EBA/GL/2021/05

2. Juli 2021

Leitlinien

zur internen Governance

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 Institute, alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

2. Leitlinien legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Die zuständige Behörde im Sinne von Artikel 4 Absatz 2 der Verordnung (EU) Nr. 1093/2010 sollte die für sie geltenden Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken integrieren (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren), und zwar einschließlich der Leitlinien, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 muss die zuständige Behörde der EBA bis zum (05.12.2021) mitteilen, ob sie diesen Leitlinien nachkommt oder nachzukommen beabsichtigt, oder die Gründe nennen, warum sie dies nicht tut. Geht innerhalb der genannten Frist keine Meldung 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/2021/05“ an compliance@eba.europa.eu zu senden. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln. 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 die internen Regelungen, Prozesse und Mechanismen für die interne Governance präzisiert, die Institute, die der Richtlinie 2013/36/EU[2] unterliegen, sowie Wertpapierfirmen, für die Titel VII der Richtlinie 2013/36/EU bei der Anwendung von Artikel 1 Absätze 2 und 5 der Verordnung (EU) 2019/2033 gilt, gemäß Artikel 74 Absatz 1 der Richtlinie 2013/36/EUR einführen sollten, um ein wirksames und umsichtiges Management sicherzustellen.

Adressaten

Diese Leitlinien richten sich an zuständige Behörden im Sinne von Artikel 4 Absatz 2 Ziffer i der Verordnung (EU) Nr. 1093/2010 und an Finanzinstitute im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010, die entweder Institute für die Zwecke der Anwendung von Richtlinie 2013/36/EU nach der Definition in Artikel 3 Absatz 1 Ziffer 3 der Richtlinie 2013/36/EU bei gleichzeitiger Berücksichtigung von Artikel 3 Absatz 3 dieser Richtlinie oder Wertpapierfirmen sind, die Titel VII der Richtlinie 2013/36/EU in Anwendung von Artikel 1 Absätze 2 und 5 der Verordnung (EU) 2019/2033 („Institute“) sind.

Anwendungsbereich

6. Die vorliegenden Leitlinien gelten für die Governance-Regelungen der Institute, einschließlich ihrer Organisationsstruktur und der entsprechenden Verantwortungsbereiche, Verfahren zur Ermittlung, Steuerung, Überwachung und Meldung aller tatsächlichen und potenziellen künftigen Risiken[3], und die internen Kontrollrahmen.

7. Die Leitlinien sollen sämtliche vorhandenen Unternehmensführungsstrukturen 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 Unternehmensführungsstruktur (monistisches und/oder dualistisches Gesellschaftsmodell und/oder eine andere Struktur) angewandt werden. Das Leitungsorgan nach der Definition in

[2] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176, 27.6.2013, S. 338).

[3] Jeder Verweis auf Risiken in diesen Leitlinien sollte Risiken bezüglich Geldwäsche und Terrorismusfinanzierung umfassen.

Artikel 3 Absatz 1 Ziffern 7 und 8 der Richtlinie 2013/36/EU ist so zu verstehen, dass es (geschäftsführende) Leitungs- und (nicht geschäftsführende) Aufsichtsfunktionen ausübt[4].

8. Die Begriffe „Leitungsorgan in seiner Leitungsfunktion“ und „Leitungsorgan in seiner Aufsichtsfunktion“ werden in diesen Leitlinien verwendet, ohne auf eine bestimmte Unternehmensführungsstruktur 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.

9. In Mitgliedstaaten, in denen das Leitungsorgan die geschäftsführenden Funktionen ganz oder teilweise an eine Person oder ein internes Exekutivorgan überträgt (z. B. Vorsitzender des Leitungsorgans in seiner Leitungsfunktion (CEO), Führungsteam oder Exekutivausschuss), sollten die Personen, die diese geschäftsführenden Funktionen auf Grundlage der Übertragung ausüben, als Leitungsfunktion des Leitungsorgans verstanden werden. Im Sinne dieser Leitlinien ist jeder Verweis 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 Leitungsorgan oder der Leitungsorgane vorgeschlagen oder bestellt worden sind.

10. In Mitgliedstaaten, in denen manche Verantwortlichkeiten direkt von den Anteilseignern, Gesellschaftern oder Eigentümern des Instituts an Stelle des Leitungsorgans ausgeübt werden, sollten die Institute sicherstellen, dass solche Verantwortlichkeiten und die entsprechenden Entscheidungen soweit möglich mit den für das Leitungsorgan geltenden Leitlinien in Einklang stehen.

11. 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.

12. Die Institute sollten diesen Leitlinien auf Einzel-, teilkonsolidierter und konsolidierter Basis gemäß der in Artikel 109 der Richtlinie 2013/36/EU festgelegten Anwendungsebene nachkommen, und die Einhaltung sollte durch die zuständigen Behörden sichergestellt werden.

[4] Siehe auch Erwägungsgrund 56 der Richtlinie 2013/36/EU.

Begriffsbestimmungen

13. Sofern nicht anders angegeben, haben die in der Richtlinie 2013/36/EU und der Verordnung (EU) Nr. 575/2013 verwendeten und definierten Begriffe in diesen Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

Aufsichtliche Konsolidierung	Die Anwendung der Aufsichtsvorschriften gemäß der Richtlinie 2013/36/EU und der Verordnung (EU) Nr. 575/2013 auf konsolidierter oder teilkonsolidierter Basis in Einklang mit Teil 1 Titel 2 Kapitel 2 der Verordnung (EU) Nr. 575/2013.[5]
Inhaber von Schlüsselfunktionen	Personen, die erheblichen Einfluss auf die Ausrichtung des Instituts haben, aber keine Mitglieder des Leitungsorgans und kein CEO sind. Zu ihnen zählen die Leiter der internen Kontrollfunktionen und der Finanzvorstand, sofern diese nicht Mitglieder des Leitungsorgans sind, sowie weitere Inhaber von Schlüsselfunktionen, die auf Grundlage eines risikobasierten Ansatzes von den Instituten als solche ermittelt werden. Weitere Inhaber von Schlüsselfunktionen können die Leiter von Geschäftsbereichen, Zweigniederlassungen im Europäischen Wirtschaftsraum (EWR)/der Europäischen Freihandelsassoziation (EFTA), Tochtergesellschaften in Drittstaaten oder anderer interner Funktionen sein.
Leiter der internen Kontrollfunktionen	Die Personen, die auf der höchsten Hierarchieebene für die wirksame Wahrnehmung der täglichen Aufgaben der unabhängigen Risikomanagementfunktion, Compliance-Funktion und internen Revision verantwortlich sind.
Lohngefälle zwischen Frauen und Männern	Differenz zwischen dem durchschnittlichen Bruttostundenverdienst von Männern und Frauen, ausgedrückt als Prozentsatz des durchschnittlichen Bruttostundenverdiensts von Männern.
Konsolidierendes Institut	Institut, das die Aufsichtsanforderungen auf der Grundlage der konsolidierten Lage gemäß Teil 1 Titel 2 Kapitel 2 der Verordnung (EU) Nr. 575/2013 befolgen muss.
Institute von erheblicher Bedeutung	Die in Artikel 131 der Richtlinie 2013/36/EU erwähnten Institute (global systemrelevante Institute oder „G-SRI“ und andere systemrelevante Institute oder „A-SRI“) sowie gegebenenfalls andere Institute, die von der zuständigen Behörde oder im nationalen Recht auf der Grundlage einer Bewertung der Größe,

[5] Siehe auch technische Regulierungsstandards zur aufsichtlichen Konsolidierung: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

	internen Organisation und der Art, des Umfangs und der Komplexität der Tätigkeiten der Institute bestimmt werden.
Börsennotiertes Institut	Institute, 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].
Anteilseigner	Person, die Anteile an einem Institut hält, bzw. abhängig von der Rechtsform eines Instituts andere Eigentümer oder Gesellschafter des Instituts.
Leitungs- oder Aufsichtsmandate	Eine Position als Mitglied eines Leitungsorgans eines Instituts oder einer anderen juristischen Person.
Risikoappetit	Das Gesamtrisikoniveau und die Arten von Risiken, die ein Institut bereit ist, innerhalb seiner Risikotragfähigkeit und in Einklang mit seinem Geschäftsmodell zum Erreichen seiner strategischen Ziele einzugehen.
Risikotragfähigkeit	Das maximale Risiko, das ein Institut angesichts seiner Eigenmittelausstattung, seiner Risikomanagement- und Kontrollkapazitäten sowie seiner regulatorischer Beschränkungen eingehen kann.
Risikokultur	Die Normen, Einstellung und Verhaltensweisen eines Instituts in 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.
Mitarbeiter	Alle Beschäftigten eines Instituts und seiner Tochtergesellschaften innerhalb seines Konsolidierungskreises, einschließlich Tochtergesellschaften, die nicht der Richtlinie 2013/36/EU unterliegen, sowie alle Mitglieder des Leitungsorgans in seiner Leitungsfunktion und in seiner Aufsichtsfunktion.
Vorsitzender des Leitungsorgans in seiner Leitungsfunktion (CEO)	Die Person, die für die Leitung und Steuerung der allgemeinen Geschäftstätigkeiten eines Instituts zuständig ist.
Finanzvorstand (CFO)	Die Person, die die Gesamtverantwortung für die Leitung sämtlicher der folgenden Tätigkeiten trägt: Verwaltung der Finanzmittel, Finanzplanung und Rechnungslegung.

[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).

3. Umsetzung

Umsetzungsfrist

14. Diese Leitlinien gelten ab dem 31. Dezember 2021.

Aufhebung

15. Die am 26. September 2017 veröffentlichten Leitlinien der Europäischen Bankenaufsichtsbehörde zur internen Governance (EBA/GL/2017/11) werden zum 31. Dezember 2021 aufgehoben.

4. Leitlinien

Titel I – Verhältnismäßigkeit

16. Der in Artikel 74 Absatz 2 der Richtlinie 2013/36/EU verankerte Grundsatz der Verhältnismäßigkeit stellt sicher, dass die internen Governance-Regelungen mit dem individuellen Risikoprofil und dem Geschäftsmodell des Instituts im Einklang stehen, sodass die aufsichtsrechtlichen Anforderungen und Vorschriften wirksam umgesetzt werden.

17. Die Institute sollten ihre Größe und interne Organisation sowie die Art, den Umfang und die Komplexität ihrer Geschäfte bei der Erarbeitung und Umsetzung interner Governance-Regelungen berücksichtigen. Institute von erheblicher Bedeutung sollten über ausdifferenziertere Governance-Regelungen verfügen, während kleine und weniger komplexe Institute einfachere Governance-Regelungen einführen können. Institute sollten jedoch beachten, dass die Größe oder systemische Bedeutung eines Instituts für sich allein hinsichtlich des Umfangs, in dem ein Institut Risiken ausgesetzt ist, nicht aussagekräftig ist.

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

    a. die Größe in Bezug auf die Bilanzsumme des Instituts und seiner Tochtergesellschaften im Anwendungsbereich des aufsichtlichen Konsolidierungskreises;

    b. die geografische Präsenz des Instituts und der Umfang seiner Tätigkeiten in den einzelnen Rechtsordnungen;

    c. die Rechtsform des Instituts, einschließlich der Tatsache, ob das Institut zu einer Gruppe gehört, und gegebenenfalls die für die Gruppe vorgenommene Bewertung der Verhältnismäßigkeit;

    d. die Tatsache, ob das Institut börsennotiert ist;

    e. die Tatsache, ob das Institut zur Verwendung von internen Modellen für die Messung der Kapitalanforderungen befugt ist (z. B. der auf internen Beurteilungen basierende Ansatz);

    f. die Art der zugelassenen Tätigkeiten und Dienstleistungen des Instituts (siehe beispielsweise auch Anhang 1 der Richtlinie 2013/36/EU und Anhang 1 der Richtlinie 2014/65/EU);

g. das zugrunde liegende Geschäftsmodell und die Strategie, die Art und Komplexität der Geschäftstätigkeiten und die Organisationsstruktur des Instituts;

h. die Risikostrategie, der Risikoappetit und das tatsächliche Risikoprofil des Instituts, auch unter Berücksichtigung der Ergebnisse der SREP-Kapital- und SREP-Liquiditätsbewertungen;

i. die Beteiligungsverhältnisse und die Finanzierungsstruktur des Instituts;

j. die Art der Kunden (z. B. Privat-, Unternehmenskunden, institutionelle Kunden, Kleinunternehmen, öffentliche Stellen) und die Komplexität der Produkte oder Verträge;

k. die ausgelagerten Funktionen und Vertriebskanäle;

l. die bestehenden informationstechnischen Systeme (IT-Systeme), einschließlich der Systeme für einen unterbrechungsfreien Geschäftsbetrieb und der Auslagerung von Funktionen in diesem Bereich; und

m. die Tatsache, ob Institute unter die Definition in Artikel 4 Absatz 1 Ziffern 145 und 146 der Verordnung (EU) Nr. 575/2013 eines kleinen und nicht komplexen Instituts oder eines großen Instituts fallen.

Titel II – Rolle und Zusammensetzung des Leitungsorgans und der Ausschüsse

1 Rolle und Pflichten des Leitungsorgans

19. Gemäß Artikel 88 Absatz 1 der Richtlinie 2013/36/EU muss das Leitungsorgan die Letzt- und die Gesamtverantwortung für das Institut tragen und ist verantwortlich für die Definition und Implementierung von Governance-Regelungen innerhalb des Instituts sowie die Überwachung ihrer Anwendung, um die wirksame und umsichtige Führung des Instituts zu gewährleisten.

20. 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 seiner Ausschüsse voll und ganz bewusst sein.

21. 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.

22. Die Zuständigkeiten des Leitungsorgans sollten die Festlegung, Genehmigung und die Überwachung der Umsetzung der folgenden Aspekte umfassen:

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

    b. die allgemeine Risikostrategie, der Risikoappetit des Instituts und sein Risikomanagementrahmen sowie Maßnahmen zur Sicherstellung, dass das Leitungsorgan Risikofragen und Fragen des Risikomanagements ausreichend Zeit widmet;

    c. ein angemessener und wirksamer Rahmen für die interne Governance und die interne Kontrolle nach der Definition in Titel V:

        i. der eine klare Organisationsstruktur und ein gut funktionierendes unabhängiges internes Risikomanagement, eine Compliance-Funktion und eine interne Revision umfasst, die über ausreichende Befugnisse, Gewicht und Ressourcen verfügen;

        ii. die Einhaltung der anwendbaren aufsichtlichen Anforderungen im Rahmen der Verhinderung von Geldwäsche und Terrorismusfinanzierung;

    d. die Beträge, Arten und Verteilung des internen Kapitals und des regulatorischen Eigenkapitals zur angemessenen Absicherung der Risiken des Instituts;

    e. Ziele für das Liquiditätsmanagement des Instituts;

    f. eine Vergütungspolitik, die mit den in den Artikeln 92 bis 95 der Richtlinie 2013/36/EU und den EBA-Leitlinien für eine solide Vergütungspolitik gemäß Artikel 74 Absatz 3 und Artikel 75 Absatz 2 der Richtlinie 2013/36/EU in Einklang steht[7];

    g. Regelungen, die auf die Sicherstellung abzielen, dass die Beurteilung 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];

[7] EBA-Leitlinien für eine solide Vergütungspolitik.

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

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

i. 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;

j. eine Risikokultur in Einklang mit Abschnitt 9 dieser Leitlinien, die auf das Risikobewusstsein und das Risikoverhalten des Instituts ausgerichtet ist;

k. eine Unternehmenskultur und Unternehmenswerte in Einklang mit Abschnitt 10, durch die verantwortliches und ethisches Verhalten gefördert wird, einschließlich eines Verhaltenskodex oder eines ähnlichen Instruments;

l. Richtlinien für den Umgang mit Interessenkonflikten auf institutioneller Ebene in Einklang mit Abschnitt 11 und für die Mitarbeiter in Einklang mit Abschnitt 12 sowie

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

23. Bei der Festlegung, Genehmigung und Kontrolle der Umsetzung der in Absatz 22 aufgeführten Aspekte sollte das Leitungsorgan darauf abzielen, ein Geschäftsmodell und Governance-Regelungen, einschließlich eines Risikomanagementrahmens, sicherzustellen, bei denen allen Risiken Rechnung getragen wird. Bei der Berücksichtigung aller Risiken, denen Institute ausgesetzt sind, sollten die Institute allen einschlägigen Risikofaktoren Rechnung tragen, einschließlich umweltbezogener, sozialer und governancebezogener Risikofaktoren. Institute sollten berücksichtigen, dass Letztere ihre aufsichtlichen Risiken verstärken können, einschließlich Kreditausfallrisiken, z. B. über Risikofaktoren in Zusammenhang mit dem Übergang zu einer nachhaltigen Wirtschaft oder externen physischen klimabezogenen Ereignissen, die Schuldner, Marktrisiken, Liquiditätsrisiken, operationelle Risiken und auch Reputationsrisiken betreffen können, etwa im Zuge von sozialen oder governancebezogenen Risikofaktoren, z. B. im Rahmen von Auslagerungsvereinbarungen[10]. Zu diesen Risiken zählen

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

[10] Im EBA-Bericht über das Management und die Beaufsichtigung von ESG-Risiken im Rahmen von Artikel 98 Absatz 8 der CRD 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.

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.

24. Das Leitungsorgan muss die Offenlegung und die Kommunikation mit externen Interessenträgern und den zuständigen Behörden überwachen.

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

26. Ein Mitglied des Leitungsorgans kann für eine interne Kontrollfunktion entsprechend Titel V Abschnitt 19.1 zuständig sein, sofern das Mitglied keine sonstigen Aufgaben wahrnimmt, durch die die internen Kontrolltätigkeiten des Mitglieds und die Unabhängigkeit der internen Kontrollfunktion beeinträchtigt würden.

27. Das Leitungsorgan sollte etwaige Schwachstellen, die mit Blick auf die Umsetzung von Prozessen, Strategien und Maßnahmen in Zusammenhang mit den in den Absätzen 22 und 23 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 das Institut von wesentlichen Änderungen betroffen ist.

2 Leitungsfunktion des Leitungsorgans

28. Das Leitungsorgan in seiner Leitungsfunktion sollte sich aktiv an der Geschäftstätigkeit eines Instituts beteiligen und Entscheidungen auf einer fundierten und sachkundigen Grundlage treffen.

29. Das Leitungsorgan in seiner Leitungsfunktion sollte 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 des Instituts vorgenommen werden.

30. Das Leitungsorgan in seiner Leitungsfunktion sollte vorgelegte Vorschläge, Erklärungen und Informationen bei seiner Ermessensausübung und Entscheidungsfindung kritisch hinterfragen und überprüfen. Das Leitungsorgan in seiner Leitungsfunktion sollte 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 das Institut auswirken oder auswirken könnten, z. B. wesentliche Entscheidungen zur Geschäftstätigkeit oder eingegangene Risiken, die Bewertung der wirtschaftlichen und geschäftlichen Rahmenbedingungen des Instituts, die Liquidität und solide Eigenkapitalausstattung sowie die Bewertung seiner wesentlichen Risikopositionen informieren.

31. Ungeachtet der nationalen Umsetzung der Richtlinie 2015/849/EU sollte das Leitungsorgan eines seiner Mitglieder in Einklang mit den Anforderungen nach Artikel 46 Absatz 4 der Richtlinie zur Bekämpfung der Geldwäsche (AMLD) (Richtlinie 2015/849/EU) bestimmen, das zur 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 dem Institut und auf Ebene des Leitungsorgans[11].

3 Aufsichtsfunktion des Leitungsorgans

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

33. 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.

34. Unbeschadet der nach dem anwendbaren 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 des Instituts;

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

[11] Das Leitungsorgan als Kollegialorgan trägt weiterhin die Verantwortung insgesamt.

c. Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach den Ausführungen in Titel I, angemessene Erfüllung der Pflichten und Funktionen des Risikoausschusses, des Vergütungsausschusses und des Nominierungsausschusses, wenn solche Ausschüsse nicht eingerichtet worden sind;

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

e. Beaufsichtigung und Überwachung, dass die strategischen Ziele, die Organisationsstruktur und Risikostrategie des Instituts, seines Risikoappetits und des Risikomanagement-Rahmens sowie sonstige Richtlinien (z. B. die Vergütungspolitik) und die Offenlegungsvorschriften durchgehend umgesetzt werden;

f. Überwachung, dass die Risikokultur des Instituts 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 Risikomanagement-Rahmens;

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 das Institut beeinträchtigen oder beeinträchtigen können; sowie

j. Überwachung der Umsetzung des Prüfungsplans der internen Revision nach vorheriger Einbeziehung des Risiko- und des Prüfungsausschusses, sofern solche Ausschüsse eingerichtet sind.

4 Rolle des Vorsitzes des Leitungsorgans

35. 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.

36. 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.

37. Grundsätzlich sollte der Vorsitz des Leitungsorgans ein nicht geschäftsführendes Mitglied sein. Falls es dem Vorsitz gestattet ist, geschäftsführende Aufgaben wahrzunehmen, sollte das Institut Maßnahmen ergreifen, um nachteilige Auswirkungen auf die Kontrollen und Gegenkontrollen des Instituts 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). Insbesondere im Einklang mit Artikel 88 Absatz 1 Buchstabe e der Richtlinie 2013/36/EU darf der Vorsitz des Leitungsorgans eines Instituts in seiner Aufsichtsfunktion in diesem Institut nicht gleichzeitig die Funktion eines CEO ausüben, es sei denn, dies wird von dem Institut begründet und von den zuständigen Behörden genehmigt.

38. 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.

39. 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

40. In Einklang mit Artikel 109 Absatz 1 der Richtlinie 2013/36/EU in Verbindung mit Artikel 76 Absatz 3, Artikel 88 Absatz 2 und Artikel 95 Absatz 1 der Richtlinie 2013/36/EU müssen alle Institute, die auf Einzel-, teilkonsolidierter und konsolidierter Basis selbst von erheblicher Bedeutung sind, einen Risiko-, einen Nominierungs-[12] und einen Vergütungsausschuss[13] einrichten, die das Leitungsorgan in seiner Aufsichtsfunktion beraten und die von diesem Organ zu treffenden Entscheidungen vorbereiten. Institute, die nicht von erheblicher Bedeutung sind, auch wenn sie zum aufsichtlichen Konsolidierungskreis eines Instituts gehören, das auf teilkonsolidierter oder konsolidierter Ebene von erheblicher Bedeutung ist, sind nicht verpflichtet, diese Ausschüsse einzurichten.

[12] 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.

[13] Hinsichtlich des Vergütungsausschusses wird auf die EBA-Leitlinien für eine solide Vergütungspolitik verwiesen.

41. Falls kein Risiko- oder Nominierungsausschuss eingerichtet ist, sind die Verweise auf diese Ausschüsse in den vorliegenden Leitlinien so auszulegen, dass sie für das Leitungsorgan in seiner Aufsichtsfunktion gelten, wobei der Grundsatz der Verhältnismäßigkeit entsprechend den Ausführungen in Titel I zu berücksichtigen ist.

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

43. Die Institute sollten eine klare Zuweisung und Aufteilung von Pflichten und Aufgaben zwischen den Fachausschüssen des Leitungsorgans sicherstellen.

44. Jeder Ausschuss sollte vom Leitungsorgan in seiner Aufsichtsfunktion ein dokumentiertes Mandat, einschließlich des Umfangs seiner Zuständigkeiten, erhalten und geeignete Arbeitsverfahren einrichten.

45. 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 entbindet das Leitungsorgan in seiner Aufsichtsfunktion keinesfalls von der kollektiven Erfüllung seiner Aufgaben und Pflichten.

5.2 Zusammensetzung der Ausschüsse[14]

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

47. Unabhängige Mitglieder[15] des Leitungsorgans in seiner Aufsichtsfunktion sollten aktiv in diese Ausschüsse eingebunden sein.

48. Sofern Ausschüsse gemäß der Richtlinie 2013/36/EU oder nach nationalem Recht eingerichtet werden müssen, sollten sich diese aus mindestens drei Mitgliedern zusammensetzen.

49. Die Institute sollten unter Berücksichtigung der Größe des Leitungsorgans und der Zahl der unabhängigen Mitglieder des Leitungsorgans in seiner Aufsichtsfunktion sicherstellen, dass sich die Ausschüsse jeweils nicht aus der gleichen Gruppe von Mitgliedern zusammensetzen, die einen anderen Ausschuss bilden.

50. Die Institute sollten eine gelegentliche Rotation der Vorsitzenden und Mitglieder von Ausschüssen in Betracht ziehen, wobei die spezifische Erfahrung, Kenntnisse und Fähigkeiten zu berücksichtigen sind, die individuell oder kollektiv für diese Ausschüsse erforderlich sind.

[14] 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.

[15] 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.

51. Der Risikoausschuss und der Nominierungsausschuss sollten sich aus nicht geschäftsführenden Mitgliedern des Leitungsorgans in seiner Aufsichtsfunktion des betreffenden Instituts zusammensetzen. Die Zusammensetzung des Prüfungsausschusses sollte den Bestimmungen in Artikel 41 der Richtlinie 2006/43/EG [16] entsprechen. Die Zusammensetzung des Vergütungsausschusses sollte den Bestimmungen in Abschnitt 2.4.1 der EBA-Leitlinien für eine solide Vergütungspolitik[17] entsprechen.

52. Bei G-SRI und A-SRI sollten dem Nominierungsausschuss mehrheitlich unabhängige Mitglieder angehören und der Vorsitz von einem unabhängigen Mitglied geführt werden. Bei anderen Instituten von erheblicher Bedeutung, die von den zuständigen Behörden oder nach nationalem Recht bestimmt werden, sollte dem Nominierungsausschuss eine ausreichende Zahl von unabhängigen Mitgliedern angehören; solche Institute können es auch als gute Verfahrenspraxis betrachten, wenn der Nominierungsausschuss von einem unabhängigen Vorsitzenden geführt wird.

53. Mitglieder des Nominierungsausschusses sollten individuell und kollektiv über ausreichende Kenntnisse, Fähigkeiten und Erfahrung betreffend das Auswahlverfahren und die Anforderungen an die Angemessenheit in Einklang mit der Richtlinie 2013/36/EU verfügen.

54. Bei G-SRI und A-SRI sollten dem Risikoausschuss mehrheitlich unabhängige Mitglieder angehören. Bei G-SRI und A-SRI sollte der Vorsitz des Risikoausschusses von einem unabhängigen Mitglied geführt werden. Bei anderen Instituten von erheblicher Bedeutung, die von den zuständigen Behörden oder nach nationalem Recht bestimmt werden, sollte dem Risikoausschuss eine ausreichende Zahl von unabhängigen Mitgliedern angehören und der Vorsitz des Risikoausschusses sollte, sofern möglich, von einem unabhängigen Mitglied wahrgenommen werden. In allen Instituten sollte der Vorsitzende des Risikoausschusses weder der Vorsitzende des Leitungsorgans noch der Vorsitzende eines anderen Ausschusses sein.

55. Die Mitglieder des Risikoausschusses sollten individuell und kollektiv über ausreichende Kenntnisse, Fähigkeiten und Erfahrung betreffend das Risikomanagement und die Kontrollverfahren verfügen.

5.3 Verfahren der Ausschüsse

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

57. Die Ausschüsse sollten soweit angemessen zusammenwirken und -arbeiten. Unbeschadet des Absatzes 49 könnte ein solches Zusammenwirken in der Form einer übergreifenden

[16] Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates (ABl. L 157 vom 9.6.2006, S. 87), zuletzt geändert durch die Richtlinie 2014/56/EU des Europäischen Parlaments und des Rates vom 16. April 2014.

[17] EBA-Leitlinien für eine solide Vergütungspolitik gemäß Artikel 74 Absatz 3 und Artikel 75 Absatz 2 der Richtlinie 2013/36/EU und Angaben gemäß Artikel 450 der Verordnung (EU) Nr. 575/2013 (EBA/GL/2015/22).

Mitwirkung erfolgen, sodass der Vorsitzende oder ein Mitglied eines Ausschusses auch Mitglied eines anderen Ausschusses sein kann.

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

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

60. Der Risiko- und der Nominierungsausschuss sollte mindestens:

    a. Zugang zu allen maßgeblichen Informationen und Daten haben, die für die Wahrnehmung ihrer jeweiligen Funktion erforderlich sind, darunter Informationen und Daten von relevanten Unternehmens- und Kontrollfunktionen (z. B. Recht, Finanzen, Personal, IT, interne Revision, Risiko, Compliance, einschließlich 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 des Instituts, seine Risikokultur und Risikolimite sowie über jegliche wesentliche Verstöße[18], die 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; sowie

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

5.4 Rolle des Risikoausschusses

61. Sofern eingerichtet, sollte der Risikoausschuss mindestens

    a. das Leitungsorgan in seiner Aufsichtsfunktion bezüglich der Überwachung der tatsächlichen und künftigen Risikostrategie sowie des Risikoappetits des Instituts insgesamt beraten und unterstützen, wobei allen Arten von Risiken Rechnung zu

[18] Mit Blick auf gravierende Verstöße im Bereich Geldwäsche/Terrorismusfinanzierung. Weiterführende Informationen finden sich 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.

tragen ist, um sicherzustellen, dass diese mit der Geschäftsstrategie, den Zielen, der Unternehmenskultur und Werten des Instituts in Einklang stehen;

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

c. die Umsetzung der Strategien für das Kapital- und Liquiditätsmanagement sowie für alle anderen relevanten Risiken eines Instituts überwachen, wie etwa Marktrisiken, Kreditrisiken, operationelle Risiken (einschließlich Rechts- und IT-Risiken) und Reputationsrisiken, um ihre Angemessenheit im Hinblick auf die festgelegte 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 des Instituts, Marktentwicklungen oder Empfehlungen der Risikomanagementfunktion ergeben;

e. Beratung zur Beauftragung externer Berater bieten, 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 des Instituts bei externen und internen Ereignissen reagieren würde;

g. die Übereinstimmung zwischen allen wesentlichen Finanzprodukten und -dienstleistungen, die den Kunden angeboten werden, und dem Geschäftsmodell und der Risikostrategie des Instituts überwachen[19]. Der Risikoausschuss sollte die mit den angebotenen Finanzprodukten und -dienstleistungen verbundenen Risiken bewerten und die Übereinstimmung zwischen den zugewiesenen Preisen und den aus diesen Produkten und Dienstleistungen erzielten Gewinnen berücksichtigen; und

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

62. Der Risikoausschuss sollte mit anderen Ausschüssen zusammenarbeiten, deren Tätigkeiten Auswirkungen auf die Risikostrategie haben können (z. B. Prüfungs- und Vergütungsausschüsse), und sich regelmäßig mit den internen Kontrollfunktionen des Instituts, insbesondere der Risikomanagementfunktion austauschen.

63. Sofern eingerichtet, muss der Risikoausschuss unbeschadet der Aufgaben des Vergütungsausschusses prüfen, ob bei den durch die Vergütungspolitik und -praxis gebotenen

[19] Siehe auch die EBA-Leitlinien für Überwachung und Governance von Bankprodukten im Privatkundengeschäft, abrufbar unter http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

Anreizen das Risiko, das Kapital, die Liquidität und die Wahrscheinlichkeit sowie der Zeitpunkt von Einnahmen des Instituts berücksichtigt werden.

5.5 Rolle des Prüfungsausschusses

64. In Einklang mit der Richtlinie 2006/43/EG [20] sollte der Prüfungsausschuss, sofern er eingerichtet ist, unter anderem

a. die Wirksamkeit der internen Qualitätskontrolle und der Systeme für das Risikomanagement des Instituts sowie gegebenenfalls der internen Revision mit Blick auf die Rechnungslegung des geprüften Instituts überwachen, ohne seine Unabhängigkeit zu verletzen;

b. die Einführung von Rechnungslegungsmethoden durch das Institut überwachen;

c. den Rechnungslegungsprozess überwachen und Empfehlungen zur Sicherstellung seiner Integrität unterbreiten;

d. die Unabhängigkeit der Abschlussprüfer oder Wirtschaftsprüfungsgesellschaften in Einklang mit den Artikeln 22, 22a, 22b, 24a und 24b der Richtlinie 2006/43/EU und Artikel 6 der Verordnung (EU) Nr. 537/2014[21] und insbesondere die Angemessenheit der nicht prüfungsbezogenen Leistungen, die für das geprüfte Institut gemäß Artikel 5 dieser Verordnung erbracht werden, überprüfen und überwachen;

e. die Abschlussprüfung der Jahresabschlüsse und konsolidierten Abschlüsse überwachen, insbesondere ihre Leistung, wobei etwaige Feststellungen und Schlussfolgerungen der zuständigen Behörde gemäß Artikel 26 Absatz 6 der Verordnung (EU) Nr. 537/2014 zu berücksichtigen sind;

f. die Verantwortung für das Verfahren zur Auswahl der externen Abschlussprüfer oder Wirtschaftsprüfungsgesellschaften tragen und dem zuständigen Organ des Instituts ihre Bestellung (gemäß Artikel 16 der Verordnung (EU) Nr. 537/2014, es sei denn, Artikel 16 Absatz 8 der Verordnung (EU) Nr. 537/2014 findet Anwendung), Vergütung und Abberufung empfehlen;

g. den Prüfungsumfang und die Häufigkeit der Abschlussprüfung der Jahresabschlüsse oder konsolidierten Abschlüsse überprüfen;

h. gemäß Artikel 39 Absatz 6 Buchstabe a der Richtlinie 2006/43/EU das Verwaltungs- oder Aufsichtsorgan des geprüften Instituts über das Ergebnis der Abschlussprüfung

[20] Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates (ABl. L 157 vom 9.6.2006, S. 87), zuletzt geändert durch die Richtlinie 2014/56/EU des Europäischen Parlaments und des Rates vom 16. April 2014.

[21] Verordnung (EU) Nr. 537/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über spezifische Anforderungen an die Abschlussprüfung bei Unternehmen von öffentlichem Interesse und zur Aufhebung des Beschlusses 2005/909/EG der Kommission (ABl. L 158 vom 27.5.2014, S. 77).

informieren und erläutern, wie die Abschlussprüfung zur Integrität der Rechnungslegung beigetragen hat und welche Rolle der Prüfungsausschuss in diesem Prozess innehatte; sowie

i. Prüfberichte entgegennehmen und beachten.

5.6 Kombinierte Ausschüsse

65. Gemäß Artikel 76 Absatz 3 der Richtlinie 2013/36/EU können es die zuständigen Behörden Instituten, die nicht als von erheblicher Bedeutung gelten, gestatten, den Risikoausschuss, sofern eingerichtet, mit dem Prüfungsausschuss gemäß Artikel 39 der Richtlinie 2006/43/EG zu kombinieren.

66. Falls in Instituten, die nicht von erheblicher Bedeutung sind, ein Risiko- und ein Nominierungsausschuss eingerichtet sind, dürfen die Ausschüsse kombiniert werden. In diesem Fall sollten die Institute die Gründe dokumentieren, aus denen sie sich entschieden haben, die Ausschüsse zu kombinieren, und wie mit dem Ansatz die Ziele der Ausschüsse verwirklicht werden.

67. Die Institute sollten zu jeder Zeit sicherstellen, dass die Mitglieder eines kombinierten Ausschusses individuell und kollektiv über die erforderlichen Kenntnisse, Fähigkeiten und Erfahrungen verfügen, um die von einem kombinierten Ausschuss wahrzunehmenden Pflichten voll und ganz zu verstehen[22].

Titel III – Rahmenwerk für die Governance

6 Organisatorischer Rahmen und Organisationsstruktur

6.1 Organisatorischer Rahmen

68. Das Leitungsorgan eines Instituts sollte sicherstellen, dass das Institut über eine geeignete und transparente organisatorische und operative Struktur für das betreffende Institut verfügt, und sollte eine schriftliche Beschreibung über diese vorlegen können. Die Struktur sollte eine wirksame und umsichtige Führung eines Instituts auf Einzel-, teilkonsolidierter und konsolidierter Basis fördern und darlegen. Das Leitungsorgan sollte sicherstellen, dass die internen Kontrollfunktionen unabhängig von den Geschäftsbereichen sind, die sie kontrollieren, einschließlich einer geeigneten Aufgabentrennung, und über angemessene finanzielle und personelle Mittel sowie Befugnisse zur wirksamen Wahrnehmung ihrer Aufgabe verfügen. Die Berichtswege sowie die Zuordnung von Verantwortlichkeiten, insbesondere unter Inhabern von Schlüsselfunktionen, innerhalb eines Instituts sollten klar,

[22] 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.

genau abgegrenzt, stimmig, durchsetzbar und ordnungsgemäß dokumentiert sein. Die Dokumentation sollte, soweit angemessen, aktualisiert werden.

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

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

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

71. Das Leitungsorgan sollte die rechtliche, organisatorische und operative Struktur des Instituts genau kennen und verstehen (Kenntnis der eigenen Struktur) sowie dafür Sorge tragen, dass diese der genehmigten Geschäfts- und Risikostrategie und dem Risikoappetit des Instituts entspricht sowie von seinem Risikomanagement-Rahmen abgedeckt ist.

72. Das Leitungsorgan sollte für die Genehmigung solider Strategien und Richtlinien bei der Schaffung neuer Strukturen zuständig sein. In Fällen, in denen ein Institut viele rechtliche Einheiten innerhalb einer Gruppe gründet, sollte deren Zahl und insbesondere die zwischen ihnen bestehenden Verbindungen und Transaktionen für die Ausgestaltung seiner 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 eines Instituts 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 des Instituts als auch für die zuständige Behörde.

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

74. Das Leitungsorgan eines konsolidierenden Instituts 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 das Institut in der

Lage ist, zeitnah Informationen zu Art, Merkmalen, Organisationsstruktur, Eigentümerstruktur und Geschäftstätigkeit jeder einzelnen rechtlichen Einheit vorzulegen, und dass die Institute innerhalb der Gruppe alle Anforderungen an die aufsichtliche Berichterstattung auf Einzel-, teilkonsolidierter und konsolidierter Basis erfüllen.

75. Das Leitungsorgan eines konsolidierenden Instituts sollte sicherstellen, dass die verschiedenen Unternehmen der Gruppe (einschließlich des konsolidierenden Instituts selbst) ausreichende Informationen erhalten, um ein klares Bild 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 erhalten. 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 konsolidierenden Instituts 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 des Instituts insgesamt bewertet und beurteilt wird, ob die einzelnen Unternehmen ihre Geschäftstätigkeit in Einklang mit der genehmigten gruppenweiten Strategie ausüben; und

    c. regelmäßigen Berichten über Themen, bei denen nach dem aufsichtsrechtlichen Rahmen eine Einhaltung auf Einzel-, teilkonsolidierter und konsolidierter Ebene erforderlich ist.

6.3 Komplexe Strukturen und nichtstandardisierte oder intransparente Tätigkeiten

76. Die Institute sollten es vermeiden, komplexe und möglicherweise intransparente Strukturen einzurichten. Die Institute sollten bei ihrer Entscheidungsfindung die Ergebnisse einer Risikobewertung, die sie durchführen, um zu ermitteln, ob solche Strukturen für einen mit Geldwäsche, Terrorismusfinanzierung oder anderen Finanzstraftaten verbundenen Zweck genutzt werden könnten, sowie die jeweiligen Kontrollen und den geltenden Rechtsrahmen berücksichtigen [23]. Zu diesem Zweck sollten die Institute mindestens folgende Aspekte berücksichtigen:

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

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[24];

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

c. den Umfang, in dem die Struktur genutzt werden könnte, um die Identität des eigentlichen 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 des Instituts oder die Fähigkeit des Instituts zur Steuerung des verbundenen Risikos behindert, und

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

77. In jedem Fall sollten die Institute keine undurchsichtigen oder unnötig komplexen Strukturen, die keine klare wirtschaftliche Begründung oder keinen rechtlichen Zweck haben, oder Strukturen einrichten, die Anlass zu Bedenken geben könnten, dass sie möglicherweise für Zwecke in Verbindung mit Finanzkriminalität geschaffen werden.

78. 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.

79. Institute sollten ihre Entscheidungen dokumentieren und in der Lage sein, ihre Entscheidungen gegenüber den zuständigen Behörden zu begründen.

80. 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:

[24] Siehe auch: 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

a. Das Institut verfügt über angemessene Richtlinien und Verfahren sowie dokumentierte Prozesse (z. B. geeignete Limite, 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 konsolidierende Institut und die internen und externen Prüfer zugänglich und werden dem Leitungsorgan in seiner Aufsichtsfunktion und der zuständigen Behörde, die die Zulassung erteilt hat, gemeldet; und

c. das Institut prüft in regelmäßigen Abständen, ob nach wie vor die Notwendigkeit besteht, diese Struktur beizubehalten.

81. Diese Strukturen und Tätigkeiten, einschließlich der Einhaltung der Rechtsvorschriften und beruflichen Standards, sollten regelmäßig von der internen Revision nach einem risikobasierten Ansatz überprüft werden.

82. Die Institute 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, die gleichen Maßnahmen des Risikomanagements wie für die eigenen Geschäftstätigkeiten des Instituts ergreifen. Insbesondere sollten die Institute den Grund analysieren, aus dem ein Kunde eine bestimmte Struktur einrichten möchte.

7 Organisatorischer Rahmen im Kontext einer Gruppe

83. In Einklang mit Artikel 109 Absatz 2 der Richtlinie 2013/36/EU sollten Mutterunternehmen und Tochtergesellschaften, die der Richtlinie unterliegen, dafür Sorge tragen, dass Regelungen, Prozesse und Mechanismen für die interne Governance kohärent und auf einer konsolidierten oder teilkonsolidierten Basis gut integriert sind. Zu diesem Zweck sollten Mutterunternehmen und Tochtergesellschaften im aufsichtlichen Konsolidierungskreis solche Regelungen, Prozesse und Mechanismen in ihren nicht der Richtlinie 2013/36/EU unterliegenden Tochtergesellschaften, einschließlich derer mit Sitz in Drittländern, unter anderem an Offshore-Finanzplätzen, einführen, um solide Governance-Regelungen auf einer konsolidierten und teilkonsolidierten Basis sicherzustellen. Hinsichtlich Vergütungsanforderungen finden in Einklang mit Artikel 109 Absätze 4 und 5 einige Ausnahmen Anwendung [25]. Die zuständigen Funktionen innerhalb des konsolidierenden Instituts und seiner Tochtergesellschaften sollten interagieren und gegebenenfalls Daten und Informationen austauschen. Die Regelungen, Prozesse und Mechanismen für die interne Governance sollten sicherstellen, dass das konsolidierende Institut über ausreichend Daten und Informationen verfügt und in der Lage ist, das gruppenweite Risikoprofil entsprechend den Ausführungen in Abschnitt 6.2 zu bewerten.

84. Das Leitungsorgan einer Tochtergesellschaft, die der Richtlinie 2013/36/EU unterliegt, sollte die auf konsolidierter oder teilkonsolidierter 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.

85. Auf konsolidierter und teilkonsolidierter Ebene sollte das konsolidierende Institut die Einhaltung der Governance-Richtlinien und des in Titel V genannten internen Kontrollrahmens auf Gruppenebene durch alle Institute und sonstigen Einrichtungen im aufsichtlichen Konsolidierungskreis, einschließlich seiner Tochtergesellschaften, die selbst nicht der Richtlinie 2013/36/EU unterliegen, sicherstellen. Bei der Umsetzung der Governance-Richtlinien sollte das konsolidierende Institut dafür Sorge tragen, dass stabile Regelungen für die Governance jeder Tochtergesellschaft bestehen und besondere Regelungen, Prozesse 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.

86. Ein konsolidierendes Institut sollte die Interessen aller seiner Tochtergesellschaften berücksichtigen und abwägen, wie Strategien und Richtlinien langfristig einen Beitrag zu den Interessen der einzelnen Tochtergesellschaft und der Gruppe als Ganzes leisten.

87. Mutter- und Tochtergesellschaften sollten dafür Sorge tragen, dass die Institute und Einheiten innerhalb der Gruppe allen spezifischen aufsichtlichen Anforderungen der einschlägigen Rechtsordnungen entsprechen.

[25] Siehe auch die EBA-Leitlinien für eine solide Vergütungspolitik.

88. Das konsolidierende Institut sollte dafür Sorge tragen, dass in einem Drittland niedergelassene Tochtergesellschaften, die in den aufsichtlichen Konsolidierungskreis fallen, über Governance-Regelungen, Prozesse und Mechanismen verfügen, die mit den Governance-Richtlinien auf Gruppenebene in Einklang stehen und den Anforderungen der Artikel 74 bis 96 der Richtlinie 2013/36/EU und den vorliegenden Leitlinien entsprechen, soweit diese nach den Gesetzen des Drittlandes nicht rechtswidrig sind.

89. Die Anforderungen an die interne Governance der Richtlinie 2013/36/EU und die Vorgaben der vorliegenden Leitlinien gelten für Institute unabhängig davon, ob sie Tochtergesellschaften eines Mutterunternehmens mit Sitz in einem Drittland sind. Falls eine EU-Tochtergesellschaft eines Mutterunternehmens mit Sitz in einem Drittland ein konsolidierendes Institut ist, umfasst der aufsichtliche Konsolidierungskreis nicht die Ebene des in einem Drittland niedergelassenen Mutterunternehmens und sonstiger direkter Tochtergesellschaften dieses Mutterunternehmens. Das konsolidierende Institut sollte sicherstellen, dass die gruppenweiten Governance-Richtlinien für das Mutterinstitut in einem Drittland im Rahmen seiner eigenen Governance-Richtlinien insoweit berücksichtigt werden, als dies nicht im Widerspruch zu den Anforderungen des maßgeblichen EU-Rechts, einschließlich der Richtlinie 2013/36/EU und weiterer Bestimmungen in den vorliegenden Leitlinien, steht.

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

8 Auslagerungsrichtlinien (Outsourcing policy)[26]

91. Das Leitungsorgan sollte die Auslagerungsrichtlinien eines Instituts genehmigen sowie regelmäßig überprüfen und aktualisieren, um sicherzustellen, dass angemessene Änderungen zeitnah umgesetzt werden.

92. Die Auslagerungsrichtlinien sollten die Auswirkungen einer Auslagerung auf die Geschäftstätigkeit eines Instituts sowie auf dessen Risikosituation (etwa operationelle Risiken, einschließlich Rechts- und IT-Risiken, Reputationsrisiken und Konzentrationsrisiken) berücksichtigen. Die Auslagerungsrichtlinien sollten auch die Berichts- und Überwachungsregelungen enthalten, die von Anfang bis Ende einer Auslagerungsvereinbarung umzusetzen sind (einschließlich der Ausarbeitung eines Business Case für eine Auslagerung, dem Abschluss eines Auslagerungsvertrages, der Erfüllung des Vertrags bis zu dessen Ablauf, der Notfallpläne und Ausstiegsstrategien). Ein Institut bleibt voll und ganz für alle ausgelagerten Dienstleistungen und Tätigkeiten sowie für alle sich daraus ergebenden Geschäftsentscheidungen verantwortlich. Dementsprechend sollte im

[26] Siehe auch: EBA-Leitlinien zu Auslagerungen, abrufbar unter: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

Rahmen der Auslagerungsrichtlinien deutlich gemacht werden, dass das Institut durch eine Auslagerung weder von seinen regulatorischen Verpflichtungen noch seinen Pflichten gegenüber seinen Kunden entbunden wird.

93. In den Auslagerungsrichtlinien sollte geregelt werden, dass Auslagerungsvereinbarungen eine wirksame Beaufsichtigung des Instituts weder im Rahmen von bankgeschäftlichen Prüfungen vor Ort („on-site“) noch im Rahmen der laufenden Aufsicht („off-site“) behindern dürfen und nicht gegen aufsichtsrechtliche Einschränkungen von Dienstleistungen und Tätigkeiten verstoßen dürfen. Die Richtlinien sollten sich außerdem auch auf gruppeninterne Auslagerungen (d. h. das Erbringen von Dienstleistungen durch eine rechtlich selbstständige Einheit innerhalb der Gruppe eines Instituts) erstrecken sowie gruppenspezifische Gegebenheiten berücksichtigen.

Titel IV – Risikokultur und Wohlverhaltensregeln

9 Risikokultur

94. Eine solide, sorgfältige und kohärente Risikokultur sollte ein Schlüsselelement eines wirksamen Risikomanagements eines Instituts sein und es ihm ermöglichen, solide und fundierte Entscheidungen zu treffen.

95. Institute sollten eine integrierte und institutsweite Risikokultur auf der Grundlage eines umfassenden Verständnisses und einer ganzheitlichen Sicht ihrer Risiken und deren Management entwickeln, wobei auch dem Risikoappetit des Instituts Rechnung zu tragen ist.

96. Institute sollten eine Risikokultur mittels Richtlinien, Kommunikation und Fortbildungen der Mitarbeiter bezüglich der Tätigkeiten, Strategie und des Risikoprofils des Instituts entwickeln und Kommunikation und Mitarbeiterfortbildungen anpassen, um der Verantwortung der Mitarbeiter bezüglich Risikoappetit und Risikomanagement Rechnung zu tragen.

97. 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 in Einklang mit den Richtlinien, Verfahren und Kontrollen des Instituts unter Berücksichtigung des Risikoappetits und der Risikotragfähigkeit des Instituts verantwortlich sein.

98. 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 des Instituts zuständig sein. Das Verhalten seiner Mitglieder sollte die Werte widerspiegeln. Die Führungskräfte des Instituts, einschließlich der Inhaber von Schlüsselfunktionen, sollten zur internen Kommunikation von Kernwerten und Erwartungen an die Mitarbeiter beitragen. Die

Mitarbeiter sollten alle anwendbaren Gesetze und Rechtsvorschriften einhalten und festgestellte Rechtsverstöße innerhalb oder außerhalb des Instituts unverzüglich melden (z. B. der zuständigen Behörde im Rahmen eines Hinweisgeberverfahrens („Whistleblowing“). Das Leitungsorgan sollte die Risikokultur des Instituts fortlaufend fördern, überwachen und bewerten, die Auswirkungen der Risikokultur auf die Finanzstabilität, das Risikoprofil und eine stabile Unternehmensführung des Instituts berücksichtigen und soweit erforderlich Änderungen vornehmen.

b. Verantwortlichkeiten: Die maßgeblichen Mitarbeiter auf allen Stufen sollten die Kernwerte des Instituts und, in dem für ihre Funktion erforderlichen Umfang, seinen Risikoappetit und seine 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 des Instituts 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 des Instituts und seine langfristigen Interessen spielen[27].

10 Unternehmenswerte und Verhaltenskodex

99. Das Leitungsorgan sollte hohe ethische und berufliche Standards entwickeln, annehmen, einhalten und fördern, wobei es die spezifischen Anforderungen und Merkmale des Instituts 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 des Instituts oder gemeinsame Standards, die von Verbänden oder sonstigen einschlägigen Organisationen herausgegeben wurden, annehmen und umsetzen.

100. Institute 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

[27] Siehe auch die EBA-Leitlinien für eine solide Vergütungspolitik gemäß Artikel 74 Absatz 3 und Artikel 75 Absatz 2 der Richtlinie 2013/36/EU und Angaben gemäß Artikel 450 der Verordnung (EU) Nr. 575/2013 (EBA/GL/2015/22), abrufbar unter https://www.eba.europa.eu/regulation-and-policy/remuneration.

Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Orientierung stattfindet.

101. Die Richtlinien der Institute 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[28] 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.[29] Institute sollten die Entwicklung des Lohngefälles zwischen Frauen und Männern getrennt für identifizierte Mitarbeiter (ohne Mitglieder des Leitungsorgans), Mitglieder des Leitungsorgans in seiner Leitungsfunktion, Mitglieder des Leitungsorgans in seiner Aufsichtsfunktion und sonstiges Personal überwachen. Institute sollten über Richtlinien verfügen, durch die die Wiedereingliederung von Mitarbeitern nach Mutterschafts-, Vaterschafts- oder Elternurlaub gefördert wird.

102. Die umgesetzten Standards sollten auf eine Verbesserung der solide Governance-Regelungen des Instituts und eine Reduzierung der Risiken abzielen, denen das Institut ausgesetzt ist, insbesondere operationelle Risiken und Reputationsrisiken, die erhebliche nachteilige Auswirkungen auf die Rentabilität und Nachhaltigkeit des Instituts 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.

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

a. die Mitarbeiter daran erinnern, dass alle Tätigkeiten des Instituts unter Einhaltung des anwendbaren Rechts und in Einklang mit den Unternehmenswerten des Instituts durchgeführt werden sollten;

b. das Risikobewusstsein durch eine starke Risikokultur in Einklang mit Abschnitt 9 der Leitlinien fördern, wobei die Erwartung des Leitungsorgans vermittelt wird, dass die Tätigkeiten nicht über den definierten Risikoappetit und die vom Institut 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

[28] 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.

[29] Siehe auch EBA-Leitlinien zu geschlechtsneutraler Vergütungspolitik.

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. klarstellen, 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; und

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.

104. Die Institute sollten die Einhaltung solcher Standards überwachen und für eine Sensibilisierung der Mitarbeiter, z. B. durch Fortbildungsangebote, Sorge tragen. Die Institute 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.

11 Richtlinien für den Umgang mit Interessenkonflikten auf Ebene des Instituts

105. 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 institutioneller Ebene, z. B. infolge der verschiedenen Tätigkeiten und Funktionen des Instituts, von verschiedenen Instituten im aufsichtlichen Konsolidierungskreis oder von verschiedenen Geschäftsbereichen oder Geschäftseinheiten innerhalb eines Instituts, oder bezüglich externer Interessenträger zuständig sein.

106. Die Institute sollten innerhalb ihrer organisatorischen und administrativen Regelungen angemessene Maßnahmen ergreifen, um zu verhindern, dass Interessenkonflikte sich nachteilig auf die Interessen ihrer Kunden auswirken.

107. Die Maßnahmen der Institute 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.

12 Richtlinien für den Umgang mit Interessenkonflikten für Mitarbeiter[30]

108. Das Leitungsorgan sollte 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 des Instituts 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 konsolidierendes Institut sollte die Interessen im Rahmen gruppenweiter Richtlinien für den Umgang mit Interessenkonflikten auf konsolidierter oder teilkonsolidierter Basis berücksichtigen.

109. Die Richtlinien sollten auf die Ermittlung von Interessenkonflikten der Mitarbeiter abzielen, einschließlich der Interessen ihrer nächsten Familienangehörigen. Die Institute 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 Institute ihre Erheblichkeit bewerten sowie gegebenenfalls über geeignete mindernde Maßnahmen entscheiden und diese umsetzen.

110. Für Interessenkonflikte, die aufgrund von Beziehungen aus der Vergangenheit bestehen können, sollten die Institute 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.

111. 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, von dem Institut einem Unternehmen im Eigentum von Mitarbeitern gewährte Darlehen, 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 dem Institut;

[30] 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.

c. persönliche oder berufliche Beziehungen mit Mitarbeitern des Instituts 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.

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

113. 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.

114. 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, die Auswahl eines Dienstleisters usw.) und in der Regel mit einer einmaligen Maßnahme gehandhabt werden können. In allen Fällen sollte das Interesse des Instituts bei den getroffenen Entscheidungen im Mittelpunkt stehen.

115. 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, Elemente, Zuständigkeiten und Maßnahmen sollten Folgendes umfassen:

a. Übertragung konfligierender Aufgaben oder Transaktionen an unterschiedliche Personen;

b. Verhindern, dass Mitarbeiter, die auch außerhalb des Instituts tätig sind, innerhalb des Instituts 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 dem Institut ordnungsgemäß nachzukommen, anderweitig gefährdet sein könnte;

d. Mitglieder des Leitungsorgans darin hindern, Leitungs- oder Aufsichtsfunktionen in konkurrierenden Instituten zu bekleiden, sofern diese nicht in Instituten, die zum gleichen institutsbezogenen Sicherungssystem entsprechend Artikel 113 Absatz 7 der Verordnung (EU) Nr. 575/2013 gehören, Kreditinstituten, die gemäß Artikel 10 der Verordnung (EU) Nr. 575/2013 einer Zentralorganisation ständig zugeordnet sind, oder Instituten im aufsichtlichen Konsolidierungskreis angesiedelt sind.

116. 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 des Instituts ausgerichtet sind. Die Institute sollten in Erwägung ziehen, dass Interessenkonflikte Auswirkungen auf die Unabhängigkeit der Mitglieder des Leitungsorgans haben können[31].

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

118. Tatsächliche oder potenzielle Interessenkonflikte, die der zuständigen Funktion innerhalb des Instituts offengelegt wurden, sollten ordnungsgemäß bewertet und geregelt werden. Wird ein Interessenkonflikt eines Mitarbeiters festgestellt, sollte das Institut 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.

119. 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.

[31] 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.

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

120. Im Rahmen ihrer Richtlinien für den Umgang mit Interessenkonflikten für Mitarbeiter (Abschnitt 12) und dem Umgang mit Interessenkonflikten von Mitgliedern des Leitungsorgans gemäß Absatz 117 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. Factoring, Leasing, Immobilientransaktionen usw.) mit Mitgliedern des Leitungsorgans und ihrer verbundenen Parteien festlegen.

121. Unbeschadet der nationalen Umsetzung der Richtlinie 2013/36/EU [32] können Institute zusätzliche Kategorien von verbundenen Parteien in Erwägung ziehen, auf die sie ihren Rahmen für Interessenkonflikte in Zusammenhang mit Darlehen und anderen Geschäften ganz oder teilweise anwenden.

122. 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.

123. 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[33], die im ordentlichen Geschäftsgang und zu marktüblichen Bedingungen getätigt werden, und Darlehen für Mitarbeiter bzw. 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 und anderen Geschäften, unterschiedlichen Arten von Darlehen und anderen Geschäften und dem Umfang der tatsächlichen oder potenziellen Interessenkonflikte, die entstehen können, unterschieden werden.

124. Als Teil des Rahmens für Interessenkonflikte sollte das Leitungsorgan angemessene Schwellenwerte (z. B. pro Produktart oder abhängig von den Bedingungen) festlegen, ab denen für das Darlehen oder andere Geschäft mit einem Mitglied des Leitungsorgans oder seinen verbundenen Parteien stets die Genehmigung des Leitungsorgans erforderlich ist. Entscheidungen über wesentliche Darlehen oder andere wesentliche Geschäfte mit

[32] Siehe auch Grundsatz 20 des Basler Ausschusses für Bankenaufsicht.

[33] Geschäftsvorgänge können Darlehen und andere Geschäfte einschließen (z. B. Leasing, Factoring, Dienstleistungen in Zusammenhang mit Börsengängen, Fusionen und Unternehmenskäufe, Verkauf und Kauf von Immobilien).

Mitgliedern des Leitungsorgans, die nicht unter normalen Marktbedingungen, sondern nach den für alle Mitarbeiter verfügbaren Bedingungen abgeschlossen werden, sollten stets vom Leitungsorgan getroffen werden.

125. 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 an der Entscheidungsfindung beteiligt sein.

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

127. Falls Darlehen als Kreditlinie gewährt werden (z. B. Überziehungskredite), sollten die ursprüngliche Entscheidung und vorgenommene Änderungen dokumentiert werden. Eine Inanspruchnahme dieser Kreditfazilitäten innerhalb der vereinbarten Kreditlinien sollte nicht als neue Entscheidung über ein Darlehen für ein Mitglied des Leitungsorgans oder seiner verbundenen Partei betrachtet werden. Falls eine Änderung einer Kreditlinie entsprechend der Richtlinie des Instituts als wesentlich gilt, sollte eine neue Bewertung vorgenommen und eine neue Entscheidung getroffen werden.

128. Um die Einhaltung der Richtlinien für den Umgang mit Interessenkonflikten sicherzustellen, sollten die Institute 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.

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

129. Im Sinne des Artikels 88 Absatz 1 der Richtlinie 2013/36/EU sollten Institute die Daten über Darlehen[34] an Mitglieder des Leitungsorgans und ihre verbundenen Parteien angemessen dokumentieren, wobei die Dokumentation mindestens die folgenden Daten einschließen muss:

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;

[34] Siehe auch EBA-Leitlinien für die Kreditvergabe und Überwachung: https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring

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 wurde oder nicht; sowie

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

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

131. Für ein Darlehen an ein Mitglied des Leitungsorgans oder seine verbundenen Parteien über einen Betrag von über 200 000 EUR sollten Institute in der Lage sein, der zuständigen Behörde auf Anfrage die folgenden zusätzlichen Informationen zur Verfügung zu stellen:

a. den Prozentsatz des Darlehens und den Prozentsatz der Summe aller ausstehenden Beträge von Darlehen, die demselben Schuldner gewährt wurden, im Vergleich zu:

i. der Summe des Kernkapitals und Ergänzungskapital sowie

ii. des harten Kernkapitals des Instituts;

b. ob das Darlehen Teil eines Großkredits[35] ist; und

c. das relative Gewicht der aggregierten Summe aller ausstehenden Beträge von Darlehen, die demselben Schuldner gewährt wurden, berechnet als Prozentsatz mittels der Division des ausstehenden Gesamtbetrags durch den Gesamtbetrag aller ausstehenden Darlehen an Mitglieder des Leitungsorgans und ihrer verbundenen Parteien.

13 Hinweisgeberverfahren (Whistleblowing-Verfahren)

132. Die Institute sollten geeignete Richtlinien und Verfahren für interne Warnungen für Mitarbeiter zur Meldung potenzieller oder tatsächlicher Verstöße gegen regulatorische oder interne Anforderungen, unter anderem Verordnung (EU) Nr. 575/2013 und nationale Vorschriften zur Umsetzung der Richtlinie 2013/36/EU, oder Vorgaben für die interne Governance über einen speziellen, unabhängigen und autonomen Berichtsweg einführen und unterhalten (Hinweisgeberverfahren/Whistleblowing-Verfahren). 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

[35] Siehe auch Teil IV der Verordnung (EU) Nr. 575/2013 und insbesondere Artikel 392.

Grund für die Einleitung einer Untersuchung bietet. Institute 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.

133. 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[36] (DSGVO) sowohl für die Person, die den Verstoß anzeigt, als auch für die natürliche Person, die mutmaßlich für den Verstoß verantwortlich ist, sicherstellen.

134. Die Warnverfahren sollten allen Mitarbeitern eines Instituts zugänglich gemacht werden.

135. Die von Mitarbeitern über die Warnverfahren bereitgestellten Informationen sollten, sofern 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 Institute können auch ein Hinweisgeberverfahren einrichten, das es ermöglicht, Informationen anonym einzureichen.

136. Die Institute 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. Das Institut sollte sicherstellen, dass sich keine Person unter der Kontrolle des Instituts 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.

137. Die Institute 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 das Institut 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.

138. Insbesondere sollten die Hinweisgeberverfahren (Whistleblowing-Verfahren)

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

[36] 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).

b. klare Regeln vorsehen, mit denen sichergestellt wird, dass Informationen über die Meldung und die gemeldeten Personen sowie den Verstoß vertraulich in Einklang mit 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;

d. sicherstellen, dass potenzielle oder tatsächliche Verstöße bewertet und eskaliert werden, einschließlich, soweit angemessen, an die einschlägige 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.

14 Meldung von Verstößen bei den zuständigen Behörden

139. Die zuständigen Behörden sollten wirksame und zuverlässige Mechanismen einrichten, um es den Mitarbeitern von Instituten zu ermöglichen, bei den zuständigen Behörden einschlägige potenzielle oder tatsächliche Verstöße gegen regulatorische Anforderungen, unter anderem mit Blick auf die Verordnung (EU) Nr. 575/2013 und nationale Vorschriften zur Umsetzung der Richtlinie 2013/36/EU, zu melden. Diese Mechanismen sollten mindestens Folgendes umfassen:

a. spezifische 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; und

d. klare Verfahren nach den Bestimmungen in Abschnitt 13.

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

Titel V – Interner Kontrollrahmen und interne Kontrollmechanismen

15 Interner Kontrollrahmen

141. Die Institute sollten eine Kultur entwickeln und pflegen, die eine positive Haltung gegenüber der Risikokontrolle und Compliance innerhalb des Instituts sowie einen stabilen und umfassenden internen Kontrollrahmen bestärkt. In diesem Rahmen sollten die Geschäftsbereiche der Institute 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 Institute über interne Kontrollfunktionen mit angemessenen und ausreichenden Befugnissen, einem ausreichenden Gewicht und Zugang zum Leitungsorgan für die Erfüllung ihrer Aufgabe sowie einen Risikomanagement-Rahmen verfügen.

142. Der interne Kontrollrahmen der Institute 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 Institute müssen 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 des Instituts.

143. Institute sollten angemessene Prozesse und Verfahren einrichten, mit denen sichergestellt wird, dass sie ihre Pflichten im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung erfüllen. Institute 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. Institute sollten Maßnahmen ergreifen, mit denen sichergestellt wird, dass sich die Mitarbeiter dieser Risiken hinsichtlich Geldwäsche/Terrorismusfinanzierung und der Auswirkungen, die Geldwäsche/Terrorismusfinanzierung auf das Institut und die Integrität des Finanzsystems haben können, bewusst sind.

144. 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.

145. Der interne Kontrollrahmen eines Instituts sollte Folgendes sicherstellen:

a. wirksame und effiziente Betriebsabläufe;

b. umsichtige Führung der Geschäfte;

c. angemessene Ermittlung, Messung und Minderung von Risiken;

d. die Zuverlässigkeit der finanziellen und nichtfinanziellen Berichterstattung, sowohl intern als auch extern;

e. solide Verwaltungs- und Rechnungslegungsverfahren sowie

f. Einhaltung von Gesetzen, Rechtsvorschriften, aufsichtlichen Anforderungen sowie der internen Richtlinien, Verfahren, Regelungen und Entscheidungen des Instituts.

16 Umsetzung eines internen Kontrollrahmens

146. 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 das Risikomanagement, die Compliance-Funktion, die Compliance in Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, sofern diese von der Compliance-Funktion getrennt ist und die interne Revision), zuständig sein. Die Institute sollten für die interne Kontrolle angemessene schriftliche Richtlinien, Mechanismen und Verfahren, die vom Leitungsorgan genehmigt werden sollten, einrichten, pflegen und regelmäßig aktualisieren.

147. Ein Institut sollte über einen klaren, transparenten und dokumentierten Entscheidungsprozess sowie eine eindeutige Aufgabenverteilung und Kompetenzregelung innerhalb seines internen Kontrollrahmens verfügen, einschließlich seiner Geschäftsbereiche, internen Einheiten und internen Kontrollfunktionen.

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

149. Bei der Einführung des internen Kontrollrahmens sollten die Institute eine angemessene Aufgabentrennung einrichten – z. B. die Übertragung konfligierender Tätigkeiten im Rahmen der Durchführung von Transaktionen oder bei der Erbringung von Dienstleistungen an

unterschiedliche Personen oder die Übertragung von Aufsichts- und Meldepflichten für konfligierende Tätigkeiten an unterschiedliche Personen – und Informationssperren vorsehen, z. B. durch die physische Trennung bestimmter Abteilungen.

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

151. 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.

17 Risikomanagement-Rahmen

152. Als Teil des gesamten internen Kontrollsystems sollten die Institute über einen ganzheitlichen institutsweiten Risikomanagement-Rahmen 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. Der Risikomanagement-Rahmen sollte das Institut in die Lage versetzen, fundierte Entscheidungen über das Eingehen von Risiken in Kenntnis der Sachlage zu treffen. Der Risikomanagement-Rahmen sollte bilanzielle und außerbilanzielle Risiken sowie aktuelle und künftige Risiken, denen das Institut 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 im gesamten Institut sowie auf konsolidierter oder teilkonsolidierter Ebene eine kohärente Terminologie und kompatible Methoden zugrunde gelegt werden sollten. Alle relevanten Risiken sollten im Risikomanagement-Rahmen berücksichtigt werden, wobei sowohl finanziellen als auch nichtfinanziellen Risiken ordnungsgemäß Rechnung getragen wird, einschließlich Kreditrisiken, Marktrisiken, Liquiditätsrisiken, Konzentrationsrisiken, operationeller Risiken, IT-Risiken, Reputationsrisiken, rechtlicher Risiken, Wohlverhaltensrisiken, Compliance-Risiken hinsichtlich Geldwäsche/Terrorismusfinanzierung und sonstiger Finanzkriminalität, ESG-Risiken und strategischer Risiken.

153. Der Risikomanagement-Rahmen eines Instituts 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 und des Instituts sowie auf konsolidierter und teilkonsolidierter Ebene sicherzustellen.

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

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

156. Bei der Ermittlung und Messung oder Beurteilung von Risiken sollte ein Institut geeignete Methoden und Verfahren entwickeln, die sowohl zukunfts- als auch vergangenheitsorientiert ausgestaltet sind. Mit diesen Methoden sollte es möglich sein, sämtliche Risiken geschäftsbereichsübergreifend zu aggregieren und Risikokonzentrationen zu identifizieren. Die Instrumente sollten die Bewertung des tatsächlichen Risikoprofils im Verhältnis zum Risikoappetit des Instituts sowie die Ermittlung und Bewertung potenzieller und angespannter Risikopositionen unter gestressten Bedingungen im Hinblick auf die Risikotragfähigkeit des Instituts umfassen. Die Instrumente sollten Informationen über etwaige eventuell notwendige Anpassungen des Risikoprofils liefern. Die Institute sollten angemessene konservative Annahmen bei der Konzeption von Stressszenarien zugrunde legen.

157. Die Institute 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 Durchführung einer Strategie durch das Institut 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.

158. Die Letztverantwortung für die Risikobeurteilung liegt einzig und allein beim Institut, das seine Risiken dementsprechend kritisch beurteilen und sich nicht ausschließlich auf externe Beurteilungen verlassen sollte. Ein Institut sollte beispielsweise ein nicht selbst entwickeltes, extern eingekauftes Risikomodell validieren und an seine individuellen Gegebenheiten anpassen, um sicherzustellen, dass mit dem Modell die Risiken genau und umfassend erfasst und analysiert werden.

159. Die Institute 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).

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

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

162. 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 im gesamten Institut als auch nach oben und unten entlang der gesamten Kette der Unternehmensführung.

18 Neue Produkte und wesentliche Änderungen[37]

163. Ein Institut sollte über gut dokumentierte Richtlinien zur Genehmigung neuer Produkte (Neu-Produkt-Prozess – NPP) verfügen, die vom Leitungsorgan genehmigt werden und sich mit der Entwicklung neuer Märkte, Produkte und Dienstleistungen sowie mit wesentlichen Änderungen der bestehenden Märkte, Produkte und Dienstleistungen und mit der Durchführung außergewöhnlicher Transaktionen befassen. Die Richtlinien sollten zudem

[37] Siehe auch die EBA-Leitlinien für Überwachung und Governance für Anbieter und Verkäufer von Bankprodukten im Privatkundengeschäft, abrufbar unter https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

wesentliche Änderungen der verbundenen Prozesse (z. B. neue Auslagerungsvereinbarungen) und Systeme (z. B. IT-Änderungsprozesse) einschließen. Der NPP sollte sicherstellen, dass genehmigte Produkte und Änderungen mit der Risikostrategie und dem Risikoappetit des Instituts sowie den festgelegten Limiten im Einklang stehen bzw. erforderliche Korrekturen vorgenommen werden.

164. Wesentliche Änderungen oder die Durchführung außergewöhnlicher Transaktionen können Fusionen und Übernahmen umfassen, einschließlich potenzieller Folgen einer mangelhaften Durchführung einer „Due Diligence“-Analyse, bei der die Risiken und Verbindlichkeiten nach einem Zusammenschluss nicht erkannt wurden, die Einrichtung von Strukturen (z. B. neue Tochtergesellschaften oder Zweckgesellschaften), neue Produkte, Änderungen an Systemen oder am Rahmen oder den Verfahren für das Risikomanagement sowie Änderungen an der Organisation des Instituts.

165. Ein Institut sollte über spezifische Verfahren für die Überprüfung der Einhaltung dieser Richtlinien unter Berücksichtigung der Beiträge der Risikomanagementfunktion verfügen. Diese sollten eine systematische vorherige Bewertung und eine dokumentierte Stellungnahme der Compliance-Funktion für neue Produkte oder wesentliche Änderungen an bestehenden Produkten umfassen.

166. Der NPP eines Instituts sollte sämtliche Überlegungen einschließen, die es zu berücksichtigen gilt, bevor die Entscheidung getroffen wird, neue Märkte zu erschließen, mit neuen Produkten zu handeln, eine neue Dienstleistung anzubieten oder die bestehenden Produkte oder Dienstleistungen wesentlich zu verändern. Der NPP sollte außerdem auch eine Definition der Begriffe „neues Produkt/ neuer Markt/ neue Geschäftstätigkeit“ sowie „wesentliche Änderungen“ umfassen, die in der Organisation zu verwenden sind, sowie eine Festlegung der internen Funktionen, die in den Entscheidungsprozess einzubinden sind.

167. Der NPP sollte die wichtigsten Problemstellungen behandeln, die geklärt werden müssen, bevor eine Entscheidung getroffen wird. Dies sollte die Einhaltung von Rechtsvorschriften, die Rechnungslegung, Preisgestaltungsmodelle, die Auswirkungen auf das Risikoprofil, eine angemessene Eigenkapitalausstattung und Rentabilität, die Verfügbarkeit angemessener Ressourcen für die Abteilungen Front Office, Middle Office und Back Office sowie angemessener interner Instrumente und Fachkenntnisse für das Verständnis und die Überwachung der damit verbundenen Risiken umfassen. Um die Pflichten gemäß der Richtlinie (EU) 2015/849 zu erfüllen, sollten Institute darüber hinaus die mit neuen Produkten oder Geschäftsgepflogenheiten verbundenen Risiken mit Blick auf Geldwäsche/Terrorismusfinanzierung ermitteln und bewerten und die Maßnahmen festlegen, die zu ergreifen sind, um diese Risiken zu mindern. In der Entscheidung, eine neue Geschäftsaktivität aufzunehmen, sollten auch die hierfür verantwortliche Geschäftseinheit und die verantwortlichen Personen eindeutig festgelegt werden. Eine neue Geschäftsaktivität sollte erst dann aufgenommen werden, wenn die entsprechenden Ressourcen für das Verständnis und die Steuerung der damit verbundenen Risiken zur Verfügung stehen.

168. Die Risikomanagementfunktion und die Compliance-Funktion sollten in die Genehmigung neuer Produkte bzw. wesentlicher Änderungen bestehender Produkte, Prozesse und Systeme einbezogen werden. Ihr Beitrag sollte eine vollständige und objektive Beurteilung der Risiken umfassen, die sich aus den neuen Tätigkeiten ergeben, unter Einbeziehung unterschiedlicher Szenarien, potenzieller Unzulänglichkeiten beim Risikomanagement-Rahmen und internen Kontrollrahmen des Instituts sowie der Fähigkeit des Instituts, neue Risiken wirksam zu steuern. Die Risikomanagementfunktion sollte außerdem einen klaren Überblick über die Markteinführung neuer Produkte (bzw. wesentliche Änderungen bestehender Produkte, Verfahren und Systeme) in verschiedenen Geschäftsbereichen und Portfolios haben und verlangen können, dass Änderungen an bestehenden Produkten den offiziellen NPP durchlaufen müssen.

19 Interne Kontrollfunktionen

169. Die internen Kontrollfunktionen sollten eine Risikomanagementfunktion (siehe Abschnitt 20), eine Compliance-Funktion (siehe Abschnitt 21) und eine interne Revision (siehe Abschnitt 22) umfassen. Die Risikomanagement- und die Compliance-Funktion sollten Gegenstand von Prüfungen durch die interne Revision sein. Die Zuständigkeiten der Kontrollfunktionen schließen auch ein, die Erfüllung von Anforderungen im Bereich der Bekämpfung von Geldwäsche/Terrorismusfinanzierung sicherzustellen.

170. Die operativen Aufgaben der internen Kontrollfunktionen können mit Zustimmung der Leitungsorgane der betreffenden Institute unter Berücksichtigung der in Titel I aufgeführten Kriterien für die Verhältnismäßigkeit an das konsolidierende Institut oder ein anderes Unternehmen innerhalb oder außerhalb der Gruppe ausgelagert werden. Selbst wenn operationelle interne Kontrollaufgaben teilweise oder vollständig ausgelagert werden, sind der Leiter der betreffenden internen Kontrollfunktion und das Leitungsorgan nach wie vor für diese Tätigkeiten und die Aufrechterhaltung der internen Kontrollfunktion innerhalb des Instituts verantwortlich.

171. Unbeschadet der Umsetzung der Richtlinie 2015/849/EU in nationales Recht sollten die Institute die Zuständigkeit für die Sicherstellung, dass das Institut die Anforderungen dieser Richtlinie und der Strategien und Verfahren des Instituts erfüllt, einem Mitarbeiter (z. B. Leiter der Compliance) zuweisen. Institute können eine separate Compliance-Funktion für Geldwäsche/Terrorismusfinanzierung als unabhängige Kontrollfunktion einrichten.[38] 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.

[38] Siehe auch EBA-Leitlinien zur Compliance-Funktion für die Bekämpfung von Geldwäsche/Terrorismusfinanzierung (derzeit in Erarbeitung).

19.1 Leiter der internen Kontrollfunktionen

172. 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. Ungeachtet der Gesamtverantwortung des Leitungsorgans sollten die Leiter der internen Kontrollfunktionen unabhängig von den Geschäftsbereichen und Einheiten sein, die sie kontrollieren. Zu diesem Zweck sollten die Leiter der Risikomanagementfunktion, Compliance-Funktion und internen Revision dem Leitungsorgan Bericht erstatten und diesem direkt unterstellt sein, und ihre Leistung sollte vom Leitungsorgan überprüft werden.

173. 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 das Institut beeinträchtigen oder beeinträchtigen könnten. Dadurch sollten die Leiter der internen Kontrollfunktionen nicht davon abgehalten werden, auch innerhalb der regulären Berichtswege Bericht zu erstatten.

174. Die Institute sollten über dokumentierte Prozesse verfügen, um die Position des Leiters einer internen Kontrollfunktion zu besetzen und ihm seine Zuständigkeiten zu entziehen. In jedem Fall sollten die Leiter der internen Kontrollfunktionen – und darf nach Artikel 76 Absatz 5 der Richtlinie 2013/36/EU der Leiter der Risikomanagementfunktion – nicht ohne die vorherige Zustimmung des Leitungsorgans seiner Funktion enthoben werden. In Instituten von erheblicher Bedeutung sollten die zuständigen Behörden unverzüglich über die Zustimmung und die wichtigsten Gründe für die Entlassung des Leiters einer internen Kontrollfunktion informiert werden.

19.2 Unabhängigkeit der internen Kontrollfunktionen

175. 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;

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

c. unbeschadet der Gesamtverantwortung der Mitglieder des Leitungsorgans für das Institut sollte der Leiter einer internen Kontrollfunktion nicht einer Person unterstellt sein, die die Verantwortung für die Durchführung der Tätigkeiten trägt, die die interne Kontrollfunktion überwacht und kontrolliert; und

d. 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[39].

19.3 Kombination von internen Kontrollfunktionen

176. Unter Berücksichtigung der in Titel I aufgeführten Kriterien für die Verhältnismäßigkeit können die Risikomanagementfunktion und die Compliance-Funktion kombiniert werden. Die interne Revision sollte nicht mit einer anderen internen Kontrollfunktion zusammengefasst werden.

19.4 Ressourcen der internen Kontrollfunktionen

177. Die internen Kontrollfunktionen sollten über ausreichende Ressourcen verfügen. Sie sollten über eine angemessene Personalausstattung (sowohl auf Ebene des Mutterunternehmens als auch auf Ebene der Tochtergesellschaften) verfügen. Die Mitarbeiter sollten ihre Qualifikation fortlaufend aufrechterhalten und nach Bedarf Weiterbildungen absolvieren.

178. 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 Tochtergesellschaften haben, insbesondere mit Blick auf diejenigen, die möglicherweise wesentliche Risiken für die Institute erzeugen können.

20 Risikomanagementfunktion

179. Die Institute sollten eine Risikomanagementfunktion für das gesamte Institut einrichten. 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 Risikomanagement-Rahmen entsprechend Abschnitt 17 umzusetzen.

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

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

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

182. 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.

183. Die Risikomanagementfunktion sollte von den Geschäftsbereichen und Organisationseinheiten, deren Risiken sie kontrolliert, unabhängig sein, sie sollte jedoch nicht an einem Zusammenwirken mit ihnen gehindert sein. Das Zusammenwirken zwischen den operativen Funktionen und der Risikomanagementfunktion sollte zur Verwirklichung des Ziels beitragen, dass alle Mitarbeiter des Instituts Verantwortung für den Umgang mit Risiken übernehmen.

184. Die Risikomanagementfunktion sollte ein zentraler organisatorischer Bestandteil des Instituts und so strukturiert sein, dass sie die Risikorichtlinien umsetzen und den Risikomanagement-Rahmen kontrollieren kann. Die Risikomanagementfunktion sollte eine Schlüsselrolle bei der Sicherstellung wirksamer Risikomanagementprozesse eines Institutes spielen. Die Risikomanagementfunktion sollte in alle wichtigen Entscheidungen im Bereich des Risikomanagements aktiv eingebunden sein.

185. Institute von erheblicher Bedeutung können auch die Einrichtung von speziell zugeordneten Risikomanagementfunktionen für jeden wesentlichen Geschäftsbereich in Erwägung ziehen. Allerdings sollte eine zentrale Risikomanagementfunktion, einschließlich einer gruppenweiten Risikomanagementfunktion im konsolidierenden Institut, eingerichtet sein, um über eine instituts- und gruppenweite ganzheitliche Übersicht über alle Risiken zu verfügen und sicherzustellen, dass die Risikostrategie eingehalten wird.

186. 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 mit der Risikostrategie und dem Risikoappetit in Einklang stehen. Die Risikomanagementfunktion kann Verbesserungen des Risikomanagement-Rahmens und Abhilfemaßnahmen empfehlen, um Verletzungen der Risikorichtlinien, -prozesse und -limite zu beheben.

20.1 Rolle der Risikomanagementfunktion im Hinblick auf Risikostrategie und Entscheidungen

187. Die Risikomanagementfunktion sollte frühzeitig und aktiv in die Erarbeitung einer Risikostrategie des Instituts eingebunden werden, wobei sicherzustellen ist, dass das Institut 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 des Instituts 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 und den Risikoappetit 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 und mit der Risikostrategie des Instituts im Einklang stehen.

188. 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.

20.2 Rolle der Risikomanagementfunktion bei wesentlichen Änderungen

189. Bevor Entscheidungen über wesentliche Änderungen oder die Durchführung außergewöhnlicher Transaktionen getroffen werden, sollte in Einklang mit Abschnitt 18 die Risikomanagementfunktion in die Bewertung der Auswirkungen solcher Änderungen und außergewöhnlicher Transaktionen auf das Gesamtrisiko des Instituts und der Gruppe eingebunden werden und sollte ihre Feststellungen direkt dem Leitungsorgan berichten, bevor eine Entscheidung getroffen wird.

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

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

191. Die Risikomanagementfunktion sollte sicherstellen, dass ein angemessener Risikomanagement-Rahmen vorhanden ist und alle Risiken von den zuständigen Einheiten des Instituts ermittelt, beurteilt, gemessen, überwacht, gesteuert und ordnungsgemäß berichtet werden.

192. 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.

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

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

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

196. Die Risikomanagementfunktion sollte Entwicklungstrends analysieren und neue oder entstehende 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.

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

20.4 Rolle der Risikomanagementfunktion bei nicht genehmigten Risikopositionen

198. 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.

199. 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.

20.5 Leiter der Risikomanagementfunktion

200. Der Leiter der Risikomanagementfunktion sollte 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 des Instituts zu

verstehen. Gleiches gilt für den Leiter der Risikomanagementfunktion eines Mutterinstituts im Hinblick auf die konsolidierte Ebene.

201. Der Leiter der Risikomanagementfunktion sollte über ausreichende Fachkenntnisse, Unabhängigkeit und Seniorität verfügen, um Entscheidungen, die die Exposure des Instituts beeinflussen, zu hinterfragen. Sofern der Leiter der Risikomanagementfunktion kein Mitglied des Leitungsorgans ist, sollten Institute von erheblicher Bedeutung 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 kombinierten Funktionen besteht. In jedem Fall sollte diese Person über ausreichende Befugnisse, ausreichendes Gewicht und Unabhängigkeit verfügen (z. B. Leiter der Rechtsabteilung).

202. Der Leiter der Risikomanagementfunktion sollte in der Lage sein, von der Geschäftsführung und dem Leitungsorgan des Instituts getroffene Entscheidungen zu hinterfragen, und Gründe für Einwände sollten formal dokumentiert werden. Sofern ein Institut 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 es den Umfang eines solchen Vetorechts sowie die Eskalations- und Beschwerdeverfahren bestimmen und festlegen, wie das Leitungsorgan eingebunden wird.

203. Die Institute 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 des Instituts übereinstimmen.

21 Compliance-Funktion

204. Die Institute sollten eine ständige und wirksame Compliance-Funktion für die Steuerung von Compliance-Risiken einrichten und eine Person benennen, die für diese Funktion im gesamten Institut zuständig ist (Compliance-Beauftragter oder Leiter der Compliance-Funktion).

205. 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 Compliance-Funktion wahrnimmt, kann diese Funktion mit der Rolle des Leiters der Risikomanagementfunktion kombiniert werden oder von einer anderen

leitenden Person (z. B. Leiter der Rechtsabteilung) wahrgenommen werden, sofern kein Interessenkonflikt zwischen den kombinierten Funktionen besteht.

206. Die Compliance-Funktion, einschließlich des Leiters der Compliance-Funktion, sollten unabhängig von den Geschäftsbereichen und internen Einheiten sein, die sie kontrollieren, und über ausreichende Befugnisse, Gewicht und Ressourcen verfügen. Unter Berücksichtigung der in Titel I aufgeführten Kriterien für die Verhältnismäßigkeit kann diese Funktion von der Risikomanagementfunktion unterstützt oder mit der Risikomanagementfunktion oder anderen geeigneten Funktionen, z. B. der Rechts- oder Personalabteilung, kombiniert werden.

207. Die Mitarbeiter innerhalb 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.

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

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

210. 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 des Instituts 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.

211. In Einklang mit Abschnitt 18 dieser Leitlinien sollte die Compliance-Funktion zudem in enger Zusammenarbeit mit der Risikomanagementfunktion und der für Rechtsfragen zuständigen Einheit überprüfen, ob neue Produkte und neue Verfahren mit dem aktuellen Rechtsrahmen und gegebenenfalls mit bekannten bevorstehenden Änderungen von Gesetzen, Rechtsvorschriften und aufsichtlichen Anforderungen in Einklang stehen.

212. Institute sollten angemessene Maßnahmen gegen interne oder externe Handlungen ergreifen, die Betrug, Geldwäsche/Terrorismusfinanzierung oder andere Finanzkriminalität

sowie Disziplinarvergehen (z. B. Verletzung interner Verfahren, Überschreitung von Limiten) erleichtern oder ermöglichen.

213. Die Institute sollten dafür Sorge tragen, dass ihre Tochtergesellschaften und Zweigstellen 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 Tochtergesellschaften und Zweigniederlassungen den Compliance-Beauftragten bzw. Leiter der Compliance-Funktion des konsolidierenden Instituts unterrichten.

22 Interne Revision

214. Die Institute sollten unter Berücksichtigung der in Titel I aufgeführten Kriterien für die Verhältnismäßigkeit eine unabhängige und wirksame interne Revision einsetzen und eine Person benennen, die für diese Funktion im gesamten Institut zuständig ist. Die interne Revision sollte unabhängig sein und über ausreichend Befugnisse, Gewicht und Ressourcen verfügen. Insbesondere sollte das Institut 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 des Instituts sowie die Art, den Umfang und die Komplexität der mit dem Geschäftsmodell, den Geschäftstätigkeiten, der Risikokultur und dem Risikoappetit des Instituts einhergehenden Risiken, angemessen sind.

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

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

217. Die interne Revision sollte nicht an der Konzeption, Auswahl, Festlegung und Umsetzung spezifischer interner Kontrollstrategien, -mechanismen und -verfahren sowie 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 anwendbaren Vorschriften zu konsultieren.

218. Die interne Revision sollte bewerten, ob der interne Kontrollrahmen des Instituts 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 des Instituts;

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 des Instituts entsprechen;

c. die Übereinstimmung der Verfahren mit den anwendbaren 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.); und

e. die Eignung, Qualität und Wirksamkeit der durchgeführten Kontrollen sowie die erfolgte Berichterstattung seitens der operativen Geschäftsbereiche, der Risikomanagementfunktion und Compliance-Funktion.

219. Die interne Revision sollte insbesondere die Integrität der Prozesse prüfen, damit die Zuverlässigkeit der Methoden und Techniken des Instituts 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.

220. Die interne Revision sollte über einen uneingeschränkten institutsweiten Zugang zu allen Aufzeichnungen, Dokumenten, Informationen und Gebäuden des Instituts verfügen. Dies sollte den Zugang zu den Management-Informationssystemen und Protokollen aller Ausschüsse und Entscheidungsorgane einschließen.

221. 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.

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

223. 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.

224. 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[40]

225. Institute sollten neben einen soliden Notfallplan einen Wiederherstellungsplan erstellen, um in der Lage zu sein, den kontinuierlichen Dienstbetrieb aufrechtzuerhalten, und Verluste im Fall von schwerwiegenden Betriebsstörungen zu begrenzen.

226. Die Institute können eine spezifische unabhängige Funktion für die Aufrechterhaltung des Geschäftsbetriebs, z. B. als Teil der Risikomanagementfunktion[41] einrichten.

227. Die Geschäftstätigkeit eines Instituts 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 des Instituts 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).

228. Bei der Einrichtung solider Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs sollte ein Institut eine sorgfältige Analyse der Risikofaktoren vornehmen und prüfen, inwieweit es 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, erstrecken und sollte deren Verflechtungen berücksichtigen. Die Ergebnisse der Analyse sollten einen Beitrag zur Definition der Prioritäten und Ziele bei der Wiederherstellung der Geschäftsabläufe des Instituts leisten.

229. Auf der Grundlage der vorstehend genannten Analyse sollte ein Institut Folgendes einrichten:

a. Notfallpläne sowie Pläne zur Aufrechterhaltung des Geschäftsbetriebs, damit ein Institut 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 kritische Ressourcen, die das Institut in die Lage versetzen, innerhalb einer angemessenen Zeitspanne seine üblichen

[40] Institute sollten auch die EBA-Leitlinien zum IKT-Risiko einbeziehen, abrufbar unter: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[41] Weitere Informationen finden sich in Artikel 312 der Verordnung (EU) Nr. 575/2013.

Geschäftsabläufe wieder aufzunehmen. Restrisiken aufgrund potenzieller Geschäftsunterbrechungen sollten mit dem Risikoappetit des Instituts vereinbar sein.

230. Notfallpläne und Wiederherstellungspläne sind zu dokumentieren und sorgfältig umzusetzen. Die Dokumentation sollte innerhalb der Geschäftsbereiche, internen Einheiten und der Risikomanagementfunktion 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, sind zu dokumentieren und zu analysieren und die Pläne entsprechend zu überarbeiten.

Titel VII – Transparenz

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

232. Dementsprechend sollte das Leitungsorgan die betroffenen Mitarbeiter über die Richtlinien und die Strategien des Instituts 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.

233. Falls die zuständigen Behörden von den Mutterunternehmen nach Artikel 106 Absatz 2 der Richtlinie 2013/36/EU die jährliche Veröffentlichung einer Beschreibung der Rechtsstruktur und Unternehmensführung sowie der Organisationsstruktur der Gruppe von Instituten verlangen, sollten die Informationen alle Unternehmen innerhalb der Gruppenstruktur nach der Definition in Richtlinie 2013/34/EU[42] nach Ländern einschließen.

234. Die Veröffentlichung sollte mindestens Folgendes umfassen:

a. eine Übersicht über die interne Organisation der Institute 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;

d. Informationen über die Struktur, Organisation und Mitglieder des Leitungsorgans, einschließlich der Zahl seiner Mitglieder und der Zahl der als unabhängig eingestuften

[42] 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).

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 Institute 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

In Einklang mit Titel III sollten die Institute 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, sofern anwendbar
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 Risikomanagement-Rahmens
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) Tochtergesellschaften, 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, Präventionsrichtlinien
    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