



European Securities and
Markets Authority

Leitlinien

zur internen Kontrolle von Ratingagenturen





Inhalt

1	Anwendungsbereich	3
2	Rechtsrahmen, Abkürzungen und Begriffsbestimmungen	4
3	Zweck	4
4	Einhaltung der Leitlinien und Berichtspflichten	5
4.1	Status der Leitlinien	5
4.2	Berichtspflichten	5
5	Leitlinien zur internen Kontrolle von Ratingagenturen	5
5.1	Interner Kontrollrahmen	6
5.2	Interne Kontrollfunktionen	11

1 Anwendungsbereich

Für wen?

1. Diese Leitlinien gelten für Ratingagenturen mit Sitz in der Union, die gemäß der Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen¹ bei der ESMA registriert sind.

Was?

2. Diese Leitlinien betreffen Angelegenheiten im Zusammenhang mit der internen Kontrollstruktur und den internen Kontrollmechanismen, die erforderlich sind, um die tatsächliche Einhaltung von Artikel 6 Abs. 1, 2 und 4 sowie Anhang I Abschnitt A der Verordnung über Ratingagenturen durch eine Ratingagentur sicherzustellen.

Wann?

3. Diese Leitlinien gelten ab dem 1. Juli 2021.

¹ ABI. L 302 vom 17.11.2009, S. 1.

2 Rechtsrahmen, Abkürzungen und Begriffsbestimmungen

Rechtsrahmen

<i>ESMA-Verordnung</i>	Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission ²
<i>Verordnung über Ratingagenturen</i>	Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen

Abkürzungen

<i>ESMA</i>	Europäische Wertpapier- und Marktaufsichtsbehörde
<i>RatingVO</i>	Verordnung über Ratingagenturen
<i>INED</i>	Unabhängige Mitglieder des Verwaltungs- oder Aufsichtsorgans der Ratingagentur (independent non-executive director)

3 Zweck

4. Diese Leitlinien betreffen Angelegenheiten im Zusammenhang mit der internen Kontrollstruktur und den internen Kontrollmechanismen, die erforderlich sind, um die tatsächliche Einhaltung von Artikel 6 Abs. 1, 2 und 4 sowie Anhang I Abschnitt A der Verordnung über Ratingagenturen (RatingVO) durch eine Ratingagentur sicherzustellen.
5. In den Leitlinien werden die Erwartungen der ESMA in Bezug auf die Bestandteile und Merkmale eines wirksamen internen Kontrollrahmens und wirksamer interner Kontrollfunktionen in einer Ratingagentur dargelegt.

² *ABl. L 331 vom 15.12.2010, S. 84.*

4 Einhaltung der Leitlinien und Berichtspflichten

4.1 Status der Leitlinien

6. Dieses Dokument enthält Leitlinien, die nach Artikel 16 der ESMA-Verordnung herausgegeben werden. Gemäß der Verordnung müssen Ratingagenturen alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

4.2 Berichtspflichten

7. Die ESMA prüft die Anwendung dieser Leitlinien durch die Ratingagenturen im Rahmen ihrer laufenden Aufsicht und Überwachung der Tätigkeiten der Ratingagenturen.
8. Die ESMA wird bei der Anwendung dieser Leitlinien die Verhältnismäßigkeit berücksichtigen. Obgleich von allen Ratingagenturen der Nachweis der in diesen Leitlinien dargelegten Merkmale eines wirksamen internen Kontrollsystems erwartet wird, kann die ESMA in einigen Fällen nicht erwarten, dass dies über eigens dafür vorgesehene, separate interne Kontrollfunktionen gemäß Abschnitt 5.2 erfolgt.
9. Die ESMA wird ihre Erwartungen gemäß Abschnitt 5.2 an die Art, den Umfang und die Komplexität einer Ratingagentur anpassen. Bei größeren Ratingagenturen geht die ESMA davon aus, dass eine Ratingagentur alle in den Leitlinien dargelegten Erwartungen erfüllt. Bei kleineren Ratingagenturen bezieht sich die ESMA auf die Bedingungen für die Registrierung der Ratingagentur. Angesichts der Tatsache, dass sich Art, Umfang und Komplexität einiger Ratingagenturen seit der Registrierung geändert haben können, wird die ESMA jedoch im Rahmen ihrer Aufsicht mitteilen, wenn die Erwartungen gemäß Abschnitt 5.2 höher als bei der Registrierung festgelegt sind.
10. Zwar wird die ESMA ihre Erwartungen an Ratingagenturen im Rahmen ihrer Aufsicht mitteilen, doch die Geschäftsleitung einer Ratingagentur bleibt unter Aufsicht ihres Verwaltungs- oder Aufsichtsorgans für die Bewertung der Angemessenheit ihrer internen Kontrolle anhand dieser Leitlinien verantwortlich.

5 Leitlinien zur internen Kontrolle von Ratingagenturen

Anforderungen im Zusammenhang mit Artikel 6 Absätze 1, 2 und 4 sowie Anhang I Abschnitt A der Verordnung über Ratingagenturen

11. Als Nachweis dafür, dass eine Ratingagentur die Ziele einer wirksamen internen Kontrollstruktur gemäß Artikel 6 Abs. 1, 2 und 4 sowie Anhang I Abschnitt A der Verordnung über Ratingagenturen erfüllt, hat sie den Erwartungen der ESMA zufolge zu belegen, dass ihre Grundsätze, Verfahren und Arbeitsmethoden die Ziele der Abschnitte **5.1** (Interner Kontrollrahmen) und **5.2** (Interne Kontrollfunktionen) dieser Leitlinien erfüllen.

12. In diesem Zusammenhang bezieht sich der Ausdruck „Grundsätze und Verfahren“ auf interne Dokumente, die regeln oder vorschreiben, wie die Ratingagentur oder ihr Personal Tätigkeiten durchführen soll, die den Anforderungen der RatingVO unterliegen.

5.1 Interner Kontrollrahmen

13. Als Nachweis für das Vorhandensein eines wirksamen internen Kontrollrahmens erwartet die ESMA, dass eine Ratingagentur in der Lage ist, die folgenden Bestandteile und Merkmale in ihren internen Grundsätzen und Verfahren sowie Arbeitsmethoden zu belegen.

Allgemeine Grundsätze

14. Das Verwaltungs- oder Aufsichtsorgan einer Ratingagentur sollte die Verantwortung für die Überwachung und Genehmigung aller Bestandteile des von der Geschäftsleitung entwickelten internen Kontrollrahmens sowie für die Überprüfung, dass dessen Bestandteile von der Geschäftsleitung überwacht und regelmäßig aktualisiert werden, tragen. Die Geschäftsleitung der Ratingagentur sollte für die Festlegung, Umsetzung und Aktualisierung der schriftlichen internen Kontrollgrundsätze und -verfahren zur Unterstützung der Bestandteile des internen Kontrollrahmens verantwortlich sein.
15. Im Rahmen der Einführung dieser Grundsätze und Verfahren sollte eine Ratingagentur über klare, transparente und dokumentierte Entscheidungsprozesse sowie über eine klare Zuweisung der Aufgaben und Zuständigkeiten innerhalb ihres internen Kontrollrahmens, einschließlich ihrer Geschäftsbereiche und internen Kontrollfunktionen, verfügen.

Bestandteil 1.1 Kontrollumfeld

16. Nach Auffassung der ESMA besteht das Kontrollumfeld aus der Gesamtheit der Standards, Prozesse und Strukturen, die für die Durchführung der internen Kontrolle innerhalb einer Organisation erforderlich sind. Nach Ansicht der ESMA bildet das Kontrollumfeld das Fundament für ein wirksames System interner Kontrollen.
17. Sowohl das Verwaltungs- oder Aufsichtsorgan als auch die Geschäftsleitung einer Ratingagentur tragen dazu bei, das Leitbild in Bezug auf die Bedeutung der internen Kontrolle zu begründen. Die Geschäftsleitung ist für die Entwicklung und Durchführung der internen Kontrolle sowie für die Bewertung der Angemessenheit und Wirksamkeit des Kontrollumfelds verantwortlich.

Merkmale

- 1.1.1** Die Geschäftsleitung der Ratingagentur sollte dafür verantwortlich sein, durch die Umsetzung von Grundsätzen und Verfahren zur Regelung des Verhaltens des Personals der Ratingagentur eine starke Kultur der Werte und Compliance

in der Ratingagentur zu schaffen. Das Verwaltungs- oder Aufsichtsorgan sollte die Aufsicht über die Geschäftsleitung in diesen Bereichen ausüben.

1.1.2 Die Geschäftsleitung der Ratingagentur sollte verantwortlich dafür sein, dass die Grundsätze und Verfahren der Ratingagentur

- i. daran erinnern, dass die Ratingtätigkeiten der Ratingagentur im Einklang mit der Verordnung über Ratingagenturen, den geltenden Rechtsvorschriften und den Unternehmenswerten der Ratingagentur durchgeführt werden sollten;
- ii. deutlich machen, dass zusätzlich zur Erfüllung der gesetzlichen und aufsichtsrechtlichen Anforderungen und internen Richtlinien vom Personal erwartet wird, dass es sich aufrichtig und integer verhält und seine Aufgaben mit der gebotenen Sachkenntnis, Sorgfalt und Gewissenhaftigkeit ausübt; und
- iii. sicherstellen, dass dem Personal die potenziellen internen und externen disziplinarischen Maßnahmen, rechtlichen Schritte und Sanktionen bekannt sind, die auf Fehlverhalten und nicht akzeptables Verhalten folgen können.

Das Verwaltungs- oder Aufsichtsorgan sollte die Aufsicht über die Geschäftsleitung in diesen Bereichen ausüben.

1.1.3 Die Geschäftsleitung der Ratingagentur sollte für die Festlegung, Pflege und regelmäßige Aktualisierung angemessener schriftlicher interner Kontrollgrundsätze und -verfahren verantwortlich sein. Das Verwaltungs- oder Aufsichtsorgan sollte die Aufsicht über die Geschäftsleitung in diesen Bereichen ausüben.

1.1.4 Die Geschäftsleitung der Ratingagentur sollte weiterhin für Tätigkeiten verantwortlich sein, die sie an externe Dienstleister oder eine Gruppenfunktion innerhalb der Gruppe der Ratingagentur ausgelagert hat. Das Verwaltungs- oder Aufsichtsorgan sollte die Aufsicht über die Geschäftsleitung in diesen Bereichen ausüben.

Bestandteil 1.2 Risikomanagement

18. Nach Auffassung der ESMA umfasst das Risikomanagement die Ermittlung, Bewertung, Überwachung und Minimierung aller Risiken, die sich wesentlich auf die Fähigkeit der Ratingagentur auswirken könnten, ihren Verpflichtungen aus der Verordnung über Ratingagenturen nachzukommen oder die Fortführung ihrer Geschäftstätigkeit bedrohen könnten. Dies ermöglicht es einer Ratingagentur, ihre internen Kontrollressourcen angemessen zuzuweisen. Ein wirksames Risikomanagement sollte ein dynamisches und sich ständig weiterentwickelndes Verfahren zur Ermittlung, Bewertung und Steuerung von Risiken für die Erreichung der Hauptziele der Ratingagentur umfassen.

Merkmale

- 1.2.1** Die Ratingagentur sollte ihre internen Risikobewertungen gemäß einer festgelegten und umfassenden Risikobewertungsmethode durchführen.
- 1.2.2** Die Risikobewertungsmethode der Ratingagentur sollte sich auf alle Geschäftsbereiche der Ratingagentur erstrecken.
- 1.2.3** Die Ratingagentur sollte im Rahmen des Risikobewertungsprozesses ihre Risikobereitschaft festlegen und Risikotoleranzschwellen ermitteln.
- 1.2.4** Im Risikobewertungsprozess der Ratingagentur sollten im Voraus die Kriterien und Ziele festgelegt und ermittelt werden, anhand derer die Risiken der Ratingagentur bewertet werden.
- 1.2.5** Die Risikobewertungsmethode der Ratingagentur sollte ständig weiterentwickelt und verbessert werden.

Bestandteil 1.3 Kontrollmaßnahmen

19. Nach Auffassung der ESMA tragen die Kontrollmaßnahmen, denen die Geschäftstätigkeit einer Ratingagentur unterliegt, dazu bei, die Auswirkungen von Risiken innerhalb einer Organisation abzuschwächen. Dabei handelt es sich um Maßnahmen, die mithilfe von Grundsätzen, Verfahren, Systemen, Mechanismen und anderen Vorkehrungen konzipiert wurden. Diese Kontrollmaßnahmen sollten präventiv, aufspürend, korrigierend oder abschreckend sein.

Merkmale

- 1.3.1** Dokumentation – Die Ratingagentur sollte ihre Grundsätze und Verfahren für alle Geschäftstätigkeiten, die den Bestimmungen der Verordnung über Ratingagenturen unterliegen, dokumentieren.
- 1.3.2** *Dokumentierte Kontrollen und Kontrolltests* – Eine Ratingagentur sollte die vorhandenen Schlüsselkontrollen dokumentieren, die die Einhaltung dieser für die RatingVO relevanten Grundsätze und Verfahren gewährleisten. Die Dokumentation der Kontrolltests sollte Folgendes umfassen:
 - i. eine Beschreibung der Kontrolle;
 - ii. das/die damit verbundene(n) wesentliche(n) Risiko/Risiken;
 - iii. die für die Durchführung der Kontrolle verantwortliche(n) Position(en) oder Funktion(en);
 - iv. die für die Überprüfung der Kontrolle verantwortliche(n) Position(en) oder Funktion(en);

- v. den Nachweis, dass die Kontrolle durchgeführt wurde;
- vi. die Häufigkeit der Durchführung der Kontrolle;
- vii. eine Beschreibung des Testverfahrens.

1.3.3 *Aufgabentrennung* – Die Ratingagentur sollte eine angemessene Aufgabentrennung sicherstellen, um Gefahren im Zusammenhang mit Interessenkonflikten, Betrug und menschlichem Versagen zu begegnen. Durch die Aufgabentrennung sollte sichergestellt werden, dass die Personen,

- i. die die Analyse eines Ratings durchführen, nicht allein für die Genehmigung des Ratings verantwortlich sind.
- ii. die die Entwicklung von Methoden, Modellen oder grundlegenden Annahmen für Ratings durchführen, nicht allein für die Genehmigung dieser Methoden, Modelle oder grundlegenden Annahmen verantwortlich sind.
- iii. die eine Validierung oder Überprüfung einer Methode, eines Modells oder einer grundlegenden Annahme für Ratings durchführen, nicht allein für die Genehmigung der Validierung oder Überprüfung der Methode, des Modells oder der grundlegenden Annahme für Ratings verantwortlich sind.

1.3.4 *Festlegung der Verantwortlichkeiten* – Die Ratingagentur sollte die Positionen oder Funktionen, die für die Durchführung von Kontrollen im Zusammenhang mit den Verpflichtungen aus der RatingVO verantwortlich sind, klar und eindeutig zuordnen und ihre jeweiligen Aufgaben und Zuständigkeiten festlegen. Dabei sollte die Ratingagentur zwischen laufenden Schlüsselkontrollen auf Unternehmensebene und Kontrollen, die von spezifischen Kontrollfunktionen durchgeführt werden, unterscheiden.

1.3.5 *Zulassungen und Genehmigungen* – Die Ratingagentur sollte die Verfahren ihrer Methoden, Modelle und grundlegenden Annahmen für Ratings dokumentieren und beschreiben. Dies sollte die Mitarbeiter einschließen, die für ihre Validierung oder Überprüfung und die Überprüfung der Ergebnisse dieser Verfahren zuständig sind.

1.3.6 *Verifizierungen, Validierungen, Abgleiche und Überprüfungen* – Die Ratingagentur sollte Maßnahmen ergreifen, die es ermöglichen, unangemessenes, nicht autorisiertes, fehlerhaftes oder betrügerisches Verhalten bei ihren Ratingtätigkeiten und den zugrundeliegenden Prozessen, wie Validierung von Methoden/Modellen für Ratings, Datenvalidierung und Dateneingabe, zu erkennen und entsprechend zu handeln.

- 1.3.7** *Generelle IT-Kontrollen* – Die Ratingagentur sollte Kontrollen durchführen, um die Wirksamkeit der IT-Umgebung der Ratingagentur bei der Unterstützung ihrer Geschäftsprozesse sicherzustellen.

Bestandteil 1.4 Information und Kommunikation

20. Nach Auffassung der ESMA ist eine angemessene interne und externe Kommunikation eine entscheidende Voraussetzung für die Erfüllung der regulatorischen Verpflichtungen einer Ratingagentur gegenüber dem Markt, den Kunden und dem Personal. Eine Ratingagentur sollte Verfahren für die Abwärtskommunikation genauer, vollständiger und qualitativ hochwertiger Informationen an das Personal und externe Interessenvertreter sowie Verfahren für die Aufwärtskommunikation sensibler Informationen über Verhaltensweisen und die Einhaltung interner Kontrollen festlegen.

Merkmale

- 1.4.1** Die Ratingagentur sollte für eine angemessene interne und externe Kommunikation sorgen und dem Markt, den Anlegern, den Kunden und den Regulierungsbehörden rechtzeitig genaue, vollständige und qualitativ hochwertige Informationen übermitteln.
- 1.4.2** Die Ratingagentur sollte Kanäle für die Aufwärtskommunikation einrichten, einschließlich eines Verfahrens zur Meldung von Missständen, um eine Eskalation wesentlicher interner Kontrollprobleme an das Verwaltungs- oder Aufsichtsorgan und die Geschäftsleitung zu ermöglichen.
- 1.4.3** Die Ratingagentur sollte Kanäle für die Abwärtskommunikation von der Geschäftsleitung und den Kontrollfunktionen zum Personal einrichten. In diesem Rahmen sollte die regelmäßige Übermittlung aktueller Informationen zu Zielen und Zuständigkeiten der internen Kontrolle, die Kommunikation festgestellter Compliance-Probleme sowie Präsentationen und Schulungen zu Grundsätzen und Verfahren erfolgen.

Bestandteil 1.5 Überwachungsmaßnahmen

21. Nach Auffassung der ESMA sind eine fortlaufende Überwachung und thematische Überprüfungen der Tätigkeiten einer Ratingagentur erforderlich, um die kontinuierliche Angemessenheit und Wirksamkeit des internen Kontrollsystems einer Ratingagentur sicherzustellen. Diese Überwachung dient der Feststellung, ob die Bestandteile des internen Kontrollsystems einer Ratingagentur vorhanden sind und wirksam funktionieren.

Merkmale

- 1.5.1** Die Ratingagentur sollte sicherstellen, dass die Beurteilung des internen Kontrollsystems auf verschiedenen Ebenen der Ratingagentur, z. B.

Geschäftsbereiche, Kontrollfunktionen und interne Revision oder unabhängige Bewertungsinstanzen durchgeführt werden.

- 1.5.2** Die Beurteilung der internen Kontrollsysteme durch die Ratingagentur sollte nach regelmäßigen oder thematischen Gesichtspunkten oder einer Kombination beider Gesichtspunkte durchgeführt werden.
- 1.5.3** Die Ratingagentur sollte laufende Beurteilungen, wie die zeitnahe Überwachung der E-Mail-Kommunikation zwischen Analysten und Emittenten, in die Geschäftsprozesse integrieren und an sich ändernde Bedingungen anpassen. Dies sollte die regelmäßige Teilnahme an Ratingausschüssen oder deren Ex-post-Überprüfung umfassen.
- 1.5.4** Die Ratingagentur sollte das Verwaltungs- oder Aufsichtsorgan und die Geschäftsleitung über die bei der Überwachung der Beurteilungen festgestellten Mängel und die erforderlichen Abhilfemaßnahmen unterrichten. Diese sollten anschließend die zeitnahe Umsetzung der Korrekturmaßnahmen überwachen.
- 1.5.5** Im Falle der Auslagerung wichtiger betrieblicher Aufgaben an eine externe Partei sollte die Ratingagentur sicherstellen, dass das Personal die unmittelbare Verantwortung für die Überwachung ausgelagerter Geschäftsprozesse trägt. Eine Ratingagentur sollte dafür sorgen, dass externe Dienstleister klare Weisungen zu den Zielen der Ratingagentur und den zu erbringenden Leistungen erhalten und dass vor der Beauftragung des Dienstleisters eine sorgfältige Prüfung durchgeführt wird.

5.2 Interne Kontrollfunktionen

- 22. Zur Sicherstellung des Vorhandenseins wirksamer interner Kontrollfunktionen in einer Ratingagentur erwartet die ESMA, dass eine Ratingagentur in der Lage ist, die folgenden Bestandteile und Merkmale in ihren Grundsätzen und Verfahren sowie Arbeitsmethoden zu belegen.

Allgemeine Grundsätze

- 23. Nach Auffassung der ESMA sollten die internen Kontrollfunktionen einer Ratingagentur über ausreichende Ressourcen verfügen und mit Personal ausgestattet sein, das über ausreichendes Fachwissen für die Wahrnehmung seiner Aufgaben verfügt. In Fällen, in denen Ratingagenturen die wichtigen betrieblichen Aufgaben einer internen Kontrollfunktion auf Gruppenebene oder an eine externe Partei ausgelagert haben, trägt eine Ratingagentur nach Auffassung der ESMA weiterhin die volle Verantwortung für die Tätigkeiten der ausgelagerten internen Kontrollfunktion. Nach Ansicht der ESMA sollte das für die internen Kontrollfunktionen der Ratingagentur zuständige Personal eine angemessene Betriebszugehörigkeit aufweisen, damit es über die für die Wahrnehmung seiner Aufgaben erforderliche Autorität verfügt. Bestimmte Aufgaben können auf

Gruppenebene oder von anderen Rechtspersönlichkeiten innerhalb einer Unternehmensstruktur wahrgenommen werden, sofern die Gruppenstruktur die Fähigkeit des Verwaltungs- oder Aufsichtsorgans einer Ratingagentur, Aufsicht auszuüben, und die Fähigkeit der Geschäftsleitung, ihre Risiken wirksam zu steuern, oder die Fähigkeit der ESMA, die Ratingagentur wirksam zu beaufsichtigen, nicht beeinträchtigt.

24. Mit Blick auf die Gewährleistung der Unabhängigkeit der internen Kontrollfunktionen einer Ratingagentur erwartet die ESMA, dass eine Ratingagentur bei der Festlegung der Aufgaben und Zuständigkeiten ihrer internen Kontrollfunktionen die folgenden Grundsätze berücksichtigt:

- i. Interne Kontrollfunktionen sollten von den Funktionen/Tätigkeiten, die ihnen zur Überwachung, Prüfung oder Kontrolle zugewiesen werden, funktional getrennt sein;
- ii. Interne Kontrollfunktionen sollten keine betrieblichen Aufgaben wahrnehmen, die in den Bereich der Geschäftstätigkeiten fallen, die sie überwachen, prüfen oder kontrollieren sollen;
- iii. der Leiter einer internen Kontrollfunktion sollte keiner Person unterstellt sein, die unmittelbar für die Durchführung der Tätigkeiten zuständig ist, die von dieser internen Kontrollfunktion überwacht, geprüft oder kontrolliert werden;
- iv. Personal, das Aufgaben im Zusammenhang mit internen Kontrollfunktionen wahrnimmt, sollte Zugang zu passenden internen oder externen Schulungen haben, damit sichergestellt ist, dass es entsprechende Fähigkeiten besitzt, um die Aufgaben auszuführen.

Verhältnismäßigkeit

25. Die Bedingungen für die Registrierung einer Ratingagentur begründen die Mindestanforderungen der ESMA in Bezug auf die interne Kontrolle, die internen Kontrollfunktionen und die Unternehmensführung einer Ratingagentur. Bei einigen Ratingagenturen ist es möglicherweise nicht verhältnismäßig, dass ihre Organisationsstruktur alle in diesem Abschnitt genannten internen Kontrollfunktionen aufzuweisen hat. Gleichwohl sollten die in diesem Abschnitt der Leitlinien beschriebenen Merkmale aller internen Kontrollfunktionen einem geeigneten Verantwortlichen zugeteilt und zugewiesen werden.

26. Nach Auffassung der ESMA sollte das Verwaltungs- oder Aufsichtsorgan der Ratingagentur Aufsicht über die Durchführung dieser Aufgaben führen und die kontinuierliche Angemessenheit der Personalausstattung und der Ressourcen ihrer internen Kontrollfunktionen für die Art, den Umfang und die Komplexität ihrer Geschäfte prüfen.

Bestandteil 2.1 Compliance-Funktion

27. Nach Ansicht der ESMA ist die Compliance-Funktion einer Ratingagentur für die Überwachung und Berichterstattung dahingehend zuständig, ob die Ratingagentur und ihre Mitarbeiter ihren Verpflichtungen im Rahmen der RatingVO nachkommen. Die Compliance-Funktion hat die Aufgabe, Änderungen der für ihre Tätigkeiten geltenden Rechts- und Verwaltungsvorschriften zu verfolgen. Die Compliance-Funktion ist darüber hinaus dafür zuständig, das Verwaltungs- oder Aufsichtsorgan darüber zu informieren, welche Gesetze, Vorschriften, Verordnungen und Standards die Ratingagentur einhalten bzw. erfüllen muss, sowie zusammen mit den anderen relevanten Funktionen die möglichen Auswirkungen von Änderungen im rechtlichen oder regulatorischen Umfeld auf die Geschäftstätigkeit der Ratingagentur zu bewerten.

Merkmale

- 2.1.1** Die Compliance-Funktion sollte ihre Aufgaben unabhängig von den Geschäftsbereichen wahrnehmen, die für die Ratingtätigkeiten zuständig sind, und den INEDs der Ratingagentur regelmäßig Bericht erstatten.
- 2.1.2** Die Compliance-Funktion sollte Mitarbeiter, die an Ratingtätigkeiten beteiligt sind, bei der Erfüllung der Verpflichtungen aus der RatingVO beraten und unterstützen. Die Compliance-Funktion sollte proaktiv Risiken und mögliche Verstöße durch die zeitnahe Überwachung und Bewertung der Tätigkeiten ermitteln und Abhilfemaßnahmen weiterverfolgen.
- 2.1.3** Die Compliance-Funktion sollte sicherstellen, dass die Überwachung der Einhaltung der Anforderungen im Rahmen eines strukturierten und genau definierten Programms zur Überwachung dieser Einhaltung erfolgt.
- 2.1.4** Die Compliance-Funktion sollte – gegebenenfalls in Zusammenarbeit mit anderen relevanten Funktionen – die möglichen Auswirkungen etwaiger Änderungen des rechtlichen oder regulatorischen Umfelds auf die Tätigkeiten der Ratingagentur bewerten und sich gegebenenfalls mit der Risikomanagementfunktion über das Compliance-Risiko der Ratingagentur austauschen.
- 2.1.5** Die Compliance-Funktion sollte sicherstellen, dass die Compliance-Richtlinien befolgt werden, und dem Verwaltungs- oder Aufsichtsorgan und der Geschäftsleitung über die Steuerung des Compliance-Risikos durch die Ratingagentur Bericht erstatten.
- 2.1.6** Die Compliance-Funktion sollte mit der Risikomanagementfunktion zusammenarbeiten, um die für ihre jeweiligen Aufgaben erforderlichen Informationen auszutauschen.

- 2.1.7** Das Verwaltungs- oder Aufsichtsorgan und die Risikomanagementfunktion sollten die Feststellungen der Compliance-Funktion im Rahmen ihrer Risikobewertungsprozesse berücksichtigen.

Bestandteil 2.2 Überprüfungsstelle

28. Nach Auffassung der ESMA ist die Überprüfungsstelle einer Ratingagentur für die fortlaufende und mindestens jährliche Überprüfung der Methoden, Modelle und grundlegenden Annahmen für Ratings zuständig. Die Überprüfungsstelle der Ratingagentur ist ferner für die Validierung und Überprüfung neuer Methoden, Modelle und grundlegender Ratingannahmen sowie für etwaige Änderungen an bestehenden Methoden, Modellen oder grundlegenden Ratingannahmen zuständig.

Merkmale

- 2.2.1** Die Überprüfungsstelle sollte ihre Aufgaben unabhängig von den Geschäftsbereichen wahrnehmen, die für die Ratingtätigkeiten zuständig sind, und den INEDs der Ratingagentur regelmäßig Bericht erstatten.
- 2.2.2** Anteilseigner oder Mitarbeiter der Ratingagentur, die an der Geschäftsentwicklung beteiligt sind, sollten keine Aufgaben der Überprüfungsstelle wahrnehmen.
- 2.2.3** Analysten sollten nicht an der Genehmigung neuer oder an der Validierung und Überprüfung bestehender Methoden, Modelle und grundlegender Ratingannahmen, die sie entwickelt haben, beteiligt sein.
- 2.2.4** Mitarbeiter der Überprüfungsstelle sollten entweder allein verantwortlich sein oder über die Mehrheit der Stimmrechte in den Ausschüssen verfügen, die für die Genehmigung von Methoden, Modellen und grundlegenden Ratingannahmen zuständig sind.

Bestandteil 2.3 Risikomanagementfunktion

29. Nach Auffassung der ESMA ist die Risikomanagementfunktion einer Ratingagentur für die Entwicklung und Umsetzung des Risikomanagementrahmens verantwortlich. Sie sollte sicherstellen, dass Risiken, die gemäß den Verpflichtungen aus der RatingVO relevant sind, von den entsprechenden Abteilungen/Funktionen innerhalb der Ratingagentur ermittelt, bewertet, gemessen, überwacht, gesteuert und ordnungsgemäß gemeldet werden.

Merkmale

- 2.3.1** Die Risikomanagementfunktion sollte ihre Aufgaben unabhängig von den Geschäftsbereichen und Einheiten, deren Risiken sie überwacht,

wahrnehmen, sie sollte jedoch nicht an einem Zusammenwirken mit ihnen gehindert werden.

- 2.3.2** Die Risikomanagementfunktion sollte sicherstellen, dass alle Risiken, die sich wesentlich auf die Fähigkeit einer Ratingagentur, ihren Verpflichtungen aus der RatingVO nachzukommen oder auf die Fortführung ihrer Geschäftstätigkeit auswirken könnten, von den entsprechenden Abteilungen der Ratingagentur ermittelt, bewertet, gemessen, überwacht, gesteuert und minimiert werden und ordnungsgemäß von diesen bzw. an diese gemeldet werden.
- 2.3.3** Die Risikomanagementfunktion sollte das Risikoprofil der Ratingagentur anhand der Risikobereitschaft der Ratingagentur überwachen, um Entscheidungen zu ermöglichen.
- 2.3.4** Die Risikomanagementfunktion sollte Beratung zu Vorschlägen und Risikoentscheidungen der Geschäftsbereiche bereitstellen und das Verwaltungs- oder Aufsichtsorgan darüber informieren, ob diese Entscheidungen mit der Risikobereitschaft und den Zielen der Ratingagentur im Einklang stehen.
- 2.3.5** Die Risikomanagementfunktion sollte Verbesserungen des Risikomanagementrahmens und Korrekturmaßnahmen für Risikostrategien und -verfahren empfehlen und Risikoschwellen im Einklang mit etwaigen Änderungen der Risikobereitschaft der Organisation überprüfen.

Bestandteil 2.4 Informationssicherheitsfunktion

30. Nach Auffassung der ESMA ist die Informationssicherheitsfunktion einer Ratingagentur für die Entwicklung und Umsetzung von Informationssicherheit in der Ratingagentur verantwortlich. Eine Ratingagentur sollte eine Informationssicherheitsfunktion einrichten, die eine Informationssicherheitskultur innerhalb der Ratingagentur fördert.

Merkmale

- 2.4.1** Die Informationssicherheitsfunktion sollte ihre Aufgaben unabhängig von den Geschäftsbereichen wahrnehmen und für die Überwachung der Einhaltung der Grundsätze und Verfahren der Ratingagentur im Bereich der Informationssicherheit zuständig sein.
- 2.4.2** Die Informationssicherheitsfunktion sollte die Tätigkeiten der Ratingagentur im Bereich der Informationssicherheit verwalten.
- 2.4.3** Die Informationssicherheitsfunktion sollte ein Sensibilisierungsprogramm zur Informationssicherheit für das Personal der Ratingagentur einsetzen, um die Sicherheitskultur zu verbessern und ein umfassendes Verständnis für die

Erfordernisse der Ratingagentur im Bereich Informationssicherheit zu entwickeln.

- 2.4.4** Die Informationssicherheitsfunktion sollte das Verwaltungs- oder Aufsichtsorgan und die Geschäftsleitung regelmäßig über die Informationssicherheit der Systeme und Tätigkeiten der Ratingagentur informieren und beraten.

Bestandteil 2.5 Interne Revisionsstelle

31. Nach Auffassung der ESMA ist die interne Revisionsstelle einer Ratingagentur für die Erbringung einer unabhängigen, objektiven Prüfungs- und Beratungstätigkeit zuständig, die auf eine Verbesserung der Tätigkeiten der Organisation abzielt. Sie unterstützt die Organisation beim Erreichen ihrer Ziele, indem sie die Wirksamkeit des internen Kontrollsystems systematisch und konsequent bewertet und verbessert.

Merkmale

- 2.5.1** Die interne Revisionsstelle sollte ihre Aufgaben unabhängig von den Geschäftsbereichen wahrnehmen und durch eine Satzung für die interne Revision geregelt werden, in der ihre Aufgaben und Zuständigkeiten festgelegt sind und die der Kontrolle des Verwaltungs- oder Aufsichtsorgans unterliegt.
- 2.5.2** Die interne Revisionsstelle sollte einen risikobasierten Ansatz verfolgen.
- 2.5.3** Die interne Revisionsstelle sollte unabhängig überprüfen und objektiv gewährleisten, dass die Tätigkeiten der Ratingagentur, einschließlich der ausgelagerten wichtigen betrieblichen Aufgaben³, mit den Grundsätzen und Verfahren der Ratingagentur sowie mit den geltenden gesetzlichen und aufsichtlichen Anforderungen im Einklang stehen.
- 2.5.4** Die interne Revisionsstelle sollte mindestens einmal jährlich auf der Grundlage der jährlichen internen Kontrollziele einen Revisionsplan und ein detailliertes Revisionsprogramm erstellen, das der Kontrolle des Verwaltungs- oder Aufsichtsorgans unterliegt.
- 2.5.5** Die interne Revisionsstelle sollte den INEDs der Ratingagentur oder gegebenenfalls dem Prüfungsausschuss regelmäßig Bericht erstatten.
- 2.5.6** Die interne Revisionsstelle sollte ihre Prüfungsempfehlungen klar und kohärent kommunizieren, damit das Verwaltungs- oder Aufsichtsorgan und die Geschäftsleitung die Wesentlichkeit der Empfehlungen verstehen und entsprechend Prioritäten festlegen können.

³ Wichtige betriebliche Aufgaben sind die in Artikel 25 Absatz 2 der Delegierten Verordnung (EU) Nr. 449/2012 der Kommission über Informationen zur Registrierung und Zertifizierung von Ratingagenturen dargelegten Aufgaben.

2.5.7

Empfehlungen der internen Revisionsstelle sollten Gegenstand eines formellen Verfahrens zur Weiterverfolgung durch die jeweils zuständige Leitungsebene sein, damit ihre wirksame und fristgerechte Umsetzung und eine entsprechende Berichterstattung sichergestellt werden.