EBA/GL/2021/14

22. November 2021

Leitlinien

zur internen Governance gemäß der Richtlinie (EU) 2019/2034

1. Einhaltung und Meldepflichten

Status dieser Leitlinien

1. Diese Leitlinien werden gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 [1] herausgegeben. Gemäß Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und Finanzinstitute, einschließlich Wertpapierfirmen, alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

2. In den Leitlinien wird dargelegt, was die EBA unter angemessenen Aufsichtspraktiken im Europäischen System der Finanzaufsicht versteht oder wie nach ihrer Auffassung das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Zuständige Behörden im Sinne von Artikel 4 Absatz 2 der Verordnung (EU) Nr. 1093/2010 sollten die für sie geltenden Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken integrieren (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren), einschließlich der Leitlinien, die in erster Linie an Wertpapierfirmen gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 16.05.2022 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständige Behörde den Anforderungen nicht nachkommt. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2021/14“ an compliance@eba.europa.eu zu senden. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, im Namen ihrer zuständigen Behörde die Einhaltung bzw. Nichteinhaltung der Leitlinien zu bestätigen. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

4. Die Mitteilungen werden gemäß Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 auf der Website der EBA veröffentlicht.

[1] Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12)

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand

5. In diesen Leitlinien werden gemäß Artikel 26 Absatz 4 der Richtlinie (EU) 2019/2034[2] die Regelungen, Verfahren und Mechanismen für die interne Governance festgelegt, die Wertpapierfirmen gemäß Titel IV Kapitel 2 Abschnitt 2 dieser Richtlinie einführen sollten, um ihre wirksame und umsichtige Führung zu gewährleisten.

6. Die Leitlinien gelten unbeschadet der Vorschriften in Artikel 9, 16, 23 und 24 der Richtlinie (EU) 2014/65, der Delegierten Verordnung (EU) 2017/565 der Kommission und der Delegierten Richtlinie (EU) 2017/593 der Kommission.

Adressaten

7. Diese Leitlinien richten sich an die zuständigen Behörden gemäß Artikel 4 Absatz 2 Ziffer viii der Verordnung (EU) Nr. 1093/2010 und im Sinne des Artikels 3 Absatz 1 Ziffer 5 der Richtlinie (EU) 2019/2034 sowie an Finanzinstitute gemäß Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010, die Wertpapierfirmen im Sinne des Artikels 4 Absatz 1 Ziffer 1 der Richtlinie 2014/65/EU sind, die nicht in den Anwendungsbereich des Artikels 2 Absatz 2 der Richtlinie (EU) 2019/2034 fallen und nicht alle Voraussetzungen für eine Einstufung als kleine und nicht verflochtene Wertpapierfirmen gemäß Artikel 12 Absatz 1 der Verordnung (EU) 2019/2033 erfüllen.

Anwendungsbereich

8. Die vorliegenden Leitlinien gelten für die Governance-Regelungen von Wertpapierfirmen, die nach der Richtlinie (EU) 2019/2034 erforderlich sind, einschließlich ihrer Organisationsstruktur und der entsprechenden Verantwortungsbereiche, sowie für die Verfahren zur Ermittlung, Steuerung, Überwachung und Meldung aller Risiken,[3] denen sie tatsächlich und potenziell ausgesetzt sind, sowie für den internen Kontrollrahmen.

9. Diese Leitlinien gelten auf Einzel- und auf konsolidierter Lage im Anwendungsbereich gemäß Artikel 25 der Richtlinie (EU) 2019/2034.

[2] Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Beaufsichtigung von Wertpapierfirmen und zur Änderung der Richtlinien 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU und 2014/65/EU.

[3] In diesen Leitlinien enthaltene Bezugnahmen auf Risiken umfassen alle Risiken, denen die Wertpapierfirmen tatsächlich oder potenziell ausgesetzt sind, einschließlich Risiken für Kunden, Risiken für den Markt, Risiken für die Wertpapierfirma sowie Liquiditätsrisiken, operationelle Risiken (einschließlich Rechts- und IT-Risiken) und Reputationsrisiken, ESG-Risiken sowie Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung.

10. Die Leitlinien sollen sämtliche vorhandenen Governance-Strukturen umfassen, ohne jedoch einer bestimmten Struktur den Vorzug zu geben. Die Leitlinien greifen nicht in die allgemeine Verteilung der Befugnisse nach dem nationalen Gesellschaftsrecht ein. Demgemäß sollten sie ungeachtet der in den Mitgliedstaaten zugrunde liegenden Governance-Struktur (monistisches und/oder dualistisches Gesellschaftsmodell und/oder eine andere Struktur) angewandt werden. Das Leitungsorgan nach der Definition in Artikel 3 Absatz 1 Ziffern 23 und 24 der Richtlinie (EU) 2019/2034 sollte so verstanden werden, dass es (geschäftsführende) Leitungs- und (nicht geschäftsführende) Aufsichtsfunktionen ausübt[4].

11. Die Begriffe „Leitungsorgan in seiner Leitungsfunktion“ und „Leitungsorgan in seiner Aufsichtsfunktion“ werden in diesen Leitlinien verwendet, ohne auf eine bestimmte Governance-Struktur Bezug zu nehmen, und Verweise auf die (geschäftsführende) Leitungs- oder (nicht geschäftsführende) Aufsichtsfunktion sollten so verstanden werden, dass sie sich auf die Organe oder Mitglieder des Leitungsorgans beziehen, die für die betreffende Funktion nach dem nationalen Recht zuständig sind. Bei der Umsetzung dieser Leitlinien sollten die zuständigen Behörden dem nationalen Gesellschaftsrecht Rechnung tragen und erforderlichenfalls festlegen, für welches Organ bzw. welche Mitglieder des Leitungsorgans diese Funktionen angewendet werden sollten.

12. In Mitgliedstaaten, in denen das Leitungsorgan die geschäftsführende Funktion ganz oder teilweise an eine Person oder ein internes Exekutivorgan überträgt (z. B. CEO, Führungsteam oder Exekutivausschuss), sollten die Personen, die auf Grundlage dieser Übertragung diese geschäftsführenden Funktionen ausüben und die Geschäfte des Instituts führen, als Leitungsfunktion des Leitungsorgans verstanden werden. Im Sinne dieser Leitlinien ist jede Bezugnahme auf das Leitungsorgan in seiner Leitungsfunktion so zu verstehen, dass auch die Mitglieder des Exekutivausschusses oder der CEO nach der Definition in diesen Leitlinien eingeschlossen sind, selbst wenn diese nach nationalem Recht nicht als formale Mitglieder des Leitungsgremiums oder der Leitungsorgane der Wertpapierfirma vorgeschlagen oder bestellt worden sind.

13. In Mitgliedstaaten, in denen manche Verantwortlichkeiten direkt von den Anteilseignern, Gesellschaftern oder Eigentümern der Wertpapierfirma anstelle des Leitungsorgans ausgeübt werden, sollten die Wertpapierfirmen sicherstellen, dass solche Verantwortlichkeiten und die entsprechenden Entscheidungen soweit möglich mit den vorliegenden für das Leitungsorgan geltenden Leitlinien in Einklang stehen.

14. Die in diesen Leitlinien verwendeten Definitionen von CEO, Finanzvorstand (CFO) und Inhabern von Schlüsselfunktionen haben lediglich rein funktionalen Charakter und sollen nicht dazu führen, die Bestellung oder Einrichtung solcher Funktionen anzuordnen, sofern diese nicht nach einschlägigem EU-Recht oder nationalem Recht vorgeschrieben sind.

[4] Siehe auch Erwägungsgrund 27 der Richtlinie (EU) 2019/2034.

Begriffsbestimmungen

15. Sofern nicht anders angegeben, haben die in der Richtlinie (EU) 2019/2034 und in der Verordnung (EU) 2019/2033 verwendeten und definierten Begriffe in den vorliegenden Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

Anteilseigner	Person, die Anteile an einer Wertpapierfirma hält, bzw. abhängig von der Rechtsform einer Wertpapierfirma andere Eigentümer oder Gesellschafter der Wertpapierfirma.
Aufsichtliche Konsolidierung	Die Anwendung der aufsichtsrechtlichen Vorschriften gemäß Artikel 25 der Richtlinie (EU) 2019/2034 sowie Artikel 7 der Verordnung (EU) 2019/2033[5].
Börsennotierte Wertpapierfirmen	Wertpapierfirmen, deren Finanzinstrumente zum Handel an einem regulierten Markt oder einem multilateralen Handelssystem (MTF) im Sinne von Artikel 4 Absätze 21 und 22 der Richtlinie 2014/65/EU in einem oder mehreren Mitgliedstaaten zugelassen sind[6].
EU-Mutterunternehmen	Eine EU-Mutterwertpapierfirma, eine EU-Mutterinvestmentholdinggesellschaft oder eine gemischte EU-Mutterfinanzholdinggesellschaft, die die Aufsichtsanforderungen auf der Grundlage der konsolidierten Lage gemäß Artikel 7 der Verordnung (EU) 2019/2033 erfüllen müssen.
Finanzvorstand (CFO)	Die Person, die die Gesamtverantwortung für die Leitung der folgenden Tätigkeiten trägt: Verwaltung der Finanzmittel, Finanzplanung und Rechnungslegung.
Inhaber von Schlüsselfunktionen	Personen, die erheblichen Einfluss auf die Ausrichtung der Wertpapierfirma haben, aber weder Mitglieder des Leitungsorgans noch CEO sind. Zu ihnen zählen die Leiter von internen Kontrollfunktionen sowie der CFO, sofern sie keine Mitglieder des Leitungsorgans sind, sowie weitere Inhaber von Schlüsselfunktionen, die auf Grundlage eines risikobasierten Ansatzes von den Wertpapierfirmen als solche ermittelt werdenn. Weitere Inhaber von Schlüsselfunktionen können die Leiter von wichtigen Geschäftsbereichen, Zweigniederlassungen im Europäischen Wirtschaftsraum (EWR)/in der Europäischen Freihandelsassoziation (EFTA), Tochterunternehmen in Drittstaaten und sonstigen internen Funktionen zählen.

[5] Siehe auch die technischen Regulierungsstandards zur Konsolidierung von Wertpapierfirmen gemäß der Richtlinie (EU) 2019/2034.

[6] Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

Leiter der internen Kontrollfunktionen	Die Personen, die auf der höchsten Hierarchieebene für die wirksame Wahrnehmung der täglichen Aufgaben der unabhängigen Risikomanagement-Funktion, der Compliance-Funktion sowie die interne Revision verantwortlich sind.
Leitungs- oder Aufsichtsmandate	Eine Position als Mitglied eines Leitungsorgans einer Wertpapierfirma oder einer anderen juristischen Person.
Mitarbeiter	Alle Beschäftigten einer Wertpapierfirma und ihrer Tochterunternehmen auf konsolidierter Lage sowie alle Mitglieder ihrer jeweiligen Leitungsorgane in ihrer Leitungsfunktion und ihrer Aufsichtsfunktion.
Risikoappetit	Das Gesamtrisikoniveau und die Arten von Risiken, die eine Wertpapierfirma bereit ist, innerhalb ihrer Risikotragfähigkeit und gemäß ihrem Geschäftsmodell zum Erreichen ihrer strategischen Ziele einzugehen.
Risikokultur	Die Normen, Einstellung und Verhaltensweisen einer Wertpapierfirma im Zusammenhang mit Risikobewusstsein, Risikobereitschaft und Risikomanagement sowie die Kontrollen, die für Entscheidungen über Risiken maßgeblich sind. Die Risikokultur beeinflusst die Entscheidungen der Geschäftsleitung und der Mitarbeiter im Tagesgeschäft und hat Auswirkungen auf die Risiken, die sie eingehen.
Risikotragfähigkeit	Das maximale Risiko, das eine Wertpapierfirma angesichts ihrer Eigenmittelausstattung, ihrer Risikomanagement- und Kontrollkapazitäten sowie ihrer regulatorischer Beschränkungen eingehen kann.
Vorsitzender des Leitungsorgans in seiner Leitungsfunktion (CEO)	Die Person, die für die Leitung und Steuerung der allgemeinen Geschäftstätigkeiten einer Wertpapierfirma zuständig ist.

3. Umsetzung

Umsetzungsfrist

16. Diese Leitlinien gelten ab dem 30. April 2022.

4. Leitlinien

Titel I – Verhältnismäßigkeit

17. Bei der Anwendung dieser Leitlinien sollten die zuständigen Behörden und Wertpapierfirmen den in Artikel 26 Absatz 3 der Richtlinie (EU) 2019/2034 verankerten und in Titel I dieser Leitlinien weiter ausgeführten Grundsatz der Verhältnismäßigkeit berücksichtigen, um sicherzustellen, dass die von den Wertpapierfirmen festgelegten Regelungen für die interne Governance, auch im Rahmen von Wertpapierfirmengruppen, mit dem individuellen Risikoprofil der Firma und der Gruppe in Einklang stehen, ihrer Größe und internen Organisation entsprechen, für ihr jeweiliges Geschäftsmodell zweckdienlich sind, für die Art, den Umfang und die Komplexität ihrer Geschäfte geeignet und für das wirksame Erreichen der Ziele der jeweiligen aufsichtlichen Anforderungen und Vorschriften ausreichend sind.

18. Für die Zwecke des vorstehenden Absatzes sollte der Vielzahl an unterschiedlichen Geschäftsmodellen Rechnung getragen werden, unter denen Wertpapierfirmen und Wertpapierfirmengruppen tätig sind, wie etwa als Anlageberater, Portfolioverwalter, Handelsplatz, Verwahrstelle, ausführender Makler, Broker im Großkundenmarkt oder Handelsunternehmen. Damit die Regelungen für die interne Governance als mit dem individuellen Risikoprofil der Firma und der Gruppe in Einklang stehend, ihrer Größe und internen Organisation entsprechend, für ihr jeweiliges Geschäftsmodell zweckdienlich, für die Art, den Umfang und die Komplexität ihrer Geschäfte geeignet und für das wirksame Erreichen der Ziele der jeweiligen aufsichtlichen Anforderungen und Vorschriften ausreichend befunden werden, sollte daher sichergestellt werden, dass Wertpapierfirmen mit einer komplexeren Organisation oder größere Wertpapierfirmen über komplexere Governance-Regelungen verfügen, während Wertpapierfirmen mit einer einfacheren Organisation oder kleinere Wertpapierfirmen einfachere Governance-Regelungen einführen können. Wertpapierfirmen sollten jedoch beachten, dass die Größe oder systemische Bedeutung einer Wertpapierfirma an sich möglicherweise bezüglich des Umfangs, in dem eine Wertpapierfirma Risiken ausgesetzt ist, nicht aussagekräftig ist.

19. Bei der Anwendung des Grundsatzes der Verhältnismäßigkeit, der in Artikel 26 Absatz 3 der Richtlinie (EU) 2019/2034 verankert und in Absatz 20 dieser Leitlinien weiter ausgeführt wird, sollten die zuständigen Behörden und Wertpapierfirmen dafür Sorge tragen, dass diese Anwendung nicht dazu führt, dass Wertpapierfirmen von aufsichtlichen Anforderungen befreit werden oder dass diese in einer Weise angewendet werden, bei der solide Governance-Regelungen, eine klare Organisationsstruktur, angemessene interne Kontrollmechanismen, ein solides und wirksames Risikomanagement sowie eine angemessene Vergütungspolitik nicht gewährleistet werden.

20. Für die Anwendung des Grundsatzes der Verhältnismäßigkeit und zur Sicherstellung einer angemessenen Umsetzung der aufsichtlichen Anforderungen und dieser Leitlinien sollten die Wertpapierfirmen und die zuständigen Behörden die folgenden Aspekte berücksichtigen:

    a. die Größe in Bezug auf die Bilanzsumme der Wertpapierfirma und ihrer Tochterunternehmen im Anwendungsbereich des aufsichtlichen Konsolidierungskreises;

    b. ob gemäß den Kriterien in Artikel 32 Absatz 4 Buchstabe a der Richtlinie (EU) 2019/2034 die bilanziellen und außerbilanziellen Vermögenswerte der Wertpapierfirma in den dem jeweiligen Geschäftsjahr unmittelbar vorangegangenen vier Jahren im Durchschnitt maximal 100 Mio. EUR wert waren;

    c. verwaltete Vermögenswerte;

    d. ob die Wertpapierfirma Kundengelder oder -vermögenswerte halten darf;

    e. die verwahrten und verwalteten Vermögenswerte;

    f. das Volumen der abgewickelten Kundenaufträge;

    g. das Volumen der täglichen Handelsströme;

    h. die geografische Präsenz der Wertpapierfirma und der Umfang ihrer Tätigkeiten in den einzelnen Rechtsordnungen, einschließlich in Drittländern und -hoheitsgebieten;

    i. die Rechtsform der Wertpapierfirma, einschließlich der Tatsache, ob die Wertpapierfirma zu einer Gruppe gehört, und gegebenenfalls die für die Gruppe vorgenommene Bewertung der Verhältnismäßigkeit;

    j. ob die Wertpapierfirma börsennotiert ist oder nicht;

    k. ob die Wertpapierfirma zur Verwendung von internen Modellen für die Messung der Kapitalanforderungen befugt ist (z. B. der auf internen Beurteilungen basierende Ansatz);

    l. die Art der genehmigten Tätigkeiten, die von der Wertpapierfirma erbrachten Dienstleistungen (z. B. Abschnitte A und B des Anhangs I zur Richtlinie 2014/65/EU) und weitere von der Wertpapierfirma erbrachte Dienstleistungen (z. B. Clearing-Dienste);

    m. das zugrunde liegende Geschäftsmodell und die Strategie, die Art und Komplexität der Geschäftstätigkeiten und die Organisationsstruktur der Wertpapierfirma;

n. die Risikostrategie, der Risikoappetit und das tatsächliche Risikoprofil der Wertpapierfirma, auch unter Berücksichtigung der Ergebnisse der SREP-Kapital- und SREP-Liquiditätsbewertungen;

o. die Beteiligungsverhältnisse und die Finanzierungsstruktur der Wertpapierfirma;

p. den Kundentyp

q. die Komplexität der Finanzinstrumente oder Verträge.

r. die ausgelagerten Funktionen und Vertriebskanäle sowie

s. die bestehenden informationstechnischen Systeme (IT-Systeme), einschließlich der Systeme für einen unterbrechungsfreien Geschäftsbetrieb und der ausgelagerten Funktionen in diesem Bereich.

21. Wertpapierfirmen, die von einer einzigen natürlichen Person verwaltete juristische Personen sind, sollten über alternative Regelungen verfügen, mit denen die solide und umsichtige Führung dieser Wertpapierfirmen und die angemessene Berücksichtigung von Regelungen für die interne Governance sichergestellt werden.

Titel II – Rolle und Zusammensetzung des Leitungsorgans und der Ausschüsse

1 Rolle und Pflichten des Leitungsorgans

22. Das Leitungsorgan muss die Letzt- und die Gesamtverantwortung für die Wertpapierfirma tragen und ist verantwortlich für die Definition und Festlegung von Governance-Regelungen innerhalb der Wertpapierfirma, auf die insbesondere in den Artikeln 26, 28 und 29 der Richtlinie (EU) 2019/2034 Bezug genommen wird, sowie die Überwachung ihrer Anwendung, um die wirksame und umsichtige Führung der Wertpapierfirma zu gewährleisten.

23. Die Pflichten des Leitungsorgans sollten klar definiert sein, wobei zwischen den Pflichten der (geschäftsführenden) Leitungsfunktion und der (nicht geschäftsführenden) Aufsichtsfunktion zu unterscheiden ist. Die Zuständigkeiten und Pflichten des Leitungsorgans sollten in einem schriftlichen Dokument beschrieben und vom Leitungsorgan ordnungsgemäß genehmigt werden. Alle Mitglieder des Leitungsorgans sollten sich der Struktur und Zuständigkeiten des Leitungsorgans sowie der Aufgabenteilung zwischen den Funktionen des Leitungsorgans und gegebenenfalls seiner Ausschüsse voll und ganz bewusst sein.

24. Das Leitungsorgan in seiner Aufsichtsfunktion und das Leitungsorgan in seiner Leitungsfunktion sollten wirksam zusammenwirken. Beide Funktionen sollten sich gegenseitig ausreichend Informationen zur Verfügung stellen, um ihre jeweiligen Funktionen ausüben zu können. Damit angemessene Kontrollen und Gegenkontrollen vorhanden sind, sollte die

Entscheidungsfindung im Leitungsorgan nicht von einem einzigen Mitglied oder einer kleinen Untergruppe seiner Mitglieder dominiert werden.

25. Unbeschadet der dem Leitungsorgan gemäß der Richtlinie 2014/65/EU übertragenen Aufgaben und Zuständigkeiten sollten die Zuständigkeiten des Leitungsorgans die Festlegung, Genehmigung und die Beaufsichtigung der Umsetzung der folgenden Aspekte umfassen:

    a. die allgemeine Geschäftsstrategie und die zentralen Strategien der Wertpapierfirma innerhalb der geltenden rechtlichen und aufsichtsrechtlichen Rahmenbedingungen unter Berücksichtigung der langfristigen finanziellen Interessen und der Solvenz der Wertpapierfirma;

    b. die allgemeine Risikostrategie, einschließlich des Risikoappetits der Wertpapierfirma und ihres Risikomanagementrahmens sowie angemessener Strategien und Verfahren, unter Berücksichtigung des makroökonomischen Umfelds und des Geschäftszyklus der Wertpapierfirma sowie Maßnahmen zur Sicherstellung, dass das Leitungsorgan Angelegenheiten des Risikomanagements ausreichend Zeit widmet; ein angemessener und wirksamer Rahmen für die interne Governance und die interne Kontrolle, der eine klare Organisationsstruktur und gut funktionierende interne Kontrollmechanismen umfasst. Diese Mechanismen sollten eine ständige und wirksame Compliance-Funktion sowie, sofern gemäß Titel I geeignet und angemessen, Funktionen des internen Risikomanagements und der internen Revision umfassen, die über ausreichende Befugnisse, ausreichendes Gewicht und ausreichende Ressourcen verfügen, um ihre Funktionen unabhängig wahrzunehmen und die Einhaltung der geltenden aufsichtlichen Anforderungen im Rahmen der Prävention von Geldwäsche und Terrorismusfinanzierung zu gewährleisten, sowie zudem auf das Liquiditätsmanagement der Wertpapierfirma ausgerichtet sind;

    c. eine Vergütungspolitik, die mit den in den Artikeln 26 sowie 30 bis 33 der Richtlinie (EU) 2019/2034 und den Leitlinien der EBA für eine solide Vergütungspolitik gemäß der Richtlinie (EU) 2019/2034 in Einklang steht[7];

    d. Regelungen, die auf die Sicherstellung abzielen, dass die Beurteilungen der individuellen und kollektiven Eignung des Leitungsorgans wirksam durchgeführt werden, die Zusammensetzung und Nachfolgeplanung des Leitungsorgans angemessen sind und das Leitungsorgan seine Funktionen wirksam wahrnimmt[8];

    e. einen Prozess für die Auswahl und Beurteilung der Eignung von Inhabern von Schlüsselfunktionen[9];

[7] Leitlinien der EBA für eine solide Vergütungspolitik gemäß der Richtlinie (EU) 2019/2034.

[8] Siehe auch die gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und Inhabern von Schlüsselfunktionen.

[9] Siehe auch die gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und Inhabern von Schlüsselfunktionen.

f. Regelungen, die darauf abzielen, die interne Funktionsweise der einzelnen Ausschüsse des Leitungsorgans, sofern diese eingerichtet sind, sicherzustellen, mit genauen Angaben zu folgenden Aspekten:

   i. Rolle, Zusammensetzung und Aufgaben der einzelnen Ausschüsse;

   ii. ein angemessener Informationsfluss, einschließlich der Dokumentation von Empfehlungen und Schlussfolgerungen, sowie Berichtswege zwischen den einzelnen Ausschüssen und dem Leitungsorgan, den zuständigen Behörden und sonstigen Parteien;

g. eine Risikokultur gemäß Abschnitt 8 dieser Leitlinien, die auf das Risikobewusstsein und das Risikoverhalten der Wertpapierfirma ausgerichtet ist;

h. eine Unternehmenskultur und Unternehmenswerte gemäß Abschnitt 9, durch die verantwortliches und ethisches Verhalten gefördert wird, einschließlich eines Verhaltenskodex oder eines ähnlichen Instruments;

i. Richtlinien für den Umgang mit Interessenkonflikten in der Wertpapierfirma gemäß Abschnitt 10 und für das Personal gemäß Abschnitt 11 sowie

j. Regelungen, die darauf abzielen, die Integrität der Systeme für die Rechnungslegung und das Berichtswesen sicherzustellen, einschließlich der finanziellen und operativen Kontrollen und der Einhaltung von Rechtsvorschriften und einschlägigen Standards.

26. Bei der Festlegung, Genehmigung und Kontrolle der Umsetzung der in Absatz 25 aufgeführten Aspekte sollte das Leitungsorgan darauf abzielen, ein Geschäftsmodell und Governance-Regelungen – einschließlich eines Risikomanagementrahmens – sicherzustellen, bei denen den Risiken Rechnung getragen wird, denen Wertpapierfirmen tatsächlich oder potenziell ausgesetzt sind oder die von ihnen für andere tatsächlich oder potenziell ausgehen[10]. Bei der Berücksichtigung aller Risiken sollten die Wertpapierfirmen allen einschlägigen Risikofaktoren Rechnung tragen, einschließlich umweltbezogener, sozialer und governancebezogener Risikofaktoren. Die Wertpapierfirmen sollten berücksichtigen, dass Letztere ihre aufsichtliche Risiken verstärken können[11]. Zu diesen ESG-Risikofaktoren zählen beispielsweise rechtliche Risiken im Bereich Vertrags- oder Arbeitsrecht, Risiken in Zusammenhang mit möglichen Verletzungen der Menschenrechte oder andere ESG-Risikofaktoren, die das Land, in dem ein Dienstleistungserbringer niedergelassen ist, oder seine Fähigkeit zur Erbringung der vereinbarten Dienstleistungsgüte betreffen können.

[10] Siehe Artikel 26 der Richtlinie (EU) 2019/2034.

[11] Im EBA-Diskussionspapier über das Management und die Beaufsichtigung von ESG-Risiken, das im Rahmen von Artikel 98 Absatz 8 der CRD veröffentlicht wurde, finden sich eine Beschreibung, was die EBA unter ESG-Risiken versteht, sowie der Übertragungskanäle und Empfehlungen für Regelungen, Verfahren, Mechanismen und Strategien, die von Instituten umzusetzen sind, um ESG-Risiken zu ermitteln, zu bewerten und zu steuern.

27. Das Leitungsorgan sollte die Offenlegung und die Kommunikation mit externen Interessenträgern und den zuständigen Behörden überwachen.

28. Alle Mitglieder des Leitungsorgans sollten über die Tätigkeiten im Allgemeinen, die Finanz- und Risikolage der Wertpapierfirma unter Berücksichtigung der wirtschaftlichen Rahmenbedingungen sowie über getroffene Entscheidungen mit wichtigen Auswirkungen auf die Geschäftstätigkeit der Wertpapierfirma informiert sein.

29. Ein Mitglied des Leitungsorgans kann für eine interne Kontrollfunktion entsprechend Titel V Abschnitt 18.1 zuständig sein, sofern das Mitglied keine sonstigen Aufgaben wahrnimmt, durch die die internen Kontrolltätigkeiten des Mitglieds und die Unabhängigkeit der internen Kontrollfunktion beeinträchtigt würden.

30. Das Leitungsorgan sollte etwaige Schwachstellen, die mit Blick auf die Umsetzung von Prozessen, Strategien und Maßnahmen in Zusammenhang mit den in den Absätzen 25 und 26 aufgeführten Zuständigkeiten ermittelt werden, überwachen, regelmäßig überprüfen und beheben. Das Rahmenwerk für die interne Governance und seine Umsetzung sollten regelmäßig überprüft und aktualisiert werden, wobei dem Grundsatz der Verhältnismäßigkeit entsprechend den weiteren Ausführungen in Titel I Rechnung zu tragen ist. Eine eingehendere Prüfung sollte durchgeführt werden, wenn die Wertpapierfirma von wesentlichen Änderungen betroffen ist.

31. Wenn Wertpapierfirmen juristische Personen sind, die von einer einzigen natürlichen Person in Übereinstimmung mit ihrer Satzung und den nationalen Rechtsvorschriften geführt werden, sollten die Bezugnahmen in diesen Leitlinien auf das Leitungsorgan so ausgelegt werden, dass sie auf die einzige Person anwendbar sind, die für die Durchführung alternativer Regelungen zur Sicherstellung einer soliden und umsichtigen Führung einer solchen Wertpapierfirma und die angemessene Berücksichtigung von Regelungen für die interne Governance verantwortlich ist.

2 Leitungsfunktion des Leitungsorgans

32. In seiner Leitungsfunktion sollte sich das Leitungsorgan aktiv an der Geschäftstätigkeit einer Wertpapierfirma beteiligen und Entscheidungen auf einer fundierten und sachkundigen Grundlage treffen.

33. In seiner Leitungsfunktion sollte das Leitungsorgan für die Umsetzung der vom Leitungsorgan festgelegten Strategien zuständig sein und die Umsetzung und Eignung dieser Strategien regelmäßig mit dem Leitungsorgan in seiner Aufsichtsfunktion erörtern. Die operative Umsetzung kann von der Geschäftsleitung der Wertpapierfirma vorgenommen werden.

34. In seiner Leitungsfunktion sollte das Leitungsorgan vorgelegte Vorschläge, Erklärungen und Informationen bei seiner Ermessensausübung und Entscheidungsfindung kritisch hinterfragen und überprüfen. In seiner Leitungsfunktion sollte das Leitungsorgan umfassend Bericht erstatten und regelmäßig, und bei Bedarf unverzüglich, das Leitungsorgan in seiner

Aufsichtsfunktion über die maßgeblichen Elemente für die Beurteilung einer Lage, die Risiken und Entwicklungen, die sich auf die Wertpapierfirma auswirken oder auswirken könnten, z. B. wesentliche Entscheidungen zur Geschäftstätigkeit oder eingegangene Risiken, die Bewertung der wirtschaftlichen und geschäftlichen Rahmenbedingungen der Wertpapierfirma, die Liquidität und solide Eigenmittelausstattung sowie die Bewertung ihrer wesentlichen Risikopositionen informieren.

35. Ungeachtet der nationalen Umsetzung der Richtlinie 2015/849/EU (Richtlinie zur Bekämpfung der Geldwäsche (AMLD)) sollte das Leitungsorgan eines seiner Mitglieder gemäß den Anforderungen nach Artikel 46 Absatz 4 der Richtlinie 2015/849/EU bestimmen, das für die für die Erfüllung dieser Richtlinie erforderliche Umsetzung der Gesetze, Rechts- und Verwaltungsvorschriften zuständig ist, einschließlich der entsprechenden Strategien und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung in der Wertpapierfirma und auf Ebene des Leitungsorgans.

3 Aufsichtsfunktion des Leitungsorgans

36. Die Rolle der Mitglieder des Leitungsorgans in seiner Aufsichtsfunktion sollte die Überwachung und konstruktive Kritik der Strategie der Wertpapierfirma einschließen.

37. Unbeschadet des nationalen Rechts sollten dem Leitungsorgan in seiner Aufsichtsfunktion unabhängige Mitglieder entsprechend den Bestimmungen in Abschnitt 9.3 der gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und von Inhabern von Schlüsselfunktionen gemäß der Richtlinie 2013/36/EU und der Richtlinie 2014/65/EU angehören.

38. Unbeschadet der nach dem geltenden nationalen Gesellschaftsrecht zugewiesenen Zuständigkeiten sollte das Leitungsorgan in seiner Aufsichtsfunktion folgende Aufgaben ausüben:

    a. Beaufsichtigung und Überwachung der Entscheidungsprozesse und Maßnahmen der Geschäftsleitung sowie eine wirksame Kontrolle des Leitungsorgans in seiner Leitungsfunktion, einschließlich der Überwachung und Prüfung seiner individuellen und kollektiven Leistung sowie der Umsetzung der Strategie und Ziele der Wertpapierfirma;

    b. konstruktive Kritik und Überprüfung von Vorschlägen und Informationen, die von den Mitgliedern des Leitungsorgans in seiner Leitungsfunktion bereitgestellt werden;

    c. angemessene Erfüllung der Pflichten und Funktionen des Risikoausschusses und des Vergütungsausschusses, wenn solche Ausschüsse nicht eingerichtet worden sind;

    d. Sicherstellung und regelmäßige Überprüfung der Wirksamkeit des Rahmenwerks für die interne Governance der Wertpapierfirma und Ergreifen geeigneter Schritte zur Behebung ermittelter Mängel;

e. Beaufsichtigung und Überwachung, dass die strategischen Ziele, die Organisationsstruktur und Risikostrategie der Wertpapierfirma, ihres Risikoappetits und des Risikomanagementrahmens sowie sonstige Richtlinien (z. B. die Vergütungspolitik) und die Offenlegungsvorschriften durchgehend umgesetzt werden;

f. Überwachung, dass die Risikokultur der Wertpapierfirma konsequent umgesetzt wird;

g. Beaufsichtigung der Umsetzung und Pflege eines Verhaltenskodex oder vergleichbarer Kodizes und wirksamer Richtlinien zur Ermittlung, Steuerung und Minderung tatsächlicher und potenzieller Interessenkonflikte;

h. Kontrolle der Integrität von Finanzinformationen und Rechnungslegung sowie des internen Kontrollrahmens, einschließlich eines wirksamen und soliden Risikomanagementrahmens;

i. Sicherstellung, dass die Leiter der internen Kontrollfunktionen in der Lage sind, unabhängig zu agieren, und ungeachtet der Verantwortung, anderen internen Organen, Geschäftsbereichen und -einheiten Bericht zu erstatten, soweit erforderlich direkt gegenüber dem Leitungsorgan in seiner Aufsichtsfunktion Bedenken äußern und dieses warnen kann, wenn nachteilige Risikoentwicklungen die Wertpapierfirma beeinträchtigen oder beeinträchtigen können;

j. Überwachung der Umsetzung des Prüfungsplans der internen Revision nach vorheriger Einbeziehung des Risikoausschusses, sofern dieser eingerichtet ist.

4 Rolle des Vorsitzes des Leitungsorgans

39. Der Vorsitz des Leitungsorgans sollte das Leitungsorgan leiten, zu einem wirksamen Informationsfluss innerhalb des Leitungsorgans sowie zwischen dem Leitungsorgan und seinen Ausschüssen, sofern diese eingerichtet sind, beitragen und für seine wirksame Funktionsweise im Allgemeinen zuständig sein.

40. Der Vorsitz sollte eine offene und kritische Diskussion fördern und anregen und gewährleisten, dass auch abweichende Ansichten geäußert und im Rahmen des Entscheidungsprozesses diskutiert werden können.

41. Falls es dem Vorsitz gestattet ist, geschäftsführende Aufgaben wahrzunehmen, sollte die Wertpapierfirma Maßnahmen ergreifen, um nachteilige Auswirkungen auf die Kontrollen und Gegenkontrollen der Wertpapierfirma zu mindern (z. B. indem ein leitendes Mitglied des Leitungsorgans oder ein führendes unabhängiges Mitglied des Leitungsorgans benannt wird oder dem Leitungsorgan in seiner Aufsichtsfunktion eine größere Zahl von nicht geschäftsführenden Mitgliedern angehört). Der Vorsitz des Leitungsorgans einer Wertpapierfirma in seiner Aufsichtsfunktion darf in dieser Wertpapierfirma nicht gleichzeitig die Funktion des CEO ausüben, es sei denn, dies wird von der Wertpapierfirma begründet und von den zuständigen Behörden genehmigt.

42. Der Vorsitz sollte die Tagesordnung für Sitzungen festlegen und sicherstellen, dass strategische Fragen vorrangig erörtert werden. Der Vorsitz sollte sicherstellen, dass Entscheidungen des Leitungsorgans auf einer fundierten und sachkundigen Grundlage getroffen werden und Unterlagen und Informationen rechtzeitig vor der Sitzung vorgelegt werden.

43. Der Vorsitz des Leitungsorgans sollte zu einer klaren Aufgabenteilung zwischen den Mitgliedern des Leitungsorgans und einem ausreichenden Informationsfluss zwischen diesen beitragen, um es den Mitgliedern des Leitungsorgans in seiner Aufsichtsfunktion zu ermöglichen, einen konstruktiven Beitrag zu Diskussionen zu leisten und ihre Stimmen auf einer fundierten und sachkundigen Grundlage abzugeben.

5 Ausschüsse des Leitungsorgans in seiner Aufsichtsfunktion

5.1 Einrichtung von Ausschüssen

44. Gemäß Artikel 28 der Richtlinie (EU) 2019/2034, und sofern im nationalen Recht nicht etwas anderes vorgesehen ist,[12] müssen Wertpapierfirmen, deren bilanziellen und außerbilanziellen Vermögenswerte in den dem jeweiligen Geschäftsjahr unmittelbar vorangegangenen vier Jahren im Durchschnitt maximal 100 Mio. EUR wert waren, einen Risiko- und einen Vergütungsausschuss einrichten, die das Leitungsorgan in seiner Aufsichtsfunktion beraten und die von diesem Organ zu treffenden Entscheidungen vorbereiten.

45. Wenn kein Risikoausschuss eingerichtet wird, sind die Bezugnahmen in diesen Leitlinien betreffend dieses Ausschusses so auszulegen, als würden sie sich auf das Leitungsorgan in seiner Aufsichtsfunktion beziehen.

46. Die Wertpapierfirmen können unter Berücksichtigung der in Titel I dieser Leitlinien aufgeführten Kriterien weitere Ausschüsse einsetzen (z. B. Ausschüsse zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, Ethik-, Verhaltens- und Compliance-Ausschüsse).

47. Die Wertpapierfirmen sollten eine klare Zuweisung und Aufteilung von Pflichten und Aufgaben zwischen den Fachausschüssen des Leitungsorgans sicherstellen. Jeder Ausschuss sollte vom Leitungsorgan in seiner Aufsichtsfunktion ein dokumentiertes Mandat, einschließlich des Umfangs seiner Zuständigkeiten, erhalten und geeignete Arbeitsverfahren einrichten.

48. Die Ausschüsse sollten die Aufsichtsfunktion in bestimmen Bereichen unterstützen und die Entwicklung und Umsetzung eines soliden Rahmenwerks für die interne Governance begünstigen. Die Übertragung von Aufgaben auf solche Ausschüsse sollte das Leitungsorgan in seiner Aufsichtsfunktion keinesfalls von der kollektiven Erfüllung seiner Aufgaben und Pflichten entbinden.

[12] Nach Artikel 28 der Richtlinie (EU) 2019/2034 müssen Wertpapierfirmen, die die in Artikel 32 Absatz 4 Buchstabe a festgelegten Kriterien nicht erfüllen, einen Risikoausschuss einsetzen, der sich aus Mitgliedern des Leitungsorgans zusammensetzt, die in der betreffenden Wertpapierfirma keine Führungsaufgaben wahrnehmen.

5.2 Zusammensetzung der Ausschüsse[13]

49. Der Vorsitz aller Ausschüsse sollte jeweils von einem nicht geschäftsführenden Mitglied des Leitungsorgans wahrgenommen werden, das in der Lage ist, objektive Entscheidungen zu treffen.

50. Unabhängige Mitglieder[14] des Leitungsorgans in seiner Aufsichtsfunktion sollten aktiv in diese Ausschüsse eingebunden sein.

51. Sofern Ausschüsse gemäß der Richtlinie (EU) 2019/2034 oder nach nationalem Recht eingesetzt werden müssen, sollten sich diese im Allgemeinen grundsätzlich aus mindestens drei Mitgliedern zusammensetzen und es sollte ihnen mindestens ein unabhängiges Mitglied angehören, wobei die in Titel I dieser Leitlinien und in den gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und von Inhabern von Schlüsselfunktionen festgelegten Kriterien zu berücksichtigen sind. Wenn sich das Leitungsorgan in seiner Aufsichtsfunktion nicht aus einer ausreichenden Zahl an Mitgliedern zusammensetzt, um eine solide Zusammensetzung von Ausschüssen nach den Ausführungen in diesem Abschnitt sicherzustellen, können die Aufgaben des Ausschusses an ein Mitglied des Leitungsorgans in seiner Aufsichtsfunktion übertragen werden, das durch Mitarbeiter angemessen unterstützt wird. Die Ausschüsse können sich aus derselben Gruppe von Mitgliedern unter Berücksichtigung der in Titel I dargelegten Kriterien und der Zahl an unabhängigen Mitgliedern des Leitungsorgans in seiner Aufsichtsfunktion mit den speziellen Erfahrungen, Kenntnissen und Fähigkeiten, die individuell oder kollektiv für die Ausschüsse erforderlich sind, zusammensetzen. Die Gründe für die Zusammensetzung der Ausschüsse sollten dokumentiert werden.

52. Der Risikoausschuss sollte sich aus nicht geschäftsführenden Mitgliedern des Leitungsorgans in seiner Aufsichtsfunktion der betreffenden Wertpapierfirma zusammensetzen. Die Zusammensetzung des Vergütungsausschusses sollte den Bestimmungen in Abschnitt 2.3 der Leitlinien der EBA für eine solide Vergütungspolitik[15] entsprechen.

53. Den Vorsitz des Risikoausschusses sollte, sofern möglich, von einem unabhängigen Mitglied geführt werden. Die Mitglieder des Risikoausschusses sollten individuell und kollektiv über ausreichende Kenntnisse, Fähigkeiten und Erfahrung betreffend das Auswahlverfahren und die Anforderungen an die Angemessenheit bzw. das Risikomanagement und die Kontrollverfahren verfügen. In allen Wertpapierfirmen sollte der Vorsitzende des Risikoausschusses, sofern möglich, weder der Vorsitzende des Leitungsorgans noch der Vorsitzende eines anderen Ausschusses sein.

5.3 Verfahren der Ausschüsse

[13] Dieser Abschnitt sollte in Verbindung mit den gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und von Inhabern von Schlüsselfunktionen gemäß der Richtlinie 2013/36/EU und der Richtlinie 2014/65/EU gelesen werden.

[14] Entsprechend der Definition in Abschnitt 9.3 der gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und von Inhabern von Schlüsselfunktionen gemäß der Richtlinie 2013/36/EU und der Richtlinie 2014/65/EU.

[15] Leitlinien der EBA für eine solide Vergütungspolitik gemäß Artikel 34 Absatz 3 der Richtlinie (EU) 2019/2034.

54. Die Ausschüsse sollten dem Leitungsorgan in seiner Aufsichtsfunktion regelmäßig Bericht erstatten.

55. Die Ausschüsse sollten soweit angemessen zusammenwirken und -arbeiten. Unbeschadet des Absatzes 51 könnte ein solches Zusammenwirken in der Form einer übergreifenden Mitwirkung erfolgen, sodass der Vorsitzende oder ein Mitglied eines Ausschusses auch Mitglied eines anderen Ausschusses sein kann.

56. Die Mitglieder von Ausschüssen sollten sich an offenen und kritischen Diskussionen beteiligen, in denen in konstruktiver Weise widersprechende Meinungen erörtert werden.

57. Die Ausschüsse sollten die Tagesordnungen der Ausschusssitzungen sowie deren wichtigste Ergebnisse und Schlussfolgerungen dokumentieren.

58. Der Risikoausschuss sollte mindestens

    a. Zugang zu allen maßgeblichen Informationen und Daten haben, die für die Wahrnehmung seiner jeweiligen Funktion erforderlich sind, darunter Informationen und Daten von relevanten Unternehmens- und Kontrollfunktionen (z. B. Recht, Finanzen, Personal, IT, interne Revision, Risiko und Compliance, einschließlich Informationen für die Compliance im Bereich Geldwäsche und Terrorismusfinanzierung sowie aggregierter Informationen über Berichte zu verdächtigen Transaktionen, sowie Risikofaktoren im Bereich Geldwäsche und Terrorismusfinanzierung);

    b. regelmäßig Berichte, Ad-hoc-Informationen, Mitteilungen und Stellungnahmen von den Leitern der internen Kontrollfunktionen betreffend das aktuelle Risikoprofil der Wertpapierfirma, ihre Risikokultur und Risikolimite sowie über jegliche wesentliche Verstöße[16], die möglicherweise aufgetreten sind, mit detaillierten Informationen und Empfehlungen für eingeleitete, einzuleitende oder vorgeschlagene Abhilfemaßnahmen, erhalten; regelmäßig den Inhalt, die Form und Häufigkeit der Informationen über Risiken, über die ihnen Bericht erstattet wird, überprüfen und entsprechend darüber entscheiden;

    c. soweit notwendig, die ordnungsgemäße Einbeziehung der internen Kontrollfunktionen und sonstiger relevanter Funktionen (Personal, Recht und Finanzen) innerhalb der jeweiligen Fachgebiete sicherstellen und/oder bei Bedarf externe fachliche Beratung in Anspruch nehmen.

5.4 Rolle des Risikoausschusses

[16] Mit Blick auf gravierende Verstöße im Bereich Geldwäsche/Terrorismusfinanzierung finden sich weiterführende Informationen in den Leitlinien, die im Einklang mit Artikel 117 Absatz 6 der Richtlinie 2013/36/EU zu erlassen sind und in denen die Art und Weise der Zusammenarbeit und des Informationsaustauschs zwischen den in Absatz 5 dieses Artikels genannten Behörden festgelegt wird, insbesondere in Bezug auf grenzübergreifend tätige Gruppen und in Zusammenhang mit der Ermittlung gravierender Verstöße gegen die Vorschriften zur Bekämpfung der Geldwäsche.

59. Sofern eingerichtet, sollte der Risikoausschuss mindestens

    a. das Leitungsorgan in seiner Aufsichtsfunktion bezüglich der aktuellen und künftigen Risikostrategie und des Risikoappetits der Wertpapierfirma insgesamt beraten und unterstützen sowie dem Leitungsorgan bei der Beaufsichtigung der Umsetzung dieser Strategie helfen, um sicherzustellen, dass diese mit den Geschäftszielen, der Unternehmenskultur und den Werten der Wertpapierfirma in Einklang stehen;

    b. das Leitungsorgan in seiner Aufsichtsfunktion bei der Überwachung der Umsetzung der Risikostrategie der Wertpapierfirma und der Festlegung der entsprechenden festgelegten Limite unterstützen;

    c. die Umsetzung der Strategien für das Kapital- und Liquiditätsmanagement sowie für alle anderen relevanten Risiken einer Wertpapierfirma überwachen, wie etwa Risiken für Kunden, Risiken für den Markt, Risiken für Unternehmen, operationelle Risiken (einschließlich Rechts- und IT-Risiken) und Reputationsrisiken, um ihre Angemessenheit im Hinblick auf die genehmigte Risikostrategie und den festgelegten Risikoappetit zu beurteilen;

    d. dem Leitungsorgan in seiner Aufsichtsfunktion Empfehlungen zu notwendigen Anpassungen an die Risikostrategie unterbreiten, die sich unter anderem aus Änderungen des Geschäftsmodells der Wertpapierfirma, Marktentwicklungen oder Empfehlungen der Risikomanagementfunktion ergeben;

    e. Beratung zur Beauftragung externer Berater anbieten, die von der Aufsichtsfunktion eventuell beratend oder unterstützend hinzugezogen werden;

    f. eine Reihe von möglichen Szenarien überprüfen, einschließlich Stressszenarien, um zu bewerten, wie das Risikoprofil der Wertpapierfirma bei externen und internen Ereignissen reagieren würde;

    g. die Übereinstimmung zwischen allen wesentlichen Finanzinstrumenten und -dienstleistungen, die den Kunden angeboten werden, und dem Geschäftsmodell und der Risikostrategie der Wertpapierfirma überwachen. Der Risikoausschuss, sofern eingerichtet, sollte die mit den angebotenen Finanzinstrumenten und -dienstleistungen verbundenen Risiken bewerten und die Übereinstimmung zwischen den zugewiesenen Preisen und den aus diesen Produkten und Dienstleistungen erzielten Gewinnen berücksichtigen;

    h. die Empfehlungen von internen oder externen Prüfern bewerten und die angemessene Umsetzung der ergriffenen Maßnahmen weiterverfolgen.

60. Der Risikoausschuss sollte mit anderen Ausschüssen zusammenarbeiten, deren Tätigkeiten Auswirkungen auf die Risikostrategie haben können (z. B. Vergütungsausschuss, sofern eingerichtet), und sich regelmäßig mit den internen Kontrollfunktionen der Wertpapierfirma, insbesondere der Risikomanagementfunktion austauschen.

Titel III – Rahmenwerk für die Governance

6 Organisatorischer Rahmen und Organisationsstruktur

6.1 Organisatorischer Rahmen

61. Das Leitungsorgan einer Wertpapierfirma sollte sicherstellen, dass die Wertpapierfirma über eine geeignete und transparente organisatorische und operative Struktur für die betreffende Wertpapierfirma verfügt, und sollte eine schriftliche Beschreibung über diese vorlegen können. Die Struktur sollte eine wirksame und umsichtige Führung einer Wertpapierfirma auf Ebene des einzelnen Unternehmens und auf konsolidierter Ebene fördern und belegen.

62. Das Leitungsorgan sollte sicherstellen, dass die internen Kontrollfunktionen über die angemessenen finanziellen und personellen Ressourcen sowie über Befugnisse zur wirksamen Wahrnehmung ihrer Funktion verfügen. Mindestens die Compliance-Funktion sollte unabhängig tätig sein, was einschließt, dass eine geeignete Aufgabentrennung vorhanden ist. Die Berichtswege sowie die Zuordnung von Verantwortlichkeiten, insbesondere unter Inhabern von Schlüsselfunktionen, innerhalb einer Wertpapierfirma sollten klar, genau abgegrenzt, stimmig, durchsetzbar und ordnungsgemäß dokumentiert sein. Die Dokumentation sollte, soweit angemessen, aktualisiert werden.

63. Durch die Struktur der Wertpapierfirma sollten die Fähigkeit des Leitungsorgans, die Risiken, denen die Wertpapierfirma oder die Gruppe ausgesetzt ist, effektiv zu überwachen und zu steuern, sowie die Fähigkeit der zuständigen Behörde, die Wertpapierfirma wirksam zu beaufsichtigen, nicht beeinträchtigt werden.

64. Das Leitungsorgan sollte bewerten, ob und wie sich wesentliche Änderungen an der Struktur der Gruppe (z. B. Gründung neuer Tochterunternehmen, Fusionen und Übernahmen, Verkauf oder Auflösung von Teilen der Gruppe oder externe Entwicklungen) auf die Belastbarkeit des organisatorischen Rahmens der Wertpapierfirma auswirken. Sofern Schwachstellen ermittelt werden, sollte das Leitungsorgan etwaige erforderliche Anpassungen unverzüglich vornehmen.

6.2 Kenntnis der eigenen Struktur („know your structure“)

65. Das Leitungsorgan sollte die rechtliche, organisatorische und operative Struktur der Wertpapierfirma genau kennen und verstehen (Kenntnis der eigenen Struktur) sowie dafür Sorge tragen, dass diese der genehmigten Geschäftsstrategie sowie der Risikostrategie und dem Risikoappetit der Wertpapierfirma entspricht und von seinem Risikomanagementrahmen abgedeckt ist.

66. Das Leitungsorgan sollte ferner für die Genehmigung solider Strategien und Richtlinien bei der Schaffung neuer Strukturen zuständig sein. In Fällen, in denen eine Wertpapierfirma viele rechtliche Einheiten innerhalb einer Gruppe gründet, sollte deren Zahl und insbesondere die

zwischen ihnen bestehenden Verbindungen und Transaktionen für die Ausgestaltung ihrer internen Governance und die wirksame Steuerung und Überwachung der Risiken der Gruppe insgesamt keine Herausforderungen darstellen. Das Leitungsorgan sollte dafür Sorge tragen, dass die Struktur einer Wertpapierfirma und gegebenenfalls die Strukturen innerhalb einer Gruppe unter Berücksichtigung der in Abschnitt 7 aufgeführten Kriterien klar, effizient und transparent sind, und zwar sowohl für die eigenen Mitarbeiter, die Anteilseigner und andere Interessenträger der Wertpapierfirma als auch für die zuständige Behörde.

67. Das Leitungsorgan sollte die Struktur, Entwicklung und Grenzen der Wertpapierfirma steuern und dafür Sorge tragen, dass die Struktur angemessen und wirksam ist und keine übermäßige oder unangemessene Komplexität mit sich bringt.

68. Das Leitungsorgan eines EU-Mutterunternehmens sollte nicht nur die rechtliche, organisatorische und operative Struktur der Gruppe, sondern auch den Gegenstand und die Tätigkeiten der einzelnen Einheiten sowie die Verbindungen und Beziehungen zwischen ihnen verstehen. Hierzu gehört auch das Verständnis für gruppenspezifische operationelle Risiken und gruppeninterne Risikopositionen sowie mögliche Beeinträchtigungen der Finanzierung der Gruppe, ihres Eigenkapitals, ihrer Liquidität und ihrer Risikoprofile unter normalen und unter Stressszenarien. Das Leitungsorgan sollte dafür Sorge tragen, dass die Mutterwertpapierfirma in der Lage ist, zeitnah Informationen zu Art, Merkmalen, Satzung, Organisationsstruktur, Eigentümerstruktur und Geschäftstätigkeit jeder einzelnen rechtlichen Einheit vorzulegen, und dass die Wertpapierfirmen innerhalb der Gruppe alle Anforderungen an die aufsichtliche Berichterstattung auf Einzel- und konsolidierter Basis erfüllen.

69. Das Leitungsorgan eines EU-Mutterunternehmens sollte sicherstellen, dass die verschiedenen Unternehmen der Gruppe (einschließlich des EU-Mutterunternehmens selbst) ausreichende Informationen erhalten, um über ein klares Verständnis der allgemeinen Ziele, Strategien und des Risikoprofils der Gruppe sowie der Einbindung des betreffenden Unternehmens der Gruppe in die Struktur und den Geschäftsbetrieb der Gruppe zu verfügen. Solche Informationen – und entsprechende Überarbeitungen – sollten dokumentiert und den betroffenen maßgeblichen Funktionen zur Verfügung gestellt werden, einschließlich des Leitungsorgans, der Geschäftsbereiche und internen Kontrollfunktionen. Die Mitglieder des Leitungsorgans eines EU-Mutterunternehmens sollten sich über die Risiken, die von der Struktur der Gruppe ausgehen, auf dem Laufenden halten, wobei die in Abschnitt 7 der Leitlinien aufgeführten Kriterien zu berücksichtigen sind. Dies umfasst den Erhalt von

    a. Informationen zu den wichtigsten Risikotreibern;

    b. regelmäßigen Berichten, in denen die Struktur der Wertpapierfirma insgesamt bewertet und beurteilt wird, ob die einzelnen Unternehmen ihre Geschäftstätigkeit gemäß der genehmigten gruppenweiten Strategie ausüben;

c. regelmäßigen Berichten über Themen, bei denen nach dem aufsichtsrechtlichen Rahmen eine Einhaltung auf Ebene des einzelnen Unternehmens und auf konsolidierter Ebene erforderlich ist.

6.3 Komplexe Strukturen und nichtstandardisierte oder intransparente Tätigkeiten

70. Die Wertpapierfirmen sollten es vermeiden, komplexe und möglicherweise intransparente Strukturen einzurichten. Die Wertpapierfirmen sollten bei ihrer Entscheidungsfindung die Ergebnisse einer Risikobewertung, die sie durchführen, um zu ermitteln, ob solche Strukturen für einen mit Geldwäsche oder anderen Finanzstraftaten verbundenen Zweck genutzt werden könnten, sowie die jeweiligen Kontrollen und den geltenden Rechtsrahmen berücksichtigen[17]. Zu diesem Zweck sollten die Wertpapierfirmen mindestens folgende Aspekte berücksichtigen:

a. den Umfang, in dem die Rechtsordnung, in der die Struktur eingerichtet wird, tatsächlich den EU- und internationalen Standards zu Steuertransparenz, Geldwäsche und Bekämpfung der Terrorismusfinanzierung entspricht[18];

b. den Umfang, in dem die Struktur einem offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck dient;

c. den Umfang, in dem die Struktur genutzt werden könnte, um die Identität des wirtschaftlichen Eigentümers zu verschleiern;

d. den Umfang, in dem das Ersuchen des Kunden, das zur möglichen Einrichtung einer Struktur führt, Anlass zur Sorge gibt;

e. den Umstand, ob die Struktur eine angemessene Überwachung durch das Leitungsorgan der Wertpapierfirma oder die Fähigkeit der Wertpapierfirma zur Steuerung des verbundenen Risikos behindert;

f. den Umstand, ob die Struktur ein Hindernis für eine wirksame Beaufsichtigung durch die zuständigen Behörden darstellt.

71. In jedem Fall sollten die Wertpapierfirmen keine undurchsichtigen oder unnötig komplexen Strukturen, die keine klare wirtschaftliche Begründung oder keinen rechtlichen Zweck haben,

[17] Für weiterführende Informationen zur Beurteilung des Länderrisikos und der mit einzelnen Produkten und Kunden verbundenen Risiken sollten die Wertpapierfirmen auch die gemeinsamen Leitlinien zu GW/TF-Risikofaktoren (EBA GL JC/2017/37) heranziehen, die derzeit überarbeitet werden.

[18] Siehe auch Delegierte Verordnung (EU) 2019/758 der Kommission vom 31. Januar 2019 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die von Kredit- und Finanzinstituten zur Minderung des Risikos von Geldwäsche und Terrorismusfinanzierung in bestimmten Drittländern mindestens zu treffenden Maßnahmen und die Art zusätzlich zu treffender Maßnahmen: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries

oder Strukturen einrichten, die Anlass zu Bedenken geben könnten, dass sie möglicherweise für Zwecke in Verbindung mit Finanzkriminalität geschaffen werden.

72. Bei der Einrichtung dieser Strukturen sollte das Leitungsorgan diese und ihren Zweck und die mit ihnen verbundenen besonderen Risiken verstehen sowie sicherstellen, dass die internen Kontrollfunktionen ordnungsgemäß eingebunden sind. Solche Strukturen sollten nur dann genehmigt und fortgeführt werden, wenn ihr Zweck definiert und verstanden wird, wenn sich das Leitungsorgan vergewissert hat, dass alle wesentlichen Risiken, einschließlich Reputationsrisiken, ermittelt wurden und alle Risiken wirksam gesteuert und angemessen berichtet werden können sowie eine wirksame Überwachung gewährleistet ist. Je komplexer und undurchsichtiger die organisatorische und operative Struktur ist, desto größer sind die Risiken und desto intensiver sollte die Überwachung der Struktur sein.

73. Die Wertpapierfirmen sollten ihre Entscheidungen dokumentieren und in der Lage sein, ihre Entscheidungen gegenüber den zuständigen Behörden zu begründen.

74. Das Leitungsorgan sollte sicherstellen, dass angemessene Maßnahmen ergriffen werden, um die Risiken von Tätigkeiten im Rahmen dieser Strukturen zu verhindern oder zu mindern. Dabei ist Folgendes sicherzustellen:

    a. Die Wertpapierfirma verfügt über angemessene Richtlinien und Verfahren sowie dokumentierte Prozesse (z. B. geeignete Limite und Informationsflüsse) zur Prüfung, Compliance, Genehmigung und zum Risikomanagement solcher Tätigkeiten und trägt dabei den Folgen für die organisatorische und operative Struktur der Gruppe, ihrem Risikoprofil und ihren Reputationsrisiken Rechnung;

    b. die Informationen über diese Tätigkeiten und die damit verbundenen Risiken sind für das EU-Mutterunternehmen und die internen und externen Prüfer zugänglich und werden dem Leitungsorgan in seiner Aufsichtsfunktion und der zuständigen Behörde, die die Zulassung erteilt hat, gemeldet;

    c. die Wertpapierfirma prüft in regelmäßigen Abständen, ob nach wie vor die Notwendigkeit besteht, diese Strukturen beizubehalten.

75. Diese Strukturen und Tätigkeiten, einschließlich der Einhaltung der Rechtsvorschriften und beruflichen Standards, sollten regelmäßig überprüft werden. Sofern die Funktion der internen Revision eingerichtet ist, sollte diese die Prüfung nach einem risikobasierten Ansatz vornehmen.

76. Die Wertpapierfirmen sollten bei der Ausführung von nicht standardisierten oder intransparenten Tätigkeiten für Kunden (z. B. Unterstützung der Kunden bei der Gründung von Zweckgesellschaften in Offshore-Jurisdiktionen; Entwicklung komplexer Strukturen und Durchführung von Finanztransaktionen für sie oder Bereitstellung von Treuhanddiensten), die die interne Governance vor ähnliche Herausforderungen stellen und mit erheblichen operationellen Risiken und Reputationsrisiken verbunden sein können, wirksame

Maßnahmen des Risikomanagements ergreifen. Insbesondere sollten die Wertpapierfirmen den Grund analysieren, aus dem ein Kunde eine bestimmte Struktur einrichten möchte.

7 Organisatorischer Rahmen im Kontext einer Gruppe

77. Gemäß Artikel 25 der Richtlinie (EU) 2019/2034 und Artikel 7 der Verordnung (EU) 2019/2033, und sofern Artikel 8 der Verordnung (EU) 2019/2033 von den zuständigen Behörden angewandt wird, sollten EU-Mutterunternehmen und ihre Tochterunternehmen, die der Richtlinie (EU) 2019/2034 unterliegen, dafür Sorge tragen, dass Regelungen, Verfahren und Mechanismen für die interne Governance kohärent und auf einer konsolidierten Lage gut integriert sind. Zu diesem Zweck sollten Unternehmen und Tochterunternehmen im aufsichtlichen Konsolidierungskreis solche Regelungen, Verfahren und Mechanismen in ihren nicht der Richtlinie (EU) 2019/2034 unterliegenden Tochterunternehmen, einschließlich derer mit Sitz in Drittländern, unter anderem an Offshore-Finanzplätzen, einführen, um solide Governance-Regelungen auf einer konsolidierten Lage sicherzustellen. Die zuständigen Funktionen innerhalb des EU-Mutterunternehmens und seiner Tochterunternehmen sollten interagieren und gegebenenfalls Daten und Informationen austauschen. Die Regelungen, Verfahren und Mechanismen für die interne Governance sollten sicherstellen, dass das EU-Mutterunternehmen über ausreichend Daten und Informationen verfügt und in der Lage ist, das gruppenweite Risikoprofil entsprechend den Ausführungen in Abschnitt 6.2 zu bewerten.

78. Das Leitungsorgan eines Tochterunternehmens, das der Richtlinie (EU) 2019/2034 unterliegt, sollte die auf konsolidierter Ebene festgelegten gruppenweiten Governance-Richtlinien annehmen und auf Einzelebene in einer Weise einführen, durch die alle speziellen Anforderungen nach dem EU- und nationalen Recht erfüllt werden.

79. Auf konsolidierter Ebene sollte das EU-Mutterunternehmen die Einhaltung der Governance-Richtlinien und des in Titel V genannten internen Kontrollrahmens auf Gruppenebene durch alle Wertpapierfirmen und sonstigen Einrichtungen im aufsichtlichen Konsolidierungskreis, einschließlich seiner Tochterunternehmen, die selbst nicht der Richtlinie (EU) 2019/2034 unterliegen, sicherstellen. Bei der Umsetzung der Governance-Richtlinien sollte das EU-Mutterunternehmen dafür Sorge tragen, dass solide Governance-Regelungen für jedes Tochterunternehmen bestehen und besondere Regelungen, Verfahren und Mechanismen in Betracht ziehen, wenn Geschäftstätigkeiten nicht in separaten rechtlichen Einheiten, sondern in einer Matrix von Geschäftsbereichen unter Einbindung mehrerer rechtlicher Einheiten organisiert sind.

80. Ein EU-Mutterunternehmen sollte die Interessen aller seiner Tochterunternehmen berücksichtigen und abwägen, wie Strategien und Richtlinien langfristig einen Beitrag zu den Interessen der einzelnen Tochterunternehmen und der Gruppe als Ganzes leisten.

81. Ein EU-Mutterunternehmen und seine Tochterunternehmen sollten dafür Sorge tragen, dass die Wertpapierfirmen und Einheiten innerhalb der Gruppe allen speziellen aufsichtlichen Anforderungen der einschlägigen Rechtsordnungen entsprechen.

82. Das EU-Mutterunternehmens sollte dafür Sorge tragen, dass in einem Drittland niedergelassene Tochterunternehmen, die in den aufsichtlichen Konsolidierungskreis fallen, über Regelungen, Verfahren und Mechanismen für die Governance verfügen, die mit den Governance-Richtlinien auf Gruppenebene in Einklang stehen und den Anforderungen der Artikel 25 bis 32 der Richtlinie (EU) 2019/2034 und den vorliegenden Leitlinien entsprechen, soweit diese nach den Gesetzen des Drittlandes nicht rechtswidrig sind.

83. Die Anforderungen an die interne Governance der Richtlinie (EU) 2019/2034 und die vorliegenden Leitlinien gelten für Wertpapierfirmen mit Sitz in der EU unabhängig davon, ob sie Tochterunternehmen eines Mutterunternehmens mit Sitz in einem Drittland sind. Falls ein EU-Tochterunternehmen eines Mutterunternehmens mit Sitz in einem Drittland ein EU-Mutterunternehmen ist, umfasst der aufsichtliche Konsolidierungskreis innerhalb der EU nicht die Ebene der in einem Drittland niedergelassenen Mutterwertpapierfirma und sonstiger direkter Tochterunternehmen dieses Mutterunternehmens. Das EU-Mutterunternehmen sollte sicherstellen, dass die gruppenweiten Governance-Richtlinien für die Mutterwertpapierfirma in einem Drittland im Rahmen seiner eigenen Governance-Richtlinien insoweit berücksichtigt werden, als dies nicht im Widerspruch zu den Anforderungen des einschlägigen EU-Rechts, einschließlich der Richtlinie (EU) 2019/2034 und weiterer Bestimmungen in den vorliegenden Leitlinien, steht.

84. Bei der Festlegung von Strategien und der Dokumentation von Governance-Regelungen sollten die Wertpapierfirmen die in Anhang I aufgeführten Aspekte berücksichtigen. Zwar können Strategien und Dokumentation in gesonderte Dokumente aufgenommen werden, doch sollten die Wertpapierfirmen ihre Zusammenfassung oder Bezugnahme in einem einzigen Rahmendokument für die interne Governance in Erwägung ziehen.

Titel IV – Risikokultur und Wohlverhaltensregeln

8 Risikokultur

85. Eine solide, sorgfältige und kohärente Risikokultur sollte ein Schlüsselelement eines wirksamen Risikomanagements einer Wertpapierfirma sein und es ihr ermöglichen, solide und fundierte Entscheidungen zu treffen.

86. Die Wertpapierfirmen sollten eine integrierte und unternehmensweite Risikokultur auf der Grundlage eines umfassenden Verständnisses und einer ganzheitlichen Sicht ihrer Risiken, einschließlich der Risiken für Kunden, Risiken für Märkte, des Risikos für die Wertpapierfirma selbst und der Liquiditätsrisiken, insbesondere derjenigen, die mit wesentlichen Auswirkungen auf die Höhe der verfügbaren Eigenmittel einhergehen oder diese aufbrauchen können, sowie deren Steuerung entwickeln, wobei die Risikotragfähigkeit und der Risikoappetit der Wertpapierfirma zu berücksichtigen sind.

87. Die Wertpapierfirmen sollten eine Risikokultur mittels Richtlinien, Kommunikation und Fortbildungen der Mitarbeiter bezüglich der Tätigkeiten, Strategie und des Risikoprofils der

Wertpapierfirma entwickeln und Kommunikation und Mitarbeiterfortbildungen anpassen, um der Verantwortung der Mitarbeiter bezüglich Risikoappetit und Risikomanagement Rechnung zu tragen.

88. Die Mitarbeiter sollten sich ihrer Verantwortung hinsichtlich des Risikomanagements voll und ganz bewusst sein. Das Risikomanagement sollte nicht auf Risikospezialisten oder interne Kontrollfunktionen beschränkt werden. Die Geschäftseinheiten sollten unter der Aufsicht des Leitungsorgans in erster Linie für das tägliche Risikomanagement gemäß den Richtlinien, Verfahren und Kontrollen der Wertpapierfirma unter Berücksichtigung des Risikoappetits und der Risikotragfähigkeit der Wertpapierfirma verantwortlich sein.

89. Eine solide Risikokultur sollte folgende Elemente umfassen, ist aber nicht notwendigerweise auf diese beschränkt:

    a. Leitungskultur (Tone from the top): Das Leitungsorgan sollte für die Festlegung und Kommunikation der Kernwerte und Erwartungen der Wertpapierfirma zuständig sein. Das Verhalten seiner Mitglieder sollte diese Werte widerspiegeln. Die Führungskräfte der Wertpapierfirma, einschließlich der Inhaber von Schlüsselfunktionen, sollten zur internen Kommunikation von Kernwerten und Erwartungen an die Mitarbeiter beitragen. Die Mitarbeiter sollten alle geltenden Gesetze und Rechtsvorschriften einhalten und festgestellte Rechtsverstöße innerhalb oder außerhalb der Wertpapierfirma unverzüglich melden (z. B. der zuständigen Behörde im Rahmen eines Hinweisgeberverfahrens („whistleblowing“). Das Leitungsorgan sollte die Risikokultur der Wertpapierfirma fortlaufend fördern, überwachen und bewerten, die Auswirkungen der Risikokultur auf die Finanzstabilität, das Risikoprofil und eine stabile Unternehmensführung der Wertpapierfirma berücksichtigen, und soweit erforderlich, Änderungen vornehmen.

    b. Verantwortlichkeiten: Die maßgeblichen Mitarbeiter auf allen Stufen sollten die Kernwerte der Wertpapierfirma und, in dem für ihre Funktion erforderlichen Umfang, ihren Risikoappetit und ihre Risikotragfähigkeit kennen und verstehen. Sie sollten in der Lage sein, ihre Aufgaben wahrzunehmen, und sich bewusst sein, dass sie für ihre Handlungen in Zusammenhang mit dem Risikoverhalten der Wertpapierfirma zur Verantwortung gezogen werden.

    c. Wirksame Kommunikation und kritischer Dialog: Eine solide Risikokultur sollte eine von offener Kommunikation und kritischem Dialog geprägte Umgebung fördern, in der bei Entscheidungsprozessen ein breites Spektrum an Sichtweisen unterstützt wird, die Erprobung aktueller Praktiken möglich ist, eine konstruktive kritische Haltung der Mitarbeiter und ein von einem offenen und konstruktiven Engagement gekennzeichnetes Umfeld in der gesamten Organisation gefördert wird.

d. Anreize: Geeignete Anreize sollten eine zentrale Rolle bei der Angleichung des Risikoverhaltens an das Risikoprofil der Wertpapierfirma und ihre langfristigen Interessen spielen[19].

9 Unternehmenswerte und Verhaltenskodex

90. Das Leitungsorgan sollte hohe ethische und berufliche Standards entwickeln, annehmen, einhalten und fördern, wobei es die speziellen Anforderungen und Merkmale der Wertpapierfirma zu berücksichtigen gilt, und sollte für die Umsetzung solcher Standards Sorge tragen (durch einen Verhaltenskodex oder ein vergleichbares Instrument). Überdies sollte es die Einhaltung dieser Standards durch die Mitarbeiter überwachen. Soweit anwendbar, kann das Leitungsorgan gruppenweite Standards der Wertpapierfirma oder gemeinsame Standards, die von Verbänden oder sonstigen einschlägigen Organisationen herausgegeben wurden, annehmen und umsetzen.

91. Die Wertpapierfirmen sollten sicherstellen, dass keine Diskriminierung der Mitarbeiter aus Gründen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Orientierung stattfindet.

92. Die Richtlinien der Wertpapierfirmen sollten geschlechtsneutral sein. Dies umfasst unter anderem die Vergütungspolitik, Einstellungspolitik, Karriereentwicklung und Nachfolgeplanung, den Zugang zu Fortbildung und die Möglichkeit, sich auf freie Stellen im Unternehmen zu bewerben. Institute sollten Chancengleichheit [20] für alle Mitarbeiter unabhängig von ihrem Geschlecht sicherstellen, auch was berufliche Perspektiven betrifft, und auf eine Verbesserung der Vertretung des unterrepräsentierten Geschlechts in Positionen innerhalb des Leitungsorgans und in der Gruppe der Mitarbeiter mit Führungsaufgaben im Sinne der Delegierten Verordnung der Kommission (technische Regulierungsstandards zu identifizierten Mitarbeitern) zielen. Wertpapierfirmen sollten die Entwicklung beim Einkommensgefälle zwischen Frauen und Männern beobachten. In Wertpapierfirmen mit mehr als 50 Mitarbeitern [21] sollte die Beobachtung getrennt für identifizierte Mitarbeiter (ohne Mitglieder des Leitungsorgans), Mitglieder des Leitungsorgans in seiner Leitungsfunktion, Mitglieder des Leitungsorgans in seiner Aufsichtsfunktion und sonstiges Personal erfolgen. Institute sollten über Richtlinien verfügen, durch die die Wiedereingliederung von Mitarbeitern nach Mutterschafts-, Vaterschafts- und Elternurlaub gefördert wird.[22]

[19] Siehe auch die Leitlinien der EBA für eine solide Vergütungspolitik gemäß der Richtlinie (EU) 2034/2019.

[20] Siehe auch Richtlinie 2006/54/EG des Europäischen Parlaments und des Rates vom 5. Juli 2006 zur Verwirklichung des Grundsatzes der Chancengleichheit und Gleichbehandlung von Männern und Frauen in Arbeits- und Beschäftigungsfragen.

[21] Siehe auch Leitlinien der EBA für eine solide Vergütungspolitik gemäß der Richtlinie (EU) 2019/2034.

[22] Siehe auch Leitlinien der EBA für eine solide Vergütungspolitik gemäß der Richtlinie (EU) 2019/2034.

93. Die umgesetzten Standards sollten auf eine Verbesserung der stabilen Governance-Regelungen der Wertpapierfirma und eine Reduzierung der Risiken abzielen, denen die Wertpapierfirma ausgesetzt ist, insbesondere operationelle Risiken und Reputationsrisiken, die erhebliche nachteilige Auswirkungen auf die Rentabilität und Nachhaltigkeit einer Wertpapierfirma aufgrund von Geldstrafen, Verfahrenskosten, von zuständigen Behörden auferlegten Beschränkungen, sonstigen finanziellen und strafrechtlichen Sanktionen und des Verlusts des Markenwerts und des Vertrauens der Verbraucher aufweisen können.

94. Das Leitungsorgan sollte klare und dokumentierte Richtlinien zu der Frage erlassen, wie diese Standards zu erfüllen sind. Diese Richtlinien sollten

    a. die Leser daran erinnern, dass alle Tätigkeiten der Wertpapierfirma unter Einhaltung des geltenden Rechts und gemäß den Unternehmenswerten der Wertpapierfirma durchgeführt werden sollten;

    b. das Risikobewusstsein durch eine starke Risikokultur gemäß Abschnitt 9 der Leitlinien fördern, wobei die Erwartung des Leitungsorgans vermittelt wird, dass die Tätigkeiten nicht über den definierten Risikoappetit und die von der Wertpapierfirma festgelegten Grenzen sowie die jeweiligen Verantwortlichkeiten der Mitarbeiter hinausgehen;

    c. Grundsätze festlegen und Beispiele für akzeptables und nicht akzeptables Verhalten liefern, insbesondere in Verbindung mit finanzieller Fehlberichterstattung und Fehlverhalten, Wirtschafts- und Finanzkriminalität (einschließlich Betrug, Geldwäsche und Terrorismusfinanzierung (GW/TF), Kartellbildung, Verstoß gegen Finanzsanktionen, Bestechung und Korruption, Marktmanipulation, missbräuchliche Verkäufe und andere Verstöße gegen Verbraucherschutzrechte, Steuervergehen, ob direkt oder indirekt begangen, einschließlich mittels rechtswidrig oder verbotener Vereinbarungen zur Dividenden-Arbitrage);

    d. klären, dass zusätzlich zur Erfüllung der gesetzlichen und aufsichtlichen Anforderungen und internen Richtlinien von den Mitarbeitern erwartet wird, dass sie sich aufrichtig und integer verhalten und ihre Aufgaben mit der gebotenen Sachkenntnis, Sorgfalt und Gewissenhaftigkeit ausüben;

    e. sicherstellen, dass den Mitarbeitern die potenziellen internen und externen disziplinarischen Maßnahmen, rechtlichen Schritte und Sanktionen bekannt sind, die auf Fehlverhalten und nicht akzeptables Verhalten folgen können.

95. Die Wertpapierfirmen sollten die Einhaltung solcher Standards überwachen und für eine Sensibilisierung der Mitarbeiter, z. B. durch Fortbildungsangebote, Sorge tragen. Die Wertpapierfirmen sollten die Funktion, die für die Überwachung der Einhaltung und die Bewertung von Verstößen gegen den Verhaltenskodex oder ein vergleichbares Instrument zuständig ist, sowie ein Verfahren für den Umgang im Falle einer Nichteinhaltung festlegen. Die Ergebnisse sollten dem Leitungsorgan regelmäßig berichtet werden.

10 Richtlinien für den Umgang mit Interessenkonflikten auf Firmenebene

96. Das Leitungsorgan sollte für die Festlegung, Genehmigung und Überwachung der Umsetzung und Pflege von wirksamen Richtlinien zur Ermittlung, Bewertung, Steuerung und Minderung oder Vermeidung tatsächlicher und potenzieller Interessenkonflikte auf Firmenebene, z. B. infolge der verschiedenen Tätigkeiten und Funktionen der Wertpapierfirma, von verschiedenen Wertpapierfirmen im aufsichtlichen Konsolidierungskreis oder von verschiedenen Geschäftsbereichen oder Geschäftseinheiten innerhalb einer Wertpapierfirma, oder bezüglich externer Interessenträger zuständig sein. Bei der Festlegung dieser Richtlinien sollten sich die Wertpapierfirmen bewusst sein, dass diese auch mit Artikel 16 Absatz 3 und Artikel 23 der Richtlinie 2014/65/EU sowie mit den Artikeln 33 bis 35 der Delegierten Verordnung (EU) 2017/565 der Kommission in Einklang stehen müssen.

97. Die Maßnahmen der Wertpapierfirmen zur Steuerung oder, soweit angemessen, Minderung von Interessenkonflikten sollten dokumentiert werden und unter anderem Folgendes umfassen:

    a. eine geeignete Aufgabentrennung, z. B. die Übertragung kollidierender Tätigkeiten im Rahmen der Verarbeitung von Transaktionen oder die Erbringung von Dienstleistungen für unterschiedliche Personen oder die Übertragung von Aufsichts- und Berichtsaufgaben bei kollidierenden Tätigkeiten auf unterschiedliche Personen;

    b. die Einrichtung von Informationssperren, z. B. durch die physische Trennung bestimmter Geschäftsbereiche oder Einheiten.

11 Richtlinien für den Umgang mit Interessenkonflikten für Mitarbeiter[23]

98. Unbeschadet Artikel 23 der Richtlinie 2014/65/EU sowie Abschnitt 3 des Kapitels 2 der Delegierten Verordnung (EU) 2017/565 der Kommission sollte das Leitungsorgan für die Festlegung, Genehmigung und Überwachung der Umsetzung und Pflege von wirksamen Richtlinien zur Ermittlung, Bewertung, Steuerung und Minderung tatsächlicher und potenzieller Interessenkonflikte zwischen den Interessen der Wertpapierfirma und den privaten Interessen der Mitarbeiter, einschließlich der Mitglieder des Leitungsorgans, zuständig sein, die sich nachteilig auf die Wahrnehmung ihrer Pflichten und Zuständigkeiten auswirken können. Ein EU-Mutterunternehmen sollte die Interessen im Rahmen gruppenweiter Richtlinien für den Umgang mit Interessenkonflikten auf konsolidierter Basis berücksichtigen.

[23] Dieser Abschnitt sollte in Verbindung mit den gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und von Inhabern von Schlüsselfunktionen gemäß der Richtlinie 2013/36/EU und der Richtlinie 2014/65/EU gelesen werden.

99. Die Richtlinien sollten auf die Ermittlung von Interessenkonflikten der Mitarbeiter abzielen, einschließlich der Interessen ihrer nächsten Familienangehörigen. Die Wertpapierfirmen sollten berücksichtigen, dass Interessenkonflikte nicht nur aus den aktuellen persönlichen oder beruflichen Beziehungen, sondern auch aus Beziehungen in der Vergangenheit entstehen können. Falls Interessenkonflikte entstehen, sollten die Wertpapierfirmen ihre Wesentlichkeit bewerten sowie gegebenenfalls über geeignete mindernde Maßnahmen entscheiden und diese umsetzen.

100. Für Interessenkonflikte, die aufgrund von Beziehungen aus der Vergangenheit bestehen können, sollten die Wertpapierfirmen einen geeigneten Zeitraum festlegen, für den die Mitarbeiter solche Interessenkonflikte melden müssen, im Hinblick darauf, dass diese nach wie vor Auswirkungen auf das Verhalten und die Beteiligung an der Entscheidungsfindung der Mitarbeiter haben können.

101. Die Richtlinien sollten zumindest die folgenden Situationen oder Beziehungen abdecken, in denen Interessenkonflikte entstehen können:

    a. wirtschaftliche Interessen (z. B. Anteile, andere Eigentumstitel und Beteiligungen, Finanzbeteiligungen und andere wirtschaftliche Interessen an Geschäftskunden, Rechte an geistigem Eigentum, Beteiligung an einer Einrichtung oder Eigentum einer Einrichtung oder Organisation mit widerstreitenden Interessen);

    b. persönliche oder berufliche Beziehungen mit den Eigentümern von qualifizierten Beteiligungen an der Wertpapierfirma;

    c. persönliche oder berufliche Beziehungen mit Mitarbeitern der Wertpapierfirma oder von Unternehmen, die zum aufsichtlichen Konsolidierungskreis gehören (z. B. familiäre Beziehungen);

    d. sonstige Beschäftigungen und frühere Beschäftigungen in der jüngsten Vergangenheit (z. B. fünf Jahre);

    e. persönliche oder berufliche Beziehungen mit einschlägigen externen Interessenträgern (z. B. Verbindung mit wesentlichen Lieferanten, Beratungsunternehmen oder anderen Dienstleistungsanbietern) und

    f. politischer Einfluss oder politische Beziehungen.

102. Unbeschadet des Vorstehenden sollten die Wertpapierfirmen berücksichtigen, dass der Umstand, dass eine Person Anteilseigner einer Wertpapierfirma ist oder andere Leistungen der Wertpapierfirma in Anspruch nimmt, nicht dazu führen sollte, dass trotz Einhaltung einer angemessenen Geringfügigkeitsschwelle von einem Interessenkonflikt der Mitarbeiter ausgegangen wird.

103. In den Richtlinien sollten die Verfahren für die Berichterstattung und Kommunikation an die nach den Richtlinien zuständige Funktion festgelegt sein. Die Mitarbeiter sollten verpflichtet sein, unverzüglich intern alle Angelegenheiten mitzuteilen, die zu einem Interessenkonflikt führen könnten oder bereits geführt haben.

104. In den Richtlinien sollte zwischen Interessenkonflikten unterschieden werden, die weiterbestehen und dauerhaft gesteuert werden müssen, und solchen Interessenkonflikten, die unerwartet in Zusammenhang mit einem einzelnen Ereignis entstehen (z. B. ein Geschäft oder die Auswahl eines Dienstleisters usw.) und in der Regel mit einer einmaligen Maßnahme gehandhabt werden können. In allen Fällen sollte das Interesse der Wertpapierfirma bei den getroffenen Entscheidungen im Mittelpunkt stehen.

105. In den Richtlinien sollten Verfahren, Maßnahmen, Dokumentationselemente und Verantwortlichkeiten für die Ermittlung und Vermeidung von Interessenkonflikten, für die Beurteilung ihrer Wesentlichkeit und das Ergreifen von mindernden Maßnahmen festgelegt werden. Diese Verfahren, Anforderungen, Zuständigkeiten und Maßnahmen sollten Folgendes umfassen:

    a. Übertragung konfligierender Aufgaben oder Transaktionen an unterschiedliche Personen;

    b. Verhindern, dass Mitarbeiter, die auch außerhalb der Wertpapierfirma tätig sind, innerhalb der Wertpapierfirma bezüglich dieser anderen Tätigkeiten einen unangemessenen Einfluss ausüben;

    c. Festlegen, dass es in der Verantwortlichkeit eines jeden Mitglieds des Leitungsorgans liegt, an der Abstimmung über eine Frage nicht teilzunehmen, wenn hierzu ein Interessenkonflikt des Mitglieds bestehen könnte bzw. wenn die Objektivität oder Fähigkeit des Mitglieds, seinen Verpflichtungen gegenüber der Wertpapierfirma ordnungsgemäß nachzukommen, anderweitig gefährdet sein könnte;

    d. Mitglieder des Leitungsorgans darin hindern, Leitungs- oder Aufsichtsfunktionen in konkurrierenden Wertpapierfirmen zu bekleiden.

106. Die Richtlinien sollten insbesondere das Risiko von Interessenkonflikten auf Ebene des Leitungsorgans abdecken und genügend Orientierungshilfen für die Ermittlung und den Umgang mit Interessenkonflikten bieten, die die Fähigkeit der Mitglieder des Leitungsorgans behindern können, objektive und unparteiische Entscheidungen zu treffen, die auf das ureigenste Interesse der Wertpapierfirmen ausgerichtet sind. Die Wertpapierfirmen sollten in Erwägung ziehen, dass Interessenkonflikte Auswirkungen auf die Unabhängigkeit der Mitglieder des Leitungsorgans haben können[24].

[24] Siehe auch die gemeinsamen Leitlinien der ESMA und der EBA zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und von Inhabern von Schlüsselfunktionen gemäß der Richtlinie 2013/36/EU und der Richtlinie 2014/65/EU.

107. Bei der Minderung ermittelter Interessenkonflikte von Mitgliedern des Leitungsorgans sollten die Wertpapierfirmen die ergriffenen Maßnahmen dokumentieren, einschließlich der Begründung, inwieweit diese wirksam sind, um eine objektive Entscheidungsfindung sicherzustellen.

108. Tatsächliche oder potenzielle Interessenkonflikte, die der zuständigen Funktion innerhalb der Wertpapierfirma offengelegt wurden, sollten ordnungsgemäß bewertet und geregelt werden. Wird ein Interessenkonflikt eines Mitarbeiters festgestellt, sollte die Wertpapierfirma die getroffene Entscheidung dokumentieren, insbesondere wenn der Interessenkonflikt und die damit verbundenen Risiken akzeptiert wurden, und sofern er akzeptiert wurde, wie der Interessenkonflikt zufriedenstellend entschärft oder behoben wurde.

109. Ein tatsächlicher oder potenzieller Interessenkonflikt auf Ebene des Leitungsorgans, sei es auf individueller oder kollektiver Grundlage, sollte angemessen dokumentiert, dem Leitungsorgan mitgeteilt, vom Leitungsorgan erörtert, entschieden und ordnungsgemäß geregelt werden.

11.1 Richtlinien für den Umgang mit Interessenkonflikten im Zusammenhang mit Darlehen und anderen Geschäften mit Mitgliedern des Leitungsorgans und ihren verbundenen Parteien

110. Im Rahmen ihrer Richtlinien für den Umgang mit Interessenkonflikten für Mitarbeiter (Abschnitt 11) und dem Umgang mit Interessenkonflikten von Mitgliedern des Leitungsorgans gemäß Absatz 107 sollte das Leitungsorgan einen Rahmen für die Ermittlung und den Umgang mit Interessenkonflikten im Zusammenhang mit der Gewährung von Krediten und dem Abschluss anderer Geschäfte, z. B. Börsengänge, Dienstleistungsvereinbarungen, Immobilientransaktionen und Auslagerungsvereinbarungen mit Mitgliedern des Leitungsorgans und ihrer verbundenen Parteien festlegen.

111. Wertpapierfirmen sollten zusätzliche Kategorien von verbundenen Parteien in Erwägung ziehen, auf die sie ihren Rahmen für Interessenkonflikte in Zusammenhang mit Darlehen und anderen Rahmen für Interessenkonflikte in Zusammenhang mit Darlehen und anderen Geschäften ganz oder teilweise anwenden.

112. Durch den Rahmen für Interessenkonflikte sollte sichergestellt werden, dass Entscheidungen bezüglich der Gewährung von Darlehen und des Abschlusses anderer Geschäfte mit Mitgliedern des Leitungsorgans und ihrer verbundenen Parteien objektiv ohne unzulässige Beeinflussung durch Interessenkonflikte und generell zu marktüblichen Konditionen getroffen werden.

113. Das Leitungsorgan sollte die anwendbaren Beschlussfassungsverfahren für die Gewährung von Darlehen und den Abschluss anderer Geschäfte mit Mitgliedern des Leitungsorgans und ihren verbundenen Parteien festlegen. In diesem Rahmen kann eine Differenzierung zwischen

normalen Geschäftsvorgängen[25], die im ordentlichen Geschäftsgang und zu marktüblichen Bedingungen getätigt werden, und Geschäften mit Mitarbeitern, die nach den für alle Mitarbeiter verfügbaren Bedingungen abgeschlossen werden, vorgesehen sein. Des Weiteren kann bei dem Rahmen für Interessenkonflikte und den Entscheidungsprozess zwischen wesentlichen und nicht wesentlichen Darlehen oder anderen wesentlichen Geschäften, unterschiedlichen Arten von Darlehen und anderen Geschäften und dem Umfang der tatsächlichen oder potenziellen Interessenkonflikte, die entstehen können, unterschieden werden.

114. Als Teil des Rahmens für Interessenkonflikte sollte das Leitungsorgan angemessene Schwellenwerte (z. B. pro Produktart, Volumen oder abhängig von den Bedingungen) festlegen, ab denen für das Geschäft mit einem Mitglied des Leitungsorgans oder seinen verbundenen Parteien stets die Genehmigung des Leitungsorgans erforderlich ist. Entscheidungen über wesentliche Darlehen und andere wesentliche Geschäfte mit Mitgliedern des Leitungsorgans, die nicht unter normalen Marktbedingungen, sondern nach den für alle Mitarbeiter verfügbaren Bedingungen abgeschlossen werden, sollten stets vom Leitungsorgan getroffen werden.

115. Das Mitglied des Leitungsorgans, dem solch ein wesentliches Darlehen oder anderes wesentliches Geschäft zugutekommt, oder das Mitglied, das mit der Gegenpartei verbunden ist, sollte nicht am Entscheidungsfindungsprozess beteiligt sein.

116. Bei einer Entscheidung über ein Darlehen oder ein anderes Geschäft mit einem Mitglied des Leitungsorgans oder dessen verbundenen Parteien sollten Wertpapierfirmen vor dem Treffen einer Entscheidung das Risiko bewerten, dem die Wertpapierfirma möglicherweise aufgrund des Geschäfts ausgesetzt ist.

117. Um die Einhaltung der Richtlinien für den Umgang mit Interessenkonflikten sicherzustellen, sollten die Wertpapierfirmen dafür Sorge tragen, dass sämtliche relevanten internen Kontrollverfahren auf Darlehen und andere Geschäfte mit Mitgliedern des Leitungsorgans oder ihrer verbundenen Parteien angewandt werden und dass ein geeigneter Kontrollrahmen auf Ebene des Leitungsorgans in seiner Aufsichtsfunktion vorhanden ist.

11.2 Dokumentation von Darlehen an Mitglieder des Leitungsorgans und ihrer verbundenen Parteien sowie zusätzliche Informationen

118. Im Sinne des Artikels 26 der Richtlinie (EU) 2019/2034 sollten Wertpapierfirmen die Daten über Darlehen an Mitglieder des Leitungsorgans und ihre verbundenen Parteien angemessen dokumentieren, wobei die Dokumentation mindestens die folgenden Daten einschließen muss:

[25] Geschäftsvorgänge können Darlehen, Leasing, Factoring, Dienstleistungen in Zusammenhang mit Börsengängen, Fusionen und Unternehmenskäufe, Verkauf und Kauf von Immobilien einschließen.

a. den Namen des Schuldners und seinen Status (d. h. Mitglied des Leitungsorgans oder verbundene Partei) und bezüglich Darlehen an eine verbundene Partei das Mitglied des Leitungsorgans, mit dem die Partei verbunden ist, sowie die Art der Beziehung zu der verbundenen Partei;

b. die Art des Darlehens und den Betrag;

c. die Konditionen des Darlehens;

d. das Datum der Genehmigung des Darlehens;

e. den Namen der Person oder des Organs und dessen Zusammensetzung, die bzw. das die Entscheidung über die Genehmigung des Darlehens und der geltenden Konditionen trifft;

f. die Angabe (ja/nein), ob das Darlehen zu Marktbedingungen gewährt wird oder nicht;

g. die Angabe (ja/nein), ob das Darlehen zu den für alle Mitarbeiter verfügbaren Konditionen gewährt wird oder nicht.

119. Wertpapierfirmen sollten sicherstellen, dass die Dokumentation aller Darlehen an Mitglieder des Leitungsorgans und ihre verbundenen Parteien vollständig und auf dem aktuellsten Stand ist und dass die Wertpapierfirma in der Lage ist, den zuständigen Behörden auf Anfrage die vollständige Dokumentation in einer geeigneten Form unverzüglich zur Verfügung zu stellen.

12 Hinweisgeberverfahren (Whistleblowing-Verfahren)

120. Wertpapierfirmen sollten geeignete Richtlinien und Verfahren für interne Warnungen für Mitarbeiter zur Meldung potenzieller oder tatsächlicher Verstöße gegen die Verordnung (EU) 2019/2033 und nationale Vorschriften zur Umsetzung der Richtlinie(EU) 2019/2034, über einen speziellen, unabhängigen und autonomen Berichtsweg einführen und unterhalten. Es sollte für die meldenden Mitarbeiter nicht erforderlich sein, einen Beleg für einen Verstoß vorzulegen, allerdings sollten sie über ein ausreichendes Maß an Gewissheit verfügen, das einen hinreichenden Grund für die Einleitung einer Untersuchung bietet. Wertpapierfirmen sollten zudem geeignete Prozesse und Verfahren einrichten, mit denen sichergestellt wird, dass sie ihre Pflichten gemäß der nationalen Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, erfüllen.

121. Zur Vermeidung von Interessenkonflikten sollte für die Mitarbeiter eine Möglichkeit bestehen, Verstöße außerhalb der regulären Berichtswege zu melden (z. B. über die Compliance-Funktion, die interne Revision oder mittels eines unabhängigen internen Hinweisgeberverfahrens). Die Warnverfahren sollten den Schutz personenbezogener Daten

im Einklang mit der Verordnung (EU) 2016/679[26] (DSGVO) sowohl für die Person, die den Verstoß anzeigt, als auch für die natürliche Person, die mutmaßlich für den Verstoß verantwortlich ist, sicherstellen.

122. Die Warnverfahren sollten allen Mitarbeitern einer Wertpapierfirma zugänglich gemacht werden.

123. Die von Mitarbeitern über die Warnverfahren bereitgestellten Informationen sollten, falls angemessen, dem Leitungsorgan und anderen verantwortlichen Funktionen, die in den Richtlinien für interne Warnungen festgelegt sind, zur Verfügung gestellt werden. Sofern dies der Mitarbeiter, der einen Verstoß meldet, verlangt, sollten die Informationen dem Leitungsorgan und anderen verantwortlichen Funktionen in anonymisierter Form vorgelegt werden. Die Wertpapierfirmen können auch ein Hinweisgeberverfahren einrichten, das es ermöglicht, Informationen anonym einzureichen.

124. Die Wertpapierfirmen sollten sicherstellen, dass die Person, die den Verstoß meldet, angemessen vor negativen Folgen geschützt ist, z. B. Vergeltung, Diskriminierung oder einer anderen Art von unfairer Behandlung. Die Wertpapierfirma sollte sicherstellen, dass sich keine Person unter der Kontrolle der Wertpapierfirma an der Viktimisierung einer Person beteiligt, die einen Verstoß gemeldet hat, und sollte geeignete Maßnahmen gegen die Personen ergreifen, die für eine etwaige Viktimisierung verantwortlich sind.

125. Die Wertpapierfirmen sollten zudem Personen, über die eine Meldung gemacht wurde, vor etwaigen negativen Folgen schützen, wenn im Zuge der Untersuchung keine Belege gefunden werden, die die Einleitung von Maßnahmen gegen die betreffende Person begründen. Falls Maßnahmen ergriffen werden, sollte die Wertpapierfirma diese in einer Weise einleiten, die auf den Schutz der betreffenden Person vor unbeabsichtigten negativen Folgen ausgerichtet ist, die über das Ziel der ergriffenen Maßnahme hinausgehen.

126. Insbesondere sollten die Verfahren für interne Warnungen

    a. dokumentiert sein (z. B. Handbücher für Mitarbeiter);

    b. klare Regeln vorsehen, mit denen sichergestellt wird, dass Informationen über die Meldung und die gemeldeten Personen sowie den Verstoß vertraulich gemäß der Verordnung (EU) 2016/679 behandelt werden, sofern nicht eine Offenlegung nach dem nationalen Recht im Rahmen weiterer Untersuchungen oder anschließender Gerichtsverfahren erforderlich ist;

    c. Mitarbeiter, die Bedenken äußern, vor einer Viktimisierung aufgrund der Tatsache, dass sie zu meldende Verstöße offengelegt haben, schützen;

[26] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

d. sicherstellen, dass potenzielle oder tatsächliche Verstöße bewertet und eskaliert werden, einschließlich, soweit angemessen, an die betreffende zuständige Behörde oder Strafverfolgungsbehörde;

e. soweit möglich, sicherstellen, dass den Mitarbeitern, die potenzielle oder tatsächliche Verstöße gemeldet haben, der Erhalt der Information bestätigt wird;

f. für die Weiterverfolgung des Ergebnisses einer Untersuchung zu einem gemeldeten Verstoß Sorge tragen und

g. das Führen geeigneter Aufzeichnungen sicherstellen.

13 Meldung von Verstößen bei den zuständigen Behörden

127. Gemäß Artikel 22 der Richtlinie (EU) 2019/2034 sollten die zuständigen Behörden wirksame und verlässliche Mechanismen schaffen, damit die Mitarbeiter von Wertpapierfirmen den zuständigen Behörden einschlägige potenzielle oder tatsächliche Verstöße gegen die Verordnung (EU) 2019/2033 und die nationalen Vorschriften zur Umsetzung der Richtlinie (EU) 2019/2034 melden können. Diese Mechanismen sollten mindestens Folgendes umfassen:

a. spezielle Verfahren für den Eingang von Berichten über Verstöße und die Weiterverfolgung, z. B. eine spezielle Abteilung, Einheit oder Funktion für Hinweisgeber;

b. einen geeigneten Schutz gemäß den Ausführungen in Abschnitt 13;

c. den Schutz personenbezogener Daten im Einklang mit der Verordnung (EU) 2016/679 (DSGVO) sowohl für die natürliche Person, die den Verstoß anzeigt, als auch für die natürliche Person, die mutmaßlich für einen Verstoß verantwortlich ist;

d. klare Verfahren nach den Bestimmungen in Abschnitt 12.

128. Unbeschadet der Möglichkeit, Verstöße über die Mechanismen den zuständigen Behörden zu melden, können die zuständigen Behörden die Mitarbeiter beaufsichtigter Wertpapierfirmen ermutigen, zuerst zu versuchen, die Hinweisgeberverfahren ihrer Wertpapierfirmen zu nutzen.

Titel V – Interner Kontrollrahmen und interne Kontrollmechanismen

14 Interner Kontrollrahmen

129. Die Wertpapierfirmen sollten eine Kultur entwickeln und pflegen, die eine positive Haltung gegenüber der Risikokontrolle und Compliance innerhalb der Wertpapierfirma sowie einen stabilen und umfassenden internen Kontrollrahmen bestärkt. In diesem Rahmen sollten die Geschäftsbereiche der Wertpapierfirmen für die Steuerung der Risiken verantwortlich sein, die sie im Zuge der Durchführung ihrer Tätigkeiten eingehen, und sollten über Kontrollmechanismen verfügen, mit denen die Einhaltung von internen und externen Anforderungen sichergestellt wird. Als Teil dieses Rahmens sollten die Wertpapierfirmen über eine ständige und wirksame interne Compliance-Funktion [27] mit angemessenen und ausreichenden Befugnissen, einem ausreichenden Gewicht und Zugang zum Leitungsorgan für die Erfüllung ihrer Aufgabe sowie einen Risikomanagementrahmen verfügen. Sofern es unter Berücksichtigung der in Titel I aufgeführten Kriterien verhältnismäßig ist, sollten Wertpapierfirmen auch über eine interne Risikomanagementfunktion und Funktion der internen Revision verfügen.

130. Der interne Kontrollrahmen der betreffenden Wertpapierfirma sollte auf individueller Basis an die Besonderheiten der Geschäftstätigkeit, der Komplexität und der verbundenen Risiken angepasst sein, wobei der Kontext der Gruppe zu berücksichtigen ist. Die betreffende Wertpapierfirma muss den erforderlichen Informationsaustausch in einer Weise organisieren, durch die sichergestellt wird, dass die einzelnen Leitungsorgane, Geschäftsbereiche und internen Einheiten, darunter die einzelnen internen Kontrollfunktionen, in der Lage sind, ihre Pflichten zu erfüllen. Dies impliziert beispielsweise einen notwendigen Austausch von angemessenen Informationen zwischen den Geschäftsbereichen und der Compliance-Funktion sowie der Compliance-Funktion zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, sofern diese eine gesonderte Kontrollfunktion ist, auf Gruppenebene sowie zwischen den Leitern der internen Kontrollfunktionen auf Gruppenebene und dem Leitungsorgan der Wertpapierfirma.

131. Wertpapierfirmen sollten angemessene Prozesse und Verfahren einrichten, mit denen sichergestellt wird, dass sie ihre Pflichten im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung erfüllen. Wertpapierfirmen sollten das Ausmaß des Risikos, dass sie für die Zwecke von Geldwäsche/Terrorismusfinanzierung missbraucht werden, bewerten und gegebenenfalls Maßnahmen zur Minderung dieser Risiken und der mit ihnen verbundenen operationellen und Reputationsrisiken ergreifen. Wertpapierfirmen sollten Maßnahmen ergreifen, mit denen sichergestellt wird, dass sich die Mitarbeiter dieser Risiken hinsichtlich Geldwäsche/Terrorismusfinanzierung und der Auswirkungen, die

[27] Unbeschadet Artikel 22 der Delegierten Verordnung (EU) 2017/565 der Kommission.

Geldwäsche/Terrorismusfinanzierung auf die Wertpapierfirma und die Integrität des Finanzsystems haben können, bewusst sind.

132. Der interne Kontrollrahmen sollte sich auf die gesamte Organisation, einschließlich der Zuständigkeiten und Aufgaben des Leitungsorgans, sowie die Tätigkeiten aller Geschäftsbereiche und internen Einheiten, einschließlich der internen Kontrollfunktionen, ausgelagerten Tätigkeiten und Vertriebskanäle, erstrecken.

133. Der interne Kontrollrahmen einer Wertpapierfirma sollte Folgendes sicherstellen:

a. wirksame und effiziente Betriebsabläufe;

b. angemessene Ermittlung, Messung und Minderung von Risiken;

c. die Zuverlässigkeit der finanziellen und nicht finanziellen Berichterstattung, sowohl intern als auch extern;

d. solide Verwaltungs- und Rechnungslegungsverfahren sowie

e. Einhaltung von Gesetzen, Rechtsvorschriften, aufsichtlichen Anforderungen sowie der internen Richtlinien, Verfahren, Regelungen und Entscheidungen der Wertpapierfirma.

15 Umsetzung eines internen Kontrollrahmens

134. Das Leitungsorgan sollte für die Festlegung und Überwachung der Angemessenheit und Wirksamkeit des internen Kontrollrahmens, der entsprechenden Verfahren und Mechanismen sowie für die Überwachung aller Geschäftsbereiche und interner Einheiten, einschließlich der internen Kontrollfunktionen (wie die Compliance-Funktion, einschließlich der Compliance in Zusammenhang mit Geldwäsche und Terrorismusfinanzierung, sofern diese von der Compliance-Funktion getrennt ist, sowie der Funktionen des Risikomanagements und der internen Revision, sofern diese eingerichtet sind), zuständig sein. Die Wertpapierfirmen sollten für die interne Kontrolle angemessene schriftliche Richtlinien, Mechanismen und Verfahren, die vom Leitungsorgan genehmigt werden sollten, einrichten, pflegen und regelmäßig aktualisieren. Sofern keine Risikomanagementfunktion eingerichtet ist, sollte das Leitungsorgan für die Festlegung und Überwachung angemessener Verfahren und Strategien für das Risikomanagement zuständig sein.

135. Eine Wertpapierfirma sollte über einen klaren, transparenten und dokumentierten Entscheidungsprozess sowie eine eindeutige Aufgabenverteilung und Kompetenzregelung innerhalb ihres internen Kontrollrahmens verfügen, einschließlich ihrer Geschäftsbereiche, internen Einheiten und internen Kontrollfunktionen.

136. Die Wertpapierfirmen sollten diese Richtlinien, Mechanismen und Verfahren sowie wesentliche Änderungen daran allen Mitarbeitern kommunizieren.

137. Die internen Kontrollfunktionen sollten überprüfen, ob die im internen Kontrollrahmen festgelegten Richtlinien, Mechanismen und Verfahren in ihren jeweiligen Zuständigkeitsbereichen korrekt umgesetzt werden.

138. Die internen Kontrollfunktionen sollten dem Leitungsorgan regelmäßig schriftliche Berichte über ermittelte größere Mängel vorlegen. Diese Berichte sollten unter anderem für jeden neu festgestellten wesentlichen Mangel die damit verbundenen maßgeblichen Risiken, eine Folgenabschätzung, Empfehlungen und die einzuleitenden Abhilfemaßnahmen enthalten. Das Leitungsorgan sollte zeitnah und wirksam die Feststellungen der internen Kontrollfunktionen weiterverfolgen und angemessene Maßnahmen zur Mängelbeseitigung einfordern. Es sollte ein formelles Mängelbeseitigungsverfahren für die Feststellungen und ergriffenen Abhilfemaßnahmen vorgesehen werden.

16 Risikomanagementrahmen

139. Als Teil des gesamten internen Kontrollrahmens sollten die Wertpapierfirmen über einen ganzheitlichen unternehmensweiten Risikomanagementrahmen verfügen, der sich auf alle Geschäftsbereiche und internen Einheiten, einschließlich der internen Kontrollfunktionen erstreckt, wobei dem wirtschaftlichen Gehalt aller Risikopositionen voll und ganz Rechnung zu tragen ist, einschließlich der Risiken, die die Wertpapierfirma für sich selbst, ihre Kunden und die Märkte darstellt, sowie Liquiditätsrisiken, insbesondere derjenigen, die mit wesentlichen Auswirkungen auf die Höhe der verfügbaren Eigenmittel einhergehen können, oder solchen, durch die die verfügbaren Eigenmittel aufgebraucht werden könnten. Der Risikomanagementrahmen sollte die Wertpapierfirma in die Lage versetzen, fundierte Entscheidungen über das Eingehen von Risiken in Kenntnis der Sachlage zu treffen. Der Risikomanagementrahmen sollte alle Risiken sowie aktuelle und künftige Risiken, denen die Wertpapierfirma möglicherweise ausgesetzt ist, einschließen. Die Risiken sollten nach dem Bottom-up-Ansatz und dem Top-down-Ansatz, innerhalb der Geschäftsbereiche und geschäftsbereichsübergreifend beurteilt werden, wobei in der gesamten Wertpapierfirma sowie auf konsolidierter Ebene eine kohärente Terminologie und kompatible Methoden zugrunde gelegt werden sollten. Alle relevanten Risiken sollten im Risikomanagementrahmen berücksichtigt werden, wobei sowohl finanziellen als auch nichtfinanziellen Risiken ordnungsgemäß Rechnung getragen wird, einschließlich Marktrisiken, Liquiditätsrisiken, Konzentrationsrisiken, operationeller Risiken, IT-Risiken, Reputationsrisiken, rechtlicher Risiken, Wohlverhaltensrisiken, Compliance-Risiken hinsichtlich Geldwäsche/Terrorismusfinanzierung und Finanzkriminalität, ESG-Risiken und strategischer Risiken.

140. Der Risikomanagementrahmen einer Wertpapierfirma sollte Richtlinien, Verfahren, Risikolimite und Risikokontrollen enthalten, um so eine angemessene, zeitnahe und laufende Ermittlung, Messung oder Bewertung, Überwachung, Steuerung, Minderung und

Berichterstattung über die Risiken auf Ebene der Geschäftsbereiche, der Wertpapierfirma sowie auf konsolidierter Ebene sicherzustellen.

141. Der Risikomanagementrahmen einer Wertpapierfirma sollte konkrete Orientierungshilfen für die Umsetzung der Strategien der Wertpapierfirma vorsehen. Mit diesen Orientierungshilfen sollten, soweit erforderlich, interne Grenzen festgelegt und aufrechterhalten werden, die mit dem Risikoappetit der Wertpapierfirma konsistent sind und mit dem ordnungsgemäßen Geschäftsbetrieb, der Ertragskraft, Eigenmittelausstattung und den strategischen Zielen in Einklang stehen. Das Risikoprofil einer Wertpapierfirma sollte sich innerhalb der festgelegten Limite bewegen. Der Risikomanagementrahmen sollte sicherstellen, dass im Fall der Verletzung der Risikolimite ein definierter Eskalationsprozess zur Adressierung dieser Verletzung im Rahmen eines angemessenen Mängelbeseitigungsverfahrens besteht.

142. Der Risikomanagementrahmen sollte einer unabhängigen internen Überprüfung unterzogen werden, beispielsweise durch die interne Revision, und regelmäßig im Hinblick auf den Risikoappetit der Wertpapierfirma unter Berücksichtigung von Informationen der Risikomanagementfunktion sowie, sofern eingerichtet, des Risikoausschusses überprüft werden. Dabei sollten unter anderem Faktoren wie interne und externe Entwicklungen, einschließlich Ertragsveränderungen, jegliche Steigerung der Komplexität der Geschäftstätigkeit der Wertpapierfirma, das Risikoprofil und die operative Struktur, eine geografische Expansion, Fusionen und Übernahmen sowie die Einführung neuer Produkte oder Geschäftsbereiche berücksichtigt werden.

143. Bei der Ermittlung und Messung oder Beurteilung von Risiken sollte eine Wertpapierfirma geeignete Methoden und Verfahren entwickeln, die sowohl zukunfts- als auch vergangenheitsorientiert ausgestaltet sind. Die Instrumente sollten die Bewertung des tatsächlichen Risikoprofils im Verhältnis zum Risikoappetit der Wertpapierfirma sowie die Ermittlung und Bewertung potenzieller und angespannter Risikopositionen unter gestressten Bedingungen im Hinblick auf die Risikotragfähigkeit der Wertpapierfirma umfassen. Die Instrumente sollten Informationen über etwaige eventuell notwendige Anpassungen des Risikoprofils liefern. Die Wertpapierfirmen sollten angemessene konservative Annahmen bei der Konzeption von Stressszenarien zugrunde legen.

144. Die Wertpapierfirmen sollten bedenken, dass die Ergebnisse von quantitativen Bewertungsmethoden, einschließlich Stresstests, weitgehend von den Grenzen und Annahmen der verwendeten Modelle abhängen (einschließlich der Schwere und Dauer des Schocks und der zugrunde liegenden Risiken). Weisen beispielsweise Modelle eine sehr hohe ökonomische Kapitalrendite auf, ist dies möglicherweise auf Schwachstellen in den Modellen (z. B. Ausschluss bestimmter wesentlicher Risiken) selbst und nicht auf eine überlegene Strategie oder eine gelungene Umsetzung einer Strategie durch die Wertpapierfirma zurückzuführen. Die Bestimmung, in welcher Höhe Risiken eingegangen werden, sollte daher nicht nur auf quantitativen Informationen oder Ergebnissen von Modellen beruhen, sondern auch qualitative Aspekte einbeziehen (einschließlich Expertenschätzungen und kritischer Analysen). Zudem sollten relevante Veränderungen des wirtschaftlichen Umfelds betrachtet

werden, um deren potenzielle Auswirkungen auf die Risikopositionen und Portfolios zu ermitteln.

145. Die Letztverantwortung für die Risikobeurteilung liegt einzig und allein bei der Wertpapierfirma, die ihre Risiken dementsprechend kritisch beurteilen und sich nicht ausschließlich auf externe Beurteilungen verlassen sollte.

146. Die Wertpapierfirmen sollten sich der Grenzen von Modellen und Metriken voll und ganz bewusst sein und nicht nur quantitative, sondern auch qualitative Risikobewertungsinstrumente verwenden (einschließlich Expertenschätzungen und kritischer Analysen).

147. Neben den eigenen Bewertungen der Wertpapierfirmen können die Wertpapierfirmen auch externe Risikobeurteilungen heranziehen (einschließlich externer Bonitätseinstufungen oder extern erworbener Risikomodelle). Den Wertpapierfirmen sollten der genaue Umfang solcher Bewertungen und ihre Grenzen vollständig bewusst sein.

148. Es sollten fortlaufende und transparente Prozesse für die Berichterstattung eingerichtet werden, damit dem Leitungsorgan, seinem Risikoausschuss, sofern eingerichtet, und allen relevanten Einheiten einer Wertpapierfirma zeitnahe, genaue, präzise, verständliche und aussagekräftige Berichte vorgelegt werden, die wesentliche Informationen über die Ermittlung, Messung oder Beurteilung sowie Überwachung und Steuerung von Risiken erhalten. Der Rahmen für die Berichterstattung sollte klar definiert und dokumentiert sein.

149. Eine effektive Kommunikation und Sensibilisierung hinsichtlich der Risiken und der Risikostrategie ist für den gesamten Risikomanagementprozess, einschließlich der Überprüfungs- und Entscheidungsprozesse, von entscheidender Bedeutung und hilft, Entscheidungen zu vermeiden, durch die unwissentlich das Risiko erhöht werden könnte. Eine effektive Risikoberichterstattung setzt eine umfassende interne Würdigung und Kommunikation der Risikostrategie sowie wichtiger Risikodaten (z. B. Risikopositionen und Risikokennzahlen) voraus, sowohl horizontal in den gesamten Wertpapierfirmen als auch nach oben und unten entlang der gesamten Kette der Unternehmensführung.

17 Interne Kontrollfunktionen

150. Die internen Kontrollfunktionen sollten eine wirksame und ständige interne Compliance-Funktion, und sofern unter Berücksichtigung der in Titel I aufgeführten Kriterien angemessen und verhältnismäßig, eine Risikomanagementfunktion und eine interne Revision umfassen. Die Zuständigkeiten der Kontrollfunktionen schließen auch ein, die Erfüllung von Anforderungen im Bereich der Bekämpfung von Geldwäsche/Terrorismusfinanzierung sicherzustellen. Wenn Wertpapierfirmen keine Risikomanagementfunktion und interne Revision einrichten und unterhalten, sollten sie in der Lage sein, auf Anfrage nachzuweisen, dass die für den internen Kontrollrahmen angenommenen und eingeführten Strategien und

Verfahren das gleiche Ergebnis erzielen, wie es in den Leitlinien unter diesem Titel V vorgesehen ist.

151. Wenn die Wertpapierfirma keine interne Risikomanagementfunktion oder keine interne Revision einrichtet, obliegen die Zuständigkeiten für diese Funktionen gemäß diesen Leitlinien den Mitarbeitern, die für die eingerichteten Verfahren zuständig sind, und letztlich dem Leitungsorgan, das die operativen Aufgaben intern oder extern übertragen kann.

152. Unbeschadet der Umsetzung der Richtlinie (EU) 2015/849 in nationales Recht sollten die Wertpapierfirmen die Zuständigkeit für die Sicherstellung, dass die Wertpapierfirma die Anforderungen dieser Richtlinie und der Strategien und Verfahren des Instituts erfüllt, einem Mitarbeiter (z. B. Leiter der Compliance) zuweisen. Wertpapierfirmenkönnen eine separate Compliance-Funktion für Geldwäsche/Terrorismusfinanzierung als unabhängige Kontrollfunktion einrichten. Die für Bekämpfung von Geldwäsche/Terrorismusfinanzierung zuständige Person sollte erforderlichenfalls in der Lage sein, dem Leitungsorgan in seiner Leitungs- und in seiner Aufsichtsfunktion direkt Bericht zu erstatten.

17.1 Leiter der internen Kontrollfunktionen

153. Die Leiter der internen Kontrollfunktionen sollten auf einer angemessenen Hierarchiestufe angesiedelt sein, die dem Leiter der Kontrollfunktion angemessene Befugnisse und ausreichendes Gewicht verleiht, die für die Erfüllung seiner Zuständigkeiten notwendig sind. De Leiter der Compliance, und sofern eingerichtet, die Leiter der Risikomanagementfunktion und der internen Revision sollten dem Leitungsorgan Bericht erstatten und diesem direkt unterstellt sein, und ihre Leistung sollte vom Leitungsorgan überprüft werden.

154. Falls notwendig, sollten die Leiter der internen Kontrollfunktionen in der Lage sein, sich direkt an das Leitungsorgan in seiner Aufsichtsfunktion zu wenden und diesem Bericht zu erstatten, um Bedenken zu äußern und die Aufsichtsfunktion gegebenenfalls zu warnen, wenn bestimmte Entwicklungen die Wertpapierfirma beeinträchtigen oder beeinträchtigen könnten. Dadurch sollten die Leiter der internen Kontrollfunktionen nicht davon abgehalten werden, auch innerhalb der regulären Berichtswege Bericht zu erstatten.

155. Die Wertpapierfirmen sollten über dokumentierte Prozesse verfügen, um die Position des Leiters einer internen Kontrollfunktion zu besetzen und ihm seine Zuständigkeiten zu entziehen. In keinem Fall sollten die Leiter von internen Kontrollfunktionen ohne die vorherige Zustimmung des Leitungsorgans in seiner Aufsichtsfunktion entlassen werden.

17.2 Unabhängigkeit der internen Kontrollfunktionen

156. Zur Wahrung der Unabhängigkeit der internen Kontrollfunktionen sollten folgende Bedingungen erfüllt sein:

    a. Die Mitarbeiter in Kontrollfunktionen nehmen keine operativen Aufgaben wahr, die in einen Tätigkeitsbereich fallen, der von den internen Kontrollfunktionen überwacht und kontrolliert werden soll, sofern nicht nachgewiesen wird, dass unter

Berücksichtigung der in Titel I für die Anwendung des Grundsatzes der Verhältnismäßigkeit aufgeführten Kriterien die internen Kontrollfunktionen weiterhin wirksam sind. In diesem Fall sollten die Wertpapierfirmen bewerten, ob die Wirksamkeit ihrer internen Kontrollfunktionen beeinträchtigt ist.

b. Gegebenenfalls sind sie in organisatorischer Hinsicht von den Geschäftstätigkeiten, die sie überwachen und kontrollieren sollen, getrennt;

c. die Vergütung der Mitarbeiter der internen Kontrollfunktionen sollte nicht an den Erfolg der Tätigkeiten gekoppelt sein, die von der internen Kontrollfunktion überwacht und kontrolliert werden, und sie sollte deren Objektivität auch nicht anderweitig beeinträchtigen können[28].

17.3 Ressourcen der internen Kontrollfunktionen

157. Die internen Kontrollfunktionen sollten über ausreichende Ressourcen verfügen. Unter Berücksichtigung des in Titel I dargelegten Grundsatzes der Verhältnismäßigkeit sollten sie über eine angemessene Zahl an qualifizierten Mitarbeitern (sowohl auf Ebene des Mutterunternehmens als auch der Tochterunternehmen) verfügen. Die Mitarbeiter sollten ihre Qualifikation fortlaufend aufrechterhalten und nach Bedarf Weiterbildungen absolvieren.

158. Die internen Kontrollfunktionen sollten angemessene IT-Systeme und Unterstützung zur Verfügung haben, mit Zugang zu internen und externen Informationen, die sie für die Wahrnehmung ihrer Aufgaben benötigen. Sie sollten Zugang zu allen erforderlichen Informationen hinsichtlich aller Geschäftsbereiche und relevanten risikobehafteten Tochterunternehmen haben, insbesondere mit Blick auf diejenigen, die möglicherweise wesentliche Risiken für die Wertpapierfirma erzeugen können.

18 Risikomanagementfunktion

159. Die Risikomanagementfunktion sollte die gesamte Wertpapierfirma abdecken. Die Risikomanagementfunktion sollte unter Berücksichtigung der in Titel I aufgeführten Kriterien für die Verhältnismäßigkeit über ausreichende Befugnisse, ausreichendes Gewicht und ausreichende Ressourcen verfügen, um die Risikorichtlinien und den Risikomanagementrahmen entsprechend Abschnitt 17 umzusetzen.

160. Die Risikomanagementfunktion sollte gegebenenfalls über direkten Zugang zum Leitungsorgan in seiner Aufsichtsfunktion und dessen Ausschüssen, sofern eingerichtet, insbesondere zum Risikoausschuss, verfügen.

[28] Siehe auch die Leitlinien der EBA für eine solide Vergütungspolitik, abrufbar unter https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

161. Die Risikomanagementfunktion sollte Zugang zu allen Geschäftsbereichen und sonstigen internen Einheiten, die das Potenzial zur Erzeugung von Risiken aufweisen, sowie zu relevanten Tochterunternehmen und verbundenen Unternehmen haben.

162. Die Mitarbeiter innerhalb der Risikomanagementfunktion sollten über ausreichende Kenntnisse, Fähigkeiten und Erfahrungen mit Blick auf die Techniken und Verfahren des Risikomanagements sowie Märkte und Produkte besitzen und Zugang zu regelmäßigen Weiterbildungen haben.

163. Die Risikomanagementfunktion sollte ein zentraler organisatorischer Bestandteil der Wertpapierfirma und so strukturiert sein, dass sie die Risikorichtlinien umsetzen und den Risikomanagementrahmen kontrollieren kann. Die Risikomanagementfunktion sollte eine Schlüsselrolle bei der Sicherstellung wirksamer Risikomanagementprozesse einer Wertpapierfirma spielen. Die Risikomanagementfunktion sollte in alle wichtigen Entscheidungen im Bereich des Risikomanagements aktiv eingebunden sein.

164. In einer Gruppe sollte die Risikomanagementfunktion im EU-Mutterunternehmen in der Lage sein, über eine gruppenweite ganzheitliche Übersicht über alle Risiken zu verfügen und sicherzustellen, dass die Risikostrategie eingehalten wird.

165. Die Risikomanagementfunktion sollte unabhängige einschlägige Informationen, Analysen und Expertenmeinungen über Risikopositionen bereitstellen und die Geschäftsbereiche oder internen Einheiten in allen risikopolitischen Fragestellungen beraten; zudem sollte sie das Leitungsorgan darüber informieren, ob diese Informationen und Empfehlungen mit der Risikostrategie und dem Risikoappetit der Wertpapierfirma in Einklang stehen. Die Risikomanagementfunktion kann Verbesserungen des Risikomanagementrahmens und Abhilfemaßnahmen empfehlen, um Verletzungen der Risikorichtlinien, -prozesse und -limite zu beheben.

18.1 Rolle der Risikomanagementfunktion im Hinblick auf Risikostrategie und Entscheidungen

166. Die Risikomanagementfunktion sollte frühzeitig und aktiv in die Erarbeitung einer Risikostrategie der Wertpapierfirma eingebunden werden, wobei sicherzustellen ist, dass die Wertpapierfirma über wirksame Verfahren im Bereich Risikomanagement verfügt. Die Risikomanagementfunktion sollte dem Leitungsorgan alle wichtigen risikobezogenen Informationen vorlegen, um es in die Lage zu versetzen, das Niveau des Risikoappetits der Wertpapierfirma festzulegen. Die Risikomanagementfunktion sollte die Stabilität und Nachhaltigkeit der Risikostrategie und des Risikoappetits bewerten. Sie sollte sicherstellen, dass der Risikoappetit angemessen in konkrete Risikolimite umgesetzt wird. Die Risikomanagementfunktion sollte die Risikostrategien der Geschäftsbereiche bewerten, einschließlich der von den Geschäftseinheiten vorgeschlagenen Ziele, und sollte eingebunden werden, bevor das Leitungsorgan eine Entscheidung bezüglich der Risikostrategien und des

Risikoappetits trifft. Die Ziele sollten plausibel sein und mit der Risikostrategie und dem Risikoappetit der Wertpapierfirma im Einklang stehen.

167. Durch die Einbindung der Risikomanagementfunktion in Entscheidungsprozesse sollte gewährleistet werden, dass Risikoerwägungen angemessen berücksichtigt werden. Die Verantwortung für die getroffenen Entscheidungen verbleibt jedoch bei den Geschäftsbereichen und internen Einheiten und letztlich beim Leitungsorgan.

18.2 Rolle der Risikomanagementfunktion bei wesentlichen Änderungen

168. Bevor Entscheidungen über wesentliche Änderungen von Prozessen oder Systemen oder die Durchführung außergewöhnlicher Transaktionen getroffen werden, sollte die Risikomanagementfunktion in die Bewertung der Auswirkungen solcher Änderungen und außergewöhnlicher Transaktionen auf das Gesamtrisiko der Wertpapierfirma und der Gruppe eingebunden werden und sollte ihre Feststellungen direkt dem Leitungsorgan berichten, bevor eine Entscheidung getroffen wird.

169. Die Risikomanagementfunktion sollte beurteilen, wie die ermittelten Risiken die Fähigkeit der Wertpapierfirma bzw. der Gruppe beeinträchtigen können, ihr Risikoprofil, ihre Liquidität und solide Eigenmittelausstattung unter normalen sowie unter widrigen Umständen zu steuern.

18.3 Rolle der Risikomanagementfunktion bei der Ermittlung, Messung, Beurteilung, Steuerung, Minderung, Überwachung und Berichterstattung von Risiken

170. Die Risikomanagementfunktion sollte sicherstellen, dass ein angemessener Risikomanagementrahmen vorhanden ist und alle Risiken von den zuständigen Einheiten der Wertpapierfirma ermittelt, beurteilt, gemessen, überwacht, gesteuert und ordnungsgemäß berichtet werden.

171. Die Risikomanagementfunktion sollte sicherstellen, dass die Ermittlung und Beurteilung nicht nur auf quantitativen Informationen oder Ergebnissen von Risikomodellen beruhen, sondern auch qualitative Ansätze berücksichtigt werden. Die Risikomanagementfunktion sollte das Leitungsorgan über die zugrunde gelegten Annahmen und potenziellen Mängel der Risikomodelle und -analysen informiert halten.

172. Die Risikomanagementfunktion sollte dafür Sorge tragen, dass Geschäfte mit verbundenen Unternehmen überprüft und die Risiken, die sich daraus für die Wertpapierfirma ergeben, erkannt und angemessen bewertet werden.

173. Die Risikomanagementfunktion sollte gewährleisten, dass alle ermittelten Risiken wirksam von den Geschäftsbereichen überwacht werden.

174. Die Risikomanagementfunktion sollte regelmäßig das tatsächliche Risikoprofil der Wertpapierfirma überwachen und es mit den strategischen Zielen und dem Risikoappetit der Wertpapierfirma abgleichen, damit das Leitungsorgan in seiner Leitungsfunktion entsprechende Entscheidungen treffen und das Leitungsorgan in seiner Aufsichtsfunktion die Entscheidungen kritisch hinterfragen kann.

175. Die Risikomanagementfunktion sollte Trends analysieren und neue oder entstehende Risiken sowie steigende Risiken erkennen, die sich aus sich ändernden Umständen und Bedingungen ergeben. Sie sollte außerdem regelmäßig die aktuellen Risikoergebnisse anhand der bisherigen Einschätzungen (d. h. Rückvergleiche) zur Bewertung und Verbesserung der Genauigkeit und Wirksamkeit des Risikomanagementprozesses überprüfen.

176. Die Risikomanagementfunktion sollte Möglichkeiten zur Risikominderung bewerten. Die Berichterstattung an das Leitungsorgan sollte vorgeschlagene geeignete Risikominderungsmaßnahmen enthalten.

18.4 Rolle der Risikomanagementfunktion bei Limiten

177. Die Risikomanagementfunktion sollte Verstöße gegen den Risikoappetit bzw. die Risikolimite unabhängig beurteilen (einschließlich einer Ermittlung der Ursache sowie Durchführung einer rechtlichen und wirtschaftlichen Analyse der tatsächlichen Kosten der Schließung, Verringerung oder Absicherung von Risikopositionen im Vergleich zu den potenziellen Kosten einer Fortführung). Die Risikomanagementfunktion sollte die betroffenen Geschäftsbereiche und das Leitungsorgan informieren und mögliche Maßnahmen empfehlen. Wenn der Verstoß wesentlich ist, sollte die Risikomanagementfunktion direkt an das Leitungsorgan in seiner Aufsichtsfunktion Bericht erstatten, unbeschadet der Tatsache, dass die Risikomanagementfunktion anderen internen Funktionen und Ausschüssen Bericht erstatten kann.

178. Die Risikomanagementfunktion sollte eine Schlüsselrolle dabei spielen, sicherzustellen, dass auf Grundlage ihrer Empfehlung eine Entscheidung auf der zuständigen Ebene getroffen, von den betroffenen Geschäftsbereichen eingehalten und dem Leitungsorgan sowie dem Risikoausschuss, sofern eingerichtet, angemessen berichtet wird.

18.5 Leiter der Risikomanagementfunktion

179. Sofern eingerichtet, sollte der Leiter der Risikomanagementfunktion dafür zuständig sein, umfassende und verständliche Informationen zu den Risiken zur Verfügung zu stellen und das Leitungsorgan zu beraten, um dieses in die Lage zu versetzen, das Gesamtrisikoprofil der Wertpapierfirma zu verstehen. Gleiches gilt für den Leiter der Risikomanagementfunktion einer Mutterwertpapierfirma im Hinblick auf die konsolidierte Ebene. Sofern keine unabhängige Funktion eingerichtet wurde, liegen die Zuständigkeiten des Leiters der Risikomanagementfunktion bei den Mitarbeitern, denen die Risikomanagementverfahren übertragen wurden, oder direkt bei den Mitgliedern des Leitungsorgans.

180. Der Leiter der Risikomanagementfunktion sollte über ausreichende Fachkenntnisse, Unabhängigkeit und Seniorität verfügen, um Entscheidungen, die die Risikoposition der Wertpapierfirma beeinflussen, zu hinterfragen. Sofern der Leiter der Risikomanagementfunktion kein Mitglied des Leitungsorgans ist, sollten Wertpapierfirmen unter Berücksichtigung des in Titel I dargelegten Grundsatzes der Verhältnismäßigkeit einen unabhängigen Leiter der Risikomanagementfunktion benennen, der keine Verantwortung für andere Funktionen trägt und direkt dem Leitungsorgan Bericht erstattet. Falls es unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach den Ausführungen in Titel I unverhältnismäßig ist, eine Person zu benennen, die ausschließlich die Aufgaben des Leiters der Risikomanagementfunktion wahrnimmt, kann diese Funktion mit der Rolle des Leiters der Compliance-Funktion kombiniert werden oder von einer anderen leitenden Person wahrgenommen werden, sofern kein Interessenkonflikt zwischen den wahrgenommenen Aufgaben besteht. In jedem Fall sollte diese Person über ausreichende Befugnisse, ausreichendes Gewicht und Unabhängigkeit verfügen (z. B. Leiter der Rechtsabteilung).

181. Der Leiter der Risikomanagementfunktion sollte in der Lage sein, von der Geschäftsführung und dem Leitungsorgan der Wertpapierfirma getroffene Entscheidungen zu hinterfragen, und Gründe für Einwände sollten formal dokumentiert werden. Sofern eine Wertpapierfirma dem Leiter der Risikomanagementfunktion ein Vetorecht gegen Entscheidungen (z. B. eine Kredit- oder Anlageentscheidung oder die Festlegung eines Limits) einräumen möchte, die auf Ebenen unterhalb des Leitungsorgans getroffen werden, sollte sie den Umfang eines solchen Vetorechts sowie die Eskalations- und Beschwerdeverfahren bestimmen und festlegen, wie das Leitungsorgan eingebunden wird.

182. Die Wertpapierfirmen sollten solide Prozesse für die Genehmigung von Entscheidungen einrichten, zu denen der Leiter der Risikomanagementfunktion eine negative Stellungnahme abgegeben hat. Das Leitungsorgan in seiner Aufsichtsfunktion sollte in der Lage sein, direkt mit dem Leiter der Risikomanagementfunktion über wichtige Risikofragen zu kommunizieren, darunter auch Entwicklungen, die möglicherweise nicht mit dem Risikoappetit und der Risikostrategie der Wertpapierfirma übereinstimmen.

19 Compliance-Funktion[29]

183. Die Wertpapierfirmen sollten eine ständige und wirksame Compliance-Funktion für die Steuerung von Compliance-Risiken einrichten und eine Person benennen, die für diese Funktion in der gesamten Wertpapierfirma zuständig ist (Compliance-Beauftragter). Die Compliance-Funktion, Richtlinien und Verfahren sollten auch mit Artikel 22 der Delegierten Verordnung (EU) 2017/565 der Kommission und den ESMA-Leitlinien zur Compliance-Funktion in Einklang stehen.

184. Die Funktion des Compliance-Beauftragten kann unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach den Ausführungen in Titel I mit der Rolle des Leiters der

[29] Dieser Abschnitt sollte unbeschadet der Leitlinien der ESMA zur Compliance-Funktion und in Verbindung mit diesen ausgelegt werden.

Risikomanagementfunktion kombiniert werden, oder falls es unverhältnismäßig ist, eine Person zu benennen, die ausschließlich diese Funktion wahrnimmt, von einer anderen leitenden Person (z. B. Leiter der Rechtsabteilung) wahrgenommen werden, sofern kein Interessenkonflikt zwischen den wahrgenommenen Aufgaben besteht.

185. Die Mitarbeiter der Compliance-Funktion sollten über ausreichende Kenntnisse, Fähigkeiten und Erfahrungen im Bereich Compliance und in den einschlägigen Verfahren verfügen sowie Zugang zu regelmäßigen Weiterbildungen haben.

186. Das Leitungsorgan in seiner Aufsichtsfunktion sollte die Umsetzung gut dokumentierter Compliance-Richtlinien überwachen, die allen Mitarbeitern kommuniziert werden sollten. Die Wertpapierfirmen sollten einen Prozess einrichten, um Änderungen der für ihre Tätigkeiten geltenden Gesetze und Rechtsvorschriften regelmäßig zu bewerten.

187. Die Compliance-Funktion sollte das Leitungsorgan zu den Maßnahmen beraten, die ergriffen werden sollten, um die Einhaltung der geltenden Gesetze, Regelungen, Verordnungen und Standards sicherzustellen, und die möglichen Auswirkungen von Änderungen im rechtlichen oder regulatorischen Umfeld auf die Geschäftstätigkeit der Wertpapierfirma und den Compliance-Rahmen bewerten.

188. Die Compliance-Funktion sollte sicherstellen, dass die Überwachung der Compliance im Rahmen eines strukturierten und genau definierten Compliance-Überwachungsprogramms erfolgt und die Compliance-Richtlinien eingehalten werden. Die Compliance-Funktion sollte dem Leitungsorgan Bericht erstatten und gegebenenfalls mit der Risikomanagementfunktion über das Compliance-Risiko der Wertpapierfirma und seine Steuerung kommunizieren. Die Compliance-Funktion und die Risikomanagementfunktion sollten zusammenarbeiten und, sofern angemessen, Informationen austauschen, um ihre jeweiligen Aufgaben wahrzunehmen. Den Feststellungen der Compliance-Funktion sollten das Leitungsorgan und die Risikomanagementfunktion bei Entscheidungsprozessen Rechnung tragen.

189. Wertpapierfirmen sollten angemessene Maßnahmen gegen interne oder externe Handlungen ergreifen, die Betrug, Geldwäsche/Terrorismusfinanzierung oder andere Finanzkriminalität sowie Disziplinarvergehen (z. B. Verletzung interner Verfahren oder Überschreitung von Limiten) erleichtern oder ermöglichen.

190. Die Wertpapierfirmen sollten dafür Sorge tragen, dass ihre Tochterunternehmen und Zweigniederlassungen Maßnahmen ergreifen, um sicherzustellen, dass ihre Tätigkeiten den regionalen Gesetzen und Rechtsvorschriften entsprechen. Sofern regionale Gesetze und Rechtsvorschriften der Anwendung strengerer Verfahren und Compliance-Systeme, die von der Gruppe eingeführt wurden, im Wege stehen, insbesondere wenn sie die Offenlegung und den Austausch erforderlicher Informationen zwischen Einheiten innerhalb der Gruppe behindern, sollten die Tochterunternehmen und Zweigniederlassungen den Compliance-Beauftragten bzw. Leiter der Compliance-Funktion des EU-Mutterunternehmens unterrichten.

20 Interne Revision

191. Sofern eingerichtet, sollte die interne Revision unabhängig sein und über ausreichend Befugnisse, Gewicht und Ressourcen verfügen. Insbesondere sollten Wertpapierfirmen dafür Sorge tragen, dass die Qualifikation der Mitarbeiter der internen Revision sowie deren Ressourcen, vor allem ihre Prüfungsinstrumente und Methoden für die Risikoanalyse, für die Größe und Standorte der Wertpapierfirma sowie die Art, den Umfang und die Komplexität der mit dem Geschäftsmodell, den Geschäftstätigkeiten, der Risikokultur und dem Risikoappetit der Wertpapierfirma einhergehenden Risiken, angemessen sind.

192. Die interne Revision sollte unabhängig von den von ihr geprüften Tätigkeiten sein. Daher sollte die interne Revision nicht mit anderen Funktionen kombiniert werden.

193. Die interne Revision sollte nach einem risikobasierten Ansatz unabhängige Prüfungen vornehmen und eine objektive Gewähr für die Compliance aller Tätigkeiten und Einheiten einer Wertpapierfirma, einschließlich der ausgelagerten Tätigkeiten, mit den Richtlinien und Verfahren der Wertpapierfirma und mit externen aufsichtlichen Anforderungen bieten. Jedes Unternehmen innerhalb der Gruppe sollte in den Zuständigkeitsbereich der internen Revision fallen.

194. Die interne Revision sollte nicht an der Konzeption, Auswahl, Festlegung oder Umsetzung konkreter interner Kontrollstrategien, -mechanismen und -verfahren oder Risikolimiten beteiligt sein. Dies sollte das Leitungsorgan in seiner Leitungsfunktion jedoch nicht davon abhalten, die interne Revision um Beiträge in Zusammenhang mit Risiken, internen Kontrollen und der Einhaltung von geltenden Vorschriften zu konsultieren.

195. Die interne Revision sollte bewerten, ob der interne Kontrollrahmen der Wertpapierfirma nach den Ausführungen in Abschnitt 15 sowohl wirksam als auch effizient sind. Insbesondere sollte die interne Revision Folgendes beurteilen:

    a. die Angemessenheit des Rahmenwerks für die interne Governance der Wertpapierfirma;

    b. den Umstand, ob bestehende Richtlinien und Verfahren nach wie vor angemessen sind und den gesetzlichen und aufsichtlichen Anforderungen sowie dem Risikoappetit und der Risikostrategie der Wertpapierfirma entsprechen;

    c. die Übereinstimmung der Verfahren mit den geltenden Gesetzen und Rechtsvorschriften sowie mit den Entscheidungen des Leitungsorgans;

    d. den Umstand, ob die Verfahren korrekt und wirksam umgesetzt werden (z. B. Compliance der Durchführung von Transaktionen, der Umfang des tatsächlich eingegangenen Risikos, usw.);

e. die Eignung, Qualität und Wirksamkeit der durchgeführten Kontrollen sowie die erfolgte Berichterstattung seitens der Geschäftseinheiten (erste Verteidigungslinie) sowie der Risikomanagementfunktion und Compliance-Funktion.

196. Die interne Revision sollte insbesondere die Integrität der Prozesse prüfen, damit die Zuverlässigkeit der Methoden und Techniken der Wertpapierfirma sowie die seinen internen Modellen zugrunde liegenden Annahmen und Informationsquellen (etwa Risikomodellierung und Bilanzierung) gewährleistet ist. Sie sollte ferner die Qualität und die Nutzung von Instrumenten für die qualitative Risikoermittlung und -bewertung und die zur Risikominderung ergriffenen Maßnahmen beurteilen.

197. Die interne Revision sollte über einen uneingeschränkten unternehmensweiten Zugang zu allen Aufzeichnungen, Dokumenten, Informationen und Gebäuden der Wertpapierfirma verfügen. Dies sollte den Zugang zu den Management-Informationssystemen und Protokollen aller Ausschüsse und Entscheidungsorgane einschließen.

198. Die interne Revision sollte nationale und internationale Normen des Berufsstandes einhalten. Ein Beispiel für die hier angeführten Normen des Berufsstandes sind die vom Institute of Internal Auditors (IIA) verfassten Standards.

199. Die Tätigkeit der internen Revision sollte entsprechend einem Prüfungsplan und einem detaillierten Prüfungsprogramm auf der Grundlage eines risikobasierten Ansatzes durchgeführt werden.

200. Mindestens einmal jährlich sollte ein interner Prüfungsplan auf der Grundlage der jährlichen Prüfungsziele der internen Revision erstellt werden. Der interne Prüfungsplan sollte vom Leitungsorgan genehmigt werden.

201. Alle Revisionsempfehlungen sollten Gegenstand eines formalen Mängelbeseitigungsverfahrens durch die jeweils zuständige Leitungsebene sein, um ihre wirksame und fristgerechte Mängelbeseitigung sicherzustellen und entsprechend Bericht zu erstatten.

Titel VI – Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs

202. Wertpapierfirmen sollten einen soliden Plan für die Aufrechterhaltung des Geschäftsbetriebs und die Wiederherstellung der Geschäftsabläufe erstellen, um in der Lage zu sein, den kontinuierlichen Dienstbetrieb aufrechtzuerhalten, und Verluste im Fall von schwerwiegenden Betriebsstörungen zu begrenzen.

203. Die Wertpapierfirmen können eine spezielle unabhängige Funktion für die Aufrechterhaltung des Geschäftsbetriebs einrichten.

204. Die Geschäftstätigkeit einer Wertpapierfirma hängt von verschiedenen entscheidenden Ressourcen (z. B. IT-Systeme, einschließlich Cloud-Diensten, Kommunikationssysteme, Stammpersonal und Gebäude) ab. Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs zielen darauf ab, die operativen, finanziellen, rechtlichen, Reputations- und sonstigen wesentlichen Folgen eines Versagens oder eines längeren Ausfalls dieser Ressourcen und der sich daraus ergebenden Unterbrechung der üblichen Geschäftsabläufe der Wertpapierfirma zu mindern. Weitere Risikomanagementmaßnahmen könnten darauf abzielen, die Wahrscheinlichkeit solcher Zwischenfälle zu verringern oder deren finanzielle Auswirkungen auf Dritte zu übertragen (z. B. im Rahmen einer Versicherung).

205. Bei der Einrichtung solider Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs sollte eine Wertpapierfirma eine sorgfältige Analyse der Risikofaktoren vornehmen und prüfen, inwieweit sie durch schwerwiegende Betriebsstörungen gefährdet ist, und deren potenzielle Auswirkungen (quantitativ und qualitativ) anhand von internen und/oder externen Daten und einer Szenario-Analyse bewerten. Diese Analyse sollte sich auf alle Geschäftsbereiche und internen Einheiten, einschließlich der Risikomanagementfunktion, oder Risikomanagementverfahren erstrecken und sollte deren Verflechtungen berücksichtigen. Die Ergebnisse der Analyse sollten einen Beitrag zur Definition der Prioritäten und Ziele bei der Wiederherstellung der Geschäftsabläufe der Wertpapierfirma leisten.

206. Auf der Grundlage der vorstehend genannten Analyse sollte eine Wertpapierfirma Folgendes einrichten:

    a. Notfallpläne sowie Pläne zur Aufrechterhaltung des Geschäftsbetriebs, damit eine Wertpapierfirma angemessen auf Notsituationen reagieren kann und in der Lage ist, seine wichtigsten Geschäftstätigkeiten im Fall einer Unterbrechung seiner üblichen Geschäftsabläufe aufrechtzuerhalten, und

    b. Pläne für die Wiederherstellung entscheidender kritischer Ressourcen, die die Wertpapierfirma in die Lage versetzen, innerhalb einer angemessenen Zeitspanne ihre üblichen Geschäftsabläufe wieder aufzunehmen. Restrisiken aufgrund potenzieller Geschäftsunterbrechungen sollten mit dem Risikoappetit der Wertpapierfirma vereinbar sein.

207. Notfallpläne, Pläne zur Aufrechterhaltung des Geschäftsbetriebs sowie Pläne zur Wiederherstellung sind zu dokumentieren und sorgfältig umzusetzen. Die Dokumentation sollte innerhalb der Geschäftsbereiche, internen Einheiten und der Risikomanagementfunktion für die für Risikomanagementverfahren zuständigen Mitarbeiter zugänglich und auf Systemen gespeichert sein, die physisch getrennt und im Fall einer Notsituation problemlos zugänglich sind. Dazu sollten geeignete Weiterbildungsmaßnahmen angeboten werden. Die Pläne sollten regelmäßig getestet und aktualisiert werden. Probleme oder Störungen, die sich bei den Tests ergeben, sollten dokumentiert und analysiert werden, und die Pläne sollten entsprechend überarbeitet werden.

Titel VII – Transparenz

208. Strategien, Richtlinien und Verfahren sollten allen betroffenen Mitarbeitern einer Wertpapierfirma mitgeteilt werden. Die Mitarbeiter einer Wertpapierfirma sollten die Richtlinien und die Verfahren, die mit ihren Aufgaben und Verantwortlichkeitsbereichen in Verbindung stehen, verstehen und befolgen.

209. Dementsprechend sollte das Leitungsorgan die betroffenen Mitarbeiter über die Richtlinien und die Strategien der Wertpapierfirma auf klare und einheitliche Art und Weise informieren, zumindest insoweit, dass sie ihre jeweiligen Aufgaben wahrnehmen können. Dies kann in Form von schriftlichen Leitlinien, Handbüchern oder anderweitig erfolgen.

210. Falls die zuständigen Behörden von den Mutterunternehmen nach Artikel 44 der Richtlinie (EU) 2019/2034 die jährliche Veröffentlichung einer Beschreibung der Rechtsstruktur und Unternehmensführung sowie der Organisationsstruktur der Gruppe von Wertpapierfirmen verlangen, sollten die Informationen alle Unternehmen innerhalb der Gruppenstruktur nach der Definition in Richtlinie 2013/34/EU[30] nach Ländern einschließen.

211. Die Veröffentlichung sollte mindestens Folgendes umfassen:

    a. eine Übersicht über die interne Organisation der Wertpapierfirma und die Gruppenstruktur nach der Definition in der Richtlinie 2013/34/EU sowie vorgenommener Änderungen, einschließlich der wichtigen Berichtswege und Zuständigkeiten;

    b. etwaige wesentliche Änderungen seit der letzten Veröffentlichung sowie das Datum der wesentlichen Änderung;

    c. neue Rechtsstrukturen, Strukturen der internen Governance oder der Organisation;

[30] Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (ABl. L 182 vom 29.6.2013, S. 19).

d. Informationen über die Struktur, Organisation und Mitglieder des Leitungsorgans, einschließlich der Zahl seiner Mitglieder und der Zahl der als unabhängig eingestuften Mitglieder, unter Angabe des Geschlechts und der Dauer des Mandats der einzelnen Mitglieder des Leitungsorgans;

e. die wichtigsten Zuständigkeiten des Leitungsorgans;

f. eine Aufstellung der Ausschüsse des Leitungsorgans in seiner Aufsichtsfunktion und ihrer Zusammensetzung;

g. eine Übersicht über die für die Wertpapierfirma und das Leitungsorgan geltenden Richtlinien für den Umgang mit Interessenkonflikten;

h. eine Übersicht über den internen Kontrollrahmen und

i. eine Übersicht über den Rahmen zur Aufrechterhaltung des Geschäftsbetriebs.

Anhang I – Bei der Entwicklung von Richtlinien zur internen Governance zu berücksichtigende Aspekte

Gemäß Titel III sollten Wertpapierfirmen die folgenden Aspekte bei der Dokumentation von Richtlinien und Regelungen zur internen Governance berücksichtigen:

1. Beteiligungsstruktur
2. Gruppenstruktur, falls zutreffend (rechtliche und funktionale Struktur)
3. Zusammensetzung und Arbeitsweise des Leitungsorgans
   a) Auswahlkriterien, einschließlich des Aspekts, wie Diversität berücksichtigt wird
   b) Zahl, Dauer des Mandats, Rotation, Alter
   c) unabhängige Mitglieder des Leitungsorgans
   d) geschäftsführende Mitglieder des Leitungsorgans
   e) nicht geschäftsführende Mitglieder des Leitungsorgans
   f) interne Aufgabenteilung, falls zutreffend
4. Struktur der internen Governance und Organisationsplan (gegebenenfalls mit Auswirkungen auf die Gruppe)
   a) Fachausschüsse
      i. Zusammensetzung
      ii. Arbeitsweise
   b) Exekutivausschuss, falls zutreffend
      i. Zusammensetzung
      ii. Arbeitsweise
5. Inhaber von Schlüsselfunktionen
   a) Leiter der Risikomanagementfunktion
   b) Leiter der Compliance-Funktion
   c) Leiter der internen Revision
   d) Finanzvorstand
   e) sonstige Inhaber von Schlüsselfunktionen
6. Interner Kontrollrahmen
   a) Beschreibung der einzelnen Funktionen, einschließlich ihrer Organisation, Ressourcen, ihres Gewichts und ihrer Befugnisse

7. Beschreibung der Risikostrategie und des Risikomanagementrahmens
8. Organisationsstruktur (gegebenenfalls mit Auswirkungen auf die Gruppe)
    a) Organisationsstruktur, Geschäftsbereiche und Zuweisung von Zuständigkeiten und Verantwortlichkeiten
    b) Auslagerung
    c) Spektrum an Produkten und Dienstleistungen
    d) geografischer Bereich der Geschäftstätigkeit
    e) Erbringung von Dienstleistungen im Rahmen des freien Dienstleistungsverkehrs
    f) Zweigniederlassungen
    g) Tochterunternehmen, Gemeinschaftsunternehmen usw.
    h) Nutzung von Offshore-Zentren
9. Verhaltenskodex und Verhalten (gegebenenfalls mit Auswirkungen auf die Gruppe)
    a) strategische Ziele und Werte des Unternehmens
    b) interne Kodizes und Regelungen, einschließlich Richtlinien zur Bekämpfung von Geldwäsche und Terrorismusbekämpfung
    c) Richtlinien für den Umgang mit Interessenkonflikten
    d) Hinweisgeberverfahren (Whistleblowing)
10. Stand der Strategie zur internen Governance, mit Datum
    a) Entwicklung
    b) letzte Änderung
    c) letzte Bewertung
    d) Genehmigung durch das Leitungsorgan