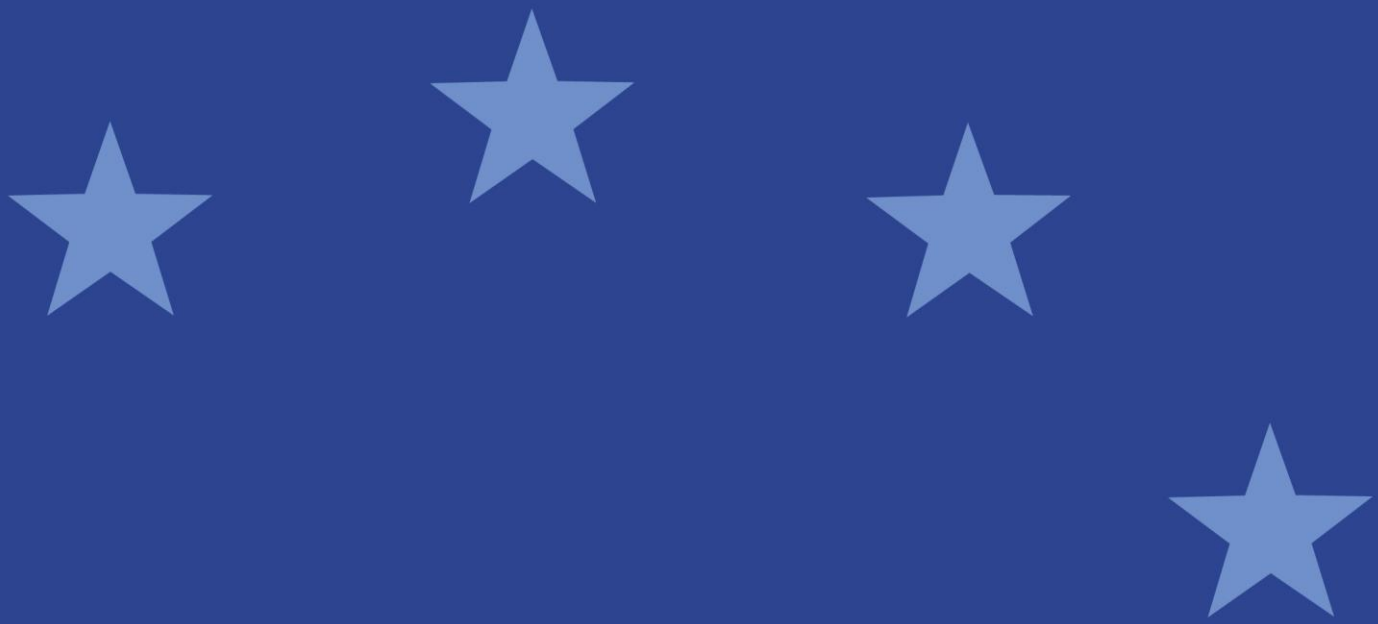
esma European Securities and Markets Authority

Richtsnoeren

met betrekking tot interne controle voor ratingbureaus



10/03/2021 | ESMA33-9-371 NL

Inhoudsopgave

1 Toepassingsgebied

Wie?

1. Deze richtsnoeren gelden voor ratingbureaus die zijn gevestigd in de Unie en bij ESMA zijn geregistreerd overeenkomstig Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad van 16 september 2009 inzake ratingbureaus[1].

Wat?

2. Deze richtsnoeren hebben betrekking op zaken die verband houden met de internecontrolestructuur en mechanismen die noodzakelijk zijn om te waarborgen dat ratingbureaus op doeltreffende wijze voldoen aan artikel 6, leden 1, 2, en 4, en bijlage I, afdeling A, van de verordening inzake ratingbureaus.

Wanneer?

3. Deze richtsnoeren gelden vanaf 1 juli 2021.

[1] PB L 302 van 17.11.2009, blz. 1.

2 Wettelijke verwijzingen, afkortingen en definities

Wetgeving waarnaar wordt verwezen

ESMA-verordening	Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie[2]
Verordening inzake ratingbureaus (CRAR)	Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad van 16 september 2009 inzake ratingbureaus

Afkortingen

ESMA	European Securities and Markets Authority (Europese Autoriteit voor effecten en markten)
CRA	Credit Rating Agency (ratingbureau)
CRAR	*CRA Regulation (verordening inzake ratingbureaus)*
IC-kader	Internecontrolekader
IC-functies	Internecontrolefuncties
ONUB	Onafhankelijke leden van het bestuurs- of toezichthoudend orgaan van het ratingbureau
Bestuurs- of toezichthoudend orgaan van het ratingbureau	Het bestuur

3 Doel

4. Deze richtsnoeren hebben betrekking op zaken die verband houden met de internecontrolestructuur en -mechanismen die noodzakelijk zijn om te waarborgen dat ratingbureaus op doeltreffende wijze voldoen aan artikel 6, leden 1, 2, en 4, en bijlage I, afdeling A, van de verordening inzake ratingbureaus (CRAR).

5. De richtsnoeren geven de verwachtingen van ESMA weer ten aanzien van de componenten en kenmerken van een doeltreffend IC-kader en IC-functies binnen een ratingbureau.

[2] *PB L 331 van 15.12.2010, blz. 84.*

4 Nalevings- en rapportageverplichtingen

4.1 Status van de richtsnoeren

6. Het onderhavige document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van de ESMA-verordening. Volgens deze verordening moeten ratingbureaus zich tot het uiterste inspannen om aan de richtsnoeren te voldoen.

4.2 Rapportage-eisen

7. ESMA beoordeelt de toepassing van deze richtsnoeren door ratingbureaus via doorlopend toezicht en monitoring van de activiteiten van de ratingbureaus.

8. ESMA past deze richtsnoeren toe met inachtneming van het evenredigheidsbeginsel. Hoewel alle ratingbureaus geacht worden aan te tonen dat zij beschikken over een doeltreffend systeem voor interne controle als uiteengezet in deze richtsnoeren, kan ESMA er niet in alle gevallen van uitgaan dat ratingbureaus dit doen via de specifieke, afzonderlijke IC-functies als omschreven in paragraaf 5.2.

9. ESMA stemt zijn verwachtingen als omschreven in paragraaf 5.2 af op de aard, schaal en complexiteit van een ratingbureau. Van grotere ratingbureaus verwacht ESMA dat zij voldoen aan alle verwachtingen die in de richtsnoeren zijn opgenomen. Bij kleinere ratingbureaus verwijst ESMA naar de voorwaarden voor registratie van het ratingbureau. Aangezien de aard, schaal en complexiteit van sommige ratingbureaus mogelijk zijn gewijzigd sinds hun registratie, zal ESMA bij het uitoefenen van toezicht laten weten of de verwachtingen met betrekking tot paragraaf 5.2 hoger zijn geworden dan die welke bij registratie waren vastgesteld.

10. Hoewel ESMA bij het uitoefenen van toezicht zal communiceren wat het verwacht van ratingbureaus, blijft het de verantwoordelijkheid van het management van een ratingbureau, onder supervisie van het bestuur, om aan de hand van deze richtsnoeren te beoordelen of de interne controle adequaat is.

5 Richtsnoeren met betrekking tot interne controle voor ratingbureaus

Eisen met betrekking tot artikel 6, leden 1, 2, en 4, en bijlage I, afdeling A, CRAR

11. Teneinde vast te stellen dat een ratingbureau de doelstellingen ten aanzien van een doeltreffende internecontrolestructuur overeenkomstig artikel 6, leden 1, 2 en 4, en bijlage I, afdeling A van de ratingbureau-verordening, verwezenlijkt, verwacht ESMA dat een ratingbureau aantoont dat het met zijn beleid, procedures en werkpraktijken de doelstellingen van de paragrafen **5.1** (Internecontrolekader) en **5.2** (Internecontrolefuncties) van deze richtsnoeren realiseert.

12. In deze context wordt onder ‘beleid en procedures’ verstaan interne documenten die regelen hoe het ratingbureau of zijn personeel activiteiten waarvoor de vereisten van de CRAR gelden, dienen uit te voeren, of die hiertoe instructies geven.

5.1 Internecontrolekader

13. ESMA verwacht dat een ratingbureau bewijs kan leveren dat zijn interne beleid, procedures en werkpraktijken de hierna genoemde componenten en kenmerken bevatten, teneinde aan te tonen dat het over een doeltreffend intern controlekader beschikt.

Algemene beginselen

14. Het bestuur van een ratingbureau is verantwoording schuldig voor het toezicht op en het goedkeuren van alle componenten van het door het management ontwikkelde IC-kader, en ziet erop toe dat de componenten worden gemonitord en regelmatig worden bijgewerkt door het management. Het management van een ratingbureau is verantwoordelijk voor het tot stand brengen, ten uitvoer leggen en bijwerken van het schriftelijke interne controlebeleid en de internecontroleprocedures ter ondersteuning van de componenten van het IC-kader.

15. Als onderdeel van de totstandbrenging van dit beleid en deze procedures beschikt een ratingbureau over duidelijke, schriftelijk vastgelegde besluitvormingsprocessen en zijn de rollen en verantwoordelijkheden binnen zijn IC-kader, met inbegrip van zijn bedrijfsonderdelen en IC-functies, duidelijk toegewezen.

Component 1.1 Controleomgeving

16. ESMA verstaat onder de controleomgeving het geheel van normen, processen en structuren die noodzakelijk zijn voor de uitvoering van interne controle in een organisatie. ESMA beschouwt de controleomgeving als het fundament waarop een doeltreffend systeem voor interne controle wordt gebouwd.

17. Het bestuur en het management van een ratingbureau dragen beide bij aan het bepalen van de toon aan de top voor wat betreft het belang van interne controle. Het management is verantwoordelijk voor de ontwikkeling en uitvoering van de interne controle en de beoordeling van de toereikendheid en doeltreffendheid van de controleomgeving.

Kenmerken

1.1.1 Het management van het ratingbureau is verantwoordelijk voor het tot stand brengen van een sterke ethische en nalevingscultuur binnen het ratingbureau door de tenuitvoerlegging van beleid en procedures voor het gedrag van het personeel van het ratingbureau. Het bestuur houdt toezicht op het management op deze terreinen.

1.1.2 Het management van het ratingbureau is er verantwoordelijk voor dat het beleid en de procedures van het ratingbureau:

i. eraan herinneren dat de ratingactiviteiten van het ratingbureau dienen te worden uitgevoerd in overeenstemming met de verordening inzake ratingbureaus, de toepasselijke wetgeving en de waarden van het ratingbureau;

ii. aangeven dat van medewerkers niet alleen wordt verwacht dat zij de wettelijke en regelgevingsvereisten en het interne beleid naleven, maar ook dat zij zich eerlijk en integer gedragen en hun taken uitvoeren met de nodige vakbekwaamheid, zorgvuldigheid en toewijding; en

iii. ervoor zorgen dat medewerkers zich bewust zijn van de potentiële interne en externe disciplinaire maatregelen, gerechtelijke stappen en sancties die kunnen volgen op wangedrag en onaanvaardbaar gedrag.

Het bestuur houdt toezicht op het management op deze terreinen.

1.1.3 Het management van het ratingbureau is verantwoordelijk voor het tot stand brengen, in stand houden en regelmatig bijwerken van adequaat internecontrolebeleid en de internecontroleprocedures. Het bestuur houdt toezicht op het management op deze terreinen.

1.1.4 Het management van het ratingbureau blijft verantwoordelijk voor activiteiten die het heeft uitbesteed aan externe dienstverleners of naar een functie op groepsniveau binnen de groep waartoe het ratingbureau behoort. Het bestuur houdt toezicht op het management op deze terreinen.

Component 1.2 Risicobeheer

18. ESMA is van mening dat risicobeheer inhoudt dat alle risico's die materiële gevolgen zouden kunnen hebben voor het vermogen van het ratingbureau om te voldoen aan zijn verplichtingen uit hoofde van de verordening inzake ratingbureaus of die de voortzetting van zijn activiteiten in gevaar kunnen brengen, worden geïdentificeerd, beoordeeld, gemonitord en beperkt. Dit stelt het ratingbureau in staat zijn internecontrolemiddelen naar behoren toe te wijzen. Doeltreffend risicobeheer omvat een dynamisch en zich continu ontwikkelend proces voor het identificeren, beoordelen en beheren van risico's die het bereiken van de belangrijkste doelen van het ratingbureau in gevaar brengen.

Kenmerken

1.2.1 Het ratingbureau verricht zijn interne risicobeoordelingen volgens een gedefinieerde, uitgebreide risicobeoordelingsmethode.

1.2.2 De risicobeoordelingsmethode van het ratingbureau omvat alle bedrijfsonderdelen van het ratingbureau.

1.2.3 Als onderdeel van het risicobeoordelingsproces bepaalt het ratingbureau zijn risicobereidheid en stelt het risicotolerantieniveaus vast.

1.2.4 In het risicobeoordelingsproces van het ratingbureau worden de criteria en de doelstellingen aan de hand waarvan de risico's van het ratingbureau zullen worden beoordeeld, vooraf gedefinieerd en vastgesteld.

1.2.5 De risicobeoordelingsmethode van het ratingbureau wordt doorlopend verder ontwikkeld en verbeterd.

Component 1.3 Controleactiviteten

19. ESMA is van mening dat controleactiviteiten met betrekking tot de zakelijke activiteiten van een ratingbureau helpen de impact van risico's binnen een organisatie te beperken. Deze activiteiten komen tot stand door middel van beleid, procedures, systemen, mechanismen en andere regelingen. Deze controleactiviteiten zijn gericht op preventie, opsporing, correctie of afschrikking.

Kenmerken

1.3.1 Documentatie – Het ratingbureau legt zijn beleid en procedures voor alle zakelijke activiteiten die zijn onderworpen aan de bepalingen van de verordening inzake ratingbureaus, schriftelijk vast.

1.3.2 *Gedocumenteerde controles en controletests* – Een ratingbureau legt schriftelijk vast wat de belangrijkste controles zijn die het heeft ingesteld om te waarborgen dat het beleid en de procedures die relevant zijn voor de CRAR, worden nageleefd. De documentatie van controletests omvat:

i. een beschrijving van de controle;

ii. de desbetreffende materiële risico's;

iii. de rollen of functies die verantwoordelijk zijn voor het uitvoeren van de controle;

iv. de rollen of functies de verantwoordelijk zijn voor het toetsen van de controle;

v. het bewijs dat de controle is uitgevoerd;

vi. de frequentie waarmee de controle wordt uitgevoerd;

vii. een beschrijving van de testprocedure.

1.3.3 *Scheiding van taken* – Het ratingbureau zorgt voor een passende scheiding van taken voor het beheren van risico's van belangenconflicten, fraude en menselijke fouten. De scheiding van taken waarborgt dat de personen die:

i. belast zijn met de analyse van een rating, niet als enigen verantwoordelijk zijn voor de goedkeuring van de rating;

ii. belast zijn met de ontwikkeling van ratingmethoden of -modellen of belangrijke aannames voor rating, niet als enigen verantwoordelijk zijn voor de goedkeuring van die methoden, modellen of belangrijke aannames voor ratings;

iii. belast zijn met een validering of toetsing van een ratingmethode of -model of belangrijke aanname voor ratings, niet als enigen verantwoordelijk zijn voor de goedkeuring van de validering of toetsing van de ratingmethode of het ratingmodel of van de belangrijke aanname voor ratings.

1.3.4 *Toewijzing van verantwoordelijkheden* – Het ratingbureau wijst op een heldere en gedefinieerde wijze de rollen of functies toe die verantwoordelijk zijn voor de uitvoering van controles in verband met verplichtingen uit hoofde van de CRAR en specificeert hun respectievelijke rollen en verantwoordelijkheden. Daarbij maakt het ratingbureau onderscheid tussen belangrijke dagelijkse controles op bedrijfsniveau en de controles die worden uitgevoerd door specifieke controlefuncties.

1.3.5 *Vergunningen en goedkeuringen* – Het ratingbureau documenteert en beschrijft de processen van zijn ratingmethoden en -modellen en zijn belangrijke aannames voor ratings. Dit betreft ook de medewerkers die verantwoordelijk zijn voor de validering en toetsing hiervan, en de toetsing van de uitkomsten van deze processen.

1.3.6 *Verificaties, valideringen, afstemmingsprocedures en toetsingen* – Het ratingbureau legt maatregelen ten uitvoer om niet-passend, niet-toegestaan, onjuist of frauduleus gedrag bij zijn ratingactiviteiten en de onderliggende processen hiervan, zoals validering van ratingmethode/model, validering en input van gegevens, op te sporen en hierop te reageren.

1.3.7 *Algemene controles IT* – Het ratingbureau stelt controles in om te waarborgen dat de IT-omgeving van het ratingbureau de bedrijfsprocessen van het ratingbureau doeltreffend ondersteunt.

Component 1.4 Informatie en communicatie

20. ESMA is van mening dat passende interne en externe communicatie essentieel is om te bereiken dat het ratingbureau voldoet aan zijn regelgevingsverplichtingen ten aanzien

van de markt, zijn cliënten en zijn personeel. Een ratingbureau stelt procedures vast voor het delen van correcte, volledige informatie van goede kwaliteit met personeel en externe belanghebbenden, evenals procedures voor het delen van gevoelige informatie over gedrag en naleving van interne controles met hogere niveaus.

Kenmerken

1.4.1 Het ratingbureau zorgt voor passende interne en externe communicatie en deelt correcte en volledige informatie van goede kwaliteit tijdig met de markt, beleggers, cliënten en regelgevers.

1.4.2 Het ratingbureau brengt communicatiekanalen naar hogere niveaus tot stand, waaronder een klokkenluidersprocedure, om materiële internecontrolekwesties door te leiden naar het management en het bestuur.

1.4.3 Het ratingbureau brengt communicatiekanalen van het management en de controlefuncties naar het personeel tot stand. Hiertoe behoren regelmatige updates over de doelstellingen en verantwoordelijkheden voor interne controle, informatie over vastgestelde nalevingsproblemen en presentaties en trainingen over beleid en procedures.

Component 1.5 Monitoringactiviteiten

21. ESMA is van mening dat doorlopende monitoring en thematische toetsingen van de activiteiten van een ratingbureau noodzakelijk zijn om te waarborgen dat het internecontrolesysteem van een ratingbureau adequaat en doeltreffend blijft. Deze monitoring helpt vaststellen of de componenten van het internecontrolesysteem van een ratingbureau aanwezig zijn en doeltreffend functioneren.

Kenmerken

1.5.1 Het ratingbureau zorgt ervoor dat evaluaties van het internecontrolesysteem worden uitgevoerd op verschillende niveaus van het ratingbureau, zoals op het niveau van bedrijfsonderdelen, controlefuncties en interne controle of onafhankelijke beoordelingsfuncties.

1.5.2 De evaluaties door het ratingbureau van internecontrolesystemen worden op regelmatige of thematische basis uitgevoerd, of via een combinatie van beide.

1.5.3 Het ratingbureau integreert doorlopende evaluaties, zoals de tijdige monitoring van e-mailuitwisselingen tussen analisten en uitgevende instellingen, in de bedrijfsprocessen en past deze aan veranderende omstandigheden aan. Hiertoe behoort ook het periodiek bijwonen van vergaderingen van ratingcomités of de toetsing achteraf daarvan.

1.5.4 Het ratingbureau rapporteert tekortkomingen die zijn geconstateerd bij monitoringevaluaties, evenals de vereiste corrigerende maatregelen, aan het bestuur en aan het management, die vervolgens monitoren of de corrigerende maatregel(en) tijdig ten uitvoer worden gelegd.

1.5.5 Indien belangrijke operationele functies worden uitbesteed aan een externe partij, zorgt het ratingbureau ervoor dat zijn personeel een directe verantwoordelijkheid draagt voor het monitoren van uitbestede processen. En ratingbureau zorgt ervoor dat externe dienstverleners duidelijk instructies ontvangen over de doelstellingen van het ratingbureau en over wat het ratingbureau verwacht van de dienstverlener, en dat due diligence wordt verricht voordat de dienstverlener wordt benoemd.

5.2 Internecontrolefuncties

22. ESMA verwacht, teneinde te waarborgen dat een ratingbureau over doeltreffende internecontrolefuncties (IC-functies) beschikt, dat een ratingbureau kan aantonen dat de volgende componenten en kenmerken aanwezig zijn in zijn beleid, procedures en werkpraktijken.

Algemene beginselen

23. ESMA is van mening dat de IC-functies van een ratingbureau dienen te beschikken over voldoende middelen en over medewerkers met voldoende deskundigheid om hun taken te vervullen. In gevallen waarin ratingbureaus de belangrijke operationele taken van een IC-functie hebben uitbesteed op het niveau van de groep of aan een externe partij, is ESMA van mening dat het ratingbureau volledige verantwoordelijkheid behoudt voor de activiteiten van de uitbestede IC-functie. ESMA is van mening dat medewerkers die belast zijn met IC-taken van een ratingbureau, over voldoende senioriteit dienen te beschikken om de autoriteit te hebben die nodig is voor het vervullen van hun verantwoordelijkheden. Sommige functies kunnen worden uitgevoerd op groepsniveau of door andere rechtspersonen binnen een ondernemingsstructuur, mits de groepsstructuur geen belemmering vormt voor het vermogen van het bestuur van een ratingbureau om toezicht uit te oefenen, en voor het vermogen van het management om zijn risico's doeltreffend te beheren, of het vermogen van ESMA om doeltreffend toezicht uit te oefenen op het ratingbureau.

24. ESMA verwacht dat een ratingbureau, om de onafhankelijkheid van zijn IC-functies te waarborgen, bij het bepalen van de rollen en functies van zijn IC-functies rekening houdt met de volgende beginselen:

    i. IC-functies zijn functioneel gescheiden van de functies/activiteiten die ze monitoren of controleren.

    ii. IC-functies verrichten geen operationele taken die vallen onder de zakelijke activiteiten die ze moeten monitoren of controleren.

iii. Het hoofd van een IC-functie rapporteert niet aan een persoon met directe verantwoordelijkheid voor het beheren van de activiteiten die de IC-functie monitort of controleert.

iv. Medewerkers die verantwoordelijkheden dragen voor IC-functies, hebben toegang tot relevante interne of externe training om te waarborgen dat zij over voldoende vakbekwaamheid beschikken voor hun taken.

Evenredigheid

25. De voorwaarden voor registratie van een ratingbureau vormen de minimale verwachtingen van ESMA ten aanzien van de interne controle, internecontrolefuncties en governance van een ratingbureau. Voor sommige ratingbureaus is het niet mogelijk om binnen hun organisatiestructuur op evenredige wijze te beschikken over alle IC-functies uit deze paragraaf. Toch dienen de kenmerken van alle IC functies, zoals beschreven in deze paragraaf van de richtsnoeren, te worden toegewezen aan een passende verantwoordelijke partij.

26. ESMA is van mening dat het bestuur van het ratingbureau toezicht dient te behouden op de uitvoering van deze taken en erop toe dient te zien dat de personeelsbezetting en de middelen van zijn IC-functies passend blijven, in overeenstemming met de aard, schaal en complexiteit van zijn activiteiten.

Component 2.1 Compliancefunctie

27. ESMA is van mening dat de compliancefunctie van een ratingbureau verantwoordelijk is voor het monitoren van en het rapporteren over de naleving door het ratingbureau en zijn werknemers van de verplichtingen uit hoofde van de CRAR. De compliancefunctie is verantwoordelijk voor het volgen van veranderingen in de wet- en regelgeving die toepasselijk is op zijn activiteiten. De compliancefunctie is ook verantwoordelijk voor het adviseren van het bestuurs- en toezichthoudend orgaan over wetten, regelgeving en normen waaraan het ratingbureau moet voldoen, en voor het beoordelen, samen met andere relevante functies, van de mogelijke impact van veranderingen in de relevante wet- en regelgeving op de activiteiten van het ratingbureau.

Kenmerken

2.1.1 De compliancefunctie verricht haar taken onafhankelijk van de bedrijfsonderdelen die verantwoordelijk zijn voor ratingactiviteiten, en rapporteert regelmatig aan de ONUB's van het ratingbureau.

2.1.2 De compliancefunctie adviseert en helpt medewerkers die betrokken zijn bij ratingactiviteiten, met betrekking tot de verplichtingen uit hoofde van de CRAR. De compliancefunctie identificeert proactief risico's en mogelijke gevallen van

niet-naleving door middel van tijdige monitoring en beoordeling van activiteiten en door follow-up van corrigerende maatregelen.

2.1.3 De compliancefunctie zorgt ervoor dat compliancemonitoring wordt uitgevoerd door middel van een goed gedefinieerd, gestructureerd compliancemonitoringprogramma.

2.1.4 De compliancefunctie beoordeelt, waar passend samen met andere relevante functies, de mogelijke impact van veranderingen in de relevante wet- en regelgeving op de activiteiten van het ratingbureau, en communiceert waar nodig met de risicobeheerfunctie over het compliancerisico van het ratingbureau.

2.1.5 De compliancefunctie zorgt ervoor dat het compliancebeleid wordt nageleefd en rapporteert aan het bestuur en het management over het beheer van het compliancerisico door het ratingbureau.

2.1.6 De compliancefunctie werkt samen met de risicobeheerfunctie wat betreft het uitwisselen van informatie die nodig is voor hun respectievelijke taken.

2.1.7 Het bestuur en de risicobeheerfunctie houden binnen hun risicobeoordelingsprocessen rekening met de bevindingen van de compliancefunctie.

Component 2.2 Toetsingsfunctie

28. ESMA is van mening dat de toetsingsfunctie van een ratingbureau er verantwoordelijk voor is dat ratingmethoden en -modellen en belangrijke aannames voor ratings op continue basis en ten minste jaarlijks worden getoetst. De toetsingsfunctie van het ratingbureau is ook verantwoordelijk voor het valideren en toetsen van nieuwe ratingmethoden en -modellen en belangrijke aannames voor ratings en eventuele wijzigingen in bestaande methoden en modellen of belangrijke aannames voor ratings.

Kenmerken

2.2.1 De toetsingsfunctie verricht haar taken onafhankelijk van de bedrijfsonderdelen die verantwoordelijk zijn voor ratingactiviteiten, en rapporteert regelmatig aan de ONUB's van het ratingbureau.

2.2.2 De taken van de toetsingsfunctie worden niet verricht door de aandeelhouders van het ratingbureau of door medewerkers die betrokken zijn bij de ontwikkeling van commerciële activiteiten.

2.2.3 Analisten nemen niet deel aan de goedkeuring van nieuwe, of de validering en toetsing van bestaande ratingmethoden en -modellen en belangrijke aannames voor ratings die zij hebben ontwikkeld.

2.2.4 Medewerkers van de toetsingsfunctie zijn ofwel als enigen verantwoordelijk voor, of hebben de meerderheid van de stemmen in de comités die verantwoordelijk zijn voor de goedkeuring van ratingmethoden en -modellen en belangrijke aannames voor ratings.

Component 2.3 Risicobeheerfunctie

29. ESMA is van mening dat de risicobeheerfunctie van een ratingbureau verantwoordelijk is voor de ontwikkeling en tenuitvoerlegging van het risicobeheerkader. De risicobeheerfunctie zorgt ervoor dat risico's die relevant zijn voor de verplichtingen van het ratingbureau uit hoofde van de CRAR, worden geïdentificeerd, beoordeeld, gemeten, gemonitord, beheerd en naar behoren gerapporteerd door de relevante afdelingen/functies binnen het ratingbureau.

Kenmerken

2.3.1 De risicobeheerfunctie verricht haar taken onafhankelijk van de bedrijfsonderdelen waarvan zij de risico's beheert, maar mag niet belet worden daarmee contact te onderhouden.

2.3.2 De risicobeheerfunctie zorgt ervoor dat alle risico's die materiële gevolgen kunnen hebben voor het vermogen van het ratingbureau om te voldoen aan zijn verplichtingen uit hoofde van de CRAR of die de voortzetting van zijn activiteiten in gevaar kunnen brengen, worden geïdentificeerd, beoordeeld, gemeten, gemonitord, beheerd en beperkt en dat deze naar behoren worden gerapporteerd door en aan de relevante afdelingen in het ratingbureau.

2.3.3 De risicobeheerfunctie monitort het risicoprofiel van het ratingbureau aan de hand van de risicobereidheid van het ratingbureau om het mogelijk te maken besluiten te nemen op dit gebied.

2.3.4 De risicobeheerfunctie geeft advies over voorstellen en risicobesluiten van bedrijfsonderdelen en informeert het bestuur over de vraag of deze besluiten in overeenstemming zijn met de risicobereidheid en de doelstellingen van het ratingbureau.

2.3.5 De risicobeheerfunctie doet aanbevelingen voor verbeteringen in het risicobeheerkader en corrigerende maatregelen ten aanzien van risicobeleid en -procedures, en kijkt opnieuw naar risicodrempels in verband met eventuele veranderingen in de risicobereidheid van de organisatie.

Component 2.4 Informatiebeveiligingsfunctie

30. ESMA is van mening dat de informatiebeveiligingsfunctie van een ratingbureau verantwoordelijk is voor de ontwikkeling en tenuitvoerlegging van de informatiebeveiliging binnen het ratingbureau. Een ratingbureau stelt een

informatiebeveiligingsfunctie in die een cultuur van informatiebeveiliging binnen het ratingbureau bevordert.

Kenmerken

2.4.1 De informatiebeveiligingsfunctie verricht haar taken onafhankelijk van de bedrijfsonderdelen en is verantwoordelijk voor het monitoren van de naleving door het ratingbureau van zijn informatiebeveiligingsbeleid en -procedures.

2.4.2 De informatiebeveiligingsfunctie beheert de informatiebeveiligingsactiviteiten van het ratingbureau.

2.4.3 De informatiebeveiligingsfunctie stelt een bewustwordingsprogramma voor informatiebeveiliging vast ten behoeve van het personeel van het ratingbureau, teneinde de beveiligingscultuur te versterken en een breed begrip te ontwikkelen van de informatiebeveiligingsvereisten van het ratingbureau.

2.4.4 De informatiebeveiligingsfunctie verstrekt het bestuur en het management regelmatige updates en adviezen over de informatiebeveiliging van de systemen en activiteiten van het ratingbureau.

Component 2.5 Internecontrolefunctie

31. ESMA is van mening dat de internecontrolefunctie van een ratingbureau verantwoordelijk is voor het tot stand brengen van een onafhankelijke, objectieve waarborgings- en adviesactiviteit die erop gericht is de activiteiten van de organisatie te verbeteren. Het helpt de organisatie haar doelen te bereiken door het instellen van een systematische, gedisciplineerde aanpak voor het evalueren en verbeteren van de doeltreffendheid van het internecontrolesysteem.

Kenmerken

2.5.1 De internecontrolefunctie verricht haar taken onafhankelijk van de bedrijfsonderdelen en is onderworpen aan een internecontrolehandvest waarin haar rol en verantwoordelijkheden zijn vastgelegd. Het bestuur houdt toezicht op de internecontrolefunctie.

2.5.2 De internecontrolefunctie werkt volgens een op risico gebaseerde aanpak.

2.5.3 De internecontrolefunctie toetst op onafhankelijke wijze en biedt objectieve waarborgen dat de activiteiten van het ratingbureau, met inbegrip van uitbestede belangrijke operationele functies[3], in overeenstemming zijn met het

[3] Belangrijke operationele functies zijn die welke worden genoemd in artikel 25, lid 2, van Gedelegeerde Verordening (EU) nr. 449/2012 betreffende te verstrekken gegevens voor de registratie en certificatie van ratingbureaus.

beleid en de procedures van het ratingbureau, en met toepasselijke wet- en regelgeving.

2.5.4 De internecontrolefunctie stelt ten minste eenmaal per jaar, op basis van de jaarlijkse doelstellingen voor de interne controle, een controleplan en een gedetailleerd controleprogramma op; het bestuur houdt hier toezicht op.

2.5.5 De internecontrolefunctie verstrekt regelmatig rapporten aan de ONUB's van het ratingbureau of aan het auditcomité, indien aanwezig.

2.5.6 De internecontrolefunctie communiceert haar controleaanbevelingen op een duidelijke, consistente wijze, zodat het bestuur en het management het belang van aanbevelingen kunnen begrijpen en in overeenstemming daarmee prioriteiten kunnen stellen.

2.5.7 Internecontroleaanbevelingen worden op de passende managementniveaus onderworpen aan een formele follow-upprocedure, zodat hierover wordt gerapporteerd en wordt gewaarborgd dat deze doeltreffend en tijdig ten uitvoer worden gelegd.