vorgeschriebenen Anfangs- und Eigenkapitals sicherstellen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| **Eigenmittel nach ZDG** | | |  |
| Bestätigung, dass die internen Verfahren, die jederzeitige Verfügbarkeit von Eigenmittel für die Erbringung von Zahlungsdiensten (Art. 2 Abs. 2 Bst. a bis h ZDG) in angemessener Höhe, sicherstellen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die Berechnungsmethodik der Eigenmittel angemessen ist und periodisch überprüft wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die Datengrundlage zur Berechnung der Eigenmittel für die Erbringung von Zahlungsdiensten angemessen und die Berechnungsmethodik korrekt angewandt wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass das Zahlungsinstitut jederzeit in der Lage ist die Eigenmittel vollständig, korrekt und nachvollziehbar zu berechnen und zu dokumentieren | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Anfangs- und Eigenkapital* | * + *Die internen Verfahren gewährleisten die dauerhafte Einhaltung des regulatorischen Anfangs- und Eigenkapitals* |
| *Eigenmittel nach ZDG* | * + *Die internen Verfahren gewährleisten die jederzeitige Verfügbarkeit von Eigenmittel für die Erbringung von Zahlungsdiensten (Art. 2 Abs. 2 Bst. a bis h ZDG) in angemessener Höhe*   + *Die internen Verfahren stellen sicher, dass die Wahl der Berechnungsmethodik der Eigenmittel der Komplexität und dem Geschäftsmodell des Zahlungsinstituts angemessen ist und periodisch überprüft wird*   + *Die internen Verfahren stellen sicher, die Datengrundlage zur Berechnung der Eigenmittel für Erbringung von Zahlungsdiensten angemessen ist und die Berechnungsmethodik korrekt angewandt wird*   + *Die internen Verfahren stellen sicher, dass die Eigenmittel jederzeit vollständig, korrekt und nachvollziehbar berechnet und dokumentiert werden können* |

*Text*

* 1. Sicherungsanforderungen (SA-1)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 20 ZDG; Art. 5 Abs. 1 Bst. b ZDV | | | |
|  | | | |
| Bestätigung, dass die internen Verfahren die jederzeitige Sicherung der mittelbar oder unmittelbar entgegengenommenen Gelder von Kunden gewährleisten | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die gewählte Sicherungsmethodik der Kundengelder gemäss Art. 20 Abs. 1 ZDG korrekt angewandt wird | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die internen Verfahren sicherstellen, dass die durchgeführten Massnahmen zur Sicherung der Kundengelder nachvollziehbar dokumentiert werden. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Sicherung der Kundengelder* | * + *Die internen Verfahren stellen die jederzeitige Sicherung der mittelbar oder unmittelbar entgegengenommenen Gelder von Kunden sicher*   + *Die internen Verfahren stellen sicher, dass die gewählte Sicherungsmethodik (A oder B) gemäss Art. 20 Abs. 1 ZDG korrekt angewandt wird*   + *Die internen Verfahren stellen sicher, dass die durchgeführten Massnahmen zur Sicherung der Kundengelder angemessen für Dritte nachvollziehbar dokumentiert werden* |

*Text*

* 1. Agenten, Vertreibern und Zweigstellen
     1. Inanspruchnahme von Agenten sowie Vertreibern (AVZ-1)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 25, 27 f ZDG; FMA-Wegleitung 2018/22 | | | |
|  | | | |
| Bestätigung, dass ein angemessener Prozess zur Auswahl und Genehmigung (Due-Diligence-Prüfung) der Inanspruchnahme von Agenten und Vertreibern unter Berücksichtigung deren Zuverlässigkeit (u.a. finanzielle und personelle Ressourcen) und fachlichen Eignung besteht und angemessen angewandt wird. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Internen Verfahren sicherstellen, dass die in Anspruch genommenen Agenten und Vertreibern über angemessene IT-Systeme, Verfahren, Interne Kontrollsysteme und Infrastrukturen verfügen | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass die Interne Organisation zur Auswahl, Genehmigung und Überwachung von Agenten und Vertreibern (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem zur Überwachung der in Anspruch genommenen Agenten und Vertreibern und der von Ihnen erbrachten Zahlungsdienste angemessen ist und im Falle der Prüftiefe „Detailprüfung“ effektiv angewendet wurde. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Auswahlverfahren / Eignung von Agenten / Vertreibern* | * + *Die internen Verfahren stellen sicher, dass vor Inanspruchnahme von Agenten und Vertreibern diese hinsichtlich ihrer Zuverlässigkeit und fachlichen Eignung im Rahmen einer Due-Diligence-Prüfung überprüft werden.*   + *Die internen Verfahren stellen sicher, dass die Auswahl von Agenten und Vertreibern angemessen genehmigt wird.*   + *Die internen Verfahren stellen sicher, dass die in Anspruch genommenen Agenten und Vertreibern über angemessene IT-Systeme, Verfahren, Interne Kontrollsysteme und Infrastrukturen verfügen.* |
| *Interne Organisation zur Auswahl, Genehmigung und Überwachung von Agenten / Vertreibern*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen* |
| *Internes Kontrollsystem*  *(dokumentierte Kontrollen, Eskalationsverfahren, Vier-Augen-Prinzip)* | * + *Die internen Verfahren stellen angemessene permanente sowie periodische Kontrollen zur Überprüfung der Tätigkeiten des Agenten / Vertreibern sicher*   + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |

*Text*

* + 1. Zweigstellen (AVZ-2)

|  |  |  |  |
| --- | --- | --- | --- |
| 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. 27 f ZDG | | | |
|  | | | |
| Bestätigung, dass die Interne Organisation der Zweigstelle (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) angemessen ausgestaltet ist. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |
| Bestätigung, dass das Interne Kontrollsystem zur Überwachung der Zweigstelle und der von Ihnen erbrachten Zahlungsdienste angemessen ist und im Falle der Prüftiefe „Detailprüfung“ effektiv angewendet wurde. | | | *Ja (Detailprüfung / Kritische Beurteilung) / Nein* |

|  |  |
| --- | --- |
| ***Prüfelemente*** | ***Mindestprüfinhalte*** |
| *Interne Organisation*  *(Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen (personell und technisch), Know-How, Interessenskonflikte)* | * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit des Geschäftsführers der Zweigstelle und der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen*   + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen der Zweigstelle* |
| *Internes Kontrollsystem*  *(dokumentierte Kontrollen, Eskalationsverfahren, Vier-Augen-Prinzip)* | * + *Die internen Verfahren stellen angemessene permanente sowie periodische Kontrollen zur Überprüfung der Tätigkeiten der Zweigstellen sicher*   + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher* |

*Text*

* 1. Andere Vorschriften / EBA/GL/2017/10 Schwerwiegende Betriebs- oder Sicherheitsvorfälle (EBA/GL/2017/10) und Starke Kundenauthentifizierung (DelVO (EU) Nr. 2018/389) (And-1)

|  |  |  |  |
| --- | --- | --- | --- |
| 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 2019:   * + Schwerwiegende Betriebs- oder Sicherheitsvorfälle: Internes Kontrollsystem (Detailprüfung) | | *Beispiel:*  *2014:* Schwerwiegende Betriebs- oder Sicherheitsvorfälle: Meldewesen (Kritische Beurteilung)  *2015*: Schwerwiegende Betriebs- oder Sicherheitsvorfälle: Internes Kontrollsystem (Kritische Beurteilung)  *2016:* Zugangsschnittstellen und dedizierte Schnittstellen (Detailprüfung)  2017: Starke Kundenauthentifizierung (Kritische Beurteilung)  2018: Schwerwiegende Betriebs- oder Sicherheitsvorfälle: Meldewesen (Detailprüfung) |
| Referenzen (demonstrativ; nicht abschliessend):  siehe unten | | | |
|  | |  | |
| *[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*** |
| *Schwerwiegende Betriebs-oder Sicherheitsvorfälle:*  *Internes Kontrollsystem*  Art. 102 ZDG; FMA-Wegleitung 2019/8; EBA/GL/2017/10 | * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Die internen Verfahren stellen sicher, dass Betriebs- oder Sicherheitsvorfälle\* zeitnah erkannt werden*   + *Die internen Verfahren stellen sicher, dass die Vorfälle korrekt anhand der Kategorien (higher impact level / lower impact level) und den zugrundeliegenden Indikatoren eingestuft werden*   + *Die internen Verfahren stellen, dass die Indikatorwerte zur Kategorisierung der Betriebs- oder Sicherheitsvorfälle korrekt berechnet und angewandt werden*   + *Die internen Verfahren stellen sicher, dass in der Betriebs- und Sicherheitsstrategie (Sicherheitsleitlinie) die Verantwortlichkeiten für die Meldung von schwerwiegenden Betriebs- oder Sicherheitsvorfälle definiert sind.* | * + *Bestätigung, dass ein angemessener Prozess zur Erkennung von Betriebs- oder Sicherheitsvorfällen sowie deren korrekte Kategorisierung als schwerwiegender Betriebs- oder Sicherheitsvorfällen existiert*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die Indikatorwerte zur Kategorisierung der Betriebs- oder Sicherheitsvorfälle korrekt berechnet und angewandt werden.*   + *Bestätigung, dass die Verantwortlichkeiten für die Meldung von schwerwiegenden Betriebs- oder Sicherheitsvorfällen in der Sicherheitsstrategie (Sicherheitsleitlinie) angemessen definiert sind* |
| *Schwerwiegende Betriebs- oder Sicherheitsvorfälle:*  *Meldeverfahren*  Art. 102 ZDG; FMA-Wegleitung 2019/8; EBA/GL/2017/10 | * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Die internen Verfahren stellen eine fristgerechte Meldung sicher*   + *Die internen Verfahren stellen eine hohe Datenqualität mittels Validierung der Meldedaten sicher*   + *Die internen Verfahren stellen einen angemessenen Prozess bei internen oder externen Rückfragen sicher*   + *Die Datenintegrität wird durch angemessene Zugriffsrechte und Berechtigungen auf die Systeme (inkl. Inputdaten) und deren regelmässige Überprüfung, sowie durch Aufzeichnung sämtlicher Prozessschritte im System sichergestellt* | * + *Bestätigung, dass interne Meldeverfahren für die Erst-, Zwischen- und Abschlussmeldung der schwerwiegenden Vorfälle existieren und gemäss den regulatorischen Bestimmungen angemessen angewandt werden* |
| *Starke Kundenauthentifizierung*  Art. 103 ZDG; DelVO (EU) Nr. 2018/389 | * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Die internen Verfahren stellen sicher, dass Sicherheitsmassnahmen für die Durchführung starker Kundenauthentifizierungen gemäss den regulatorischen Vorgaben (DelVO (EU) Nr. 2018/389 Art. 4 ff) verlangt und implementiert werden (zwei Elemente der Kategorien Wissen, Besitz und Inhärenz)*   + *Die internen Verfahren stellen das regelmässige Testen dieser Sicherheitsmassnahmen und die Dokumentation der Ergebnisse sicher*   + *Die internen Verfahren stellen die fachliche Eignung (Fachwissen IT-Sicherheit, Zahlungsverkehr) und Unabhängigkeit jener Personen sicher, welche die Tests der Sicherheitsmassnahmen durchführen.*   + *Die internen Verfahren stellen sicher, dass die Kundenauthentifizierung ausreichend „stark“ ist*   + *Die internen Verfahren stellen bei der Anwendung von Ausnahmen (DelVO (EU) Nr. 2018/389, Art. 10) sicher, dass die Daten für jede Zahlungsart aufgeschlüsselt nach Fernzahlungsvorgängen und Nicht-Fernzahlungsvorgängen gemäss den regulatorischen Vorgaben angemessen überwacht, ausgewertet und dokumentiert werden*   + *Die internen Verfahren stellen sicher, dass die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer, einschliesslich Authentifizierungscodes, in jeder Phase der Authentifizierung geschützt werden*   + *Die internen Verfahren stellen sicher, dass die Risiken einer Fehlleitung der Kommunikation an Unbefugte wirksam eingedämmt wird*   + *Die internen Verfahren stellen sicher, dass sämtliche Zahlungsvorgänge und Interaktionen zwischen mehreren Parteien (z.B. Zahlungsdienstnutzer, Zahlungsdienstleister, Händler etc.) verlässlich zurückverfolgt werden (u.a. durch Erfassung des Zeitstempels, Sicherheitsmassnahmen für die ausführliche Protokollierung der Transaktion, eindeutige Kennung der Sitzung)* | * + *Bestätigung, dass die internen Verfahren sicherstellen, dass Sicherheitsmassnahmen für die Durchführung starker Kundenauthentifizierungen gemäss den regulatorischen Vorgaben (DelVO (EU) Nr. 2018/389 Art. 4 ff) gefordert und implementiert und werden.*   + *Bestätigung, dass die internen Verfahren das regelmässige Testen der Sicherheitsmassnahmen für die Durchführung einer starken Kundenauthentifizierung durch fachkundige unabhängige Experten sicherstellen.*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die Ergebnisse der durchgeführten Tests der Sicherheitsmassnahmen angemessen dokumentiert werden*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die Kundenauthentifizierung ausreichend „stark“ ist*   + *Bestätigung, dass die internen Verfahren bei Ausnahmen von der starken Kundenauthentifizierung die Überwachung der Ausnahmen nach DelVO (EU) Nr. 2018/389 Art. 21 sicherstellen und dokumentieren*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer geschützt werden.*   + *Bestätigung, dass die internen Verfahren die Risiken einer Fehlleitung der Kommunikation an Unbefugte wirksam eindämmen.*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass die Rückverfolgbarkeit sämtlicher Interaktionen und Zahlungsvorgängen gewährleistet ist* |
| *Zugangsschnittstellen und dedizierte Schnittstellen*  Art. 103 ZDG; DelVO (EU) Nr. 2018/389 | * + *Es bestehen angemessene Zugangsschnittstellen zwischen dem Kontoinformationsdienstleister, Zahlungsauslösedienstleister und kontoführender Zahlungsdienstleister*   + *Die internen Verfahren stellen sicher, dass die Schnittstellen die von internationalen oder europäischen Standardisierungsorganisationen ausgegebenen Kommunikationsstandards erfüllen.*   + *Die internen Verfahren stellen sicher, dass die technische Spezifikation einer jeden Schnittstelle angemessen dokumentiert ist.*   + *Die internen Verfahren stellen sicher, dass die regulatorischen Anforderungen an eine dedizierte Schnittstelle (Verfügbarkeit, Leistung.) jederzeit eingehalten und laufend überwacht werden*   + *Die internen Verfahren stellen sicher, dass für die dedizierte Schnittstelle transparente wesentliche Leistungsindikatoren und Service-Level-Ziele definiert werden,*   + *Die internen Verfahren stellen sicher, dass die dedizierte Schnittstelle anhand der Leistungsindikatoren und der Service-Level-Ziele regelmässig überwacht und Stresstests unterzogen werden*   + *Die internen Verfahren stellen sicher, dass vierteljährliche Statistiken über die Verfügbarkeit und die Leistung der dedizierten Schnittstelle auf der Homepage veröffentlicht werden*   + *Die internen Verfahren stellen sicher, dass angemessene Notfallmassnahmen (inkl. Kommunikationspläne, Beschreibung der sofort verfügbaren alternativen Optionen) für eine unvorhergesehene Nichtverfügbarkeit der Schnittstelle, Systemausfall oder mangelnde Leistungsfähigkeit der dedizierten Schnittstelle bestehen*   + *Die internen Verfahren gewährleisten, dass Probleme mit den dedizierten Schnittstellen unverzüglich der FMA gemeldet werden* | * + *Bestätigung, dass die internen Verfahren die Einhaltung der allgemeinen regulatorischen Anforderung an Zugangsschnittstellen sicherstellen*   + *Bestätigung, dass die internen Verfahren die Einhaltung und laufende Überwachung der regulatorischen Anforderungen an eine dedizierte Schnittstelle (Verfügbarkeit, Leistung) anhand von transparenten wesentlichen Leistungsindikatoren, Service-Level-Zielen und der Durchführung von Stresstests sicherstellen*   + *Bestätigung, dass die internen Verfahren die vierteljährliche Veröffentlichung der Statistiken über die Verfügbarkeit und Leistung der dedizierten Schnittstelle auf der Homepage sicherstellen*   + *Bestätigung, dass die internen Verfahren sicherstellen, dass angemessene Notfallmassnahmen (inkl. Kommunikationspläne, Beschreibung der sofort verfügbaren alternativen Optionen) für eine unvorhergesehene Nichtverfügbarkeit der Schnittstelle, Systemausfall oder mangelnde Leistungsfähigkeit der dedizierten Schnittstelle bestehen*   + *Bestätigung, dass die internen Verfahren gewährleisten, dass Probleme mit den dedizierten Schnittstellen unverzüglich der FMA gemeldet werden* |

\*ein einzelnes Ereignis oder eine Reihe zusammenhängender Ereignisse, das vom Zahlungsdienstleister nicht beabsichtigt wurde und das sich negativ auf die Integrität, die Verfügbarkeit, die Vertraulichkeit, die Authentizität und/oder die Kontinuität von zahlungsbezogenen Diensten auswirkt oder aller Wahrscheinlichkeit nach eine solche negative Auswirkungen haben wird (EBA/GL/2017/10)

*Text*

* 1. Periodisches Meldewesen (MW-1)

|  |  |  |  |
| --- | --- | --- | --- |
| 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 2019:   * + Nachweis des Eigenkapitals und der erforderlichen Eigenmittel (Detailprüfung) | | *Beispiel:*  *2014: Bestätigung der Gewährleistung der Sicherungsanforderungen (Detailprüfung)*  *2015: Finanzreporting (Kritische Beurteilung)*  *2016: Kundenbeschwerden (Kritische Beurteilung)*  *2017: Betrugsfälle (Detailprüfung)*  *2018: Umgang mit operationellen und sicherheitsrelevanten Risiken (Detailprüfung)* |
| Referenzen (demonstrativ; nicht abschliessend):  siehe unten | | | |
|  | |  | |
| *[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*** |
| *Meldung: Nachweis des Eigenkapitals und der erforderlichen Eigenmittel*  *(Art. 18 f ZDG; Art. 5 Abs. 1 Bst. a ZDV)* | *Interne Organisation*   * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen*   + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   *Internes Kontrollsystem*   * + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips beim Erstellungsprozess der Meldedaten vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen und der Meldedaten sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher*   *Datenqualität / Datenintegrität / Validierung*   * + *Die internen Verfahren stellen eine fristgerechte Meldung, eine hohe Datenqualität und die Aufzeichnung sämtlicher manueller Anpassungen der Meldedaten sicher*   + *Die internen Verfahren stellen eine regelmässige Validierung der Meldedaten sicher*   + *Die Meldedaten sind konsistent mit den internen Annahmen im Risikomanagement*   + *Die internen Verfahren stellen einen angemessenen Prozess bei internen oder externen Rückfragen sicher*   + *Die Datenintegrität wird durch angemessene Zugriffsrechte und Berechtigungen auf die Systeme (inkl. Inputdaten) und deren regelmässige Überprüfung, sowie durch Aufzeichnung sämtlicher Prozessschritte im System sichergestellt*   + *Es bestehen wirksame Schnittstellen für eine vollständige und korrekte Integration der Inputdaten* | * + *Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das periodische Meldewesen „Angaben über die Einhaltung der Anforderungen für das Anfangs- und Eigenkapital sowie Eigenmittel und über die Methodik der Eigenmittelberechnung“ angemessen ausgestaltet ist.*   + *Bestätigung, dass das Interne Kontrollsystem für die Erstellung und Übermittlung des periodischen Meldewesens „Angaben über die Einhaltung der Anforderungen für das Anfangs- und Eigenkapital sowie Eigenmittel und über die Methodik der Eigenmittelberechnung“ angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.*   + *Bestätigung, dass die Methoden zur Validierung der Meldedaten, zur Aufrechterhaltung der Datenintegrität und zur Sicherstellung einer hohen Datenqualität bzgl. dem periodischen Meldewesens „Angaben über die Einhaltung der Anforderungen für das Anfangs- und Eigenkapital sowie Eigenmittel und über die Methodik der Eigenmittelberechnung“ angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.* |
| *Bestätigung der Gewährleistung der Sicherungsanforderungen*  *(Art. 20 ZDG; Art. 5 Abs. 1 Bst. b ZDV)* | *Interne Organisation*   * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen*   + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   *Internes Kontrollsystem*   * + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips beim Erstellungsprozess der Meldedaten vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen und der Meldedaten sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher*   *Datenqualität*   * + *Die internen Verfahren stellen eine fristgerechte Meldung und eine hohe Datenqualität sicher*   + *Die internen Verfahren stellen eine regelmässige Validierung der Meldedaten sicher*   + *Die internen Verfahren stellen einen angemessenen Prozess bei internen oder externen Rückfragen sicher* | * + *Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das periodische Meldewesen „Bestätigung der Gewährleistung der Sicherungsanforderungen (Sicherung der Kundengelder)“ angemessen ausgestaltet ist.*   + *Bestätigung, dass das Interne Kontrollsystem für die Erstellung und Übermittlung des periodischen Meldewesens „Bestätigung der Gewährleistung der Sicherungsanforderungen (Sicherung der Kundengelder)“ angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.*   + *Bestätigung, dass die Methoden zur Sicherstellung einer hohen Datenqualität bzgl. dem periodischen Meldewesens „Bestätigung der Gewährleistung der Sicherungsanforderungen (Sicherung der Kundengelder)“ angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.* |
| *Finanzreporting*  *(Art. 5 Abs. 1 Bst. c und d ZDV)* | *Interne Organisation*   * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen*   + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   *Internes Kontrollsystem*   * + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips beim Erstellungsprozess der Meldedaten vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen und der Meldedaten sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher*   *Datenqualität / Datenintegrität / Validierung*   * + *Die internen Verfahren stellen eine fristgerechte Meldung, eine hohe Datenqualität und die Aufzeichnung sämtlicher manueller Anpassungen der Meldedaten sicher*   + *Die internen Verfahren stellen eine regelmässige Validierung der Meldedaten sicher*   + *Die Meldedaten sind konsistent mit den internen Annahmen im Risikomanagement*   + *Die internen Verfahren stellen einen angemessenen Prozess bei internen oder externen Rückfragen sicher*   + *Die Datenintegrität wird durch angemessene Zugriffsrechte und Berechtigungen auf die Systeme (inkl. Inputdaten) und deren regelmässige Überprüfung, sowie durch Aufzeichnung sämtlicher Prozessschritte im System sichergestellt*   + *Es bestehen wirksame Schnittstellen für eine vollständige und korrekte Integration der Inputdaten* | * + *Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das periodische Meldewesen „Finanzreporting“ angemessen ausgestaltet ist.*   + *Bestätigung, dass das Interne Kontrollsystem für die Erstellung und Übermittlung des periodischen Meldewesens „Finanzreporting“ angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.*   + *Bestätigung, dass die Methoden zur Validierung der Meldedaten, zur Aufrechterhaltung der Datenintegrität und zur Sicherstellung einer hohen Datenqualität bzgl. dem periodischen Meldewesens „Finanzreporting“ angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.* |
| *Kundenbeschwerden*  *(Art. 106 ZDG; FMA-Mitteilung 2015/2; JC/GL/2018/35)* | *Interne Organisation*   * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen*   + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   *Internes Kontrollsystem*   * + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips beim Erstellungsprozess der Meldedaten vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen und der Meldedaten sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher*   *Datenqualität / Datenintegrität / Validierung*   * + *Die internen Verfahren stellen eine fristgerechte Meldung, eine hohe Datenqualität und die Aufzeichnung sämtlicher manueller Anpassungen der Meldedaten sicher*   + *Die internen Verfahren stellen eine regelmässige Validierung der Meldedaten sicher*   + *Die Meldedaten sind konsistent mit den internen Annahmen im Risikomanagement*   + *Die internen Verfahren stellen einen angemessenen Prozess bei internen oder externen Rückfragen sicher*   + *Die Datenintegrität wird durch angemessene Zugriffsrechte und Berechtigungen auf die Systeme (inkl. Inputdaten) und deren regelmässige Überprüfung, sowie durch Aufzeichnung sämtlicher Prozessschritte im System sichergestellt*   + *Es bestehen wirksame Schnittstellen für eine vollständige und korrekte Integration der Inputdaten* | * + *Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das periodische Meldewesen „Kundenbeschwerden“ angemessen ausgestaltet ist.*   + *Bestätigung, dass das Interne Kontrollsystem für die Erstellung und Übermittlung des periodischen Meldewesens „Kundenbeschwerden“ angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.*   + *Bestätigung, dass die Methoden zur Validierung der Meldedaten, zur Aufrechterhaltung der Datenintegrität und zur Sicherstellung einer hohen Datenqualität bzgl. dem periodischen Meldewesens „Kundenbeschwerden“ angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.* |
| *Betrugsfälle*  *(Art. 102 Abs. 3 ZDG; EBA/GL/2018/05)* | *Interne Organisation*   * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen*   + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   *Internes Kontrollsystem*   * + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips beim Erstellungsprozess der Meldedaten vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen und der Meldedaten sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher*   *Datenqualität / Datenintegrität / Validierung*   * + *Die internen Verfahren stellen eine fristgerechte Meldung, eine hohe Datenqualität und die Aufzeichnung sämtlicher manueller Anpassungen der Meldedaten sicher*   + *Die internen Verfahren stellen eine regelmässige Validierung der Meldedaten sicher*   + *Die Meldedaten sind konsistent mit den internen Annahmen im Risikomanagement*   + *Die internen Verfahren stellen einen angemessenen Prozess bei internen oder externen Rückfragen sicher*   + *Die Datenintegrität wird durch angemessene Zugriffsrechte und Berechtigungen auf die Systeme (inkl. Inputdaten) und deren regelmässige Überprüfung, sowie durch Aufzeichnung sämtlicher Prozessschritte im System sichergestellt*   + *Es bestehen wirksame Schnittstellen für eine vollständige und korrekte Integration der Inputdaten* | * + *Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das periodische Meldewesen „Meldewesens „Meldung von Betrugsfällen“ angemessen ausgestaltet ist.*   + *Bestätigung, dass das Interne Kontrollsystem für die Erstellung und Übermittlung des periodischen Meldewesens „Meldung von Betrugsfällen“ angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.*   + *Bestätigung, dass die Methoden zur Validierung der Meldedaten, zur Aufrechterhaltung der Datenintegrität und zur Sicherstellung einer hohen Datenqualität bzgl. dem periodischen Meldewesens „Meldewesens „Meldung von Betrugsfällen“ angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.* |
| *Umgang mit operationellen und sicherheitsrelevanten Risiken*  *(Art. 101 Abs. 2 ZDG; EBA/GL/2017/17)* | *Interne Organisation*   * + *Die Verantwortlichkeiten und Kompetenzen sind klar geregelt*   + *Die internen Verfahren stellen die fachliche Eignung und Zuverlässigkeit der Mitarbeiter sicher*   + *Es bestehen angemessene Verfahren zur Vermeidung, Reduzierung und Offenlegung von Interessenkonflikten;*   + *Anzahl und Zusammensetzung der internen Ressourcen sind angemessen*   + *Es besteht eine angemessene Funktionentrennung zwischen Back- und Frontoffice auf allen wesentlichen Organisationsebenen des Zahlungsinstituts;*   *Internes Kontrollsystem*   * + *Die internen Verfahren sehen durchgehend die Anwendung des 4-Augen-Prinzips beim Erstellungsprozess der Meldedaten vor*   + *Die internen Verfahren stellen ein angemessenes Dokumentations- und Archivierungswesen der durchgeführten Kontrollen und der Meldedaten sicher;*   + *Es bestehen wirksame interne Eskalationsmechanismen bei festgestellten Verstössen*   + *Die internen Verfahren stellen den internen Wissenstransfer (Berichterstattung) angemessen sicher*   *Datenqualität / Datenintegrität / Validierung*   * + *Die internen Verfahren stellen eine fristgerechte Meldung, eine hohe Datenqualität und die Aufzeichnung sämtlicher manueller Anpassungen der Meldedaten sicher*   + *Die internen Verfahren stellen eine regelmässige Validierung der Meldedaten sicher*   + *Die Meldedaten sind konsistent mit den internen Annahmen im Risikomanagement*   + *Die internen Verfahren stellen einen angemessenen Prozess bei internen oder externen Rückfragen sicher*   + *Die Datenintegrität wird durch angemessene Zugriffsrechte und Berechtigungen auf die Systeme (inkl. Inputdaten) und deren regelmässige Überprüfung, sowie durch Aufzeichnung sämtlicher Prozessschritte im System sichergestellt*   + *Es bestehen wirksame Schnittstellen für eine vollständige und korrekte Integration der Inputdaten* | * + *Bestätigung, dass die interne Organisation (Organisationsstruktur, Verantwortlichkeiten und Kompetenzen, Internes Weisungswesen, Ressourcen, Know-How, Interessenskonflikte) für das periodische Meldewesen „Meldewesens „Umgang mit operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit Zahlungsdiensten“ angemessen ausgestaltet ist.*   + *Bestätigung, dass das Interne Kontrollsystem für die Erstellung und Übermittlung des periodischen Meldewesens „Umgang mit operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit Zahlungsdiensten“ angemessen ist und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.*   + *Bestätigung, dass die Methoden zur Validierung der Meldedaten, zur Aufrechterhaltung der Datenintegrität und zur Sicherstellung einer hohen Datenqualität bzgl. dem periodischen Meldewesens „Meldewesens „Umgang mit operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit Zahlungsdiensten“ angemessen sind und im Falle der Prüftiefe Detailprüfung effektiv angewendet wurden.* |

*Text*

* 1. Prüfresultate aus von der FMA Liechtenstein zusätzlich festgelegten Prüfgebieten / Risikoarten bzw. Prüffelder

*Unter diesem Abschnitt sind die Prüfresultate sämtlicher, von der FMA Liechtenstein vorgängig kommunizierten, zusätzlich festgelegter Prüfgebiete / Risikoarten bzw. Prüffelder, welche im Rahmen der Aufsichtsprüfung abzudecken sind, aufzuführen.*

*Die vorgängige Kommunikation durch die FMA Liechtenstein gibt an, welche Prüffelder im Rahmen der Aufsichtsprüfung mit welcher Prüftiefe abzudecken sind und welche Prüfbestätigungen des jeweiligen Prüffelds im Rahmen des vorliegenden Berichts über die Aufsichtsprüfung aufzuführen und zu beurteilen sind.*

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 von Zahlungsinstitute 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. Formular Risikoanalyse / Prüfstrategie; falls Abweichungen zu an die FMA eingereichten Versionen bestehen
2. Aktuelle Organigramme (im Minimum mit Angabe der verantwortlichen Personen pro Geschäftsbereich bzw. Abteilung) inkl. Auflistung von Agenten, Zweigstellen und Beschreibung der Teilnahme an einem Zahlungssystems