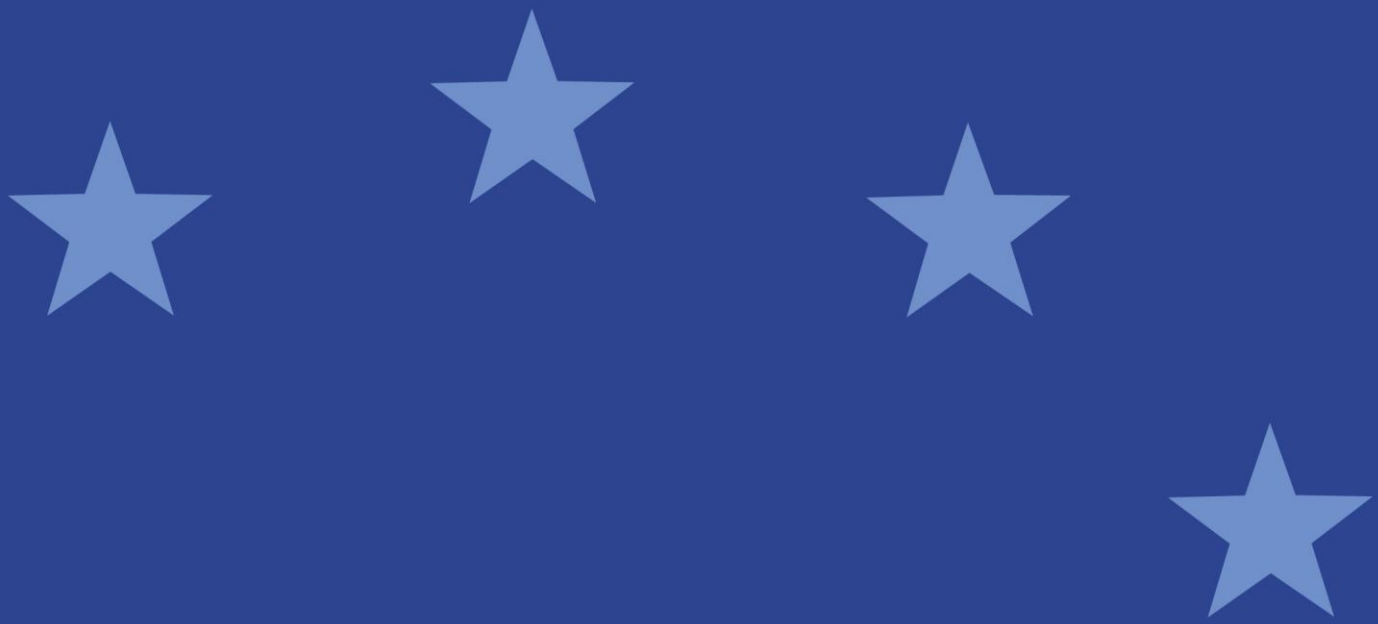
esma European Securities and Markets Authority

Final Report

Guidelines on Internal Control for CRAs



30 September 2020 | ESMA33-9-371

Table of Contents

Legislative references, abbreviations and definitions

Legislative References

ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC[1]
CRA Regulation	Regulation (EC) No 1060/2009 of the European Parliament and of the council of 16 September 2009 on credit rating agencies

Abbreviations

ESMA	European Securities and Markets Authority
CRA	Credit Rating Agency
CRAR	The CRA Regulation
IC Framework	Internal Control Framework
IC Functions	Internal Control Functions
CP	Consultation Paper
INED	Independent members of the administrative or supervisory board of the CRA

[1] *OJ L 331, 15.12.2010, p. 84.*

1. Executive Summary

1. The CRA Regulation (CRAR) includes a number of requirements relating to the internal control system that a credit rating agency (CRA) must have in place in order to prevent or mitigate any possible conflicts of interest and ensure the integrity of its credit rating activities.

2. The purpose of these Guidelines is to communicate what ESMA considers to be the characteristics and components of an effective internal control structure within a CRA. ESMA identified the need to provide this guidance during supervisory engagements, risk assessments and on-site investigations carried out during 2017 and 2018. ESMA formally communicated its intention to provide guidance on this topic in its supervisory work programme published in January 2019[2].

3. In developing the guidance, ESMA has considered a wide range of relevant requirements and standards, including the CRA Regulations' provisions relevant to internal controls; ESMA's supervisory experience and existing CRA industry practices; EU approaches and guidance on internal control; and internationally recognised internal control standards.

4. ESMA has conducted a public consultation on these Guidelines in order to gather the views of CRAs and other relevant stakeholders. A number of amendments and clarifications have been introduced into the final guidelines in order to take into account the views expressed during this consultation.

   - The guidelines are structured into two main parts, establishing:

     - ESMA's views on the components and characteristics that should be present in a CRA to demonstrate a strong framework for internal controls (IC framework);

     - ESMA's views on the components and characteristics that should be evidenced by a CRA in order to demonstrate the effectiveness of internal control functions within such a framework (IC functions).

Next Steps

5. The Guidelines in Annex I will be translated into all official languages and published on ESMA's website. The Guidelines will apply from 1 July 2021.

[2] Section 3.2 ESMA Supervisory Annual Report 2019

2. Feedback Statement

1. Responses to the CP were received from a number of respondents including academics, industry associations and CRAs. Following a review of these responses ESMA has introduced amendments to the guidelines in order to improve the clarity around ESMA's expectations.

2. This feedback statement provides a summary of the principal comments received to the different questions of the CP. The approach is to summarise the comments on a component by component basis, followed by a response that explains the rationale behind ESMA's decision to introduce, or not introduce, changes to that section.

Guidelines – General

3. Overall responses to the CP were supportive of ESMA's objectives and stressed that to a large degree CRAs were already implementing a number of the requirements. At the same time concerns were expressed that some of the CP's proposals were overly prescriptive and that a greater focus should be made on the substance of what a control should achieve, rather than the form in which it is achieved.

4. A number of respondents provided general comments on: the timeline for implementation, the possibility of flexibility for different organisational structures and the levels of proportionality for smaller CRAs. Regarding the timeline for implementation, comments under this point were to a large degree connected with possible need for changes to organisational structures. Regarding proportionality, smaller CRAs requested greater clarity on which sections covering IC Functions applied to them. In addition, some respondents were looking for clarification on the scope of the activities or policies and procedures covered by the Guidelines.

5. **ESMA Response:** ESMA has sought to address these general comments in various ways. Regarding the timeline for implementation, ESMA has lengthened the proposed implementation period from 6 months to 9 months. It had been originally foreseen that the Guidelines would be published in July 2020, with October 2020 as a start date for implementation. With the extension of the period for consultation in light of COVID 19, the timeline for implementation has also been deferred. It is now proposed that the start date for implementation should be 1 July 2021. This will allow CRAs additional amount of time in order to finalise the necessary measures to demonstrate that they are implementing the guidelines. In addition, ESMA has amended some provisions that were interpreted as requiring significant organisational change through a strict delineation of responsibilities between CRA staff. For example, ESMA has introduced new wording that clarifies the guidelines' original intention of ensuring that staff who conduct a task are not also responsible for approving that task.

6. Regarding proportionality, ESMA has clarified in the guidelines that while all CRAs are expected to demonstrate that an activity is performed, ESMA will not expect all CRAs to

do this through a separate stand-alone function. ESMA will apply proportionality by calibrating its expectations according to the nature, scale and complexity of a CRA. ESMA will communicate its expectations to CRAs through its supervision, but it will nonetheless remain the responsibility of a CRA to ensure that they have assessed the appropriateness of its internal control given the expectations set out in these guidelines.

Internal Control Framework – General

7. Comments in the general section of the IC Framework focused on a few key issues. First, there was a concern that the guidelines did not distinguish between the differing responsibilities of a CRA's board and its management. Second, there were comments requesting clarification of a number of terms used interchangeably in the text of the CP such as "board" and "Board" and "Independent non-Executive Director" and "INED". Third, there were comments relating to the proposals concerning the segregation of duties under 1.3.3; these issues are addressed in the following sections.

1.1 Control Environment

8. Comments in this section requested that the guidelines be clearer about the roles of the CRA's board and management. There was a concern that the wording in the CP did not distinguish sufficiently between the two different roles. In particular, the respondents requested clarification in the guidelines that the role of the CRA's board is to monitor and oversee the parts of the IC Framework, whereas it is the role of management to develop and implement the framework. Similar comments were made with regards to the accountability and responsibility of the board and management in respect of activities outsourced by the CRA to external providers or the wider group.

9. **ESMA Response:** ESMA's intention with the guidelines was to highlight that while the CRA's board is ultimately accountable for the activities of the CRA, it is the management that is responsible for implementing the guidelines and the day-to-day business activities of the CRA. However, ESMA recognises that referring to the role and responsibilities of these different bodies in the same sentence may lead to confusion. In addition, the use of the term "senior management" in the guidelines resulted in a lack of clarity as this term is defined under the CRA Regulation as including both management and members of the board[3]. As a result, ESMA has introduced wording that more clearly distinguishes between these positions. Under the new wording it is the role of the CRA's management to develop and implement the internal control framework, while it is the role of the board to approve the components of the framework and oversee their implementation.

1.2 Risk Management

10. Comments in this section focused on three elements of the CP's proposals. Some respondents considered it unrealistic or unachievable for CRAs to identify, monitor and

[3] Article 3(1)(n): 'senior management' means the person or persons who effectively direct the business of the credit rating agency and the member or members of its administrative or supervisory board;

mitigate all the risks relevant to the CRA. Instead it was suggested that CRAs should focus on those risks that could have a material impact on the activities of the CRA. Second, respondents requested that CRAs be given sufficient latitude under the Guidelines to conduct a risk-based approach to their risk management. Finally, some respondents noted that it would be useful if ESMA were to recommend relevant international standards that could be taken into account for the purposes of their risk management processes, or materiality thresholds to enable them to identify whether in ESMA's view a risk is material or not.

11. **ESMA Response:** ESMA has further clarified that the scope of the risk management activities it expects CRAs to carry out should be, at a minimum, those risks that could materially impact a CRA's ability to meet its obligations under CRAR. ESMA considers that internal risk assessments should be conducted according to a defined and comprehensive risk assessment methodology, however ESMA has removed reference to the requirement for it to take into account international standards and industry-leading practices as this could indirectly introduce standards or practices not approved by ESMA into the Guidelines. Similar changes have been made in the characteristics relating to Internal Audit Function in the Guidelines for the same reason.

1.3 Control Activities

12. Comments in this section recommended that the policies and procedures that should be documented should be limited to those that are relevant under CRAR. Respondents suggested that it would not be proportionate for them to document all the controls that exist within their rating processes, and that the focus of the guidelines should be on key controls.

13. The most significant comments received related to the proposals around segregation of duties. Here respondents questioned whether ESMA was proposing a rigid system of segregation of tasks within CRAs, which would require that they have dedicated methodology development and methodology review staff. This was cited as being particularly difficult for smaller CRAs, but also problematic for the working practices of larger CRAs.

14. **ESMA Response:** ESMA has clarified that the policies and procedures that should be documented are those that concern a CRA's activities subject to the requirements of CRAR. Likewise, the controls to be documented are those relevant to a CRA's activities subject to the requirements of CRAR.

15. Regarding the segregation of duties, it is important for ESMA to clarify the intention of the proposed guidelines and the changes that have been made to the guidelines. The goal of ESMA has been to ensure that staff members who conduct the analytical work of a credit rating should not be solely responsible for the approval of that credit rating. Likewise, staff members who conduct the development of methodologies, models or criteria should not be solely responsible for the approval of those methodologies, and staff members who conduct the validation or review of a credit rating methodology should not be solely

responsible for the approval of that validation or review. New wording has been introduced to clarify this section of the guidelines.

1.4 Information and Communication

16. There were limited or no material comments on the proposals in this section of the CP. However, comments in other sections required some limited changes to the original wording.

17. **ESMA Response:** Given the limited number of comments on this section of the CP, changes have been limited to those necessary to ensure consistency with changes made to other sections of the CP.

1.5 Monitoring Activities

18. Comments in this section of the CP focused mainly on the difficulties posed by the CP's proposals that CRAs implement real time compliance monitoring. Respondents raised two main issues with this proposal. It was suggested that the real time monitoring of credit rating activities was not as necessary or practicable as the real time monitoring of trading activities, and that in any event the necessary checks could be carried out more effectively on an ex-post basis. In addition, some respondents suggested that the wording used in the guidelines, specifically the "participation" of compliance in rating committees, could lead to a blurring of the first and second lines of defence and undermine the responsibility of the business lines for ensuring their activities are carried out in accordance with the CRA Regulation. Finally, other comments highlighted the difficulties that smaller CRAs might face in terms of implementing real time monitoring on a systematic basis, in particular to procure systems to enable the automation of these tasks.

19. **ESMA Response**: ESMA considers that, resources permitting, the compliance function should take an active role in monitoring the CRAs' activities to ensure they meet the requirements of the CRA Regulation. In this regard the CP suggested certain activities that a CRA's compliance function could carry out in order to give effect to this objective. However, following consideration of the responses provided and with due regard for proportionality for smaller CRAs, ESMA has introduced a limited number of revisions to these proposals. In this regard ESMA has removed reference to the real-time element of the monitoring requirement. The revised wording now states that CRAs should instead build ongoing evaluations into their processes, which can include, for example, the timely monitoring of e-mail interactions between analysts and issuers. This could also be done on an ex-post basis. In addition, ESMA has revised the wording that was interpreted as saying compliance staff could "participate" in a rating committee. The wording here has been amended to emphasise attendance rather than participation. This is so as not to preclude the possibility of compliance attending a rating committee meeting as part of its monitoring activities.

Internal Control Functions - General

20. The most significant comments provided under this section of the CP related to the feasibility of CRAs of less significant scale and complexity implementing the proposed guidance. These comments requested greater clarity on what IC Functions needed to be in place within these CRAs and what combinations of IC Functions were permissible under the guidelines. ESMA has addressed this concern by introducing further proportionality into the guidelines and will communicate to CRAs through its supervision where a CRA may apply proportionality in its application of the guidelines. ESMA has also removed the requirements for organisational separation of the information security function.

2.1 Compliance Function

21. A limited number of comments were received to this section of the guidelines. The main comments related to the proposal that the compliance function should be responsible for assessing the possible impact of any changes in the legal or regulatory framework on the CRA's activities. In this respect, respondents highlighted that the compliance function may lack the required expertise to fully assess the impact of any future regulatory changes on the activities of the CRA. As a result, these respondents requested flexibility in terms of which internal function is capable of fulfilling this role.

22. **ESMA Response**: While the compliance function is best placed to monitor for changes in the CRA Regulatory framework, ESMA does not expect that the evaluation of the impact of changes in the CRA Regulatory framework on the activities of the CRA, will be performed in isolation by the compliance function; this evaluation should be performed by the compliance function in collaboration with other relevant functions of the CRA. ESMA has clarified this expectation in the guidelines. In addition, ESMA has amended the proposed wording to clarify that the compliance function's findings should be taken into account in the risk management function's assessments rather than its decision-making processes.

2.2 Review Function

23. A significant number of comments were received to the proposals in this section of the CP. First, a number of respondents questioned whether the proposed guidelines were proposing that the review function should report exclusively to the independent members of the board, as opposed to the administrative or supervisory board itself. Second, comments were provided by CRAs requesting clarification regarding the participation of different types of staff in the approval of methodologies, models or key rating assumptions, for example whether the participation of analytical staff in this process was permitted. Finally, some respondents questioned why the CP's proposals refer to models or key rating assumptions, given the requirements of Article 8(5) of the CRA Regulation only refer to credit ratings and methodologies.

24. **ESMA Response**: The CRA Regulation requires a CRA's review function to report to members of the administrative or supervisory board. This includes the CRA's independent non-executive directors. The proposed guidelines do not contradict this requirement and do not propose that the review function should report exclusively to the INEDs. However,

ESMA has clarified that, in addition to its formal reporting obligations to the members of the board, it should provide regular reports to the CRA's INEDs. This regular reporting could occur in the context of a CRA's board meetings or on a more frequent basis. ESMA has additionally made slight changes to the proposals concerning the involvement of analytical and review staff in the approval processes relating to methodologies, models and key rating assumptions. In addition, ESMA has introduced a change of wording in 2.2.3 in order to ensure the text is aligned with the revised wording in 1.3.3. Here the revised wording states that while analytical staff may participate in the approval of methodologies by the review function, they should not participate in the approval of methodologies they developed themselves. In line with the principle of 1.3.3. staff who conduct the validation or review of a methodology, model or key rating assumption, may participate in the approval process of that methodology, model or key rating assumption but should not themselves be solely responsible for the outcome of that process. Therefore, where staff participates in the approval process for that methodology, model or key rating assumption where they have conducted part of the validation for that methodology, model or key rating assumption, there should be at least one other review function staff member in that approval process. Finally, reference is maintained to methodologies, models and key rating assumptions to ensure alignment with the relevant provisions of Annex I Section A (9) of the CRA Regulation.

2.3 Risk Management Function

25. Comments to this section focused mainly on the need to ensure proportionality of the risks to be assessed. Respondents requested clarification that CRAs were not obliged to identify, monitor or mitigate all risks, but rather those risks that could materially impact their regulated activities. A number of respondents queried whether greater flexibility could be provided to smaller CRAs who lacked the ability to establish a dedicated or stand-alone risk management function. Respondents also had similar comments to those on other control functions requesting a greater flexibility for how IC functions are structured. These comments emphasised that the independence of an IC function could be secured without requiring it to be organisationally separate. For example, there could be a dedicated CRA risk management section within an organisation's wider risk management function. Comments noted the risk management function's requirement to monitor the risk profile of the CRA against the CRA's strategic goals. Specifically, it was highlighted that this is a more appropriate role for the board rather than risk management function. The rationale for this is that the risk management function should advise and report on operational risks, while the board decides on strategic risks.

26. **ESMA Response:** The CP's proposals have been updated in several areas in this section to reflect the comments received. This includes providing for flexibility in terms of how the risk management function is located within the CRAs structure. The revised wording is to ensure that the risk management's responsibilities are carried out independently of the business lines, but also allow this to be done as part of a wider risk management function within the company structure. Finally, ESMA has introduced some additional clarifications to make it clear that the risk management function is responsible for monitoring the risk

profile of the CRA against the CRA's risk appetite, to enable effective decision making by the CRA's board.

2.4 Information Security Function

27. A significant number of comments were received to the proposals under this section of the CP. The vast majority of respondents agreed with the importance of focusing on information security and the general principle that this should be carried out separately from the work of the general IT function. However, a large number of respondents, in particular CRAs of less significant scale and complexity, pushed back on the CP's proposals that the information security function be organisationally independent from the IT function.

28. **ESMA Response**: In response to the comments received to the guidance in this section ESMA has made changes to its proposals. First, ESMA has clarified that the characteristics of this component are relevant for CRAs of all sizes. However, to ensure it is feasible for all CRAs to implement these recommendations, ESMA has removed the wording requiring that the Information Security function (or the designated party responsible for carrying out these characteristics) be organisationally separate from operational functions such as IT, but nonetheless should be independent. The independence of the function should instead be achieved through functional separation, such as through independent reporting lines. The purpose of this is to ensure that these requirements can be implemented by CRAs of all sizes without creating conflicts within existing organisational structures. This has also involved clarifying the CP's proposals that the Information Security function should provide reports to the board and management, in accordance with the CRA's organisational structure. In terms of the specific characteristics, ESMA has refined the tasks that the Information Security function should carry out, for example ESMA considers that the function should be responsible for monitoring the CRA's compliance with information security policies and procedures. In addition, the Information Security function should manage the CRA's information security activities.

2.5 Internal Audit Function

29. A number of comments in this section of the CP found the reference to 'international audit standards and leading practices' ambiguous or overly-burdensome where INEDs performed this activity. Also, a large number of respondents commented that while the Internal Audit function should provide reports to the INEDs, its reporting line should be to the board itself, or to the Audit Committee if this is in place.

30. **ESMA Response**: ESMA recognises that the inclusion of reference to international audit standards and leading practices without defining which specific standards and practices it refers to could introduce a degree of ambiguity into the requirements. ESMA has amended the proposal to remove these references. ESMA will continue to monitor through its supervision the appropriateness of internal audit activities performed by CRAs, including where it is performed by INEDs.

31. In addition, ESMA has clarified that, with regard to outsourced activities, the Internal Audit Function's oversight extends only to a CRA's important operational functions (as defined in Art 25 of the Commission Delegated Regulation 449/2012[4]), rather than all outsourced activities. In order to accommodate CRAs whose corporate structures rely on a group level Internal Audit function, ESMA has clarified the internal audit charter, internal audit control objectives, audit plan and audit programme should be subject to oversight by the board of the CRA, rather than approved by the board. Finally, ESMA has clarified that the Internal Audit function should provide regular reports to the INEDs or if the function is being performed by an INED, to the board, or Audit Committee where this is in place. ESMA recognises that for CRAs where it is proportionate to allow the INED to perform the IA function, there is a risk that the objectivity of the internal audit, or the oversight of the INED may be affected. ESMA will monitor for this risk through its ongoing supervision.

Cost Benefit Analysis

32. Comments provided in response to the Cost Benefit Analysis fell into two main categories. The first group of comments requested a longer timeline for implementation than that originally foreseen. The second group of comments highlighted that the CP's proposals concerning segregation of duties may entail significant organisational changes.

33. **ESMA Response:** Following the extension of the period of consultation, ESMA has extended the foreseen period for implementation. Originally foreseen as October 2020, ESMA has revised this to July 2021. This will provide CRAs with sufficient time to make the necessary internal preparations. In addition, ESMA has revised the wording in the section dealing with segregation of duties in 1.3.3; this should reduce the level of expected changes a CRA needs to implement.

[4] COMMISSION DELEGATED REGULATION (EU) No 449/2012 on Information for Registration and Certification of Credit Rating Agencies

Annex I

1 Scope

Who?

1. These guidelines apply to credit rating agencies established in the Union and registered with ESMA in accordance with Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies[5].

What?

2. These guidelines concern matters relating to the internal control structure and mechanisms necessary to ensure a CRA's effective compliance with Article 6(1)(2) and (4) and Section A of Annex I of the CRA Regulation.

When?

3. These Guidelines apply from 1 July 2021.

[5] OJ L 302, 17.11.2009, p.1.

2 Legislative references, abbreviations and definitions

Legislative References

ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC[6]
CRA Regulation	Regulation (EC) No 1060/2009 of the European Parliament and of the council of 16 September 2009 on credit rating agencies

Abbreviations

ESMA	European Securities and Markets Authority
CRA	Credit Rating Agency
CRAR	*CRA Regulation*
IC Framework	Internal Control Framework
IC Functions	Internal Control Functions
INED	Independent members of the administrative or supervisory board of the CRA
CRA's administrative or supervisory board	The board

3 Purpose

4. These guidelines concern matters relating to the internal control structure and mechanisms necessary to ensure a CRA's effective compliance with Article 6(1)(2) and (4) and Section A of Annex I of the CRA Regulation (CRAR).

5. The guidelines set out ESMA's expectations regarding the components and characteristics of an effective IC framework and IC functions within a credit rating agency.

[6] *OJ L 331, 15.12.2010, p. 84.*

4 Compliance and reporting obligations

4.1 Status of the guidelines

6. This document contains guidelines issued pursuant to Article 16 of the ESMA Regulation. In accordance with the Regulation, a CRA must make every effort to comply with the guidelines.

4.2 Reporting requirements

7. ESMA will assess the application of these guidelines by CRAs through its ongoing supervision and monitoring of CRA's activities.

8. ESMA will apply proportionality in the application of these Guidelines. While all CRAs are expected to demonstrate the characteristics of an effective internal control system outlined in these Guidelines, in some instances ESMA may not expect a CRA to do this through dedicated and separate IC Functions under Section 5.2.

9. ESMA will calibrate its expectations under Section 5.2 according to the nature, scale and complexity of a CRA. For larger CRAs, ESMA will expect a CRA to comply with all the expectations set out in the Guidelines For smaller CRAs, ESMA will refer to the conditions of the CRA's registration. However, given that some CRAs' nature, scale and complexity may have changed since registration, ESMA will communicate through its supervision if it has a higher threshold of expectations under Section 5.2 than those established at registration.

10. While ESMA will communicate its expectation of CRAs through its supervision it nonetheless remains the responsibility of a CRA's management, with oversight from its Board, to assess the appropriateness of its internal control against these guidelines.

5 Guidelines on Internal Controls for CRAs

Requirements Relating to Article 6(1), (2), (4) and Section A of Annex I of CRAR

11. In order to demonstrate that a CRA meets the objectives of an effective internal control structure in accordance with Article 6(1), (2), (4) and Section A of Annex I of the CRA Regulation, ESMA expects that a CRA demonstrates that its policies, procedures and working practices achieve the objectives of Sections **5.1** (Internal Control Framework) and **5.2** (Internal Control Functions) of these Guidelines.

12. In this context, the term "policies and procedures" should be understood as referring to internal documents that govern or direct how the CRA or its staff should perform activities that are subject to the requirements of CRAR.

5.1 Internal Control Framework

13. In order to demonstrate that it has an effective Internal Control Framework (IC framework), ESMA expects that a CRA is able to evidence the presence of the following components and characteristics in its internal policies and procedures and working practices.

General Principles

14. The board of a CRA should be accountable for overseeing and approving all components of the IC framework that is developed by management, as well as overseeing that its components are subject to monitoring and regular update by management. CRA's management should be responsible for establishing, implementing and updating the written internal control policies and procedures supporting the components of the IC framework.

15. As part of putting these policies and procedures in place, a CRA should have clear, transparent and documented decision-making processes as well as a clear allocation of roles and responsibilities within its IC framework, including its business lines and IC functions.

Component 1.1 Control Environment

16. ESMA considers that the control environment is the set of standards, processes and structures necessary for carrying out internal control across an organisation. In ESMA's view, the control environment is the foundation on which an effective system of internal controls is built.

17. A CRA's board and management both contribute to establishing the tone at the top regarding the importance of internal control. The management is responsible for development and performance of internal control and assessing the adequacy and effectiveness of the control environment.

Characteristic

1.1.1 The CRA's management should be responsible for establishing a strong culture of ethics and compliance within the CRA through the implementation of policies and procedures that govern the conduct of the CRA's staff. The board should exercise oversight of management in these areas.

1.1.2 The CRA's management should be responsible for ensuring that the CRA's policies and procedures:

i. Recall that the CRA's credit rating activities should be conducted in compliance with the CRA Regulation, applicable laws and the CRA's corporate values;

ii. Clarify that in addition to the compliance with legal and regulatory requirements and internal policies, staff are expected to conduct themselves with honesty and integrity and perform their duties with due skill, care and diligence; and

iii. Ensure that staff are aware of the potential internal and external disciplinary actions, legal actions and sanctions that may follow misconduct and unacceptable behaviours.

The board should exercise oversight of management in these areas.

1.1.3 The CRA's management should be responsible for establishing, maintaining and regularly updating adequate written internal control policies and procedures. The board should exercise oversight of management in these areas.

1.1.4 The CRA's management should retain responsibility for activities it has outsourced to external service providers or to a group level function within the CRA's group. The board should exercise oversight of management in these areas.

Component 1.2 Risk Management

18. ESMA considers that risk management involves the identification, assessment, monitoring and mitigation of all risks that could materially impact the CRA's ability to meet its obligations under the CRA Regulation or threaten its continued operation. This enables a CRA to allocate its internal control resources appropriately. Effective risk management should involve a dynamic and continuously evolving process for identifying, assessing and managing risks to the achievement of the CRA's main objectives.

Characteristic

1.2.1 The CRA should conduct their internal risk assessments in accordance with a defined and comprehensive risk assessment methodology.

1.2.2 The CRA's risk assessment methodology should encompass all business lines of the CRA.

1.2.3 The CRA should set its risk appetite and identify risk tolerance levels as part of the risk assessment process.

1.2.4 The CRA's risk assessment process should define and identify in advance the criteria and objectives against which the CRA's risks are going to be assessed.

1.2.5 The CRA's risk assessment methodology should be subject to continuous evolution and improvement.

Component 1.3 Control Activities

19. ESMA considers that control activities governing a CRA's business activities help mitigate the impact of risks within an organisation. They are actions designed through policies, procedures, systems, mechanisms and other arrangements. These control activities should be preventative, detective, corrective or deterrent in nature.

Characteristics

1.3.1 Documentation – The CRA should document its policies and procedures covering all business activities that are subject to the provisions of the CRA Regulation.

1.3.2 *Documented Controls and Control Testing* – A CRA should document the key controls in place to ensure adherence to those policies and procedures relevant to CRAR. The documentation of controls testing should set out:

i. A description of the control.

ii. The associated material risk(s).

iii. The role(s) or function(s) responsible for performing the control;

iv. The role(s) or functions(s) responsible for reviewing the control;

v. The evidence that the control has been executed;

vi. The frequency of execution of the control;

vii. A description of the testing procedure.

1.3.3 *Segregation of Duties* – The CRA should ensure appropriate segregation of duties to manage risks of conflicts of interest, fraud and human error. The segregation of duties should ensure that the persons:

i. Conducting the analysis of a credit rating are not solely responsible for the approval of the credit rating.

ii. Conducting the development of credit rating methodologies, models or key rating assumptions are not solely responsible for approval of those methodologies, models or key rating assumptions;

iii. Conducting a validation or review of a credit rating methodology, model or key rating assumption are not solely responsible for the approval of the validation or review of the credit rating methodology, model or key rating assumption.

1.3.4 *Designation of Responsibilities* – The CRA should designate in a clear and defined manner the roles or functions responsible for carrying out controls relating to obligations under CRAR and specify their respective roles and responsibilities. In doing so the CRA should distinguish between day-to-day key controls at the business level and those carried out by specific control functions.

1.3.5 *Authorisations and Approvals* – The CRA should document and describe the processes of its credit rating methodologies, models and key rating assumptions. This should include the staff members responsible for their validation or review, and the review of the results of these processes.

1.3.6 *Verifications, validations, reconciliations and reviews* – The CRA should implement measures to detect and act upon inappropriate, non-authorised, erroneous or fraudulent behaviour in its credit rating activities and the processes underlying these activities such as credit methodology/model validation, data validation and input.

1.3.7 *IT General Controls* – The CRA should implement controls to ensure the effectiveness of the IT environment of the CRA in supporting the CRA's business processes.

Component 1.4 Information and Communication

20. ESMA considers that appropriate internal and external communication is critical to a CRA meeting their regulatory obligations to the market, clients and staff. A CRA should establish procedures for the downward sharing of accurate, complete and good quality information to staff and external stakeholders as well as procedures for the upward sharing of sensitive information relating to behaviour and adherence to internal controls.

Characteristics

1.4.1 The CRA should ensure appropriate internal and external communication, sharing accurate, complete and good quality information in a timely manner to the market, investors, clients and regulators.

1.4.2 The CRA should establish upward communication channels, including a whistle-blowing procedure, to enable the escalation of material internal control issues to the board and management.

1.4.3 The CRA should establish downward communication channels from management and control functions to the staff. This should encompass regular updates on the objectives and responsibilities for internal control, communication of identified compliance issues and presentations and training on policies and procedures.

Component 1.5 Monitoring Activities

21. ESMA considers that ongoing monitoring and thematic reviews of a CRA's activities are necessary to ensure the continued adequacy and effectiveness of a CRA's internal control system. This monitoring will help ascertain whether the components of a CRA's internal control system are present and functioning effectively.

Characteristics

1.5.1 The CRA should ensure evaluations of the internal control system are carried out at different levels of the CRA such as business lines, control functions and internal audit or independent assessment functions.

1.5.2 The CRA's evaluations of internal control systems should be carried out on a regular or thematic basis, or through a mix of both.

1.5.3 The CRA should build ongoing evaluations, such as the timely monitoring of e-mail interactions between analysts and issuers, into the business processes and adjust them to changing conditions. This should include the periodic attendance in, or ex-post review of, rating committees.

1.5.4 The CRA should report deficiencies identified from monitoring evaluations and the required remediation actions to the board and management who should then monitor the timely implementation of corrective action(s).

1.5.5 In the case of outsourcing of important operational functions to an external party, the CRA should ensure staff have direct responsibility over the monitoring of outsourced business processes. A CRA should ensure that external service providers are provided with clear directions on the CRA's objectives and its delivery expectations, and that due diligence is conducted prior to the appointment of the provider.

5.2 Internal Control Functions

22. In order to ensure that a CRA has effective Internal Control Functions (IC functions), ESMA expects that a CRA should be able to evidence the presence of the following components and characteristics in its policies, procedures and working practices.

General Principles

23. ESMA considers that a CRA's IC functions should have sufficient resources and be staffed with individuals with sufficient expertise to discharge their duties. In cases where CRAs have outsourced the important operational tasks of an IC function to group level or to an external party, ESMA considers that a CRA retains full responsibility for the activities of the outsourced IC function. ESMA considers that staff in charge of CRA's IC functions should be of an appropriate seniority to have the necessary authority to fulfil

their responsibilities. Certain functions may be carried out at group level or by other legal entities within a corporate structure provided that the group structure does not impede the ability of a CRA's board to provide oversight, and the ability of management to effectively manage its risks, or ESMA's ability to effectively supervise the CRA.

24. To ensure the independence of a CRA's IC functions, ESMA expects a CRA to consider the following principles in establishing the roles and responsibilities of their IC functions:

    i. IC functions should be functionally separate from the functions/activities they are assigned to monitor, audit or control;

    ii. IC functions should not perform any operational tasks that fall within the scope of the business activities they are intended to monitor, audit or control;

    iii. The head of an IC function should not report to a person who has direct responsibility for managing the activities the IC function monitors, audits or controls.

    iv. Staff performing responsibilities relating to IC functions should have access to relevant internal or external training to ensure the adequacy of their skills to the tasks performed.

Proportionality

25. The conditions of registration for a CRA establish ESMA's minimum expectations for a CRA's internal control, internal control functions and governance. For some CRAs, it may not be proportionate for it to have all IC Functions under this section present within its organisational structure. Nonetheless, the characteristics of all IC functions, as described in this section of the guidelines, should still be allocated and assigned to an appropriate responsible party.

26. ESMA considers that the board of the CRA should retains oversight of the conduct of these tasks, and the ongoing appropriateness of the staffing and resources of its IC functions according to the nature, scale and complexity of its operations.

Component 2.1 Compliance Function

27. ESMA considers that the compliance function of a CRA is responsible for monitoring and reporting on the compliance of the CRA and its employees with its obligations under CRAR. The compliance function is responsible for following changes in the law and regulation applicable to its activities. The compliance function is also responsible for advising the administrative or supervisory board on laws, rules, regulations and standards that the CRA needs to comply with, and to assess in conjunction with other relevant functions the possible impact of any changes in the legal or regulatory environment on the CRA's activities.

Characteristics

2.1.1 The compliance function should perform its functions independently of the business lines that are responsible for credit rating activities and should provide regular reports to the CRA's INEDs.

2.1.2 The compliance function should advise and assist staff members involved in credit rating activities to comply with the obligations under the CRAR. The compliance function should be proactive in identifying risks and possible non-compliance through the timely monitoring and assessment of activities, as well as follow-up on remediation.

2.1.3 The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance-monitoring programme.

2.1.4 The compliance function, where appropriate in conjunction with other relevant functions, should assess the possible impact of any changes in the legal or regulatory environment on the CRA's activities and communicate, as appropriate, with the risk management function on the CRA's compliance risk.

2.1.5 The compliance function should ensure that compliance policies are observed and report to the board and management on the CRA's management of compliance risk.

2.1.6 The compliance function should cooperate with the risk management function to exchange information necessary for their respective tasks.

2.1.7 The findings of the compliance function should be taken into account by the board and the risk management function within their risk assessment processes.

Component 2.2 Review Function

28. ESMA considers that the review function of a CRA is responsible for reviewing credit rating methodologies, models and key rating assumptions on an ongoing basis and at least annually. The CRA's review function is also responsible for the validation and review of new methodologies, models and key rating assumptions and any changes to existing methodologies, models or key rating assumptions.

Characteristics

2.2.1 The review function should perform its functions independently of the business lines that are responsible for credit rating activities and should provide regular reports to the CRA's INEDs.

2.2.2 The CRA's shareholders or staff involved in business development should not perform the tasks of the review function.

2.2.3 Analytical staff should not participate in the approval of new, or validation and review of existing, methodologies, models and key rating assumptions which they have developed.

2.2.4 Review function staff should either be solely responsible or have the majority of the voting rights in the committees that are responsible for approving methodologies, models and key rating assumptions.

Component 2.3 Risk Management Function

29. ESMA considers that the risk management function of a CRA is responsible for the development and implementation of the risk management framework. It should ensure that risks relevant to its obligations under CRAR are identified, assessed, measured, monitored, managed and properly reported by the relevant departments/functions within the CRA.

Characteristics

2.3.1 The risk management function should perform its functions independently of the business lines and units whose risks it oversees but should not be prevented from interacting with them.

2.3.2 The risk management function should ensure that all risks that could materially impact a CRA's ability to perform its obligations under CRAR, or its continued operation, are identified, assessed, measured, monitored, managed, mitigated and properly reported by and to the relevant units in the CRA.

2.3.3 The risk management function should monitor the risk profile of the CRA against the CRA's risk appetite to enable decision-making.

2.3.4 The risk management function should provide advice on proposals and risk decisions made by business lines and inform the board as to whether those decisions are consistent with the CRA's risk appetite and objectives.

2.3.5 The risk management function should recommend improvements to the risk management framework and corrective measures to risk policies and

procedures and revisiting risk thresholds, in accordance with any changes in the organisation's risk appetite.

Component 2.4 Information Security Function

30. ESMA considers that the information security function of a CRA is responsible for the development and implementation of information security within the CRA. A CRA should establish an information security function that promotes an information security culture within the CRA.

Characteristics

2.4.1 The information security function should perform its functions independently of the business lines and should be responsible for monitoring the CRA's compliance with the CRA's information security policies and procedures.

2.4.2 The information security function should manage the CRA's information security activities.

2.4.3 The information security function should deploy an information security awareness program for the CRA's personnel to enhance the security culture and develop a broad understanding of the CRA's information security requirements.

2.4.4 The information security function should provide regular updates and advice to the board and management on the information security of the CRA's systems and activities.

Component 2.5 Internal Audit Function

31. ESMA considers that the internal audit function of a CRA is responsible for providing an independent, objective assurance and advisory activity designed to improve the organisation's operations. It helps the organisation to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of the internal control system.

Characteristics

2.5.1 The internal audit function should perform its functions independently of the business lines and be governed by an internal audit charter that defines it role and responsibilities and is subject to oversight by the board.

2.5.2 The internal audit function should follow a risk-based approach.

2.5.3 The internal audit function should independently review and provide objective assurance that the CRA's activities, including outsourced important operational

functions[7], are in compliance with the CRA's policies and procedures as well as with applicable legal and regulatory requirements.

2.5.4 The internal audit function should establish at least once a year, on the basis of the annual internal audit control objectives, an audit plan and a detailed audit programme, which is subject to oversight by the board.

2.5.5 The internal audit function should provide regular reports to the CRA's INEDs or to the Audit Committee, if in place;

2.5.6 The internal audit function should communicate its audit recommendations in a clear and consistent way that allows the board and management to understand the materiality of recommendations and prioritise accordingly.

2.5.7 Internal audit recommendations should be subject to a formal follow-up procedure by the appropriate levels of management to report on and ensure their effective and timely implementation.

[7] Important operational functions are those set out in Article 25 paragraph 2 of Commission Delegated Regulation 449/2012 on Information for Registration and Certification of Credit Rating Agencies.

Annex II Cost Benefit Analysis

Introduction

1. The need for a CRA to have a robust and appropriately resourced system of internal controls is clearly set out in Article 6 and Annex I Section A of the CRA Regulation. ESMA set out its intention to deliver this guidance in its 2019 supervisory work programme. The motivation for providing such guidance arose as a result of the identification of deficiencies in CRA's practices during supervisory risk assessments and on-site investigations carried out in 2017 and 2018.

2. The purpose of these guidelines is to ensure that ESMA's expectations are shared with all registered CRAs and future applicants to ensure a level playing field and the adoption of consistent good practice. The guidelines achieve this by communicating ESMA's expectations as to what steps a CRA should take in order to demonstrate the presence of an effective internal control system.

3. Once implemented the guidelines will be integrated into ESMA's supervisory assessment practices and guide how ESMA supervisors interact with CRAs in relation to their internal controls systems.

The Impact of the Draft ESMA Guidelines

4. The approach of the guidelines is to propose a framework of practices against which CRAs can compare and judge their own internal control systems and mechanisms.

5. The guidelines have also been drafted in such a way that they do not require specific organisational structures. Rather they recommend a number of principles that a CRA's internal control system should adhere to in order to demonstrate it meets the objectives of the regulation. As such it is not expected that the guidelines will require any CRA to fundamentally re-structure their internal organisational structure.

6. However, given that the guidance has drawn upon a wide range of standards and best practice it is expected that even for CRAs who are currently implementing well defined and sufficiently resourced internal control systems some revisions to current practices will be necessary. These revisions could entail changes to existing work practices or delegation of internal reporting lines and responsibilities.

Benefits

7. It is anticipated that the guidelines will provide benefits to ESMA, CRAs and the users of credit ratings. For ESMA, the guidelines will help to provide clarity and consistency in ESMA's supervision of CRAs' internal control systems and mechanisms. For CRAs it will act as a tool against which they can assess the effectiveness and appropriateness of their existing internal control systems and mechanisms. It will also provide clarity to CRAs on ESMA's supervisory expectations. For any new entrants into the CRA market the guidelines will likewise provide clarity on the practical application of the CRA Regulation's

internal control requirements. Finally, for the users of ratings, the guidelines will increase the likelihood that CRA's credit rating activities are independent and less likely to be affected by any conflicts of interest.

Costs

8. The costs imposed by these guidelines are likely three-fold. First, CRAs will be required to assess the guidelines provisions against their existing internal control systems and mechanisms. Second, following this review CRAs may be required to review their internal policies and procedures or internal control processes. Third, following any changes CRAs would be required to inform and update all relevant staff as to the changes in the internal processes, providing training where necessary.

Conclusions

9. The CRA Regulation is prescriptive in the area of CRA's internal control systems due to the systemic importance of credit ratings to financial stability and investor protection in the EU. Ensuring that CRA's credit rating activities are of high quality and free from any conflicts of interests is one of the key objectives of the CRA Regulation. As such guidelines which recommend a set of measures to ensure that CRAs are better able to meet this objective are justified on the basis that the costs of implementation will be limited to compliance assessments, revisions to internal policies and procedures, and potentially the recruitment and training of staff. Following the extension of the period for consultation the foreseen implementation period for the Guidelines has also been extended