



Europäische Bankenaufsichtsbehörde EBA BS 2011 116 endgültig

27. September 2011

EBA-Leitlinien zur Internen Governance (GL 44)

London, 27. September 2011

EBA-Leitlinien zur Internen Governance

Status der Leitlinien

1. Das vorliegende Dokument beinhaltet Leitlinien gemäß Artikel 16 der 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 („EBA-Verordnung“). Nach Maßgabe von Artikel 16 Absatz 3 der EBA-Verordnung müssen die zuständigen Behörden und Finanzmarktteilnehmer alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

2. In den Leitlinien wird dargelegt, was die EBA unter angemessenen Aufsichtspraktiken im Europäischen System der Finanzaufsicht versteht bzw. wie nach ihrer Auffassung das Unionsrecht in einem bestimmten Bereich anzuwenden ist. EBA erwartet daher von allen zuständigen Behörden und Finanzmarktteilnehmern, an die diese Leitlinien gerichtet sind, dass sie diese befolgen, sofern sie nichts anderes angegeben haben. Dazu sollten die zuständigen Behörden die an sie gerichteten Leitlinien gegebenenfalls in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsvorschriften und/oder Veränderungen in ihren Lenkungs- bzw. Aufsichtsprozessen) integrieren, einschließlich solcher Leitlinien in diesem Dokument, die in erster Linie an Institute gerichtet sind.

Mitteilungserfordernisse

3. Die zuständigen Behörden müssen der EBA bis zum 28. November 2011 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, bzw. die Nichteinhaltung unter Angabe von Gründen mitteilen. Die Meldung sollte an die E-Mail-Adresse compliance@eba.europa.eu durch Personen erfolgen, die hierzu von den zuständigen Behörden bevollmächtigt worden sind.

4. Die im vorstehenden Absatz erwähnte Mitteilung der zuständigen Behörden wird nach Artikel 16 der EBA-Verordnung auf der Website der EBA veröffentlicht.

Im nachstehenden Text der Leitlinien werden gelegentlich zwischendurch spezifische Aspekte der Leitlinien anhand von Beispielen oder durch Begründung bestimmter Regelungen weiter erläutert. In diesem Fall erscheint der Text der Erläuterung in einem umrahmten Textfeld.

Inhaltsverzeichnis

EBA-Leitlinien zur Internen Governance	2
Titel I – Gegenstand, Anwendungsbereich und Begriffsbestimmungen	6
1. Gegenstand.....	6
2. Anwendungsbereich und -ebene	6
3. Begriffsbestimmungen	6
Titel II – Anforderungen an die interne Governance von Instituten.....	7
A. Unternehmensstruktur und Organisation	7
4. Organisatorischer Rahmen	7
5. Gegenseitige Kontrollen innerhalb einer Gruppenstruktur.....	7
6. „Kennen Sie Ihre Struktur“	9
7. Nicht-standardisierte oder nicht-transparente Tätigkeiten	10
B. Leitungsorgan	12
B.1 Pflichten und Aufgaben des Leitungsorgans.....	12
8. Aufgaben des Leitungsorgans	12
9. Beurteilung des Rahmens für die interne Governance	13
10. Leitungs- und Aufsichtsfunktionen des Leitungsorgans.....	13
B.2 Zusammensetzung und Arbeitsweise des Leitungsorgans	14
11. Zusammensetzung, Bestellung und Nachfolgeregelung für das Leitungsorgan	14
12. Verpflichtungen, Unabhängigkeit und Umgang mit Interessenkonflikten im Leitungsorgan	15
13. Qualifikationen des Leitungsorgans	16
14. Ablauforganisation und Arbeitsweise des Leitungsorgans.....	17
Bewertung der Arbeitsweise des Leitungsorgans.....	18
Rolle des/der Vorsitzenden des Leitungsorgan.....	18
Fachausschüsse des Leitungsorgans	19

Prüfungsausschuss.....	19
Risikoausschuss.....	20
B.3 Rahmen für das Geschäftsgebaren.....	20
15. Unternehmenswerte und Verhaltenskodex	20
16. Interessenkonflikte auf Ebene des Instituts	21
17. Interne Frühwarnmechanismen	22
B.4 Outsourcing- und Vergütungspolitik	23
18. Outsourcing.....	23
19. Steuerung der Vergütungspolitik	23
C. Risikomanagement	24
20. Risikokultur	24
21. Anpassung der Vergütung an das Risikoprofil	25
22. Rahmenwerk für das Risikomanagement.....	26
23. Neue Produkte	29
D. Interne Kontrolle	29
24. Interne Kontrollrichtlinien	29
25. Risikocontrolling-Funktion (RCF).....	31
26. Rolle der Risikocontrolling-Funktion	32
Rolle der RCF im Hinblick auf Strategie und Entscheidungen	32
Rolle der RCF bei Geschäften mit nahe stehenden Unternehmen.....	32
Rolle der RCF im Hinblick auf die Komplexität der Rechtsstruktur.....	33
Rolle der RCF bei wesentlichen Änderungen.....	33
Rolle der RCF bei Messungen und Bewertungen.....	33
Rolle der RCF bei der Überwachung	34
Rolle der RCF bei nicht genehmigten Risikopositionen	34
27. Chief Risk Officer.....	35
28. Compliance-Funktion	36
29. Interne Revision.....	37
E. Informationssysteme und Aufrechterhaltung des Geschäftsbetriebs.....	38

30.	Informationssystem und Kommunikation	38
31.	Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs.....	39
F.	Transparenz	40
32.	Nachvollziehbare Kommunikation	40
33.	Transparenz der internen Governance	40
Titel III – Schlussbestimmungen und Umsetzung		42
34.	Aufhebung	42
35.	Umsetzungsfrist	42

Titel I – Gegenstand, Anwendungsbereich und Begriffsbestimmungen

1. Gegenstand

Die Leitlinien sollen die Anforderungen der Aufsichtsbehörden harmonisieren und die korrekte Umsetzung der Regeln über die interne Governance in Einklang mit Artikel 22 und Anhang V der Richtlinie 2006/48/EG und dem nationalen Gesellschaftsrecht verbessern.

2. Anwendungsbereich und -ebene

1. Die zuständigen Behörden sollten von den Instituten die Einhaltung der in diesen Leitlinien zur Internen Governance verankerten Bestimmungen verlangen.
2. Die Anwendung dieser Leitlinien sollte von den zuständigen Behörden im Rahmen ihres aufsichtlichen Überprüfungs- und Bewertungsverfahrens überprüft werden.

Erläuterung

CEBS/EBA hat Leitlinien zum aufsichtlichen Überprüfungsverfahren erlassen, die auf der Website der EBA abrufbar sind.

3. Die Leitlinien gelten für Institute auf Einzelinstitutsebene sowie für Mutterunternehmen und Tochtergesellschaften auf konsolidierter oder subkonsolidierter Basis, sofern nicht anders angegeben.
4. Der Grundsatz der Verhältnismäßigkeit im Sinne der Richtlinien 2006/48/EG und 2006/49/EG (in der jeweils gültigen Fassung) findet Anwendung auf alle in diesen Leitlinien enthaltenen Bestimmungen. Ein Institut kann nachweisen, wie mit seiner Vorgehensweise, die Art, Umfang und Komplexität seiner Tätigkeiten widerspiegelt, das von den Leitlinien verlangte Ergebnis erreicht wird.

3. Begriffsbestimmungen

1. In diesen Leitlinien hat der Begriff *Leitungsorgan* folgende Bedeutung: das Lenkungsorgan (bzw. die Lenkungsorgane) eines Instituts, das die Aufsichts- und/oder die Leitungsfunktion umfasst, die oberste Entscheidungskompetenz besitzt und befugt ist, die Strategie, Ziele und die allgemeine Ausrichtung des Instituts festzulegen. Das Leitungsorgan umfasst diejenigen Personen, die die Geschäfte eines Instituts tatsächlich führen.
2. In diesen Leitlinien hat der Begriff *Institute* folgende Bedeutung: Kreditinstitute und Wertpapierfirmen im Sinne der Richtlinien 2006/48/EG und 2006/49/EG.

Titel II – Anforderungen an die interne Governance von Instituten

A. Unternehmensstruktur und Organisation

4. Organisatorischer Rahmen

1. Das Leitungsorgan eines Instituts sollte eine geeignete und transparente Unternehmensstruktur für dieses Institut gewährleisten. Die Struktur sollte eine wirksame und umsichtige Führung eines Instituts sowohl auf Einzelinstitutsebene als auch auf Gruppenebene fördern und unter Beweis stellen. Die Berichtswege sowie die Aufgabenverteilung und Kompetenzregelungen innerhalb eines Instituts sollten klar, genau abgegrenzt, stimmig und durchsetzbar sein.
2. Das Leitungsorgan sollte dafür Sorge tragen, dass die Struktur eines Instituts und ggf. die Strukturen innerhalb einer Gruppe klar und transparent sind, und zwar sowohl für das eigene Personal des Instituts als auch für die Aufsichtsbehörde.
3. Das Leitungsorgan sollte beurteilen, wie die unterschiedlichen Bestandteile der Unternehmensstruktur sich gegenseitig ergänzen und zusammenwirken. Durch die Struktur darf die Leistungsfähigkeit des Leitungsorgans, die Risiken des Instituts oder der Gruppe effektiv zu überwachen und zu steuern, nicht beeinträchtigt werden.
4. Das Leitungsorgan sollte beurteilen, wie sich Veränderungen der Struktur der Gruppe auf deren Solidität auswirken. Das Leitungsorgan sollte jegliche erforderlichen Anpassungen unverzüglich vornehmen.

Erläuterung

Veränderungen können sich beispielsweise aus der Gründung neuer Tochtergesellschaften, aus Fusionen und Übernahmen, aus dem Verkauf oder der Auflösung von Teilen der Gruppe oder aus externen Entwicklungen ergeben.

5. Gegenseitige Kontrollen innerhalb einer Gruppenstruktur

1. Innerhalb einer Gruppenstruktur sollte das Leitungsorgan des Mutterunternehmens eines Instituts die Gesamtverantwortung für eine angemessene gruppenweite interne Governance tragen und sicherstellen, dass es ein Governance Rahmenwerk gibt, das der Struktur, dem Geschäftsmodell und den Risiken der Gruppe und der ihr zugehörigen Einzelunternehmen entspricht.
2. Das Leitungsorgan einer regulierten Tochtergesellschaft einer Gruppe sollte sich auf Einzelunternehmensebene zu den gleichen internen Governance Werten und Richtlinien bekennen wie das Mutterunternehmen, sofern aufgrund rechtlicher oder aufsichtlicher Anforderungen oder

Verhältnismäßigkeitserwägungen nichts anderes bestimmt wird. Dementsprechend sollte das Leitungsorgan einer regulierten Tochtergesellschaft innerhalb der eigenen internen Governance Verantwortung seine Strategien festlegen und sämtliche Entscheidungen oder Praktiken auf Gruppenebene auswerten, damit gewährleistet ist, dass die regulierte Tochtergesellschaft nicht gegen geltende Rechtsvorschriften oder aufsichtliche Regeln verstößt. Das Leitungsorgan der regulierten Tochtergesellschaft sollte ferner gewährleisten, dass solche Entscheidungen oder Praktiken

- a. der korrekten und umsichtigen Führung der Tochtergesellschaft;
- b. der finanziellen Gesundheit der Tochtergesellschaft; oder
- c. den rechtlichen Interessen der Stakeholder (Anspruchsberechtigte) der Tochtergesellschaft

nicht abträglich sind.

3. Die Leitungsorgane sowohl des Mutterunternehmens als auch der Tochtergesellschaften sollten die nachfolgenden Absätze unter Berücksichtigung der Auswirkungen der Größe der Gruppe auf die interne Governance anwenden.
4. Bei der Wahrnehmung der Governancepflichten sollte sich das Leitungsorgan des Mutterunternehmens eines Instituts sämtliche wesentliche Risiken und Sachverhalte bewusst machen, die sich auf die Gruppe, das Mutterinstitut selbst sowie dessen Tochtergesellschaften auswirken könnten. Es sollte daher in geeigneter Weise und unter Berücksichtigung der unabhängigen rechtlichen Aufgaben und Governancepflichten, die für Leitungsorgane regulierter Tochtergesellschaften gelten, Aufsicht über seine Tochtergesellschaften ausüben.
5. Zur Wahrnehmung seiner internen Governance-Verantwortung das Leitungsorgan des Mutterunternehmens eines Instituts
 - a. eine Governancestruktur schaffen, die zu einer wirksamen Aufsicht über seine Tochtergesellschaften beiträgt und die der Art, dem Umfang und der Komplexität der unterschiedlichen Risiken der Gruppe und ihrer Tochtergesellschaften Rechnung trägt;
 - b. eine interne Governance Richtlinie auf Gruppenebene für seine Tochtergesellschaften verabschieden, in welcher auch die Verpflichtung enthalten ist, alle geltenden Governance Anforderungen zu erfüllen;
 - c. gewährleisten, dass ausreichend Ressourcen für jede Tochtergesellschaft zur Verfügung stehen, damit diese sowohl die Gruppen- als auch die lokalen Governance-Standards erfüllen kann;
 - d. angemessene Mittel und Möglichkeiten bereitstellen, um zu überwachen, dass jede Tochtergesellschaft allen geltenden Anforderungen an die interne Governance nachkommt; und

- e. gewährleisten, dass die Berichtswege innerhalb einer Gruppe klar und transparent sind, insbesondere dann, wenn die Geschäftsfelder nicht der rechtlichen Struktur der Gruppe entsprechen.
- 6. Eine regulierte Tochtergesellschaft sollte in Betracht ziehen, als Element einer soliden Governance auch eine ausreichende Anzahl unabhängiger Mitglieder in das Leitungsorgan zu berufen. Unabhängige Mitglieder des Leitungsorgans sind solche ohne Geschäftsführungsverantwortung, die unabhängig von der Tochtergesellschaft und von deren Gruppe sowie vom beherrschenden Anteilseigner sind.

6. „Kennen Sie Ihre Struktur“

- 1. Das Leitungsorgan sollte die operative Struktur eines Instituts („Kennen Sie Ihre Struktur“) genau kennen und verstehen sowie dafür Sorge tragen, dass diese der genehmigten Geschäftsstrategie und dem Risikoprofil entspricht.

Erläuterung

Es ist von maßgeblicher Bedeutung, dass das Leitungsorgan die operative Struktur eines Instituts genau kennt und versteht. In Fällen, in denen viele rechtliche Einheiten innerhalb einer Gruppe bestehen, können deren Anzahl und insbesondere die zwischen ihnen bestehenden Verbindungen und Geschäftsvorgänge die Ausgestaltung seiner internen Governance und die Steuerung und Überwachung der Risiken der Gruppe insgesamt vor große Herausforderungen stellen, was an sich schon ein Risiko darstellt.

- 2. Das Leitungsorgan sollte die Struktur, Entwicklung und Grenzen des Instituts steuern und verstehen und dafür Sorge tragen, dass die Struktur angemessen ist und keine übermäßige oder unangemessene Komplexität mit sich bringt. Es ist ferner für die Genehmigung solider Strategien und Richtlinien bei der Schaffung neuer Strukturen zuständig. Ebenso sollte das Leitungsorgan die Risiken, die sich aus der Komplexität der Struktur der Rechtseinheit selbst ergeben, erkennen und gewährleisten, dass das Institut in der Lage ist, rechtzeitig Informationen zu Art, Satzung, Eigentümerstruktur und Geschäftstätigkeit jeder einzelnen Rechtseinheit vorzulegen.
- 3. Das Leitungsorgan des Mutterunternehmens eines Instituts sollte nicht nur die Unternehmensorganisation der Gruppe, sondern auch den Gegenstand der einzelnen rechtlichen Einheiten sowie die Verbindungen und Beziehungen zwischen ihnen verstehen. Hierzu gehört auch das Verständnis für gruppenspezifische operative Risiken, das gruppeninterne Engagement und Beeinträchtigungen der Finanzierung der Gruppe, ihr Eigenkapital und ihre Risikoprofile unter normalen sowie unter widrigen Bedingungen.
- 4. Das Leitungsorgan des Mutterunternehmens eines Instituts sollte dafür Sorge tragen, dass die verschiedenen Unternehmen der Gruppe (einschließlich des

Instituts selbst) ausreichend Informationen erhalten, damit sich alle ein klares Bild von den allgemeinen Zielen und Risiken der Gruppe verschaffen können. Wichtige Informationsflüsse zwischen den Einheiten, die für den operativen Betrieb der Gruppe wichtig sind, sollten dokumentiert und auf Anfrage und soweit erforderlich, dem Leitungsorgan, den Kontrollfunktionen und den Aufsehern unverzüglich zur Verfügung gestellt werden.

5. Das Leitungsorgan des Mutterunternehmens eines Instituts sollte dafür Sorge tragen, dass es über die Risiken, die durch die Struktur der Gruppe verursacht werden, immer auf dem Laufenden ist. Dies umfasst
 - a. Informationen zu den wichtigsten Risikotreibern und
 - b. regelmäßige Berichte, in denen die Struktur des Instituts insgesamt bewertet und beurteilt wird, ob die einzelnen Unternehmen ihre Geschäftstätigkeit in Einklang mit der verabschiedeten Strategie ausüben.

7. Nicht-standardisierte oder nicht-transparente Tätigkeiten

1. Bei Instituten, die im Rahmen von Zweckgesellschaften oder ähnlichen Strukturen oder aber in Ländern tätig sind, in denen die Transparenz nicht gegeben ist oder die nicht den internationalen Bankenstandards entsprechen, sollte das Leitungsorgan deren Gegenstand und Struktur sowie die damit verbundenen besonderen Risiken verstehen. Das Leitungsorgan darf solchen Tätigkeiten nur dann zustimmen, wenn es sich selbst davon überzeugt hat, dass die Risiken sachgerecht gesteuert werden.

Erläuterung

Neben diesem Grundsatz können die zuständigen Behörden aber auch die „*Core Principles for Effective Banking Supervision*“ anwenden, die vom Basler Ausschuss für Bankenaufsicht für die Beurteilung der Geschäftsaktivitäten in Rechtsordnungen entwickelt wurden, die nicht vollständig transparent sind oder nicht dem internationalen Bankenstandard entsprechen.

Das Institut kann berechtigte Gründe haben, in bestimmten Rechtsordnungen tätig zu werden (oder mit in diesen Rechtsordnungen tätigen juristischen Personen oder Geschäftspartnern zusammenzuarbeiten) oder bestimmte Strukturen einzuführen (z. B. Zweckgesellschaften oder Firmentrusts). Doch Tätigkeiten in Ländern, die nur eingeschränkt transparent sind oder nicht den internationalen Bankenstandards entsprechen (z. B. in den Bereichen aufsichtliche Überwachung, Steuerhinterziehung, Geldwäsche oder Terrorismusfinanzierung), oder Tätigkeiten im Rahmen komplexer oder nicht transparenter Strukturen können mit spezifischen rechtlichen, Reputations- und finanziellen Risiken verbunden sein. Sie behindern möglicherweise auch das Leitungsorgan in seiner Fähigkeit, die Geschäfte angemessen zu überwachen, und verhindern eine wirksame Bankenaufsicht. Sie sollten daher nur dann genehmigt und fortgeführt werden, wenn ihr Zweck definiert und verstanden

wird, wenn eine wirksame Überwachung gewährleistet ist und wenn alle wesentlichen Risiken, die durch diese Strukturen möglicherweise verursacht werden, in geeigneter Weise gesteuert werden können.

Aus diesem Grund, und da diese eine erhebliche Herausforderung für das Verständnis der Gruppenstruktur darstellen, sollte das Leitungsorgan all diesen Fällen besonderes Augenmerk widmen.

2. Das Leitungsorgan sollte kontinuierlich geeignete Strategien, Richtlinien und Verfahren für die Genehmigung und Aufrechterhaltung solcher Strukturen und Tätigkeiten festlegen, beibehalten und überprüfen, um zu gewährleisten, dass diese nach wie vor ihrem beabsichtigten Zweck entsprechen.
3. Das Leitungsorgan sollte dafür Sorge tragen, dass angemessene Maßnahmen ergriffen werden, um die Risiken in Verbindung mit derartigen Tätigkeiten zu verhindern oder zu mindern. Hierzu gehört auch, dass
 - a. das Institut über angemessene Richtlinien und Verfahren sowie dokumentierte Prozesse (z. B. geeignete Grenzwerte, Informationspflichten) zur Prüfung, Genehmigung und zum Risikomanagement solcher Tätigkeiten verfügt und dabei den Folgen für die operative Struktur der Gruppe Rechnung trägt;
 - b. Informationen über diese Tätigkeiten und die damit verbundenen Risiken dem Hauptsitz des Instituts und den Abschlussprüfern zugänglich gemacht und dem Leitungsorgan sowie den Aufsehern mitgeteilt werden;
 - c. das Institut in regelmäßigen Abständen prüft, ob nach wie vor die Notwendigkeit besteht, Tätigkeiten auszuführen, die die Transparenz beeinträchtigen.
4. Dieselben Maßnahmen sollten ergriffen werden, wenn ein Institut nicht standardisierte oder nicht transparente Tätigkeiten für Kunden wahrnimmt.

Erläuterung

Nicht standardisierte oder nicht transparente Tätigkeiten für Kunden (z. B. Unterstützung der Kunden bei der Gründung von Zweckgesellschaften in Offshore-Ländern; Entwicklung komplexer Strukturen und Durchführung von Finanzgeschäften für sie oder Bereitstellung von Treuhanddiensten) stellen die interne Governance vor ähnliche Herausforderungen und können mit erheblichen operativen und Reputationsrisiken verbunden sein. Daher sind dieselben Risikomanagementmaßnahmen zu ergreifen wie für die eigenen Geschäftstätigkeiten der Institute.

5. All diese Strukturen und Tätigkeiten sollten Gegenstand regelmäßiger interner und externer Prüfungen sein.

B. Leitungsorgan

B.1 Pflichten und Aufgaben des Leitungsorgans

8. Aufgaben des Leitungsorgans

1. Das Leitungsorgan sollte die Gesamtverantwortung für das Institut tragen und die Strategie des Instituts festlegen. Die Aufgaben des Leitungsorgans sollten klar definiert, schriftlich festgelegt und genehmigt werden.

Erläuterung

Die umsichtige Wahrnehmung der Aufgaben des Leitungsorgans ist die Grundlage für die solide und umsichtige Führung des Instituts. Die dokumentierten Aufgaben sollten außerdem mit dem nationalen Unternehmensrecht in Einklang stehen.

2. Zu den wichtigsten Aufgaben des Leitungsorgans gehört die Festlegung und die Überwachung:
 - a. der allgemeinen Geschäftsstrategie des Instituts innerhalb der geltenden rechtlichen und aufsichtsrechtlichen Rahmenbedingungen unter Berücksichtigung der langfristigen finanziellen Interessen und der Solvenz des Instituts;
 - b. der allgemeinen Risikostrategie und -politik des Instituts einschließlich seiner Risikobereitschaft und Risikoneigung sowie seines Rahmens für das Risikomanagement;
 - c. zur Absicherung der Risiken des Instituts angemessener Beträge, Art und Verteilung von Eigenkapital und Eigenmitteln.;
 - d. einer robusten und transparenten Organisationsstruktur mit wirksamen Kommunikations- und Berichtswegen;
 - e. einer Politik für die Bestellung und Nachfolgeregelung von Personen mit Schlüsselfunktionen im Institut;
 - f. eines Entgeltrahmens, der auf die Risikostrategien des Instituts abgestimmt ist;
 - g. der Governance-Grundsätze und Unternehmenswerte des Instituts einschließlich eines Verhaltenskodexes oder vergleichbaren Dokuments; und
 - h. eines angemessenen und wirksamen internen Kontrollrahmens, der gut funktionierende Risikokontroll- und Compliance-Funktionen, eine interne

Revision sowie einen angemessenen Rahmen für die Finanzberichterstattung und Rechnungslegung umfasst.

3. Das Leitungsorgan sollte außerdem regelmäßig diese Richtlinien und Strategien überprüfen und anpassen. Das Leitungsorgan ist für eine angemessene Kommunikation mit den Aufsichtsbehörden und sonstigen Beteiligten verantwortlich.

9. Beurteilung des Rahmens für die interne Governance

1. Das Leitungsorgan sollte die Wirksamkeit des Rahmens des Instituts für die interne Governance in regelmäßigen Abständen überwachen und prüfen.
2. Eine solche Überprüfung des Rahmens für die interne Governance und dessen Umsetzung sollte mindestens einmal pro Jahr erfolgen. Den Schwerpunkt sollten dabei Veränderungen interner und externer Faktoren bilden, die sich auf das Institut auswirken.

10. Leitungs- und Aufsichtsfunktionen des Leitungsorgans

1. Die Leitungs- und Aufsichtsfunktion des Leitungsorgans eines Instituts sollten effektiv zusammenwirken.

Erläuterung

In den Mitgliedstaaten ist eine der beiden folgenden **Governancestrukturen** – eine monistische oder dualistische Führungsstruktur – üblich. Bei beiden Strukturen spielt das Leitungsorgan in seiner Leitungsfunktion und das Aufsichtsfunktion in seiner Aufsichtsfunktion jeweils eine eigene Rolle bei der Leitung des Instituts, und zwar entweder direkt oder über Ausschüsse.

Die Leitungsfunktion schlägt die allgemeine Ausrichtung des Instituts vor, gewährleistet die wirksame Umsetzung der Strategie und ist für den täglichen Geschäftsbetrieb des Instituts verantwortlich.

Die Aufsichtsfunktion überwacht die Leitungsfunktion und berät sie. Ihre Aufsichtsfunktion besteht darin, die Erstellung der Strategie eines Instituts konstruktiv zu begleiten und zu hinterfragen, die Leistung der Leitungsfunktion und die Verwirklichung der vereinbarten Ziele zu überwachen und die Verlässlichkeit und Vollständigkeit der Finanzinformationen sowie ein wirksames Risikomanagement und interne Kontrollen zu gewährleisten.

Für eine gute Unternehmensführung sollten die Leitungs- und die Aufsichtsfunktion eines Instituts effizient zusammenwirken, um die vereinbarte Strategie des Instituts umzusetzen und insbesondere die Risiken des Instituts zu steuern. Auch wenn sich die Rechts- und Regulierungsrahmen verschiedener Länder möglicherweise erheblich voneinander unterscheiden, sollte dadurch ein

effizientes Zusammenwirken dieser beiden Funktionen nicht ausgeschlossen werden, unabhängig davon, ob das Leitungsorgan monistischer oder dualistischer Natur ist.

2. Das Leitungsorgan in seiner Aufsichtsfunktion soll
 - a. willens und in der Lage sein, Vorschläge, Erläuterungen und Informationen, die von den Mitgliedern des Leitungsorgans in seiner Leitungsfunktion bereitgestellt werden, kritisch zu hinterfragen und zu überprüfen;
 - b. überwachen, ob die Strategie, die Risikobereitschaft und Risikoneigung und die Richtlinien des Instituts konsequent umgesetzt und ob die Leistungsstandards im Einklang mit dessen langfristigen finanziellen Interessen und Solvenz eingehalten werden; und
 - c. die Leistung der Mitglieder des Leitungsorgans in seiner Leitungsfunktion anhand dieser Standards überwachen.
3. Das Leitungsorgan sollte in seiner Leitungsfunktion die Geschäfts- und Risikostrategien des Instituts zusammen mit dem Leitungsorgan in seiner Aufsichtsfunktion koordinieren und mit dem Leitungsorgan in seiner Aufsichtsfunktion regelmäßig die Umsetzung dieser Strategien erörtern.
4. Jede Funktion sollte der anderen Funktion ausreichende Informationen zur Verfügung stellen. Das Leitungsorgan in seiner Leitungsfunktion sollte das Leitungsorgan in seiner Aufsichtsfunktion umfassend und regelmäßig und ggf. unverzüglich über die Sachverhalte informieren, die für die Beurteilung einer Situation, die Führung des Instituts und den Erhalt seiner finanziellen Sicherheit wichtig sind.

B.2 Zusammensetzung und Arbeitsweise des Leitungsorgans

11. Zusammensetzung, Bestellung und Nachfolgeregelung für das Leitungsorgan

1. Das Leitungsorgan sollte aus einer ausreichenden Zahl von Mitgliedern bestehen und eine geeignete Zusammensetzung aufweisen. Das Leitungsorgan sollte über Richtlinien für die Auswahl, Überwachung und Planung der Nachfolge seiner Mitglieder verfügen.
2. Ein Institut sollte die Größe und Zusammensetzung seines Leitungsorgans unter Berücksichtigung der Größe und Komplexität des Instituts sowie der Art und des Umfangs seiner Tätigkeiten festlegen. Bei der Auswahl der Mitglieder des Leitungsorgans sollte sichergestellt werden, dass diese gemeinsam über eine ausreichende Fachkompetenz verfügen.
3. Das Leitungsorgan sollte qualifizierte und erfahrene Kandidaten finden und auswählen und für das Leitungsorgan eine angemessene Nachfolgeplanung

sicherstellen, wobei rechtliche Anforderungen an die Zusammensetzung, Bestellung und Nachfolgeregelung gebührend berücksichtigt werden.

4. Das Leitungsorgan sollte dafür Sorge tragen, dass ein Institut über Richtlinien zur Auswahl neuer Mitglieder und zur Wiederbestellung der amtierenden Mitglieder verfügt. Diese Richtlinien sollten auch eine Beschreibung der erforderlichen Fähigkeiten, Fertigkeiten und Kompetenzen umfassen, um eine ausreichende Sachkenntnis zu gewährleisten.
5. Die Mitglieder des Leitungsorgans sollten für einen angemessenen Zeitraum bestellt werden. Die erneute Nominierung amtierender Mitglieder sollte auf dem vorstehend genannten Profil beruhen und erst nach einer sorgfältigen Prüfung der Leistung der Mitglieder in der letzten Amtszeit erfolgen.
6. Bei der Erstellung eines Nachfolgeplans für seine Mitglieder sollte das Leitungsorgan das Ende des Vertrags bzw. Mandats der einzelnen Mitglieder berücksichtigen, um möglichst zu verhindern, dass zu viele Mitglieder gleichzeitig ersetzt werden müssen.

12. Verpflichtungen, Unabhängigkeit und Umgang mit Interessenkonflikten im Leitungsorgan

1. Mitglieder des Leitungsorgans sollten sich aktiv mit den Geschäften eines Instituts beschäftigen und in der Lage sein, eigene fundierte, objektive und unabhängige Entscheidungen zu treffen und Urteile abzugeben.
2. Bei der Auswahl der Mitglieder des Leitungsorgans sollte sichergestellt werden, dass das Leitungsorgan über ausreichend Sachkenntnis und Unabhängigkeit verfügt. Ein Institut sollte dafür Sorge tragen, dass den Mitgliedern des Leitungsorgans genügend Zeit und Kapazitäten für die effiziente Wahrnehmung ihrer Aufgaben zur Verfügung stehen.
3. Mitglieder des Leitungsorgans sollten nur eine begrenzte Anzahl von Mandaten haben bzw. einer begrenzten Zahl sonstiger zeitaufwändiger beruflicher Tätigkeiten nachgehen. Darüber hinaus sollten die Mitglieder das Institut über ihre nebenberuflichen Tätigkeiten (z. B. Mandate bei anderen Unternehmen) unterrichten. Da der/die Vorsitzende mehr Aufgaben und Pflichten hat, wird von ihm/ihr erwartet, dass er/sie auch mehr Zeit für diese Aufgabe aufbringt.
4. Der von allen Mitgliedern des Leitungsorgans erwartete Mindestzeitaufwand sollte schriftlich festgehalten werden. Wenn die Bestellung eines neuen Mitglieds in Betracht gezogen wird oder ein aktuelles Mitglied ein neues Mandat übernimmt, sollten die Mitglieder des Leitungsorgans prüfen, inwieweit diese Person für die Wahrnehmung ihrer Aufgaben für das Institut ausreichend Zeit aufbringen kann. Die Teilnahme der Mitglieder des Leitungsorgans in seiner Aufsichtsfunktion sollte offen gelegt werden. Ein Institut sollte außerdem in Betracht ziehen, den langfristigen Ausfall von Mitgliedern des Leitungsorgans in seiner Leitungsfunktion ebenfalls offen zu legen.
5. Die Mitglieder des Leitungsorgans sollten in der Lage sein, objektiv, kritisch und unabhängig zu handeln. Die Maßnahmen zur Verbesserung der Fähigkeit,

objektiv, kritisch und unabhängig zu entscheiden, sollten auch die Bestellung von Mitgliedern aus einer ausreichend breit gefächerten Kandidatengruppe sowie eine ausreichende Anzahl von Mitgliedern ohne Geschäftsführungsverantwortung umfassen.

Erläuterung

In Fällen, in denen das Leitungsorgan in seiner Aufsichtsfunktion ausdrücklich vom Leitungsorgan in seiner Leitungsfunktion getrennt ist, sollte die Objektivität und Unabhängigkeit des Leitungsorgans in seiner Aufsichtsfunktion dennoch durch eine geeignete Auswahl unabhängiger Mitglieder gewährleistet werden.

6. Das Leitungsorgan sollte über schriftliche Richtlinien für den Umgang mit Interessenkonflikten für seine Mitglieder verfügen. In diesen Richtlinien sollten folgende Punkte geregelt sein:
 - a. die Pflicht eines Mitglieds, Interessenkonflikte zu vermeiden, die dem Leitungsorgan nicht mitgeteilt und von ihm nicht gebilligt wurden, oder ansonsten die Pflicht sicherzustellen, dass Konflikte angemessen gelöst werden;
 - b. ein Überprüfungs- oder Genehmigungsverfahren, das Mitglieder durchlaufen müssen, bevor sie bestimmte Tätigkeiten (etwa ein Amt in einem anderen Leitungsorgan) übernehmen, damit sichergestellt ist, dass das neue Amt nicht zu einem Interessenkonflikt führt;
 - c. die Pflicht eines Mitglieds, dem Institut alles mitzuteilen, was zu einem Interessenkonflikt führen könnte bzw. bereits geführt hat;
 - d. die Verpflichtung eines Mitglieds, auf die Teilnahme an der Entscheidungsfindung oder an der Abstimmung über eine Frage zu verzichten, wenn hierzu ein Interessenskonflikt des Mitglieds bestehen könnte bzw. wenn die Objektivität oder Fähigkeit des Mitglieds, seinen Verpflichtungen gegenüber dem Institut ordnungsgemäß nachzukommen, anderweitig gefährdet sein könnte;
 - e. angemessene Verfahren für Geschäfte mit nahe stehenden Dritten zu marktüblichen Konditionen; und
 - f. die Modalitäten für den Umgang des Leitungsorgans mit einer Nichteinhaltung dieser Richtlinien.

13. Qualifikationen des Leitungsorgans

1. Die Mitglieder des Leitungsorgans sollten für ihr Amt qualifiziert sein und bleiben, was auch Fortbildungsmaßnahmen einschließt. Sie sollten eine klare

Vorstellung zu den Governancemaßnahmen des Instituts und ihrer diesbezüglichen Aufgaben haben.

2. Die Mitglieder des Leitungsorgans sollten individuell und kollektiv über die für die ordnungsgemäße Wahrnehmung ihrer Aufgaben erforderliche Sachkenntnis, Erfahrung, Kompetenzen, das Verständnis und die persönlichen Qualitäten einschließlich Professionalität und persönlicher Integrität verfügen.
3. Die Mitglieder des Leitungsorgans sollten einen aktuellen, ihren Aufgaben entsprechenden Kenntnisstand von den Geschäften des Instituts besitzen. Dies umfasst auch angemessene Kenntnis über diejenigen Bereiche, für die sie zwar nicht direkt verantwortlich, jedoch gemeinsam rechenschaftspflichtig sind.
4. Gemeinsam sollten sie die Art der Geschäftstätigkeit des Instituts und die damit verbundenen Risiken in vollem Umfang verstehen können und über ausreichende Fachkenntnisse und Erfahrung in allen wesentlichen, vom Institut beabsichtigten Tätigkeiten verfügen, damit eine wirksame Governance und Aufsicht möglich sind.
5. Ein Institut sollte über ein solides Verfahren verfügen, damit gewährleistet ist, dass die Mitglieder des Leitungsorgans individuell und kollektiv über ausreichende Qualifikationen verfügen.
6. Die Mitglieder des Leitungsorgans sollten zur Wahrnehmung ihrer Aufgaben Kenntnisse und Fertigkeiten erwerben, pflegen und vertiefen. Institute sollten sicherstellen, dass die Mitglieder Zugang zu individuell zugeschnittenen Fortbildungsprogrammen haben, die den Lücken in dem vom Institut benötigten Wissensprofil sowie den tatsächlichen Kenntnissen der Mitglieder Rechnung tragen. Hierzu gehören Bereiche wie z. B. Risikomanagementinstrumente und -modelle des Instituts, neue Entwicklungen, Organisationsänderungen, komplexe Produkte, neue Produkte oder Märkte und Fusionen. Die Fortbildungsmaßnahmen sollten sich aber auch auf Geschäftsbereiche erstrecken, die nicht unmittelbar in den Zuständigkeitsbereich der einzelnen Mitglieder fallen. Das Leitungsorgan sollte genügend Zeit, Mittel und sonstige Ressourcen für Fortbildungsmaßnahmen aufwenden.

14. Ablauforganisation und Arbeitsweise des Leitungsorgans

1. Das Leitungsorgan sollte angemessene interne Governancepraktiken und -verfahren für seine eigene Organisation und Arbeitsweise festlegen und über die Mittel verfügen, um sicherzustellen, dass diese Praktiken eingehalten und in regelmäßigen Abständen im Hinblick auf mögliche Verbesserungen überprüft werden.

Erläuterung

Solide Governancepraktiken und -verfahren des Leitungsorgans senden intern und extern wichtige Signale bezüglich Governancerichtlinien und -ziele des Instituts aus. Zu den Praktiken und Verfahren gehören auch die Häufigkeit, der

Ablauf und die Protokolle der Sitzungen, die Rolle des Vorsitzenden und die Nutzung von Ausschüssen.

2. Das Leitungsorgan sollte regelmäßig zusammentreten, um seinen Aufgaben angemessen und wirksam nachkommen zu können. Die Mitglieder des Leitungsorgans sollten genügend Zeit für die Vorbereitung der Sitzungen aufbringen. Diese Vorbereitung umfasst auch die Erstellung einer Tagesordnung. Aus dem Protokoll sollten die Tagesordnungspunkte, die gefassten Beschlüsse und die vereinbarten Maßnahmen klar hervorgehen. Diese Praktiken und Verfahren sowie die Rechte, Aufgaben und wichtigsten Tätigkeiten des Leitungsorgans sollten dokumentiert und in regelmäßigen Abständen vom Leitungsorgan überprüft werden.

Bewertung der Arbeitsweise des Leitungsorgans

3. Das Leitungsorgan sollte die individuelle und kollektive Effizienz und Wirksamkeit seiner Tätigkeiten, Governancepraktiken und -verfahren sowie die Arbeitsweise der Ausschüsse regelmäßig bewerten. Mit dieser Bewertung können Externe beauftragt werden.

Rolle des/der Vorsitzenden des Leitungsorgan

4. Der/Die Vorsitzende sollte dafür sorgen, dass das Leitungsorgan fundierte und sachkundige Beschlüsse fassen kann. Er/Sie sollte eine offene und kritische Diskussion fördern und anregen und gewährleisten, dass auch abweichende Ansichten geäußert und im Rahmen des Entscheidungsprozesses diskutiert werden können.

Erläuterung

Der/Die Vorsitzende des Leitungsorgans spielt für das ordnungsgemäße Arbeiten des Leitungsorgans eine maßgebliche Rolle. Er/Sie leitet das Leitungsorgan und ist dafür verantwortlich, dass dieses insgesamt wirksam arbeiten kann.

5. In einem monistischen System sollte der/die Vorsitzende des Leitungsorgans nicht gleichzeitig ein Geschäftsleiter desselben Instituts sein. Ist der/die Vorsitzende/r des Leitungsorgans auch ein Geschäftsleiter des Instituts, sollte das Institut über Maßnahmen verfügen, um die potenzielle Beeinträchtigung der gegenseitigen Kontrolle auf ein Mindestmaß zu reduzieren.

Erläuterung

Die gegenseitige Kontrolle könnte beispielsweise auch darin bestehen, dass ein langjähriges unabhängiges Mitglied des Leitungsorgans in seiner Aufsichtsfunktion eine führende oder dem vergleichbare Position einnimmt.

Fachausschüsse des Leitungsorgans

6. Das Leitungsorgan in seiner Aufsichtsfunktion sollte unter Berücksichtigung der Größe und Komplexität eines Instituts die Einrichtung von Fachausschüssen in Erwägung ziehen, denen Mitglieder des Leitungsorgans angehören (weitere Personen können zur Teilnahme eingeladen werden, sofern ihre spezifischen Fachkenntnisse oder ihr Rat in einer bestimmten Frage wichtig sind). Fachausschüsse können auch einen Prüfungsausschuss, einen Risikoausschuss, einen Vergütungsausschuss, einen Nominierungs- oder einen Personalausschuss und/oder einen Governance- bzw. Ethik- bzw. Compliance-Ausschuss umfassen.

Erläuterung

Die Übertragung von Aufgaben auf solche Ausschüsse entbindet das Leitungsorgan in seiner Aufsichtsfunktion keinesfalls von der kollektiven Erfüllung seiner Aufgaben und Pflichten, sondern kann es in bestimmten Bereichen unterstützen, wenn dies die Entwicklung und Umsetzung guter Governancepraktiken sowie von Entscheidungen erleichtert.

7. Ein Fachausschuss sollte über eine optimale Mischung aus Fachkenntnissen, Kompetenzen und Erfahrung verfügen, die es ihm in ihrer Kombination ermöglichen, relevante Fragen objektiv zu beurteilen und neue Ideen einzubringen. Dem Fachausschuss sollte eine ausreichend hohe Anzahl unabhängiger Mitglieder angehören. Jeder Ausschuss sollte vom Leitungsorgan in seiner Aufsichtsfunktion ein dokumentiertes Mandat (einschließlich seines Wirkungsbereichs) erhalten und über festgelegte Arbeitsverfahren verfügen. Die Mitgliedschaft in und der Vorsitz eines Ausschusses können gelegentlich rotieren.

Erläuterung

Mithilfe der Rotation der Mitglieder und des Vorsitzes können eine unzulässige Machtkonzentration verhindert und neue Perspektiven erschlossen werden.

8. Die jeweiligen Ausschussvorsitzenden sollten regelmäßig an das Leitungsorgan berichten. Die Fachausschüsse sollten ggf. zusammenwirken und -arbeiten, um die Konsistenz zu gewährleisten und Defiziten vorzubeugen. Dies kann durch die gegenseitige Mitwirkung geschehen, d. h. der Vorsitzende oder ein Mitglied eines Fachausschusses könnte zugleich auch Mitglied eines anderen Fachausschusses sein.

Prüfungsausschuss

9. Ein Prüfungsausschuss (oder ein vergleichbarer Ausschuss) sollte u. a. die Wirksamkeit der innerbetrieblichen Kontrolle des Unternehmens, der Innenrevision und der Risikomanagementsysteme überwachen, die externen Rechnungsprüfer des Instituts beaufsichtigen, dem Leitungsorgan Vorschläge

zur Bestellung, Entschädigung und Abberufung der externen Rechnungsprüfer unterbreiten, den Umfang und die Häufigkeit der Revisionen überprüfen und genehmigen, die Revisionsberichte überprüfen und kontrollieren, ob das Leitungsorgan in seiner Leitungsfunktion rechtzeitig die erforderlichen Abhilfemaßnahmen zur Beseitigung von Schwachstellen in der Kontrolle, bei der Nichterfüllung von Gesetzen, Rechtsvorschriften und Richtlinien und anderen von den Prüfern festgestellten Problemen ergreift. Der Prüfungsausschuss sollte darüber hinaus die Einführung von Rechnungslegungsstandards durch das Institut überwachen.

Erläuterung

Siehe auch Art. 41 der Richtlinie 2006/43/EG über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen.

10. Der/Die Vorsitzende des Ausschusses sollte unabhängig sein. Falls der/die Vorsitzende ein ehemaliges Mitglied der Leitungsfunktion des Instituts ist, sollte er/sie eine angemessene Frist verstreichen lassen, bevor er/sie das Amt des/der Ausschussvorsitzenden antritt.
11. Mitglieder des Prüfungsausschusses insgesamt sollten über aktuelle und einschlägige Praxiserfahrung im Bereich Finanzmärkte oder aufgrund ihres beruflichen Hintergrunds über ausreichende Berufserfahrung verfügen, die eine unmittelbare Verbindung mit dem Bereich Finanzmärkte widerspiegelt. Der/die Vorsitzende des Prüfungsausschusses sollte in jedem Fall Fachkenntnisse und Erfahrung in der Anwendung von Rechnungslegungsgrundsätzen und internen Kontrollverfahren besitzen.

Risikoausschuss

12. Ein Risikoausschuss (oder ein vergleichbarer Ausschuss) sollte dafür zuständig sein, das Leitungsorgan in Fragen der aktuellen und künftigen Risikobereitschaft/Risikoneigung und -strategie des Instituts insgesamt zu beraten und die Umsetzung dieser Strategie zu beaufsichtigen. Zur Steigerung seiner Effizienz sollte der Risikoausschuss regelmäßig mit der Risikokontrollfunktion und dem Chief Risk Officer des Instituts kommunizieren und ggf. externe Berater hinzuziehen können, insbesondere in Bezug auf vorgeschlagene strategische Transaktionen wie Fusionen und Übernahmen.

B.3 Rahmen für das Geschäftsgebaren

15. Unternehmenswerte und Verhaltenskodex

1. Das Leitungsorgan sollte höchste ethische und professionelle Standards entwickeln und fördern.

Erläuterung

Wenn der Ruf eines Instituts in Frage gestellt wird, kann es sich als schwierig erweisen, das verlorene Vertrauen wiederzugewinnen, was im gesamten Markt Auswirkungen zeigen kann.

Die Umsetzung geeigneter Standards (z. B. Verhaltenskodex) für professionelles und verantwortungsbewusstes Verhalten auf allen Ebenen eines Instituts kann dazu beitragen, die Risiken, denen es ausgesetzt ist, zu mindern. So werden insbesondere operative und Reputationsrisiken gemindert, wenn diesen Standards eine hohe Priorität eingeräumt und sie ordnungsgemäß umgesetzt werden.

2. Das Leitungsorgan sollte klare Richtlinien zu der Frage erlassen, wie diese Standards zu erfüllen sind.
3. Ihre Umsetzung sowie die Einhaltung dieser Standards sollten kontinuierlich überprüft werden. Die Ergebnisse sollten dem Leitungsorgan regelmäßig mitgeteilt werden.

16. Interessenkonflikte auf Ebene des Instituts

1. Das Leitungsorgan sollte wirksame Richtlinien zur Erkennung tatsächlicher und potenzieller Interessenkonflikte aufstellen, diese umsetzen und befolgen. Mit Interessenkonflikten, die dem Leitungsorgan mitgeteilt und von ihm genehmigt wurden, sollte auf geeignete Art und Weise umgegangen werden.
2. In schriftlichen Richtlinien sollten die Beziehungen, Dienstleistungen, Tätigkeiten oder Transaktionen eines Instituts, bei denen Interessenkonflikte auftreten könnten, sowie die Vorgehensweise zu ihrer Bewältigung beschrieben werden. Diese Richtlinien sollten sich auf die Beziehungen und Transaktionen zwischen verschiedenen Kunden eines Instituts sowie zwischen einem Institut und
 - a. seinen Kunden (aufgrund des Geschäftsmodells und/oder der unterschiedlichen, vom Institut bereitgestellten Dienstleistungen und/oder Tätigkeiten);
 - b. seinen Aktionären;
 - c. den Mitgliedern seines Leitungsorgans;
 - d. seinem Personal;
 - e. wichtigen Lieferanten oder Geschäftspartnern; und
 - f. anderen nahe stehenden Unternehmen (z. B. seinem Mutterunternehmen oder seinen Tochtergesellschaften)erstrecken.

3. Ein Mutterunternehmen sollte die Interessen aller ihrer Tochtergesellschaften berücksichtigen und abwägen sowie prüfen, wie diese Interessen langfristig zum gemeinsamen Zweck und den gemeinsamen Interessen der Gruppe als Ganzes beitragen können.
4. In den Richtlinien zu Interessenkonflikten sollten Maßnahmen enthalten sein, die zur Verhinderung bzw. Bewältigung von Interessenkonflikten zu ergreifen sind. Solche Verfahren und Maßnahmen können
 - a. eine angemessene Funktionstrennung, z. B. die Übertragung kollidierender Tätigkeiten innerhalb der Transaktions- oder Leistungskette auf unterschiedliche Personen oder die Übertragung von Aufsichts- und Berichtsaufgaben bei kollidierenden Tätigkeiten auf unterschiedliche Personen;
 - b. die Errichtung von Informationsschranken, wie z. B. die physische Trennung bestimmter Abteilungen; und
 - c. die Aufgabe, Personen, die auch außerhalb des Instituts tätig sind, davon abzuhalten, dass sie innerhalb des Instituts bezüglich dieser Tätigkeiten einen unangemessenen Einfluss ausüben,umfassen.

17. Interne Frühwarnmechanismen

1. Das Leitungsorgan sollte entsprechende interne Frühwarnmechanismen einrichten, damit das Personal Probleme in Verbindung mit der internen Governance melden kann.
2. Ein Institut sollte geeignete interne Frühwarnmechanismen einrichten, mithilfe derer das Personal auf wichtige und legitime Bedenken in Bezug auf Angelegenheiten in Verbindung mit der internen Governance hinweisen kann. Bei diesen Verfahren sollte die Vertraulichkeit der Personalangehörigen, die solche Bedenken äußern, gewahrt bleiben. Zur Vermeidung von Interessenkonflikten sollte eine Möglichkeit geschaffen werden, solche Bedenken außerhalb der regelmäßigen Berichtswege (z. B. über die Compliance-Funktion oder die Innenrevision oder eine interne Informantenregelung [„Whistleblower“]) zu äußern. Die Frühwarnmechanismen sind allen Mitarbeitern eines Instituts zugänglich zu machen. Die von den Mitarbeitern im Rahmen dieses Verfahrens mitgeteilten Informationen sollten, sofern sie sachdienlich sind, auch dem Leitungsorgan zur Kenntnis gebracht werden.

Erläuterung

In einigen Mitgliedstaaten haben die Mitarbeiter zusätzlich zu internen Frühwarnmechanismen innerhalb eines Instituts eventuell auch die Möglichkeit, die Aufsichtsbehörde über derartige Bedenken zu informieren.

B.4 Outsourcing- und Vergütungspolitik

18. Outsourcing

1. Das Leitungsorgan genehmigt die Outsourcing-Politik eines Instituts und überprüft sie regelmäßig.

Erläuterung

Die vorliegenden Leitlinien sind auf die Outsourcing-Politik beschränkt; spezifische Aspekte des Outsourcings werden in den CEBS-Leitlinien zum Outsourcing behandelt, die auf der Website der EBA verfügbar sind.

Es wird von Instituten erwartet, dass sie beiden Leitlinien nachkommen. Im Fall von Diskrepanzen haben die (CEBS-)Leitlinien zum Outsourcing Vorrang, da sie spezifischer sind. Falls ein Thema nicht in den CEBS-Leitlinien geregelt ist, findet der allgemeine Grundsatz der vorliegenden Leitlinien Anwendung.

2. Im Rahmen der Outsourcing-Politik sollten die Auswirkungen einer Auslagerung auf die Geschäftstätigkeit eines Instituts sowie auf dessen Risikosituation (etwa operationelle Risiken und Reputations- und Konzentrationsrisiken) bedacht werden. Die Outsourcing-Politik sollte sich auf die Berichts- und Überwachungsregelungen erstrecken, die von Anfang bis Ende einer Outsourcing-Vereinbarung umzusetzen sind (einschließlich Ausarbeitung eines Business Case für eine Auslagerung, Abschluss eines Outsourcing-Vertrags, Erfüllung des Vertrags bis zu dessen Ablauf, Notfallpläne und Ausstiegsstrategien). Die Outsourcing-Politik sollte regelmäßig überprüft und aktualisiert werden, Änderungen sollten rechtzeitig umgesetzt werden.
3. Ein Institut bleibt voll und ganz für alle ausgelagerten Dienstleistungen und Tätigkeiten sowie für alle sich daraus ergebenden Managemententscheidungen verantwortlich. Dementsprechend sollte im Rahmen der Outsourcing-Politik deutlich gemacht werden, dass eine Auslagerung das Institut nicht von seinen regulatorischen Verpflichtungen und seinen Pflichten gegenüber seinen Kunden entbindet.
4. In der Outsourcing-Politik sollte auch erklärt werden, dass Outsourcing-Vereinbarungen eine wirksame Beaufsichtigung des Instituts sowohl im Rahmen von bankgeschäftlichen Prüfungen vor Ort („on-site“) als auch im Rahmen der laufenden Aufsicht („off-site“) nicht behindern und nicht gegen aufsichtsrechtliche Einschränkungen der Dienstleistungen und Tätigkeiten verstoßen sollten. Die Outsourcing-Politik sollte sich außerdem auch auf internes Outsourcing (z. B. durch eine rechtlich selbständige Einheit innerhalb der Gruppe eines Instituts) sowie auf gruppenspezifische Gegebenheiten erstrecken, die es zu berücksichtigen gilt.

19. Steuerung der Vergütungspolitik

1. Die Verantwortung für die Vergütungspolitik hat das Leitungsorgan des Instituts.

Erläuterung

Die vorliegenden Leitlinien bilden den *allgemeinen* Rahmen für die Steuerung der Vergütungspolitik. Auf *spezifische* Aspekte der Frage der Vergütung gehen die CEBS-Vergütungsrichtlinien vom Dezember 2010 näher ein. Es wird erwartet, dass Institute beiden Leitlinien nachkommen.

2. Das Leitungsorgan in seiner Aufsichtsfunktion (Aufsichtsorgan) sollte die Grundsätze der allgemeinen Vergütungspolitik für sein Institut erhalten, genehmigen und überwachen. Die Verfahren des Instituts zur Festlegung der Vergütung sollten klar, gut dokumentiert und intern transparent sein.
3. Neben der generellen Verantwortung des Leitungsorgans für die Vergütungspolitik insgesamt und deren Überprüfung sollten auch die Kontrollfunktionen angemessen einbezogen werden. Mitglieder des Leitungsorgans, Mitglieder des Vergütungsausschusses und sonstige Mitarbeiter, die an der Ausgestaltung und Umsetzung der Vergütungspolitik beteiligt sind, sollten über einschlägige Fachkenntnisse verfügen und in der Lage sein, sich ein unabhängiges Urteil über die Angemessenheit der Vergütungspolitik einschließlich ihrer Auswirkungen auf das Risikomanagement zu bilden.
4. Die Vergütungspolitik sollte außerdem darauf abzielen, Interessenkonflikte zu vermeiden. Das Leitungsorgan in seiner Leitungsfunktion sollte nicht seine eigene Vergütung festsetzen; um dies zu verhindern, könnte es beispielsweise in Erwägung ziehen, einen unabhängigen Vergütungsausschuss mit dieser Frage zu befassen. Ein Organisationsbereich sollte nicht die Möglichkeit haben, die Vergütung seiner Kontrolleinheiten festzulegen.
5. Das Leitungsorgan sollte die Aufsicht über die Anwendung der Vergütungspolitik führen, um zu gewährleisten, dass diese wie vorgesehen funktioniert. Die Umsetzung der Vergütungspolitik sollte zentral und unabhängig überprüft werden.

C. Risikomanagement

20. Risikokultur

1. Ein Institut sollte eine integrierte und institutsweite Risikokultur auf der Grundlage eines umfassenden Verständnisses seiner Risiken und deren Management entwickeln, wobei auch den Risikotoleranzen und dem Risikoappetit Rechnung zu tragen ist.

Erläuterung

Da die Geschäfte der Institute überwiegend die Übernahme von Risiken zur Folge haben, ist ein angemessenes Risikomanagement von entscheidender Bedeutung. Eine solide und konsistente Risikokultur im gesamten Institut ist ein Schlüsselement für ein wirksames Risikomanagement.

2. Ein Institut sollte seine eigene Risikokultur in Form von Richtlinien, Beispielen, Kommunikation und Schulungsmaßnahmen für Mitarbeiter entsprechend ihres Verantwortungsbereichs für Risiken entwickeln.
3. Jedes Mitglied der Organisation sollte sich seiner Aufgaben und Verantwortlichkeiten in Verbindung mit dem Risikomanagement voll und ganz bewusst sein. Das Risikomanagement sollte nicht auf Risikospezialisten oder Kontrollfunktionen beschränkt werden. Geschäftsbereiche unter der Aufsicht des Leitungsorgans sollten in erster Linie für das tägliche Management von Risiken unter Berücksichtigung der Risikotoleranzen und des Risikoappetits verantwortlich sein, in Einklang mit den Richtlinien, Verfahren und Kontrollen des Instituts.
4. Ein Institut sollte über einen ganzheitlichen Ansatz für das Risikomanagement verfügen, der sich auf sämtliche Geschäftsbereiche, Unterstützungs- und Kontrolleinheiten erstreckt, die wirtschaftliche Substanz seiner Risikopositionen voll erkennt und alle wichtigen Risiken abdeckt (z. B. finanzielle und nicht finanzielle, bilanzielle und außerbilanzielle, potenzielle und vertragliche/außervertragliche Risiken). Der Umfang sollte nicht auf Kredit-, Markt-, Liquiditäts- und operationelle Risiken beschränkt sein, sondern auch Konzentrations-, Reputations-, Compliance- und strategische Risiken umfassen.
5. Das Risikomanagement sollte das Institut in die Lage versetzen, fundierte Entscheidungen in Kenntnis der Sachlage zu treffen. Diese sollten auf Informationen beruhen, die sich aus der Identifizierung, Messung oder Bewertung und Überwachung von Risiken herleiten. Die Risiken sollten von unten nach oben („Bottom up“) und von oben nach unten („Top down“) entlang der gesamten Managementkette und geschäftsfeldübergreifend mittels einer einheitlichen Terminologie und kompatibler Methoden im gesamten Institut und gruppenweit bewertet werden.
6. Das Risikomanagement sollte einer unabhängigen internen oder externen Überprüfung unterzogen und regelmäßig im Hinblick auf die Risikotoleranzen sowie den Risikoappetit des Instituts unter Berücksichtigung von Informationen der Risikocontrolling-Funktion sowie ggf. auch des Risikoausschusses überprüft werden. Dabei sollten u. a. Faktoren wie interne und externe Entwicklungen einschließlich Bilanz- und Umsatzwachstum, zunehmende Komplexität der Geschäftstätigkeit des Instituts, Risikoprofil und operative Struktur, geografische Expansion, Fusionen und Übernahmen sowie die Einführung neuer Produkte oder Geschäftsfelder berücksichtigt werden.

21. Anpassung der Vergütung an das Risikoprofil

1. Die Vergütungspolitik und Vergütungsregelungen eines Instituts sollten mit seinem Risikoprofil übereinstimmen und einem soliden und wirksamen Risikomanagement förderlich sein.

Erläuterung

Die vorliegenden Leitlinien bilden den *allgemeinen* Rahmen für die Anpassung der Vergütungspolitik an das Risikoprofil eines Instituts. Auf *spezifische* Aspekte der Vergütungspolitik gehen die CEBS-Vergütungsrichtlinien vom Dezember 2010 näher ein. Es wird erwartet, dass Institute beiden Leitlinien nachkommen.

2. Die Vergütungspolitik eines Instituts insgesamt sollte mit dessen Werten, Geschäftsstrategie, Risikotoleranz / Risikoappetit und seinen langfristigen Interessen übereinstimmen. Sie sollte keine Anreize zur Eingehung übermäßig hoher Risiken setzen. Eine garantierte variable Vergütung oder Abfindungen, die letztlich dazu führen, dass Versagen belohnt wird, stehen nicht im Einklang mit einem soliden Risikomanagement oder mit dem Prinzip der leistungsorientierten Entlohnung und sollten generell verboten werden.
3. Für Mitarbeiter, deren berufliche Tätigkeiten sich erheblich auf das Risikoprofil eines Instituts auswirken (z. B. Mitglieder des Leitungsorgans, Führungskräfte, Mitarbeiter, die hohe Risikopositionen begründen können, sog. „risk taker“, für die interne Kontrolle zuständige Mitarbeiter und allgemein Beschäftigte, die eine Gesamtvergütung beziehen, aufgrund derer sie in die gleiche Vergütungskategorie eingestuft werden wie Führungskräfte und Risk Taker), sollte die Vergütungspolitik besondere Regelungen treffen, damit sichergestellt ist, dass ihre Vergütung auf ein solides und wirksames Risikomanagement abgestimmt ist.
4. Mitarbeiter von Kontrolleinheiten sollten angemessen entlohnt werden, und zwar im Einklang mit ihren Zielen und ihrer Leistung und nicht mit der Leistung der von ihnen kontrollierten Geschäftsbereiche.
5. Im Fall einer leistungsorientierten Vergütung sollte die Vergütung auf einer Kombination aus einem individuellen Erfolgsbeitrag und dem Gesamterfolg beruhen. Die Festlegung des individuellen Erfolgsbeitrags sollte anhand nicht-finanzieller Parameter erfolgen. Bei einer Messung der Leistung im Hinblick auf die Gewährung von Leistungsprämien sollten alle Arten von eingegangenen Risiken sowie die Kapital- und Liquiditätskosten mit einbezogen werden.
6. Grundgehalt und Prämie sollten in einem ausgewogenen Verhältnis zueinander stehen. Eine hohe Prämie sollte nicht einfach eine Vorauszahlung sein, sondern eine flexible und risikogewichtete Komponente enthalten, die zurückbehalten wird. Bei der zeitlichen Planung für die Auszahlung der Prämie ist auch die zugrunde liegende Risiko-Performance zu berücksichtigen.

22. Rahmenwerk für das Risikomanagement

1. Das Risikomanagement eines Instituts sollte Richtlinien, Verfahren, Limitsysteme und Kontrollen enthalten, um so eine angemessene, frühzeitige und laufende Identifizierung, Messung oder Beurteilung, Überwachung, Minderung und Berichterstattung über die Risiken auf Ebene der Geschäftsbereiche sowie auf Gesamtinstitutsebene zu ermöglichen.
2. Das Rahmenwerk für das Risikomanagement eines Instituts sollte konkrete Anhaltspunkte für die Umsetzung der Strategien des Instituts umfassen. Diese sollten, wo es zweckmäßig erscheint, ein internes System zur Begrenzungen von Risiken festlegen und befolgen, das konsistent zur Risikotoleranz / zum Risikoappetit des Instituts ist sowie dem intakten Betrieb, der finanziellen Stärke und den strategischen Zielen entspricht. Das Risikoprofil eines Instituts (d. h. die Summe aller tatsächlichen und potenziellen Risiken) sollte sich in diesen Grenzen bewegen Das Risikomanagement sollte sicherstellen, dass eine Nichteinhaltung der Grenzen eskaliert und angemessen weiterverfolgt wird.
3. Bei der Identifizierung und Messung von Risiken sollte ein Institut zukunfts- und rückwärtsgerichtete Instrumente entwickeln, die die Arbeit zu den gegenwärtigen Risikopositionen ergänzen. Mit diesen Instrumenten sollte es möglich sein, sämtliche Risiken geschäftsfeldübergreifend zusammenzufassen und Risikokonzentrationen identifizieren.
4. Mithilfe der zukunftsgerichteten Instrumente (etwa Szenario-Analysen und Stresstests) sollten potenzielle Risiken unter verschiedenen adversen Entwicklungen erkannt werden; die rückwärtsgerichteten Instrumente sollten dabei helfen, das tatsächliche Risikoprofil gegenüber den Risikotoleranzen / dem Risikoappetit und dem Risikomanagementsystem des Instituts zu überprüfen anzupassen.

Erläuterung

Die Stresstest-Leitlinien sind auf der Website der EBA abrufbar.

5. Die abschließende Verantwortung für die Risikobewertung liegt einzig und allein beim Institut, das seine Risiken dementsprechend kritisch beurteilen und sich nicht ausschließlich auf externe Beurteilung verlassen soll.

Erläuterung

Ein Institut sollte beispielsweise ein nicht selbst entwickeltes, extern eingekauftes Risikomodell validieren und an seine individuellen Gegebenheiten anpassen, um die Risiken genau und umfassend erfassen und analysieren zu können.

Externe Risikobeurteilungen (einschließlich externer Ratings oder extern erworbener Risikomodelle) können zu einer umfassenderen Risikoschätzung beitragen. Institute sollten sich den Umfang solcher Beurteilungen bewusst machen.

6. Entscheidungen darüber, in welcher Höhe Risiken eingegangen werden, sollten nicht nur auf quantitativen Informationen oder Ergebnissen von Risikomodellen beruhen, sondern auch die praktischen und konzeptionellen Begrenzungen von Metriken und Modellen anhand eines qualitativen Ansatzes (einschließlich Expertenmeinungen und kritischen Analysen) berücksichtigen. Zudem sollten einschlägige Veränderungen des wirtschaftlichen Umfelds herangezogen werden, um deren potenzielle Auswirkungen auf die Risikopositionen und Portfolios zu ermitteln. Derartige Bewertungen sollten offiziell in Entscheidungen über wesentliche Risiken mit einfließen.

Erläuterung

Ein Institut sollte bedenken, dass die Ergebnisse einer zukunftsorientierten quantitativen Beurteilung und von Stresstests weitgehend von den Grenzen und Annahmen der verwendeten Modelle und Verfahren 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 souveräne Durchführung durch das Institut zurückzuführen.

7. Es sollten regelmäßige und transparente Mechanismen für die Berichterstattung eingerichtet werden, damit dem Leitungsorgan und allen wichtigen Geschäftseinheiten eines Instituts rechtzeitige, präzise, prägnante, verständliche und aussagekräftige Berichte vorgelegt werden und sie wesentliche Informationen über die Identifizierung, Messung oder Beurteilung und Überwachung von Risiken erhalten. Die Berichterstattung sollte klar definiert, dokumentiert und vom Leitungsorgan genehmigt sein.
8. Falls ein Risikoausschuss eingesetzt wurde, sollte dieser regelmäßig formelle Berichte und, sofern angemessen, informelle Benachrichtigungen von der Risikocontrolling-Funktion und von der Leitung der Risikocontrolling-Funktion erhalten.

Erläuterung

Eine effiziente Kommunikation von Informationen über die Risikosituation ist für den gesamten Risikomanagementprozess von entscheidender Bedeutung; sie erleichtert Überprüfungs- und Entscheidungsprozesse und hilft, Entscheidungen zu vermeiden, die unwissentlich das Risiko erhöhen könnten. Eine effiziente Risikoberichterstattung setzt eine solide Betrachtung und Kommunikation der Risikostrategie sowie wichtiger Risikodaten (z. B. Risikopositionen und Risikokennzahlen) sowohl horizontal durch das gesamte Institut hindurch als auch nach oben und unten entlang der gesamten Managementkette voraus.

23. Neue Produkte

1. Ein Institut sollte über ein ausführlich dokumentiertes Konzept zur Genehmigung neuer Produkte (*Neu-Produkt-Prozess* – NPP) verfügen, das vom Leitungsorgan genehmigt wird und sich mit der Entwicklung neuer Märkte, Produkte und Dienstleistungen sowie mit wichtigen Änderungen der bestehenden Märkte, Produkte und Dienstleistungen befasst.
2. 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 des Begriffs „neues Produkt/ neuer Markt/ neue Geschäftstätigkeit“ umfassen, der in der Organisation verwendet werden soll, sowie eine Festlegung der Organisationseinheiten, die in den Entscheidungsprozess einzubinden sind.
3. Der NPP sollte die wichtigsten Fragen behandeln, die geklärt werden müssen, bevor eine Entscheidung getroffen wird. Hierzu sollten die Erfüllung gesetzlicher Auflagen, Preisfindungsmodelle, 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 angemessene interne Instrumente und Fachkenntnisse für das Verständnis und die Überwachung der damit verbundenen Risiken gehören. Die Entscheidung, eine neue Geschäftsaktivität aufzunehmen, sollte auch die hierfür verantwortliche Organisationseinheit und die verantwortlichen Personen festlegen. 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.
4. Die Risikocontrolling-Funktion sollte in die Genehmigung neuer Produkte bzw. wesentlicher Änderungen der bestehenden Produkte einbezogen werden. Ihr Beitrag sollte eine vollständige und objektive Bewertung der Risiken umfassen, die sich aus den neuen Aktivitäten ergeben, unter Einbeziehung unterschiedlicher Szenarien, potenzieller Unzulänglichkeiten beim Risikomanagement- und internen Kontrollsystem sowie der Fähigkeit des Instituts, neue Risiken effizient zu steuern. Die Risikocontrolling-Funktion sollte außerdem einen klaren Überblick über die Markteinführung neuer Produkte (bzw. wesentliche Änderungen der bestehenden Produkte) in verschiedenen Geschäftsfeldern und Portfolios haben und verlangen können, dass Änderungen der bestehenden Produkte den offiziellen NPP durchlaufen müssen.

D. Interne Kontrolle

24. Interne Kontrollrichtlinien

1. Ein Institut sollte wirksame und umfassende interne Kontrollrichtlinien einrichten und weiterentwickeln, einschließlich der Ausgestaltung spezifischer

unabhängiger Kontrollfunktionen mit entsprechender Handlungskompetenz, um ihren Auftrag zu erfüllen.

2. Die internen Kontrollrichtlinien eines Instituts sollten eine effektive und effiziente operative Tätigkeit, eine angemessene Kontrolle der Risiken, eine umsichtige Führung der Geschäfte, die Zuverlässigkeit der finanziellen und nicht finanziellen Berichterstattung intern wie extern und die Einhaltung von Gesetzen, Rechtsvorschriften, aufsichtlichen Anforderungen sowie der internen Regelungen und Entscheidungen des Instituts gewährleisten. Die internen Kontrollrichtlinien sollten sich auf die gesamte Organisation einschließlich aller Geschäftsbereiche, Unterstützungs- und Kontrolleinheiten erstrecken. Die internen Kontrollrichtlinien sollten der Geschäftstätigkeit eines Instituts entsprechend ausgestaltet sein und mit angemessenen Regelungen zur Aufbau- und Ablauforganisation und Rechnungslegungsverfahren einhergehen.
3. Bei der Einrichtung der internen Kontrollrichtlinien sollte ein Institut sicherstellen, dass ein klarer, transparenter und dokumentierter Entscheidungsprozess sowie eine eindeutige Aufgabenverteilung und Kompetenzregelung gegeben sind, damit die Einhaltung der internen Regelungen und Entscheidungen sichergestellt ist. Zur Umsetzung effektiver interner Kontrollrichtlinien in allen Bereichen des Instituts sollten die Geschäftsbereiche und Unterstützungseinheiten primär für die Einrichtung und Weiterentwicklung angemessener interner Kontroll- und Überwachungsstrukturen (inkl. Arbeitsanweisungen) und deren Umsetzung zuständig sein.
4. Geeignete interne Kontrollrichtlinien setzen voraus, dass unabhängige Kontrollfunktionen die Einhaltung dieser Richtlinien und Verfahren überprüfen. Die Kontrollfunktionen sollten eine Risikocontrolling-Funktion, eine Compliance-Funktion und eine Innenrevision umfassen.
5. Die Kontrollfunktionen sollten auf einer geeigneten hierarchischen Ebene eingerichtet werden und direkt an die Geschäftsleitung berichten. Sie sollten von den Geschäftsbereichen und Unterstützungseinheiten, die sie überwachen und kontrollieren, sowie auch organisatorisch voneinander unabhängig sein (da sie unterschiedliche Funktionen erfüllen). In weniger komplexen oder kleineren Instituten können die Aufgaben der Risikocontrolling- und die Compliance-Funktion miteinander verknüpft werden. Die Kontrollfunktionen der Gruppe sollten die Kontrollfunktionen der Tochtergesellschaften beaufsichtigen.
6. Zur Wahrung der Unabhängigkeit der Kontrollfunktionen sollten folgende Bedingungen erfüllt sein:
 - a. die Mitarbeiter in Kontrollfunktionen nehmen keine Aufgaben wahr, die in den Tätigkeitsbereich fallen, die von dieser überwacht und kontrolliert werden soll;
 - b. die Kontrollfunktion ist in organisatorischer Hinsicht von den Geschäftstätigkeiten, die sie überwachen und kontrollieren soll, getrennt;

- c. der Leiter der Kontrollfunktion ist einer Person unterstellt, die nicht für die Durchführung der Tätigkeiten zuständig ist, die von der Kontrollfunktion überwacht und kontrolliert werden. Der Leiter der Kontrollfunktion sollte in der Regel direkt an das Leitungsorgan und an die entsprechenden Ausschüsse berichten und regelmäßig an deren Sitzungen teilnehmen; und
 - d. die Vergütung der Mitarbeiter der Kontrollfunktion sollte nicht an den Erfolg von Tätigkeiten gekoppelt sein, die von der Kontrollfunktion überwacht und kontrolliert werden, und sie sollte deren Objektivität auch nicht anderweitig beeinträchtigen können.
7. Kontrollfunktionen sollten über eine angemessene Personalausstattung (sowohl im Mutterunternehmen als auch in den Tochtergesellschaften bei Gruppen) verfügen. Die Mitarbeiter sollten die Möglichkeit erhalten, kontinuierlich weitere Qualifikationen zu erwerben und angemessene Schulungen zu absolvieren. Außerdem sollten ihnen angemessene Datensysteme und Unterstützung einschließlich Zugang zu internen und externen Informationen zur Verfügung gestellt werden, die sie für die Wahrnehmung ihrer Aufgaben benötigen.
 8. Kontrollfunktionen sollten dem Leitungsorgan regelmäßig über die als wesentlich identifizierten Mängel schriftlich berichten. Diese Berichte sollten den Stand der Abarbeitung festgestellter Mängel sowie neu identifizierte wesentliche Mängel verbunden mit der Betrachtung relevanter Risiken, eine Folgenabschätzung und Empfehlungen über Maßnahmen enthalten. Die Geschäftsleitung sollte rechtzeitig und effizient auf die Erkenntnisse der Kontrollfunktionen reagieren und angemessene Maßnahmen zur Mängelbehebung einfordern.

25. Risikocontrolling-Funktion (RCF)

1. Ein Institut sollte eine umfassende und unabhängige Risikocontrolling-Funktion (RCF) einrichten.
2. Die RCF sollte dafür Sorge tragen, dass alle wesentlichen Risiken des Instituts erkannt und von den entsprechenden Einheiten des Instituts sachgemäß gesteuert werden und dass dem Leitungsorgan eine ganzheitliche Betrachtung aller relevanten Risiken (Gesamtrisikoprofil) zur Verfügung gestellt wird. Die RCF unterstützt die Geschäftsleitung und die Geschäftsbereiche bzw. Unterstützungseinheiten mit relevanten Informationen, Analysen und Expertenmeinungen und berät in allen risikopolitischen Fragestellungen, ob diese im Einklang mit der Risikotoleranz/-appetit des Instituts stehen. Die RCF kann Verbesserungen des Rahmens für das Risikomanagement und Maßnahmen empfehlen, um Verletzungen der Risikostrategie, -prozesse und -limite zu beheben.
3. Die RCF sollte ein zentraler organisatorischer Bestandteil des Instituts und so gegliedert sein, dass sie die Risikostrategie umsetzen und den Rahmen für das Risikomanagement kontrollieren kann. Große, komplexe und erfahrene Institute

können auch die Einrichtung von fest zugeordneten RCF für jedes wichtige Geschäftsfeld in Erwägung ziehen. Das Institut sollte jedoch über eine zentrale RCF (ggf. einschließlich einer RCF im Mutterunternehmen einer Gruppe) verfügen, die sämtliche Risiken aus einer ganzheitlichen Perspektive wahrnehmen kann.

4. Die RCF sollte von den Geschäftsbereichen und Unterstützungseinheiten, deren Risiken sie kontrolliert, unabhängig, jedoch nicht von ihnen getrennt sein. Sie sollte über ausreichende Kenntnisse der Methoden und Verfahren des Risikomanagements sowie der Märkte und Produkte verfügen. Das Zusammenwirken zwischen den operativen Funktionen und der RCF sollten dem Ziel dienen, dass alle Mitarbeiter des Instituts Verantwortung für das Management von Risiken übernehmen.

26. Rolle der Risikocontrolling-Funktion

1. Die RCF sollte frühzeitig und aktiv in die Erarbeitung einer Risikostrategie des Instituts sowie in alle wichtigen Entscheidungen im Bereich Risikomanagement eingebunden werden. Die RCF sollte eine Schlüsselrolle bei der Sicherstellung wirksamer Risikomanagementprozesse eines Institutes spielen.

Rolle der RCF im Hinblick auf Strategie und Entscheidungen

2. Die RCF sollte der Geschäftsleitung alle wichtigen Risikoinformationen (z. B. durch eine technische Analyse der Risikolage) vorlegen, um sie in die Lage zu versetzen, Risikotoleranz/Risikoappetit des Instituts festzulegen.
3. Außerdem sollte die RCF die Risikostrategie einschließlich der von den Geschäftseinheiten vorgeschlagenen Ziele bewerten und das Leitungsorgan vor Entscheidungsfindung beraten. Zielvorgaben einschließlich von Ratings und der Höhe der Eigenkapitalrendite sollten plausibel und konsistent sein.
4. Die RCF sollte die Verantwortung für die Umsetzung der Risikostrategie und -politik eines Instituts mit allen Geschäftseinheiten des Instituts gemeinsam tragen. Während die Geschäftseinheiten die Limite umsetzen sollten, sollte die RCF dafür Sorge tragen, dass die Limite dem Risikoappetit/Risikotoleranz des Instituts insgesamt entsprechen und laufend überwachen, dass das Institut keine übermäßigen Risiken eingeht.
5. Durch die Einbindung der RCF in Entscheidungsprozesse sollte gewährleistet werden, dass Risikoabwägungen angemessen berücksichtigt werden. Die Verantwortung für die getroffenen Entscheidungen verbleibt jedoch bei den Geschäftsbereichen und Unterstützungseinheiten und letztlich beim Leitungsorgan.

Rolle der RCF bei Geschäften mit nahe stehenden Unternehmen

6. Die RCF sollte dafür Sorge tragen, dass Geschäfte mit verbundenen Unternehmen überprüft und die tatsächlichen oder potenziellen Risiken, die sich daraus für das Institut ergeben, erkannt und angemessen bewertet werden.

Rolle der RCF im Hinblick auf die Komplexität der Rechtsstruktur

7. Die RCF sollte darauf abzielen, wesentliche Risiken, die sich aus der Komplexität der rechtlichen Struktur eines Instituts ergeben, zu identifizieren.

Erläuterung

Risiken können auch mangelnde Transparenz in der Leitung, operative Risiken aufgrund miteinander verbundener, komplexer Refinanzierungsstrukturen, gruppeninterne Risikopositionen oder Besicherungs- und Kontrahentenausfallrisiko umfassen.

Rolle der RCF bei wesentlichen Änderungen

8. Die RCF sollte beurteilen, wie die ermittelten wesentlichen Risiken die Fähigkeit des Instituts bzw. der Gruppe beeinträchtigen können, sein/ihr Risikoprofil zu steuern und Finanzmittel und Kapital unter normalen sowie unter adversen Umständen einzusetzen.
9. Bevor Entscheidungen über wesentliche Änderungen oder außergewöhnliche Geschäfte getroffen werden, sollte die RCF in die Bewertung der Auswirkungen solcher Änderungen und außergewöhnlicher Geschäfte auf das Gesamtrisiko des Instituts und der Gruppe eingebunden werden.

Erläuterung

Wesentliche Änderungen oder außergewöhnliche Geschäfte können Fusionen und Übernahmen, die Schaffung oder den Verkauf von Tochtergesellschaften oder Zweckgesellschaften, neue Produkte, Änderungen von Systemen, Verfahren oder des Rahmens für das Risikomanagement oder auch Änderungen der Organisation des Instituts umfassen.

Hierzu wird auf die gemeinsamen Leitlinien des Jahres 2008 über die aufsichtsrechtliche Beurteilung des Erwerbs und der Erhöhung von Beteiligungen im Finanzsektor der drei Stufe-3-Ausschüsse der europäischen Finanzaufsichtsbehörden (CEBS, CESR und CEIOPS) verwiesen, die auf der Website der EBA einsehbar sind. Die RCF sollte frühzeitig und aktiv in die Erkennung der relevanten Risiken (einschließlich potenzieller Folgen einer mangelhaften Durchführung einer „Due Diligence“-Analyse, bei der die Risiken nach einem Zusammenschluss nicht erkannt wurden) in Verbindung mit Änderungen der Gruppenstruktur (einschließlich Fusionen und Übernahmen) eingebunden werden; ihre Ergebnisse sollte sie direkt an das Leitungsorgan berichten.

Rolle der RCF bei Messungen und Bewertungen

10. Die RCF sollte dafür sorgen, dass sich die Messungen und Bewertungen der internen Risiken eines Instituts auf eine entsprechend breite Palette von

Szenarios erstrecken und auf ausreichend konservativen Annahmen im Hinblick auf Interdependenzen und Korrelationen beruhen. Darunter sollten auch qualitative unternehmensweite Betrachtungen (einschließlich Expertenmeinungen) zu den Beziehungen zwischen den Risiken und der Rentabilität des Instituts und seinem externen Tätigkeitsumfeld fallen.

Rolle der RCF bei der Überwachung

11. Die RCF sollte gewährleisten, dass alle erkannten Risiken wirksam von den Geschäftsbereichen überwacht werden können. Die RCF sollte regelmäßig das tatsächliche Risikoprofil des Instituts überwachen und es mit den strategischen Zielen und der Risikotoleranz/dem Risikoappetit des Instituts abgleichen, damit die Geschäftsleitung entsprechende Entscheidungen treffen und das Aufsichtsorgan die Entscheidungen kritisch hinterfragen kann.
12. Die RCF sollte Entwicklungstrends analysieren und neue oder neu auftretende Risiken erkennen, die sich aus geänderten Gegebenheiten und Bedingungen ergeben. Sie sollte außerdem regelmäßig die aktuellen Risikoergebnisse anhand der bisherigen Ergebniserwartungen (d. h. Rückvergleiche) zur Bewertung und Verbesserung der Genauigkeit und Effizienz des Risikomanagementprozesses überprüfen.
13. Die RCF der Gruppe sollte die von den Tochtergesellschaften eingegangenen Risiken überwachen. Unstimmigkeiten mit der genehmigten Gruppenstrategie sind dem zuständigen Leitungsorgan zu melden.

Rolle der RCF bei nicht genehmigten Risikopositionen

14. Die RCF sollte in angemessener Art und Weise bei Änderungen der Strategie des Instituts, der Risikotoleranz/dem Risikoappetit und der Limite einbezogen werden.
15. Die RCF sollte unabhängig Verstöße oder Verletzungen beurteilen (einschließlich deren Ursache sowie einer rechtlichen und wirtschaftlichen Analyse der tatsächlichen Kosten der Schließung, der Verringerung oder der Absicherung von Risikopositionen im Vergleich zu den potenziellen Kosten einer Fortführung). Die RCF sollte die betroffenen Geschäftsbereiche informieren und mögliche Maßnahmen empfehlen.

Erläuterung

Verstöße oder Verletzungen von Strategien und der Risikotoleranz/des Risikoappetits oder die Überschreitung von Limiten können durch neue Geschäfte, Änderungen der Marktgegebenheiten oder durch eine Weiterentwicklung der Strategie, der Politik oder Verfahren des Instituts verursacht werden, die dann eintreten, wenn die Limite oder die Risikotoleranz/der Risikoappetit nicht dementsprechend geändert werden.

16. Die RCF sollte darauf hinwirken, dass auf der Grundlage ihrer Empfehlung eine Entscheidung auf der zuständigen Ebene getroffen wird, die zuständigen Geschäftsbereiche dieser nachkommen und sie dem Leitungsorgan, dem Risikoausschuss und dem Geschäftsbereich bzw. der Unterstützungseinheit in geeigneter Art und Weise zur Kenntnis gebracht wird.
17. Ein Institut sollte angemessene Maßnahmen zur Bekämpfung interner oder externer betrügerischer Handlungen und Disziplinarvergehen (z. B. Verletzung interner Verfahren, Überschreitung von Limiten) ergreifen.

Erläuterung

Für den Geltungsbereich dieser Leitlinien umfasst der Begriff „Betrug“ internen und externen Betrug gemäß Definition in der Richtlinie 2006/48/EG Anhang X Teil 5. Dies umfasst auch Verluste infolge von Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum, Umgehung von Verwaltungs-, Rechts- oder internen Vorschriften, mit Ausnahme von Verlusten aufgrund von Diskriminierung, wenn mindestens eine interne Partei beteiligt ist (interner Betrug), sowie Verlusten aufgrund von Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum und Umgehung von Rechtsvorschriften durch einen Dritten (externer Betrug).

27. Chief Risk Officer

1. Ein Institut sollte eine Person, den Leiter der RCF, ernennen, der in exklusiver Weise für die RCF und für die unabhängige Überwachung des Risikomanagements in der gesamten Organisation verantwortlich ist („Chief Risk Officer“).
2. Der Chief Risk Officer (oder eine gleichwertige Position) sollte dafür zuständig sein, umfassende und verständliche Informationen zu den Risiken zur Verfügung zu stellen, die das Leitungsorgan in die Lage versetzen, das Gesamtrisikoprofil des Instituts zu verstehen. Gleiches gilt für den Chief Risk Officer eines Mutterinstituts im Hinblick auf die gesamte Gruppe.
3. Der Chief Risk Officer sollte über ausreichende Fachkenntnisse, Betriebserfahrung, Unabhängigkeit und eine ausreichend lange Dauer der Betriebszugehörigkeit verfügen, um Entscheidungen, die die Risikoposition des Instituts beeinflussen, zu hinterfragen. Ein Institut sollte in Erwägung ziehen, dem Chief Risk Officer ein Vetorecht einzuräumen. Der Chief Risk Officer und das Leitungsorgan bzw. entsprechende Ausschüsse sollten in der Lage sein, direkt untereinander über wichtige Risikofragen zu kommunizieren, einschließlich der Entwicklungen, die mit der Risikotoleranz und -strategie oder dem Risikoappetit des Instituts möglicherweise nicht übereinstimmen.
4. Wenn ein Institut dem Chief Risk Officer das Recht einräumen möchte, ein Veto gegen Beschlüsse einzulegen, sollte es in seinen Richtlinien die Umstände

beschreiben, unter denen der Chief Risk Officer ein solches Veto einlegen kann, sowie die Art der Vorschläge (z. B. Kredit- oder Investitionsentscheidungen oder die Festlegung von Limiten). In den Richtlinien sollten die Eskalations- oder Beschwerdeverfahren sowie die Modalitäten für die Unterrichtung des Leitungsorgans beschrieben werden.

5. Wenn es aufgrund der Besonderheiten eines Instituts – insbesondere seiner Größe, Organisation und der Art seiner Geschäftstätigkeit – nicht gerechtfertigt ist, eine speziell hierzu ernannte Person mit diesen Aufgaben zu betrauen, könnte die Funktion auch von einer anderen leitenden Person aus dem Institut übernommen werden, sofern kein Interessenkonflikt vorliegt.
6. Das Institut sollte über dokumentierte Prozesse verfügen, um die Position des Chief Risk Officer zu besetzen und ihm seine Verantwortung zu entziehen. Falls der Chief Risk Officer ersetzt wird, sollte dies nur nach vorheriger Zustimmung durch das Leitungsorgan in seiner Aufsichtsfunktion geschehen. Im Allgemeinen sollten die Ablösung oder Ernennung eines Chief Risk Officer offen gelegt und die Aufsichtsbehörde über die Gründe informiert werden.

28. Compliance-Funktion

1. Ein Institut sollte eine Compliance-Funktion zur Steuerung seines Compliance-Risikos schaffen.
2. Ein Institut sollte eine Compliance-Richtlinien genehmigen und umsetzen, über die alle Mitarbeiter informiert werden sollten.

Erläuterung

Ein Compliance-Risiko (das definiert wird als bestehendes oder künftiges Ertrags- oder Kapitalrisiko infolge von Verletzungen oder der Nichteinhaltung von Gesetzen, Vorschriften, Rechtsvorschriften, Vereinbarungen, vorgeschriebenen Praktiken oder ethischen Standards) kann zu Geldstrafen, Schadenersatz und/oder zur Nichtigkeit von Verträgen führen und den Ruf eines Instituts schädigen.

3. Ein Institut sollte eine ständige und effektive Compliance-Funktion einrichten und eine Person benennen, die für diese Funktion im gesamten Institut sowie gruppenweit zuständig ist („Compliance-Beauftragte“). In kleineren und weniger komplexen Instituten kann diese Funktion auch mit der Risikocontrolling- oder mit den Unterstützungsfunktionen (z. B. Personal- oder Rechtsabteilung u. ä.) kombiniert oder von ihnen unterstützt werden.
4. Die Compliance-Funktion sollte gewährleisten, dass die Compliance-Richtlinien befolgt werden und dem Leitungsorgan sowie ggf. der RCF über die Steuerung von Compliance-Risiken durch das Institut Bericht erstatten. Die Ergebnisse der Compliance-Funktion sollten vom Leitungsorgan und der RCF bei Entscheidungsprozessen berücksichtigt werden.

5. Die Compliance-Funktion sollte das Leitungsorgan darüber informieren, welche Gesetze, Vorschriften, Rechtsvorschriften und Standards das Institut einhalten bzw. erfüllen muss, und die möglichen Auswirkungen von Änderungen im rechtlichen oder ordnungspolitischen Umfeld auf die Geschäftstätigkeit des Instituts bewerten.
6. Die Compliance-Funktion sollte ferner sicherstellen, dass neue Produkte (Neu-Produkt-Prozess) und neue Verfahren mit dem derzeitigen rechtlichen Umfeld sowie mit bekannten bevorstehenden Änderungen von Gesetzen, Rechtsvorschriften und aufsichtlichen Anforderungen in Einklang stehen.

Erläuterung

Ein besonderes Augenmerk ist dann erforderlich, wenn das Institut bestimmte Dienstleistungen erbringt oder im Namen seiner Kunden Strukturen schafft (z. B. wenn es als Vermittler bei der Gründung von Unternehmen oder Partnerschaften auftritt, Treuhanddienste anbietet oder komplex strukturierte Geldgeschäfte für Kunden entwickelt), die die interne Governance vor besondere Herausforderungen stellen und mit aufsichtsrechtlichen Problemen einhergehen können.

29. Interne Revision

1. Die Interne Revision sollte die Angemessenheit und Wirksamkeit des internen Kontrollsystems eines Instituts prüfen.
2. Die Interne Revision sollte ungehinderten Zugang zu allen einschlägigen Unterlagen und Informationen in allen operativen Einheiten und Kontrolleinheiten haben.
3. Die Interne Revision sollte beurteilen, ob alle Aktivitäten und Einheiten eines Instituts (einschließlich RCF und Compliance-Funktion) dessen Richtlinien und Prozesse einhalten. Daher sollte die Interne Revision nicht mit anderen Funktionen kombiniert werden. Die Interne Revision sollte außerdem bewerten, ob die bestehenden Richtlinien und Prozesse nach wie vor angemessen sind und den Anforderungen der Gesetze und Rechtsvorschriften entsprechen.
4. Die Interne Revision sollte insbesondere die Angemessenheit der Prozesse prüfen, damit die Zuverlässigkeit der den internen Modellen zugrunde liegenden Methoden und Verfahren, Annahmen und Informationsquellen des Instituts (etwa Risikomodellierung und Bilanzierung) gewährleistet ist. Sie sollte ferner die Qualität und die Verwendung von Instrumenten für die qualitative Risikoidentifizierung und -bewertung beurteilen. Zur Wahrung ihrer Unabhängigkeit sollte die Interne Revision jedoch nicht unmittelbar in die Ausgestaltung oder Auswahl von Modellen oder anderen Instrumenten des Risikomanagements einbezogen werden.

5. Das Leitungsorgan sollte die Interne Revision dazu anhalten, nationale und internationale Normen und Methoden des Berufstandes einzuhalten. Die Interne Revision ist entsprechend einem Prüfungsplan sowie detaillierten Revisionsprogrammen auf der Grundlage eines „risikobasierten“ Ansatzes durchzuführen. Der Prüfungsplan sollte vom Revisionsausschuss und/oder vom Leitungsorgan genehmigt werden.

Erläuterung

Ein Beispiel für die hier angeführten Normen und Methoden des Berufstandes sind Standards, die vom Institute of Internal Auditors (IIA) erstellt wurden.

6. Die Interne Revision sollte ihre Feststellungen und Maßnahmvorschläge für wesentliche Verbesserungen der internen Kontrollen/ des Internen Kontrollsystems direkt dem Leitungsorgan und/oder (ggf.) dessen Prüfungsausschuss mitteilen. Im Rahmen eines Follow-Up sollte die Abarbeitung aller festgestellten Mängel durch die jeweils zuständigen Leitungsebenen gegenüber der Internen Revision berichtet werden.

E. Informationssysteme und Aufrechterhaltung des Geschäftsbetriebs

30. Informationssystem und Kommunikation

1. Ein Institut sollte über wirksame und zuverlässige Informations- und Kommunikationssysteme verfügen, die alle wichtigen Geschäftstätigkeiten umfassen.

Erläuterung

Managemententscheidungen könnten durch unzuverlässige oder irreführende Informationen, die von schlecht konzipierten oder kontrollierten Systemen bereitgestellt werden, negativ beeinträchtigt werden. Damit ist ein unverzichtbarer Bestandteil der Tätigkeiten eines Instituts die Einrichtung und Wartung von Informations- und Kommunikationssystemen, die sich auf das gesamte Spektrum seiner Tätigkeiten erstrecken. Diese Informationen werden normalerweise auf elektronischen sowie nicht elektronischen Datenträgern bereitgestellt.

Ein Institut sollte sich insbesondere der organisatorischen und internen Kontrollanforderungen an die Verarbeitung elektronischer Informationen sowie der Notwendigkeit eines angemessenen Prüfpfads bewusst sein. Dies gilt auch dann, wenn IT-Systeme an einen IT-Dienstleister fremdvergeben werden.

2. Informationssysteme einschließlich Systemen, die Daten in elektronischer Form verwalten und verwenden, sollten sicher und unabhängig überprüfbar sein und durch geeignete Notfallverfahren unterstützt werden. Ein Institut sollte bei der

Implementierung von IT-Systemen die allgemein anerkannten IT-Standards einhalten.

31. Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs

1. Ein Institut sollte solide Verfahren zur Aufrechterhaltung seines Geschäftsbetriebs entwickeln, um in der Lage zu sein, den kontinuierlichen Dienstbetrieb aufrechtzuerhalten, und Verluste im Fall von schwerwiegenden Betriebsstörungen zu begrenzen.

Erläuterung

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

2. Bei der Einrichtung solider Maßnahmen für die Aufrechterhaltung des Geschäftsbetriebs sollte ein Institut sorgfältig analysieren, 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 Unterstützungseinheiten sowie auf die RCF erstrecken und dabei deren Verflechtungen und Wechselbeziehungen berücksichtigen. Darüber hinaus sollte eine spezifische unabhängige Funktion für die Geschäftskontinuität, die RCF oder die Funktion Operatives Risikomanagement aktiv einbezogen werden. Die Ergebnisse der Analyse sollten in die Definition der Prioritäten und Ziele bei der Wiederherstellung der Geschäftsabläufe des Instituts mit einfließen.

Erläuterung

Im Hinblick auf die Funktion Operatives Risikomanagement wird auch auf die Richtlinie 2006/48/EG Anhang X Teil 3 Absatz 4 verwiesen, die eine solche unabhängige Funktion für Institute vorschreibt, die einen AMA verwenden; die mit dieser Funktion verbundenen Aufgaben sind in den Leitlinien zur Validierung in Absatz 615-620 beschrieben (2006 veröffentlicht), die auf der Website der EBA abrufbar sind.

3. Aufgrund der vorstehenden 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.
 - b. Pläne für die Wiederherstellung entscheidender Ressourcen, die das Institut in die Lage versetzen, innerhalb einer angemessenen Zeitspanne seine üblichen Geschäftsabläufe wieder aufzunehmen. Restrisiken aufgrund potenzieller Geschäftsunterbrechungen sollten mit der Risikobereitschaft/Risikoneigung des Instituts vereinbar sein.
4. Notfallpläne, Pläne zur Aufrechterhaltung des Geschäftsbetriebs sowie Pläne zur Wiederherstellung sind zu dokumentieren und gewissenhaft umzusetzen. Die Dokumentation sollte innerhalb der Geschäftsbereiche, Unterstützungseinheiten und der RCF zugänglich und auf Systemen abgespeichert sein, die physisch getrennt und im Fall einer Notsituation problemlos zugänglich sind. Dazu sollten geeignete Schulungsmaßnahmen 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.

F. Transparenz

32. Nachvollziehbare Kommunikation

1. Richtlinien und Strategien sollten allen betroffenen Mitarbeitern eines Instituts mitgeteilt werden.
2. Die Mitarbeiter eines Instituts sollten die Richtlinien und die Verfahren, die mit ihren Aufgaben und Verantwortungsbereichen in Verbindung stehen, verstehen und befolgen.
3. 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.

33. Transparenz der internen Governance

1. Die interne Governance eines Instituts sollte transparent sein. Ein Institut sollte seine derzeitige Position und seine künftigen Vorstellungen klar, ausgewogen, präzise und rechtzeitig darlegen.

Erläuterung

Die Transparenz im Bereich der internen Governance zielt darauf ab, allen wichtigen Interessengruppen eines Instituts (einschließlich Aktionären, Mitarbeitern, Kunden und der breiten Öffentlichkeit) Schlüsselinformationen zur Verfügung zu stellen, die sie benötigen, damit sie die Leistungsfähigkeit der Geschäftsleitung bei der Führung des Instituts beurteilen können.

Nach Maßgabe von Artikel 72 der Richtlinie 2006/48/EG und von Artikel 2 der Richtlinie 2006/49/EG sollten EU-Mutterinstitute sowie von einer EU-Mutterfinanzholdinggesellschaft kontrollierte Institute umfassende und aussagekräftige Informationen offen legen, die ihre interne Governance auf konsolidierter Ebene beschreiben. Es empfiehlt sich, dass jedes Institut Informationen über seine interne Governance auf Einzelinstitutsebene in angemessener Weise zur Verfügung stellt.

2. Ein Institut sollte mindestens folgende Angaben offen legen:
 - a. seine Governancestrukturen und -richtlinien einschließlich seiner Ziele, Organisationsstruktur, Regelungen zur internen Governance, die Struktur und Organisation des Leitungsorgans einschließlich seiner Mitglieder sowie die Anreiz- und Vergütungsstruktur des Instituts;
 - b. Art, Umfang, Zweck und wirtschaftliche Substanz der Geschäfte mit verbundenen und nahe stehenden Dritten, sofern sich diese wesentlich auf das Institut auswirken;
 - c. seine Geschäfts- und Risikostrategie (einschließlich der Einbeziehung des Leitungsorgans) und voraussehbare Risikofaktoren;
 - d. seine Ausschüsse und deren Mandate und Zusammensetzung;
 - e. seinen internen Kontrollrichtlinien und die Art und Weise der Organisation seiner Kontrollfunktionen, die wichtigsten Aufgaben, die sie wahrnehmen, die Methode zur Überwachung der Leistung durch das Leitungsorgan sowie geplante wesentliche Änderungen dieser Funktionen; und
 - f. wichtige Informationen über seine operativen- und Finanzergebnisse.
3. Informationen über die aktuelle Lage des Instituts sollten den gesetzlichen Offenlegungspflichten entsprechen. Die Informationen sollten klar, genau, wesentlich, rechtzeitig und zugänglich sein.
4. In Fällen, in denen ein hohes Maß an Genauigkeit zur Verzögerung der Bekanntgabe zeitkritischer Informationen führen würde, sollte ein Institut beurteilen, wie ein ausgewogenes Verhältnis zwischen Rechtzeitigkeit und Genauigkeit hergestellt werden könnte, und gleichzeitig das Erfordernis beachten, ein den tatsächlichen Verhältnissen entsprechendes Bild seiner Situation zu vermitteln, und Verzögerungen auf zufrieden stellende Art und Weise erklären. Diese Erklärung sollte jedoch nicht dazu verwendet werden, der Pflicht einer regelmäßigen Berichterstattung nur mit Zeitverzug nachzukommen.

Titel III – Schlussbestimmungen und Umsetzung

34. Aufhebung

Mit Verabschiedung und Veröffentlichung dieser Leitlinien zur Internen Governance werden folgende Leitlinien aufgehoben: Abschnitt 2.1 der CEBS-Guidelines on the Application of the Supervisory Review Process (vom 25. Januar 2006) mit dem Titel „Guidelines on Internal Governace“; die „High Level Principles for Remuneration Policies“ (vom 20. April 2009) und die „High Level Principles for Risk Management“ (vom 16. Februar 2010).

35. Umsetzungsfrist

Die zuständigen Behörden sollten die Leitlinien zur Internen Governance bis spätestens 31. März 2012 durch Einbeziehung in ihre Aufsichtsverfahren umsetzen. Anschließend sollten sie sicherstellen, dass die Institute den Leitlinien wirksam nachkommen.