Anhang C2 zu FMA-Richtlinie 2026/1: Gliederung und Inhalt des Berichts über die Aufsichtsprüfung von Wertpapierfirmen

[1. Wesentliche Eigenheiten der Wertpapierfirma 4](#_Toc216425867)

[2. Zusammenfassung der Prüfungsergebnisse 5](#_Toc216425868)

[2.1 Beanstandungen 5](#_Toc216425869)

[2.2 Beanstandungen zum Vorjahr 5](#_Toc216425870)

[2.3 Empfehlungen 5](#_Toc216425871)

[2.4 Empfehlungen zum Vorjahr 6](#_Toc216425872)

[2.5 Wesentliche Feststellungen der Innenrevision 6](#_Toc216425873)

[2.6 Wesentliche Feststellungen durch Dritte 6](#_Toc216425874)

[2.7 Wichtige Informationen 6](#_Toc216425875)

[3. Konsolidierte und zusätzliche Beaufsichtigung 7](#_Toc216425876)

[4. Einhaltung der Zulassungsvoraussetzungen 7](#_Toc216425877)

[4.1 Eigenmittelvorschriften und Liquiditätsanforderungen 7](#_Toc216425878)

[4.2 Geschäftsplan 7](#_Toc216425879)

[4.3 Inländische Betriebsstätte und geeignete Organisation 8](#_Toc216425880)

[4.4 Zulassungs- und meldepflichtige Änderungen 8](#_Toc216425881)

[5. Pflichten der Wertpapierfirma 9](#_Toc216425882)

[5.1 Organisatorische Anforderungen 9](#_Toc216425883)

[5.1.1 Risikomanagement-Funktion 9](#_Toc216425884)

[5.1.2 Compliance-Funktion 9](#_Toc216425885)

[5.1.3 Innenrevisionsfunktion 10](#_Toc216425886)

[5.1.4 Beschwerdemanagement 10](#_Toc216425887)

[5.2 Auslagerung von betrieblichen Aufgaben 11](#_Toc216425888)

[5.3 Vergütungspolitik 11](#_Toc216425889)

[5.4 Vermeidung von Interessenkonflikten 11](#_Toc216425890)

[5.5 Freier Dienstleistungsverkehr 12](#_Toc216425891)

[5.6 Offenlegungspflichten 12](#_Toc216425892)

[5.7 Vorschriften zum Anlegerschutz 12](#_Toc216425893)

[5.7.1 Anlageberatung und Portfolioverwaltung 12](#_Toc216425894)

[5.7.2 Aufzeichnungs- und Aufbewahrungspflichten 13](#_Toc216425895)

[5.7.3 Zuwendungen 13](#_Toc216425896)

[5.7.4 Geeignetheit und Angemessenheit 13](#_Toc216425897)

[5.7.5 Produktüberwachung 14](#_Toc216425898)

[5.7.6 Information und Berichterstattung gegenüber Kunden 14](#_Toc216425899)

[5.7.7 Erbringung von Dienstleistungen über Dritte 14](#_Toc216425900)

[5.7.8 Bestmögliche Ausführung und Bearbeitung von Kundenaufträgen 15](#_Toc216425901)

[5.7.9 Geeignete Gegenpartei 15](#_Toc216425902)

[5.7.10 Verdachtsmitteilung gemäss MAR 15](#_Toc216425903)

[6. Betrieb von Multilateralen Handelssystemen (MTF) oder Organisierten Handelssystemen (OTF) 16](#_Toc216425904)

[6.1 Handel und Abschluss von Geschäften 16](#_Toc216425905)

[6.2 Vorkehrungen des Art. 23 bis 27 HPBG 16](#_Toc216425906)

[6.2.1 Organisatorische Belastbarkeit der Systeme und Notfallsicherungen 16](#_Toc216425907)

[6.2.2 Algorithmischer Handel 17](#_Toc216425908)

[6.2.3 Direkter elektronischer Zugang 17](#_Toc216425909)

[6.2.4 Gebühren 17](#_Toc216425910)

[6.2.5 Tick-Grössen 17](#_Toc216425911)

[6.3 Besondere Anforderungen an einen MTF 17](#_Toc216425912)

[6.4 Besondere Anforderungen an einen OTF 18](#_Toc216425913)

[6.5 Überwachungspflichten 18](#_Toc216425914)

[6.6 KMU-Wachstumsmarkt 18](#_Toc216425915)

[6.7 Zentrale Gegenpartei/Clearing und Abrechnung 18](#_Toc216425916)

[6.8 Vorhandels-/Nachhandelstransparenz in Bezug auf Aktien, Aktienzertifikate, börsengehandelte Fonds, Zertifikate und andere vergleichbare Finanzinstrumente 18](#_Toc216425917)

[6.9 Vorhandels-/Nachhandelstransparenz in Bezug auf Schuldverschreibungen, strukturierte Finanzprodukte, Emissionszertifikate und Derivate 19](#_Toc216425918)

[6.10 Offenlegung von Vorhandels- und Nachhandelsdaten zu angemessenen kaufmännischen Bedingungen 19](#_Toc216425919)

[6.11 Meldung von Transaktionsdaten 19](#_Toc216425920)

[6.12 Meldung von Referenzdaten für die einzelnen Finanzinstrumente 19](#_Toc216425921)

[6.13 Vorbeugung und Aufdeckung von Marktmissbrauch für die einzelnen Finanzinstrumente 19](#_Toc216425922)

[7. Digitale operationale Resilienz 20](#_Toc216425923)

[7.1 Governance & Organisation 20](#_Toc216425924)

[7.2 IKT-Risikomanagementrahmen 20](#_Toc216425925)

[7.3 Reaktion & Wiederherstellung 21](#_Toc216425926)

[7.4 IKT-bezogene Vorfälle 22](#_Toc216425927)

[7.5 Testen der digitalen operationalen Resilienz 22](#_Toc216425928)

[7.6 Management des IKT-Drittparteienrisikos 23](#_Toc216425929)

[8. Ausserordentliche Prüfung 24](#_Toc216425930)

[9. Anhang zum Bericht über die Aufsichtsprüfung 24](#_Toc216425931)

# Wesentliche Eigenheiten der Wertpapierfirma

|  |
| --- |
| Die Revisionsstelle vermerkt die folgenden Informationen in diesem Abschnitt:   * Tatsächlich ausgeübte Dienstleistungen (Haupttätigkeit), Geschäftsbereiche, Kundenstruktur und Cross-Border-Tätigkeit unter Angabe der Veränderung zum Vorjahr * Erbringung von Zusatzdienstleistungen * Einstufung der Wertpapierfirm (*Kleine und nicht verflochtene Wertpapierfirma* oder keine *kleine und nicht verflochtene Wertpapierfirma*) gemäss Art. 1 Abs. 2 bzw. Art. 12 IFR, unter Angabe der Veränderung zum Vorjahr * Betrieb von multilateralen Handelssystemen und/oder organisierten Handelssystemen * Beteiligungen an der Wertpapierfirma * Enge Verbindungen/wesentliche Beziehungen mit Banken, bei denen Vermögenswerte der Kunden gehalten werden * Abhängigkeiten wie von Kunden, Aktionären, nahestehenden Personen, Mitarbeitern, die einen wesentlichen Einfluss auf die Geschäftstätigkeit oder Auswirkungen auf die Einhaltung der Zulassungsvoraussetzungen haben, sowie einseitig gelagerte Geschäftsbereiche und Interessenkonflikte * Überblick über sämtliche Aufgabenübertragungen an Dritte (insbesondere Delegationen von internen Funktionen) * Heranziehung von vertraglich gebundenen Vermittlern und/oder Zweigniederlassungen unter Angabe der Veränderungen zum Vorjahr * Personalbestand sowie organisatorische Aufstellung unter Angabe der Veränderungen zum Vorjahr unter Hinweis auf Abgänge von Schlüsselpersonen ausserhalb der Geschäftsleitung sowie fehlende Stellvertretungsregelungen * Wechsel im Verwaltungsrat und in der Geschäftsleitung * Beteiligungen der Gesellschaft * Wesentliche Änderungen im Geschäftsjahr (z.B. Fusionen, Reorganisationen, Restrukturierungen) * Aussage zu den im Zusammenhang mit der aktuellen und beabsichtigten zukünftigen Geschäftstätigkeit eingegangenen Risiken, insbesondere unter Berücksichtigung der Zielmärkte, der Expansionsabsichten, der erwarteten Volumina sowie der Produkte und Dienstleistungspalette * Hängige Verfahren gegen die Gesellschaft, Mitglieder der Leitungsorgane und Aktionäre   Die vorgenannten Punkte sind in Tabellenform aufzulisten. Ebenfalls ist zu beachten, dass Änderungen nach dem Bilanzstichtag bis zur Erstellung der Berichterstattung zu kennzeichnen bzw. aufzuzeigen sind. |

# Zusammenfassung der Prüfungsergebnisse

## Beanstandungen

|  |
| --- |
| Die Revisionsstelle nennt hier die Beanstandungen. Die Klassifizierung von Beanstandungen in tief, mittel und hoch richtet sich nach dem allgemeinen Teil der Richtlinie.  Die Beanstandungen erfolgen unter angemessenen Fristansetzungen und mit Hinweis auf die Seitenzahlen des Berichts mit der Detailinformation der jeweiligen Beanstandung.  Hat die Revisionsstelle keine Beanstandungen aufzuzeigen, hält sie dies ebenfalls fest.  Die Revisionsstelle gewährt der Wertpapierfirma die Möglichkeit zu einer eigenen Stellungnahme und kennzeichnet diese im Bericht entsprechend. |

## Beanstandungen zum Vorjahr

|  |
| --- |
| Die Revisionsstelle führt die Beanstandungen aufgrund des Berichtes über die Aufsichtsprüfung im Vorjahr auf, die zum Berichtszeitpunkt des Vorjahres nicht erledigt waren. Sie berichtet über die Ergebnisse der Nachprüfungund nimmt zur Einhaltung der gesetzten Fristen Stellung. Hat die Revisionsstelle im Vorjahr keine Beanstandungen mit Fristansetzungen vermerkt, hält sie dies fest. Konnte eine Beanstandung nicht fristgerecht erledigt werden, so sind die Gründe anzugeben und es ist eine neuerliche Beanstandung zu verzeichnen. |

## Empfehlungen

|  |
| --- |
| Die Revisionsstelle erläutert Empfehlungen, welche nicht als Beanstandungen eingestuft werden, aber für die Wertpapierfirma abgegeben wurden. Die Klassifizierung von Empfehlungen in tief, mittel und hoch richtet sich nach dem allgemeinen Teil der Richtlinie.  Die Empfehlungen erfolgen unter angemessenen Fristansetzungen und mit Hinweis auf die Seitenzahlen des Berichts mit der Detailinformation der jeweiligen Empfehlung.  Hat die Revisionsstelle keine Empfehlungen aufzuzeigen, hält sie dies ebenfalls fest.  Die Revisionsstelle gewährt der Wertpapierfirma die Möglichkeit zu einer eigenen Stellungnahme und kennzeichnet diese im Bericht entsprechend. |

## Empfehlungen zum Vorjahr

|  |
| --- |
| Die Revisionsstelle führt die Empfehlungen aufgrund des Berichts über die Aufsichtsprüfung im Vorjahr auf, die zum Berichtszeitpunkt des Vorjahres nicht erledigt waren. Sie berichtet über die Ergebnisse der Nachprüfung und nimmt zur Einhaltung der gesetzten Fristen Stellung. Hat die Revisionsstelle im Vorjahr keine Empfehlungen vermerkt, hält sie dies fest. Konnte eine Empfehlung mit Fristsetzung nicht fristgerecht erledigt werden, so sind die Gründe anzugeben und es ist eine neuerliche Empfehlung zu verzeichnen. |

## Wesentliche Feststellungen der Innenrevision

|  |
| --- |
| Die Revisionsstelle beschreibt an dieser Stelle allfällige wesentliche, aufsichtsrechtlich relevante Feststellungen (v.a. Feststellungen mit hoher Gewichtung) durch die Innenrevisionsfunktion. Die Revisionsstelle hat die Feststellungen sowie deren Auswirkungen auf das Risikoprofil der Wertpapierfirma angemessen zu würdigen. Sofern die Feststellungen an anderer Stelle im Bericht dargestellt werden, ist eine entsprechende Referenz ausreichend. |

## Wesentliche Feststellungen durch Dritte

|  |
| --- |
| Die Revisionsstelle beschreibt an dieser Stelle allfällige wesentliche, aufsichtsrechtlich relevante Feststellungen durch Dritte (z.B. die FMA, inländische/ausländische Behörden oder andere Revisionsstellen), über die sie innerhalb oder ausserhalb der Prüfungstätigkeit Kenntnis erlangt hat. Die Revisionsstelle hat die Feststellungen, sowie deren Auswirkungen auf das Risikoprofil der Wertpapierfirma angemessen zu würdigen. Sofern die Feststellungen an anderer Stelle im Bericht dargestellt werden, ist eine entsprechende Referenz ausreichend. |

## Wichtige Informationen

|  |
| --- |
| Hierunter fallen insbesondere:   * Hinweis auf allfällige Schwierigkeiten bei der Prüfung; * Abstützung auf Arbeiten der Innenrevision (Prüffelder und Umfang); * Berichtszeitraum, sofern dieser nicht mit dem Geschäftsjahr der Wertpapierfirma übereinstimmt. * Wesentliche Ereignisse nach dem Bilanzstichtag. Bei Änderungen nach dem Bilanzstichtag welche bereits unter Tz 1 aufgezeigt wurden, kann ein entsprechender Verweis angebracht werden.   Hat die Revisionsstelle keine wichtigen Hinweise anzubringen, hält sie dies ebenfalls fest. |

# Konsolidierte und zusätzliche Beaufsichtigung

|  |
| --- |
| Gestützt auf Art. 7 IFR und Art. 8 IFR bzw. Art. 70 WPFG nimmt die Revisionsstelle Stellung über das Erfordernis einer konsolidierten und zusätzlichen Beaufsichtigung und ob die diesbezüglichen Vorschriften eingehalten sind.  Die Revisionsstelle nimmt Stellung, ob eine EWR/Unions-Mutterwertpapierfirma gemäss Art. 4 Abs. 1 Z. 56 IFR, EWR/Unions-Mutterinvestmentholdinggesellschaft gemäss Art. 4 Abs. 1 Z. 57 IFR oder gemischte EWR/Unions-Mutterfinanzholdinggesellschaft gemäss Art. 4 Abs. 1 Z. 58 IFR eine Beteiligung an der Wertpapierfirma hält. |

# Einhaltung der Zulassungsvoraussetzungen

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur dauernden Einhaltung Zulassungsvoraussetzungen nach Art. 6 WPFG i.V.m. den entsprechend konkretisierenden Voraussetzungen der Verordnung über die Tätigkeit und Beaufsichtigung von Wertpapierfirmen. Sofern die Vorschriften nicht eingehalten sind oder in der Berichtsperiode nicht eingehalten waren, legt die Revisionsstelle die Umstände ausführlich im Bericht dar. Sie äussert sich dazu, inwieweit die Beanstandungen zum Berichtsjahr die Einhaltung in Frage stellen. |

## Eigenmittelvorschriften und Liquiditätsanforderungen

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Eigenmittelvorschriften nach Art. 6 Abs. 1 Bst. k i.V.m. Art. 16 WPFG i.V.m. Art. 9, 11, 13 und 14 IFR und bestätigt die Richtigkeit der Meldung zum Stichtag 31. Dezember gemäss Anhang I oder Anhang III der Delegierte Verordnung (EU) 2021/2284.  Die Revisionsstelle nimmt weiters Stellung zur Einhaltung der Liquiditätsanforderungen nach Art. 43 IFR und bestätigt bei einer Befreiung von den Liquiditätsanforderungen nach Art. 43 IFR, dass die Voraussetzungen für diese Befreiung weiterhin gegeben sind. Die Berechnungen sind im Bericht über die Aufsichtsprüfung oder dessen Anhang offenzulegen.  Die Revisionsstelle nimmt ebenfalls dazu Stellung, ob die Wertpapierfirma über solide, wirksame und umfassende Regelungen, Strategien und Verfahren bzgl. Höhe, Arten und Verteilung des internen Kapitals und der liquiden Aktiva gemäss Art. 32 WPFG verfügt. |

## Geschäftsplan

|  |
| --- |
| Die Revisionsstelle nimmt Stellung, ob die tatsächliche Geschäftstätigkeit mit den Angaben im Geschäftsplan/-reglement übereinstimmen. Sie bestätigt, dass abweichend vom Zulassungsumfang, keine unerlaubten Geschäfte getätigt werden und geht darauf ein, welche Wertpapierdienstleistungen und Anlagetätigkeiten gemäss Anhang 1 WPDG tatsächlich ausgeführt werden bzw. seit mehr als sechs Monaten nicht ausgeführt werden (Art. 10 Abs. 1 Bst. b WPFG).  Bei Heranziehung von Zweigniederlassungen und/oder vertraglich gebundenen Vermittlern nimmt die Revisionsstelle Bezug auf die von diesen angebotenen bzw. erbrachten Wertpapier- und Nebendienstleistungen. |

## Inländische Betriebsstätte und geeignete Organisation

|  |
| --- |
| Die Revisionsstelle stellt die Grundzüge der Organisation und internen Kontrollmechanismen dar. Sie nimmt zusammenfassend Stellung zur Angemessenheit der Organisation in den wesentlichen Geschäftsbereichen und der internen Kontrollmechanismen nach Art. 6 Abs.1 Bst. f i.V.m. Art. 15 WPFG.  Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften zur internen Unternehmensführung gemäss Art. 15 und Art. 34 WPFG eingehalten sind und beurteilt zudem die Wahrnehmung der Kontrollen durch die Geschäftsleitung und den Verwaltungsrat.  Weiter nimmt die Revisionsstelle Stellung zur Ressourcenausstattung der Wertpapierfirma. Sie beurteilt, ob die Organisation sowie die verfügbaren Kompetenzen und Fähigkeiten angemessen sind, sofern die betroffenen Personen keiner Zulassungspflicht unterliegen. Dabei wird die wirksame Einbeziehung von Nachhaltigkeitsrisiken berücksichtigt.  Bei Heranziehung von Zweigniederlassungen und/oder vertraglich gebundenen Vermittlern prüft die Revisionsstelle die Angemessenheit der Organisationsstruktur inklusive Berichtslinien sowie die Einhaltung des Art. 24 WPDG in Bezug auf vertraglich gebundene Vermittler. |

## Zulassungs- und meldepflichtige Änderungen

|  |
| --- |
| Die Revisionsstelle nimmt Stellung, ob im Berichtsjahr zulassungs- und meldepflichtige Ereignisse nach Art. 28 WPFG vorlagen und die gesetzliche Pflicht eingehalten wurde. Dabei ist auch Art. 18 WPFG zu berücksichtigen.  Zusätzlich nimmt die Revisionsstelle Stellung, ob im Berichtsjahr Kryptowerte-Dienstleistungen gemäss Art. 3 Abs. 1 Z. 16 der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCAR)angeboten oder erbracht wurden und die gesetzlichen Voraussetzungen hierfür vorliegen (insbesondere Art. 60ff MiCAR). |

# Pflichten der Wertpapierfirma

## Organisatorische Anforderungen

### Risikomanagement-Funktion

|  |
| --- |
| Die Revisionsstelle beschreibt die Grundsätze der Risikomanagement-Funktion und nimmt Stellung zur Ausgestaltung nach Art. 36 und 37 WPFG und der Delegierte Verordnung (EU) 2017/565. Sie beurteilt, ob die Wertpapierfirma über solide Strategien, Grundsätze, Verfahren und Systeme nach Art. 37 WPFG verfügt. Sofern anwendbar beurteilt sie, die Funktion des Leitungsorgans im Risikomanagement nach Art. 36 WPFG.  Sie beurteilt, ob die Risikomanagement-Funktion den komplexen Verhältnissen (komplexe Anlagestrategien oder andere besondere Risiken) genügen kann, hinsichtlich Identifikation, Messung, Bewirtschaftung und Überwachung der Risiken sowie der Einhaltung der einschlägigen Bestimmungen.  Die Revisionsstelle beurteilt, unter Berücksichtigung der Art und Komplexität der betriebenen Geschäfte, die Organisation, die Ressourcen sowie die Qualität der Arbeit. In diesem Zusammenhang prüft die Revisionsstelle die Handhabung von Cross-Border-Risiken (FMA-Mitteilung 2015/3) und nimmt hierzu Stellung.  Dabei prüft sie auch, dass die Risikomanagement-Funktion Nachhaltigkeitsfaktoren in ihrer Bewertung und Überwachung angemessen miteinbezieht und die Offenlegung betreffend die Strategien für den Umgang mit Nachhaltigkeitsrisiken nach Art. 3 Verordnung (EU) 2019/2088 den implementierten Verfahren entspricht.  Erfolgt eine Delegation der Risikomanagement-Funktion ist die zuständige Person (ausführende Person) beim Delegationsnehmer zu benennen. Weiter ist anzugeben, wer bei der Wertpapierfirma für die Überwachung der Delegation (Auslagerung) zuständig ist.  Die Einhaltung der Vorschriften bei Auslagerung (Delegation) ist zu prüfen.  Zur Beurteilung der Angemessenheit der Risikomanagement-Funktion kann sich die Revisionsstelle auf die Arbeit der Revisionsstelle des Delegationsnehmers stützen. Dies ersetzt jedoch nicht die abschliessende Beurteilung der Angemessenheit hinsichtlich Organisation und Ressourcen sowie Qualität der Arbeit der Funktion. |

### Compliance-Funktion

|  |
| --- |
| Die Revisionsstelle nimmt, unter Berücksichtigung der Art und Komplexität der betriebenen Geschäfte, Stellung zur angemessenen Ausgestaltung der Compliance-Funktion gemäss Art. 21 WPFG und Art. 22 der Delegierte Verordnung (EU) 2017/565. In diesem Zusammenhang wird auf die ESMA-Leitlinie zu einigen Aspekten der MiFID-Anforderungen an die Compliance-Funktion, welche die FMA für comply erklärt hat, verwiesen.  Erfolgt eine Delegation der Compliance-Funktion ist die zuständige Person (ausführende Person) beim Delegationsnehmer zu benennen. Weiter ist anzugeben, wer bei der Wertpapierfirma für die Überwachung der Auslagerung (Delegation) zuständig ist.  Die Einhaltung der Vorschriften bei Auslagerung (Delegation) ist zu prüfen.  Zur Beurteilung der Angemessenheit der Compliance-Funktion kann sich die Revisionsstelle auf die Arbeit der Revisionsstelle des Delegationsnehmers stützen. Dies ersetzt jedoch nicht die abschliessende Beurteilung der Angemessenheit hinsichtlich Organisation und Ressourcen sowie Qualität der Arbeit der Funktion. |

### Innenrevisionsfunktion

|  |
| --- |
| Die Revisionsstelle hält die von der Innenrevisionsfunktion durchgeführten Prüfungen fest und nimmt Stellung zu den wesentlichen Prüfergebnissen sowie den diesbezüglich von der Wertpapierfirma getroffenen Massnahmen.  Sie äussert sich ebenfalls zur Qualität der Arbeiten der Innenrevisionsfunktion sowie dazu, ob, unter Berücksichtigung der Art und Komplexität der von der Wertpapierfirma betriebenen Geschäfte, die Organisation und die Ressourcen der Innenrevision den besonderen Anforderungen gemäss Art. 24 der Delegierte Verordnung (EU) 2017/565 entsprechen. Sie erläutert dabei kurz die organisatorische Eingliederung und die personelle Zusammensetzung der Innenrevisionsfunktion und die Form der Zusammenarbeit mit der Revisionsstelle.  Erfolgt eine Delegation der Innenrevisionsfunktion ist die zuständige Person (ausführende Person) beim Delegationsnehmer zu benennen. Weiter ist anzugeben, wer bei der Wertpapierfirma für die Überwachung der Delegation zuständig ist.  Die Einhaltung der Vorschriften bei Auslagerungen (Delegationen) ist zu prüfen.  Zur Beurteilung der Angemessenheit der Innenrevisionsfunktion kann sich die Revisionsstelle auf die Arbeit der Revisionsstelle des Delegationsnehmers stützen. Dies ersetzt jedoch nicht die Abschliessende Beurteilung der Angemessenheit hinsichtlich Organisation und Ressourcen sowie Qualität der Arbeit der Funktion. |

### Beschwerdemanagement

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Angemessenheit des Beschwerdemanagements gemäss Art. 26 der Delegierte Verordnung (EU) 2017/565.  Zudem prüft sie, ob die Dokumentation und Aufbewahrung der Beschwerden und die zur Beilegung getroffenen Massnahmen zweckmässig erfolgte. |

## Auslagerung von betrieblichen Aufgaben

|  |
| --- |
| Bei der Auslagerung von betrieblichen Aufgaben nimmt die Revisionsstelle Stellung zur Einhaltung der Anforderungen bei der Aufgabenübertragung gemäss Art. 24 WPFG.  Hierbei beurteilt die Revisionsstelle die Anforderungen bei der Auslagerung und stellt die Prozesse der Überwachung der ausgelagerten betrieblichen Aufgaben dar. |

## Vergütungspolitik

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften zu folgenden Punkten eingehalten werden:   * Vergütungspolitik (Art. 38 und 39 WPFG sowie Art. 11 WPDG) * Variable Vergütung (Art. 40 WPFG) * Vergütungsausschuss (Art. 41 WPFG) * Überwachung der Vergütungspolitik (Art. 42 WPFG)   Die Revisionsstelle stellt die von der Wertpapierfirma festgelegten und angewendeten Vergütungsgrundsätze und -praktiken dar und nimmt Stellung zur Einhaltung der Offenlegung nach Art. 5 der Verordnung (EU) 2019/2088. |

## Vermeidung von Interessenkonflikten

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Angemessenheit der Vorkehrungen zur Vermeidung von Interessenkonflikten nach Art. 15 und 21 WPFG, Art. 5 WPDG sowie gemäss Abschnitt 3 der Delegierte Verordnung (EU) 2017/565. In diesem Zusammenhang wird auf die ESMA-Leitlinien zu Vergütungsgrundsätzen und ‑verfahren (MiFID), welche die FMA für comply erklärt hat, verwiesen.  Ferner prüft die Revisionsstelle die Verfahren zur Ermittlung der Arten von Interessenkonflikten, die sich aus der Einbeziehung von Nachhaltigkeitsrisiken in ihre Prozesse, Systeme und internen Kontrollen ergeben können.  Die Revisionsstelle hält die Ausleihungen an Aktionäre bzw. an andere an der Wertpapierfirma Beteiligte oder diesen nahestehenden natürlichen und juristische Personen fest. Hat die Revisionsstelle keine solchen Geschäften festgestellt, hält sie dies ebenfalls fest.  Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften im Hinblick auf Organ- und Mitarbeitergeschäfte gemäss Artikel 28 und 29 der Delegierte Verordnung (EU) 2017/565. |

## Freier Dienstleistungsverkehr

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Organisationsstruktur sowie internen Vorkehrungen für die Erbringung von Wertpapierdienstleistungen und/oder Anlagetätigkeiten gemäss Art. 45, 47 und 49 WPFG ausreichend sind, unter Berücksichtigung von Art und Ausmass der Dienstleistungen und/oder Anlagetätigkeiten, wobei insbesondere auch geprüft wird, ob die WPF in den relevanten Staaten jeweils tatsächlich tätig ist bzw. Kunden tatsächlich akquiriert. Ist die Wertpapierfirma in Staaten ausschliesslich auf eigene Initiative der Kunden tätig, ist dies ebenso anzuführen. In Bezug auf Tätigkeiten in Drittstaaten ist eine allfällige Bewilligungspflicht zu prüfen.  Die Revisionsstelle prüft insbesondere die Ausstattung der internen Kontrollfunktionen in Bezug auf die Erbringung von grenzüberschreitenden Dienstleistungen in anderen Mitgliedstaaten und berücksichtigt dabei die Notwendigkeit von entsprechenden Fremdsprachenkenntnissen sowie Kenntnissen von rechtlichen Gegebenheiten in den Aufnahmemitgliedstaaten. |

## Offenlegungspflichten

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zu den Offenlegungspflichten gemäss Art. 46 bis 53 IFR unter Berücksichtigung der Delegierte Verordnung (EU) 2022/1159 sowie der Delegierte Verordnung (EU) 2021/2284. |

## Vorschriften zum Anlegerschutz

### Anlageberatung und Portfolioverwaltung

|  |
| --- |
| Die Revisionsstelle nimmt im Falle einer entsprechenden Dienstleistung im Bereich der Anlageberatung Stellung zur Einhaltung der Vorschriften im Hinblick auf die Anlageberatung, insbesondere in Bezug auf nachfolgende Punkte:   * Prüfung ob Anlageberatung angeboten wird * Unabhängige/nicht unabhängige Anlageberatung   + Anlageberatungsvertrag   + Prozessbeschreibung   + angebotene Produktpalette   + Einhaltung der Informationspflichten * Organisatorische Anforderungen an die Wertpapierfirma bei der Erbringung von unabhängiger und nicht-unabhängiger Anlageberatung |

### Aufzeichnungs- und Aufbewahrungspflichten

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften im Hinblick auf die Aufzeichnungs- und Aufbewahrungspflichten, insbesondere in Bezug auf nachfolgende Punkte:   * Interne Weisungen * Aufzeichnungspflichten Kommunikation und Telefongespräche * Aufbewahrungspflicht * Offenlegung * Compliance   Bei Zweigniederlassungen in einem anderen Mitgliedsstaat prüft die Revisionsstelle die Einhaltung des Art. 26 WPFG. |

### Zuwendungen

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften im Hinblick auf die Entgegennahme oder Zahlung von Zuwendungen (Inducements), insbesondere in Bezug auf nachfolgende Punkte:   * Klassierung der Gesellschaft * Interne Weisungen * Aufzeichnung der Zuwendungen und Klassierung * Weitergabe/Einbehalt von monetären Zuwendungen * Einbehalt von nicht monetären Zuwendungen * Offenlegung * Interessenkonflikte * Analysen und Analysenkonto |

### Geeignetheit und Angemessenheit

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften betreffend die Geeignetheit und Angemessenheit, insbesondere in Bezug auf nachfolgende Punkte:   * Interne Weisungen * Organisation * Einholung der Informationen über den Kunden, einschliesslich der Nachhaltigkeitspräferenzen * Durchführung der S&A Tests * Umschichtung von Anlagen * Vereinbarungen bei Portfolioverwaltungsdienstleistungen und allgemeine Überwachung der Anlagevorschriften * Produktauswahl und potenzielle Interessenkonflikte * Dokumentation * Reporting und Berichtspflichten gegenüber dem Kunden |

### Produktüberwachung

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften betreffend die Produktüberwachung, insbesondere in Bezug auf die nachfolgenden Punkte (Produktvertreiber/Zielmarkt):   * Prozess zur regelmässigen Überprüfung der Kompatibilität der Finanzinstrumente mit dem Zielmarkt (dabei werden ebenfalls etwaige Nachhaltigkeitsfaktoren berücksichtigt) * Prozess in Bezug auf den Vertrieb des Finanzinstruments ausserhalb des positiven Zielmarkts * Prozess zur Dokumentation beim Vertrieb im negativen Zielmarkt * Prozess zur Festlegung von Zielmarktkriterien * Zielmarkt-Konzepte * Anwendbarkeit der Produktüberwachung auf Drittlandprodukte * Kontrollprozess und Compliance-Berichte zu konzipierten Finanzinstrumenten |

### Information und Berichterstattung gegenüber Kunden

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften betreffend die Information und Berichterstattung gegenüber Kunden insbesondere in Bezug auf nachfolgende Punkte:   * Interne Weisungen * Kostenreporting * Ausführungsreporting * Verwaltungsreporting * Verlustschwellenreporting * Kundeninformation/Marketingmitteilungen |

### Erbringung von Dienstleistungen über Dritte

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften betreffend die Erbringung von Dienstleistungen über eine andere Bank, Wertpapierfirma oder Vermögensverwaltungsgesellschaft insbesondere über die Vollständigkeit und Richtigkeit der weitergeleiteten Anweisungen gemäss Art. 19 WPDG. |

### Bestmögliche Ausführung und Bearbeitung von Kundenaufträgen

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften betreffend die bestmögliche Ausführung von Kundenaufträgen gemäss Art. 20 bis Art. 22 WPDG sowie der Bearbeitung von Kundenaufträgen gemäss Art. 23 WPDG. |

### Geeignete Gegenpartei

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften betreffend Geschäfte mit geeigneten Gegenparteien gemäss Art. 25 WPDG. |

### Verdachtsmitteilung gemäss MAR

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften betreffend Verdachtsmitteilung nach Art. 16 Verordnung (EU) Nr. 596/2014 (MAR) i.V.m. Delegierte Verordnung (EU) 2016/957 und Delegierte Verordnung (EU) 2016/522. Sie prüft insbesondere die Angemessenheit der Prozesse und Weisungen. Die Revisionsstelle nimmt Einsicht in die überreichten Verdachtsmitteilungen, unabhängig der Prüftiefe. |

# 

# Betrieb von Multilateralen Handelssystemen (MTF) oder Organisierten Handelssystemen (OTF)

## Handel und Abschluss von Geschäften

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 7, Art. 8 Abs. 5 und Art. 11 HPBG durch den Betreiber eines MTF oder OTF zu folgenden Punkten eingehalten werden:   * Vorhandensein öffentlich zugänglicher Allgemeiner Geschäftsbedingungen (Art. 7 Abs. 2 Bst. a und b HPBG) * Vorhandensein von angemessenen Vorkehrungen zu Interessenkonflikten (Art. 7 Abs. 2 Bst. c HPBG) * Informationen über die Abrechnung (Art. 7 Abs. 2 Bst. e und f HPBG) * Nachweis über drei aktive Mitglieder (Art. 7 Abs. 3 HPBG) * Nachweis über die Synchronisierung von Uhren (Art. 7 Abs. 4 und Art. 7 Abs. 3 Bst. d i.V.m. Art. 28 HPBG) |

## Vorkehrungen des Art. 23 bis 27 HPBG

|  |
| --- |
| Gemäss Art. 7 Abs. 2 Bst. d HPBG haben Betreiber eines MTF oder OTF insbesondere mit den Artikeln 23 bis 27 HPBG im Einklang zu stehen und hierfür über wirksame Systeme, Verfahren und Vorkehrungen zu verfügen. Die Revisionsstelle nimmt zu den Prüfungsergebnissen der nachfolgenden Prüffelder zusammenfassend Stellung. |

### Organisatorische Belastbarkeit der Systeme und Notfallsicherungen

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 23 HPBG durch den Betreiber eines MTF oder OTF zu folgenden Punkten eingehalten werden:   * Vorhandensein wirksamer Systeme, Verfahren und Massnahmen um sicherzustellen, dass Handelssysteme belastbar sind und über ausreichende Kapazitäten für Spitzenvolumina an Aufträgen und Mitteilungen verfügt sowie ob wirksame Notfallvorkehrungen vorliegen (Art. 23 Abs. 1 und 5 HPBG) * Vorhandensein schriftlicher Vereinbarungen mit den Mitgliedern (Art. 23 Abs. 2 Bst. a und b und Abs. 3 HPBG) * Vorhandensein von angemessenen Regeln zur Einstellung oder Einschränkung des Handels (Art. 23 Abs. 6 und 7 HPBG) * Gewährleistung eines reibungslosen und rechtzeitigen Abschlusses der innerhalb ihrer Systeme ausgeführten Geschäfte (Art. 8 Abs. 3 Bst. b HPBG) * Vorhandensein ausreichender Finanzmittel (Art. 8 Abs. 3 Bst. c HPBG) |

### Algorithmischer Handel

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 24 HPBG durch den Betreiber eines MTF oder OTF, sofern ein algorithmischer Handel vorliegt, eingehalten sind. |

### Direkter elektronischer Zugang

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 25 HPBG durch den Betreiber eines MTF oder OTF zu folgenden Punkten eingehalten sind:   * Vorhandensein wirksamer Systeme, Verfahren und Massnahmen für den direkten elektronischen Zugang (Art. 25 Abs. 1 HPBG) * Vorhandensein angemessener Standards in Bezug auf die Risikokontrolle und Schwellen für den Handel über einen elektronischen Zugang (Art. 25 Abs. 2 HPBG) * Vorhandensein eines angemessenen Systems für einen Kunden im Falle der Nichteinhaltung des Art. 25 HPBG (Art. 25 Abs. 3 HPBG) |

### Gebühren

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften in Bezug auf das Vorhandensein einer Gebührenstrukturen des Art. 26 HPBG durch den Betreiber eines MTF oder OTF zu eingehalten sind. |

### Tick-Grössen

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 27 HPBG durch den Betreiber eines MTF oder OTF eingehalten sind. Sie prüft das Vorhandensein von angemessenen Regelungen für die Tick-Grössen bei Aktien, Aktienzertifikaten, börsengehandelten Fonds, Zertifikaten und anderen vergleichbaren Finanzinstrumenten sowie anderen Finanzinstrumenten nach der Delegierte Verordnung (EU) 2017/588. |

## Besondere Anforderungen an einen MTF

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 8 HPBG durch den Betreiber eines MTF zu folgenden Punkten eingehalten werden:   * Einhaltung der Voraussetzungen (Art. 8 Abs. 1 HPBG) * Vorhandensein der angemessenen Vorkehrungen in Bezug zur Ausführung der Kundenaufträge (Art. 8 Abs. 2 HPBG) * Einhaltung der Regeln nach Art. 8 Abs. 3 Bst. a bis d HPBG * Einhaltung der Regeln nach Art. 8 Abs. 8 HPBG |

## Besondere Anforderungen an einen OTF

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 9 HPBG durch den Betreiber eines OTF zu folgenden Punkten eingehalten werden:   * Einhaltung der Voraussetzungen (Art. 9 Abs. 1 HPBG) * Vorhandensein der angemessenen Vorkehrungen in Bezug zur Ausführung der Kundenaufträge (Art. 9 Abs. 2 HPBG) * Einhaltung der Regeln nach Art. 9 Abs. 3 Bst. a bis d HPBG * Einhaltung der Regeln nach Art. 9 Abs. 8 HPBG |

## Überwachungspflichten

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 10 HPBG durch den Betreiber eines MTF oder OTF zu folgenden Punkten eingehalten werden:   * Vorhandensein von wirksamen Vorkehrungen und Verfahren im Hinblick auf die Einhaltung aller Regeln des MTF oder OTF (Art. 10 Abs. 1 HPBG) * Überwachung der Aufträge (Art. 10 Abs. 2 HPBG) |

## KMU-Wachstumsmarkt

|  |
| --- |
| Sofern der MTF als KMU-Wachstumsmarkt registriert ist, nimmt die Revisionsstelle dazu Stellung, ob die Vorschriften des Art. 12 HPBG eingehalten werden. |

## Zentrale Gegenpartei/Clearing und Abrechnung

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob der Betreiber eines MTF gemäss Art. 13 HPBG mit einer zentralen Gegenpartei oder Clearingstelle und einem Abwicklungssystem eines anderen EWR-Mitgliedstaats geeignete Vereinbarungen über Clearing und/oder Abwicklung abgeschlossen haben und diesfalls die Voraussetzungen der Nutzung eines solchen Abrechnungssystems nach Art. 13 Abs. 2 HPBG eingehalten werden. |

## Vorhandels-/Nachhandelstransparenz in Bezug auf Aktien, Aktienzertifikate, börsengehandelte Fonds, Zertifikate und andere vergleichbare Finanzinstrumente

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften über die Veröffentlichung der aktuellen Geld- und Briefkurse und der Tiefe der Handelspositionen zu den Kursen gemäss Art. 3 der Verordnung (EU) Nr. 600/2014 (MiFIR) und über die Veröffentlichung des Preises, des Volumens und des Zeitpunkts der Geschäfte gemäss Art. 6 der Verordnung (EU) Nr. 600/2014 (MiFIR) durch den Betreiber eines MTF oder OTF (i.V.m. Art. 12 Verordnung (EU) Nr. 600/2014 (MiFIR)). |

## Vorhandels-/Nachhandelstransparenz in Bezug auf Schuldverschreibungen, strukturierte Finanzprodukte, Emissionszertifikate und Derivate

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften über die Veröffentlichung der aktuellen Geld- und Briefkurse und der Tiefe der Handelspositionen zu den Kursen gemäss Art. 8 der Verordnung (EU) Nr. 600/2014 (MiFIR) und über die Veröffentlichung des Preises, des Volumens und des Zeitpunkts der Geschäfte gemäss Art. 10 der Verordnung (EU) Nr. 600/2014 (MiFIR) durch den Betreiber eines MTF oder OTF. OTF (i.V.m. Art. 12 der Verordnung (EU) Nr. 600/2014 (MiFIR)). |

## Offenlegung von Vorhandels- und Nachhandelsdaten zu angemessenen kaufmännischen Bedingungen

|  |
| --- |
| Die Revisionsstelle nimmt Stellung zur Einhaltung der Vorschriften, ob der Betreiber des MTF oder OTF die nach den Artikeln 3, 4 und 6 bis 11 der Verordnung (EU) Nr. 600/2014 (MiFIR) zu veröffentlichenden Informationen zu angemessenen kaufmännischen Bedingungen offenlegt und ob ein diskriminierungsfreier Zugang zu den Informationen besteht (Art. 13 der Verordnung (EU) Nr. 600/2014 (MiFIR)). |

# Meldung von Transaktionsdaten

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Vorschriften des Art. 26 Abs. 5 der Verordnung (EU) Nr. 600/2014 (MiFIR) durch den Betreiber eines MTF oder OTF eingehalten werden. |

# Meldung von Referenzdaten für die einzelnen Finanzinstrumente

|  |
| --- |
| Die Revisionsstelle nimmt dazu Stellung, ob die Betreiber des MTF oder OTF Referenzdaten an die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) nach Art. 27 der Verordnung (EU) Nr. 600/2014 (MiFIR) i.V.m. der Delegierte Verordnung (EU) 2017/585 und nach Art. 4 der Verordnung (EU) Nr. 596/2014 (MAR) melden. |

# Vorbeugung und Aufdeckung von Marktmissbrauch für die einzelnen Finanzinstrumente

|  |
| --- |
| Die Revisionsstelle nimmt Stellung dazu, ob der Betreiber des MTF oder OTF über wirksame Regeln, Systeme und Verfahren zur Verhütung und Aufdeckung von Insidergeschäften, Marktmissbrauch, versuchten Insidergeschäften und versuchtem Marktmissbrauch gemäss Art. 16 der Verordnung (EU) Nr. 596/2014 (MAR) verfügt und ob die Mitarbeiter diesbezüglich geschult sind. |

# Digitale operationale Resilienz

Die Revisionsstelle kann das Prüffeld mittels einer graduellen Abdeckung über vier Jahre prüfen. Das Prüffeld ist hierzu in die Prüfelemente Governance & Organisation, IKT-Risikomanagementrahmen, Reaktion & Wiederherstellung, IKT-bezogene Vorfälle, Testen der digitalen operationalen Resilienz und Management des IKT-Drittparteienrisikos aufzuteilen. Der Umfang der Prüfung im jeweiligen Prüfungsjahr ist anzugeben.

Die mit \* gekennzeichneten Mindestprüfinhalte oder Bestätigungen weisen Erleichterungen für Kleinstunternehmen nach DORA aus, die bei einer Klassifizierung als Kleinstunternehmen zu berücksichtigen sind. Dabei ist zu beachten, dass diese Mindestprüfinhalte für Kleinstunternehmen nicht gänzlich entfallen, jedoch die Erleichterungen zu berücksichtigen sind.

## Governance & Organisation

|  |
| --- |
| Die Revisionsstelle prüft die Einhaltung der Bestimmungen betreffend Governance und Organisation, insbesondere hinsichtlich der nachfolgenden Aspekte:   * Es besteht ein angemessener interner Governance- und Kontrollrahmen, welcher ein effektives Management von IKT-Risiken gewährleistet und die Verantwortlichkeiten des Leitungsorgans angemessen berücksichtigt. * Es werden angemessene Budgetmittel zugewiesen und regelmässig überprüft, um den Anforderungen in Bezug auf die digitale operationale Resilienz gerecht zu werden (Programme zur Sensibilisierung für IKT-Sicherheit, Schulungen und IKT-Kompetenzen für Mitarbeitende). * Die Geschäftsleitung hält ausreichende Kenntnisse und Fähigkeiten aktiv auf dem neuesten Stand, unter anderem indem sie regelmässig spezielle Schulungen absolviert. |

## IKT-Risikomanagementrahmen

|  |
| --- |
| Die Revisionsstelle prüft die Einhaltung der Bestimmungen zum IKT‑Risikomanagementrahmen, insbesondere hinsichtlich der nachfolgenden Aspekte:   * Die Wertpapierfirma verfügt über einen angemessenen, soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil ihres Gesamtrisikomanagementsystems ist. * Die Wertpapierfirma überträgt die Zuständigkeit für das Management und die Überwachung des IKT-Risikos an eine Kontrollfunktion und stellt ein angemessenes Mass an Unabhängigkeit dieser Kontrollfunktion sicher.\* * Der IKT-Risikomanagementrahmen wird mindestens einmal jährlich (im Falle von Kleinstunternehmen regelmässig) sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach aufsichtsrechtlichen Anweisungen oder Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, dokumentiert und überprüft.\* * Im Einklang mit dem Revisionsplan wird der IKT-Risikomanagementrahmen regelmässig der Prüfung durch die Innenrevision unterzogen.\* * Um IKT-Risiken zu bewältigen und zu managen, verwendet und unterhält die Wertpapierfirma angemessene und stets auf dem neuesten Stand gehaltene und zuverlässige IKT‑Systeme, ‑Protokolle und -Tools. * Die Wertpapierfirma muss alle IKT-gestützten Geschäftsprozesse, Systeme, Rollen und Verantwortlichkeiten, Assets und deren interne sowie externe Abhängigkeiten systematisch identifizieren, klassifizieren, dokumentieren und führen regelmässig Risikobewertungen durch.\* * Es existieren geeignete und angemessene Schutz- und Präventionsmassnahmen, um IKT-Systeme und Daten wirksam gegen Bedrohungen, Angriffe und Störungen abzusichern – unter Berücksichtigung von Vertraulichkeit, Integrität und Verfügbarkeit sowie durch Anwendung angemessener IKT-Sicherheitstools, -Richtlinien und ‑Verfahren, Kontrollen der Zugangs- und Zugriffsrechte, Verschlüsselung, Netzwerksegmentierung und regelmässiger Überprüfung. |

## Reaktion & Wiederherstellung

|  |
| --- |
| Die Revisionsstelle prüft die Einhaltung der Bestimmungen zur Reaktion und Wiederherstellung nach IKT-bezogenen Störungen und Vorfällen, insbesondere hinsichtlich der nachfolgenden Aspekte:   * Die Wertpapierfirma verfügt über eine umfassende IKT-Geschäftsfortführungsrichtlinie, die integraler Bestandteil der allgemeinen Geschäftsfortführungsrichtlinie ist. * Die Wertpapierfirma hat über angemessene Pläne und Verfahren zur Reaktion auf sowie zur Wiederherstellung nach IKT-bezogenen Störungen und Vorfällen entwickelt, getestet und in der Mehrjahresplanung der Innenrevision entsprechend integriert.\* * Die internen Verfahren stellen sicher, dass eine angemessene Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen als Teil der allgemeinen Geschäftsfortführungsleitlinie durchgeführt wird.\* * Es wurde eine Krisenmanagementfunktion eingerichtet, die bei Aktivierung ihrer IKT‑Geschäftsfortführungspläne oder ihrer IKT-Reaktions- und Wiederherstellungspläne unter anderem klare Verfahren für die Abwicklung interner und externer Krisenkommunikation gemäss Art. 14 DORA festlegt.\* * Die Wertpapierfirma hat angemessene Richtlinien und Verfahren sowie Wiedergewinnungs- und Wiederherstellungsverfahren und ­‑methoden für die Datensicherung erstellt und dokumentiert. Sie besitzt angemessene Datensicherungssysteme und testet diese regelmässig. * Die Wertpapierfirma unterhält redundante IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind.\* * Die internen Verfahren stellen sicher, dass bei der Wiederherstellung nach IKT-bezogenen Vorfällen die erforderlichen Prüfungen durchgeführt werden, einschliesslich jeglicher Mehrfachprüfungen und Abgleiche, um die grösstmögliche Datenintegrität sicherzustellen, wobei diese Prüfungen auch bei der Rekonstruktion von Daten externer Interessenträger durchgeführt werden. * Die Wertpapierfirma verfügt über Kapazitäten und Personal, um Informationen über Schwachstellen und Cyberbedrohungen, IKT-bezogene Vorfälle, insbesondere Cyberangriffe, zu sammeln und die wahrscheinlichen Auswirkungen auf ihre digitale operationale Resilienz zu untersuchen. * Die internen Verfahren stellen sicher, dass die Wertpapierfirma aus IKT-bezogenen Vorfällen, Tests und Bedrohungen systematisch durch nachträgliche Prüfungen lernen, ihre Sicherheitsmassnahmen kontinuierlich verbessern und organisatorisches Lernen fördern.\* * Die Wertpapierfirma hat im Rahmen des IKT-Risikomanagementrahmens angemessene und klare Kommunikationsstrategien, -verfahren und -pläne für den Umgang mit IKT-bezogenen Vorfällen und Schwachstellen etabliert. * Die internen Verfahren stellen sicher, dass mindestens eine Person in der Wertpapierfirma mit der Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt ist und zu diesem Zweck die entsprechende Aufgabe gegenüber der Öffentlichkeit und den Medien wahrnimmt. |

## IKT-bezogene Vorfälle

|  |
| --- |
| Die Revisionsstelle prüft betreffend die Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle insbesondere nachfolgende Aspekte:   * Die Wertpapierfirma verfügt über angemessene Verfahren und Mechanismen zur effektiven Erkennung von IKT-bezogenen Anomalien, Vorfällen und potenziellen Bedrohungen. * Die Wertpapierfirma stellt ausreichende Ressourcen und Kapazitäten bereit, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen. * Es bestehen angemessene Prozesse und Verfahren zur Identifikation, Behandlung, Klassifizierung und Berichterstattung von IKT-bezogenen Vorfällen sowie zur Behandlung und Kommunikation hinsichtlich erhebliche Cyberbedrohungen. * Es wurden alle IKT-bezogenen Vorfälle und erheblichen Cyberbedrohungen im Prüfungsjahr erfasst. |

## Testen der digitalen operationalen Resilienz

|  |
| --- |
| Die Revisionsstelle prüft, dass ein angemessenes, solides und umfassendes Programm sowie angemessene Verfahren und Richtlinien für das Testen der digitalen operationalen Resilienz als integraler Bestandteil des IKT-Risikomanagementrahmens bestehen, welche laufend gepflegt und überprüft werden. Diese zielen darauf ab, die Vorbereitung auf IKT-bezogene Vorfälle zu bewerten, Schwächen und Mängel zu identifizieren und die umgehende Umsetzung entsprechender Massnahmen zu ermöglichen.\* |

## Management des IKT-Drittparteienrisikos

|  |
| --- |
| Die Revisionsstelle prüft, dass die Bestimmungen betreffend das Management des IKT-Drittparteienrisikos eingehalten sind. Dabei sind insbesondere folgende Aspekte zu beurteilen:   * Die Wertpapierfirma verfügt im Umgang mit IKT-Drittdienstleistern über klare Governance-Strukturen sowie angemessene Auswahl- und Bewertungsverfahren. * Die Leitlinie zur Nutzung von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen und von IKT-Drittdienstleistern bereitgestellt werden, enthält die erforderlichen Anforderungen, Prinzipien, Verantwortlichkeiten und Prozesse für jede Hauptphase des Lebenszyklus dieser IKT-Dienstleistungen und wird zumindest einmal jährlich überprüft bzw. aktualisiert. * Die wesentlichen Risiken, welche durch vertragliche Vereinbarungen mit IKT-Drittdienstleisters entstehen, werden laufend identifiziert, bewertet, gemessen, begrenzt, überwacht, gesteuert und dokumentiert. * Die internen Verfahren stellen sicher, dass die Wertpapierfirma im Rahmen der Risikobewertung regelmässig bewertet, ob eine kritische Abhängigkeit von einzelnen IKT-Drittdienstleistern oder -Infrastrukturen besteht, die zu Konzentrationsrisiken führen kann. * Die internen Verfahren und Prozesse sowie die gegebene Datenlage stellen sicher, dass das Informationsregister korrekt befüllt und der FMA fristgerecht gemeldet werden kann. * Die Verträge mit IKT-Drittdienstleistern enthalten klare, überprüfbare und durchsetzbare Anforderungen, insbesondere zu Dienstleistungsgüte, Sicherheitsstandards, Zugangs- und Prüfungsrechten, Kündigungsrechte, Beendigungsszenarien sowie zum Verfahren bei IKT-bezogenen Vorfällen. * Die internen Prozesse und Verfahren stellen sicher, dass die vertraglichen Vereinbarungen sowie die Leistungserbringung entsprechend der Kritikalität der betroffenen Funktion angemessen und der festgelegten Zuständigkeit mit angemessenen Personalressourcen überwacht werden. * Die internen Verfahren stellen sicher, dass die in den vertraglichen Vereinbarungen enthaltenen Kündigungsregelungen im Sinne der Exit-Planung gewährleisten, dass die vertragliche Vereinbarung beendet werden kann, ohne die Geschäftstätigkeiten zu unterbrechen oder die Einhaltung der regulatorischen Anforderungen zu gefährden. * Die internen Verfahren stellen sicher, dass für jede vertragliche IKT-Vereinbarung über IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen und von einem IKT-Drittdienstleister bereitgestellt werden, ein dokumentierter und angemessener Ausstiegsplan vorliegt. |

# Ausserordentliche Prüfung

|  |
| --- |
| Die Revisionsstelle nimmt zum Prüfergebnis der von der FMA definierten zusätzlichen Prüfungen Stellung. Sofern hierzu keine Vorgaben der FMA publiziert werden, erfolgt die Berichterstattung im Sinne dieser Richtlinie. |

# Anhang zum Bericht über die Aufsichtsprüfung

|  |
| --- |
| Der Anhang zum Bericht über die Aufsichtsprüfung besteht aus:   * Anhang 1: dem testierten Geschäftsbericht der Wertpapierfirma, ggf. inklusive länderspezifischer Berichterstattung gemäss Art. 35 WPFG * Anhang 2: dem Organigramm der Gesellschaft und der Gruppenstruktur * Anhang 3: der Risikoanalyse/Prüfstrategie |

Die Ausführungen zu den einzelnen Prüffeldern sind nicht abschliessend. Vielmehr sind diese als Mindestinhalt des Berichts über die Aufsichtsprüfung zu verstehen.

Definiert die Revisionsstelle weitere Prüffelder, sind diese in der Risikoanalyse/Prüfstrategie (Anhang C1) zu ergänzen und die Ergebnisse der Prüfung im Bericht über die Aufsichtsprüfung zu beschreiben. Ferner beschreibt die Revisionsstelle die Gründe, welche zur Aufnahme von zusätzlichen Prüffeldern führten.

Die FMA weist darauf hin, dass für die jeweiligen Prüffelder die liechtensteinischen Rechtsvorschriften (WPFG, WPDG, HPBG), die Delegierte Verordnung (EU) 2017/565, die Verordnung (EU) 2019/2033 (IFR), die Verordnung (EU) Nr. 596/2014 (MAR) und die Verordnung (EU) Nr. 600/2014 (MiFIR) zitiert wurden. Diese referenzierten Artikel stellen keine abschliessende Auflistung der anwendbaren Rechtsvorschriften im jeweiligen Prüffeld dar. Darüberhinausgehende sind FMA-Richtlinien und FMA-Mitteilungen sowie alle relevanten europäischen Rechtsakte unter Berücksichtigung von Leitlinien und Empfehlungen, welche die FMA für comply erklärt hat, als auch Fragen & Antworten der ESMA und der EBA, anzuwenden.