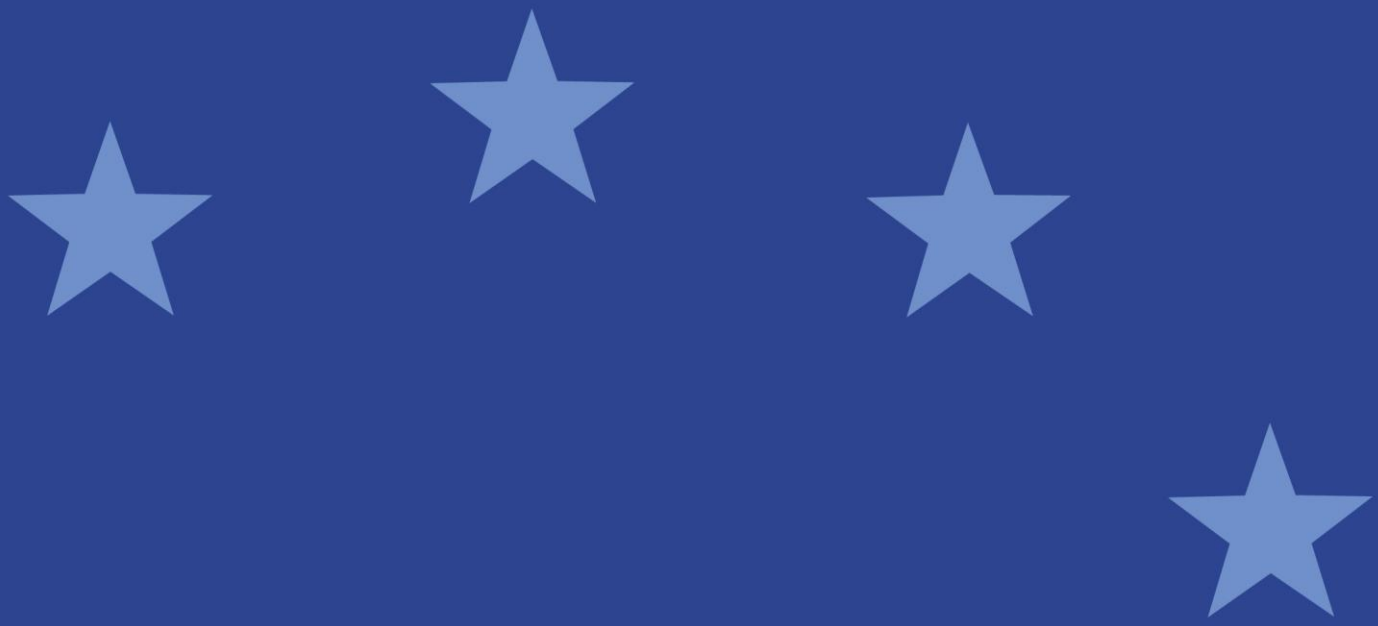
esma European Securities and Markets Authority

Consultation Paper

Guidelines on Internal Controls for CRAs



5 December 2019 | ESMA33-9-355

Table of Contents

Responding to this paper

ESMA invites comments on all matters in this paper and in particular on the specific questions summarised in Annex III. Comments are most helpful if they:

- respond to the question stated;
- indicate the specific question to which the comment relates;
- contain a clear rationale; and
- describe any alternatives ESMA should consider.

ESMA will consider all comments received by 16 March 2020.

All contributions should be submitted online at www.esma.europa.eu under the heading 'Your input - Consultations'.

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA's rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA's Board of Appeal and the European Ombudsman.

The collection of confidential responses is without prejudice to the scope of Regulation (EC) No 1049/20011. Possible requests for access to documents will be dealt in compliance with the requirements and obligations laid down in Regulation (EC) No 1049/2001.

Data protection

Information on data protection can be found at https://www.esma.europa.eu/data-protection under the heading Data Protection.

Who should read this paper

This paper may be of interest to users of credit ratings, credit rating agencies and entities interested in applying to be a registered CRA.

Legislative references, abbreviations and definitions

CP	Consultation paper
CRA	Credit Rating Agency
CRA Regulation or CRAR	Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit ratings agencies as amended by Regulation (EU) No 513/2011 of the European Parliament and of the Council of 11 May 2011, Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011, Regulation (EU) No 462/2013 of the European Parliament and of the Council of 21 May 2013, and Directive 2014/51/EU of the European Parliament and of the Council of 16 April 2014
EU CRA	A credit rating agency registered with ESMA
ESMA	European Securities and Markets Authority
IC Framework	Internal Control Framework
IC Function	Internal Control Function

1. Executive Summary

Reasons for publication

1. The CRA Regulation 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 that may impact the independence of its credit rating activities.

2. The purpose of this Consultation Paper (CP) is to clarify what ESMA considers to be the characteristics and components of an effective internal control system 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[1].

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.

Contents

4. The guidance is structured according to two main parts, establishing:

    - ESMA's views on the components and characteristics that should be evidenced by CRAs in order to demonstrate the presence of a strong framework for internal controls (IC framework);

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

Cost-benefit analysis

5. A preliminary cost-benefit analysis of the Guidelines is included in Annex I of the CP.

Next Steps

6. ESMA will consider the responses it receives to this CP in Q1 2020 and expects to publish a final report by end of Q2 2020.

[1] Section 3.2 ESMA Supervisory Annual Report 2019

2. Introduction

1. The need for a CRA to have a robust and appropriately resourced system of internal controls is set out in Article 6[2] and Annex I Section A of the CRA Regulation. However, although the regulation is prescriptive about what minimum requirements a CRA's internal control system must conform to, it is less detailed about how the various elements of the internal control system relate to each other as complementary parts of a unified framework.

2. As ESMA has already communicated some of its expectations on internal controls bilaterally with some CRAs during supervisory engagements, the purpose of these guidelines is to ensure that ESMA's expectations are shared with all registered CRAs as well as future applicants. This will not only help ensure a level playing field but will also facilitate the adoption of consistent good practices across CRAs.

3. The proposed guidance in this paper have been developed with reference to a range of contributing sources including the CRA Regulation's provisions relevant to internal controls[3]; ESMA's supervisory experience and existing CRA industry practices; EU approaches and guidance on internal control[4]; and internationally recognised internal control frameworks[5]. This has enabled ESMA to propose a set of practices that draw on existing good practices while taking into account the specificities of the CRA Regulation and CRA's business practices.

4. The proposed guidance is structured according to two main parts, the first part focusing on a CRA's overall framework for internal controls (IC Framework), the second part focusing on the roles and responsibilities of different internal control functions within this framework (IC Functions).

5. Each part, IC Framework and IC Function, is further split into different components. The guidance under the IC framework is split into the following five components: (i) control environment, (ii) risk management (iii) control activities (iv) information and communication and (v) monitoring activities.

6. Under the IC Framework, ESMA sets out its expectations as to what steps should be taken to evidence the presence of each component in a CRA's internal control system. For example, with respect to the "control environment", the guidance outlines the actions the CRA's administrative or supervisory board need to take to establish a strong control environment and set the right tone at the top.

[2] See Article 6(1), 6(2), 6(4) and Section A of Annex I of the CRA Regulation (OJ L 302, 17.11.2009, p.1).
[3] See Article 6 and points 2-6 and 10 of Section A of Annex I of the CRA Regulation
[4] European Commission's 'Internal Control Framework': Communication to the Commission from Commissioner Oettinger, Revision of the Internal Control Framework, Brussels, 19.4.2017C(2017) 2373 final; European Banking Authority, Final Guidelines on Internal Governance, EBA/GL/2017/11.
[5] COSO Internal Control – Integrated Framework, May 2013 © 2013, Committee of Sponsoring Organisations of the Treadway Commission (COSO), U.S.A.

7. The proposed guidance on IC functions is similarly split into components which match specific internal control functions, namely; (i) compliance (ii) review (iii) risk management (iv) information security (v) internal audit. For these IC functions, ESMA sets out what the role of each function should be, what its reporting lines should be, and whether it can be merged or combined with other functions.

8. Each of the components of the IC Framework and the IC Functions are discussed in the following sections of this CP. The approach of each section is to first provide a general introduction together with a description of roles and responsibilities in relation to the IC Framework or Functions. At the end of each section, there is a table setting out the proposed guidance.

9. Finally, these guidelines have also been developed with a view to accommodating the proportionality that is provided for smaller CRAs under Article 6(3) of the CRA Regulation. Smaller CRAs may be granted an exemption from certain requirements under Section A of Annex I of the CRA Regulation. In these cases, the guidelines set out that a CRA should demonstrate that the responsibilities under each specific IC Function, even the ones for which an exemption was granted at registration, have been allocated and assigned within the CRA and are being achieved through other means.

3. Internal Control Framework – Component Parts and Characteristics

General - Internal Control Framework

10. The first part of these guidelines discusses ESMA's expectations for an effective IC Framework. Specifically, the different components and characteristics that should be evidenced by CRAs within their policies, procedures and practices in order to demonstrate the presence of an effective IC Framework.

11. The five components of this section are drawn from the COSO framework[6]. The approach of the guidance is to provide a general overview of ESMA's view on the importance of the role of each component within an IC Framework. Following this, the guidance describes the specific characteristics that ESMA would expect to see within a CRA's internal policies, procedures and practices.

12. The precise naming, format or classification these policies, procedures and practices can vary across CRAs. For example, some CRAs may choose to communicate their requirements through the form of "guidance", "standard operating procedures", "process descriptions" or "walkthroughs". For this purpose, the term "policies and procedures" should be understood as a general term that refers to any internal document that governs how the CRA or its staff should perform activities or adhere to requirements set out by the CRA Regulation.

13. Irrespective of name, format or classification, documented internal policies and procedures are important to ensure that the different components and characteristics of the IC Framework are embedded in a CRA's practices. In this regard, the administrative or supervisory board should be accountable for the implementation and approval of these policies and procedures. It should also be accountable for ensuring that the CRA's policies and procedures are subject to ongoing monitoring and regular update.

14. There should be a clear, transparent and documented decision-making process for the monitoring and updating of these policies and procedures. These policies and procedures should include a clear allocation of responsibilities and authority within its IC framework, which includes the business lines, internal units and IC functions.

Proportionality – Internal Control Framework

15. It is not necessary to provide principles relating to proportionality in the guidance relating to IC Framework as these elements should be present within a CRA's internal policies and procedures regardless of organisational structure or resources.

[6] COSO Internal Control – Integrated Framework, May 2013 © 2013, Committee of Sponsoring Organisations of the Treadway Commission (COSO), U.S.A.

Component – Control Environment

16. The first component of the IC Framework is the control environment. An effective control environment begins with the CRA's Board and senior management setting the right tone at the top of the CRA. In creating the conditions for an effective control environment, the guidance establishes that the CRA's administrative or supervisory board is accountable for the adoption of a high level of ethical and professional standards relating to the conduct of the CRA's staff. The CRA's senior management are subsequently responsible for the development and implementation of these standards and ensuring they take into account the specific needs and characteristics of the CRA.

17. The CRA's board should be accountable for ensuring that equivalent ethical standards are put in place for external services providers. The CRA's senior management should be responsible for developing these standards and putting in place mechanisms to oversee adherence to these standards by external staff. The CRA's board is ultimately accountable for the effectiveness of these mechanisms.

18. The CRA's senior management should be responsible for ensuring that the CRA's staff are aware of the potential internal and external disciplinary actions for not adhering to the CRA's policies and procedures. The CRA's board should be accountable for the oversight of these policies and procedures, this oversight should include assessing whether any transgressions have been properly addressed.

Part 1: Internal Control Framework		
Component	**1.1**	Control Environment
The control environment is the set of standards, processes and structures necessary for carrying out internal control across an organisation and the foundation on which an effective system of internal controls is built. A CRA's administrative or supervisory Board ('the Board') and senior management are accountable and responsible for establishing the tone at the top regarding the importance of internal control and exercise oversight of the development and performance of internal control. It is the Board that is accountable for the adequacy and effectiveness of the control environment.		
Characteristics	**1.1.1**	The CRA's Board and senior management should be accountable and 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.

	1.1.2	The CRA's Board and senior management should be accountable and 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.
	1.1.3	The CRA's Board and senior management should be accountable and responsible for establishing, maintaining and regularly updating adequate written internal control policies, mechanisms and procedures.
	1.1.4	The CRA's Board and senior management should retain ultimate accountability and responsibility for activities it has outsourced to external service providers or to a group level function within the CRA's group.

Component – Risk Management

19. The second component of the IC Framework is effective risk management. This includes the identification, assessment, monitoring and mitigation of all risks relevant to the CRA. To ensure this is conducted effectively, the CRA's risk management processes should be carried out according to a defined and objective methodology. A high standard of risk management will ensure that the CRA is conscious of, and prepared for, the risks posed by its business activities. In turn, this will enable the CRA to establish its risk appetite and allocate its internal control resources accordingly. This component of the guidelines proposes that as part of their internal control framework, CRAs should adopt a holistic entity-wide approach to risk management that encompasses all business lines and internal control functions.

20. These risk assessments should enable the CRA to make fully informed decisions as to whether the risks that it has identified across its business lines are within its risk appetite.

In this regard, risks should be evaluated from both the bottom up and from the top down, within and across business lines, using consistent terminology and methodologies.

21. The CRA's approach to risk management should be embedded through policies and procedures that ensure the adequate identification, assessment, monitoring, management, mitigation and reporting of risks across the CRA.

Part 1: Internal Control Framework		
Component	**1.2**	Risk Management
Risk management involves the identification, assessment, monitoring and mitigation of all risks relevant to the CRA. 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.		
Characteristics	**1.2.1**	The CRA should conduct its internal risk assessments in accordance with a defined and comprehensive risk assessment methodology, taking into account international standards and industry-leading practices.
	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 an outcome 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 – Control Activities

22. The third component of the IC Framework relates to the CRA's control activities. This component is focused on ensuring that a CRA has appropriate controls and safeguards in

place for the day to day business activities of its staff. It builds upon the presence of a strong control environment in which the risks to which the CRA is exposed have been identified and its risk appetite appropriately defined by effective risk management.

23. As part of this component, CRAs should ensure that there is appropriate segregation of duties between staff in certain controlled activities. For example, staff members in charge of carrying out the analytical work of a credit rating should not be responsible for the approval of that credit rating. In addition, staff members responsible for the development of credit rating methodologies, models or criteria should not be involved in their implementation. Finally, staff members responsible for the development or implementation of credit rating methodologies should not be responsible for their review or validation.

24. The policies and procedures governing these activities should be documented with clearly designated responsibilities and establish that only staff with the relevant authorisations are allowed to carry out sensitive tasks such as methodology validation or credit rating approval.

25. These Control Activities are applicable across the CRA's IC Functions and business lines, including the CRA's IT related controls. They also facilitate and contribute to the effectiveness of individual IC Functions in the fulfilment of their tasks by ensuring the presence of an effective audit trail for determining and assessing responsibility across the CRA's activities.

<table>
<tr><th colspan="3">Part 1: Internal Control Framework</th></tr>
<tr><td>Component</td><td>1.3</td><td>Control Activities</td></tr>
<tr><td colspan="3">Control activities governing 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.</td></tr>
<tr><td rowspan="2">Characteristics</td><td>1.3.1</td><td>Documentation – The CRA should document its policies and procedures covering all areas of their business activities.</td></tr>
<tr><td>1.3.2</td><td>Documented Controls – The CRA should document the controls it puts in place to ensure its business activities adhere to its policies and procedures. The documentation of these controls should set out:
i. A description of the control.
ii. The associated risk(s).
iii. The person(s) responsible for performing the control.</td></tr>
</table>

		iv. The person(s) responsible for reviewing the control. v. The evidence that it has been executed. vi. The frequency of execution. A description of the testing procedure.
	1.3.3	*Segregation of Duties* – The CRAs 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. Responsible for the development of credit rating methodologies, models or key rating assumptions are not involved in their implementation; iii. Responsible for the validation, assessment or review of a credit rating methodology, model or key rating assumption are not involved in their development, implementation or approval.
	1.3.4	*Designation of Responsibilities* – The CRA should designate and document the staff members responsible for carrying out controls and specify their respective roles and responsibilities. In doing so the CRA should distinguish between day-to-day controls at the business level and those carried out by specific control functions.
	1.3.5	*Authorisations and Approvals* – The CRA should ensure that the credit rating process, the validation of methodologies, models and key rating assumptions and the review of the results of validation are only carried out by persons with appropriate authorisation.
	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 controls and reviews of lists for authorised recipients of confidential information

	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 – Information and Communication

26. Building upon a strong compliance culture, effective risk management and controls in business practices, the fourth element of the IC Framework concerns CRA's internal and external communication. In this respect, to ensure that the CRA is capable of ensuring an effective level of communication with all stakeholders it should ensure it policies and procedures support appropriate upward (whistleblowing) and downward (announcements on activities and updates on new policies and procedures) communication within the CRA.

27. Internal communication involves ensuring that all staff are aware of new policies and procedures, business developments, training opportunities and obligations relating to conflict of interest declarations. Effective external communication[7] involves timely communication with regulators, clients and the market in general.

28. Accordingly, it is the board that is ultimately accountable for ensuring that the relevant staff are informed and updated about the CRA's strategies and policies in a consistent manner to the level necessary for them to carry out their particular duties. The means by which this communication can be tailored to the CRA's internal requirements could take the form of guidelines, employee manuals, training or other means.

Part 1: Internal Control Framework		
Component	**1.4**	Information and Communication
Appropriate internal and external communication is critical to CRAs meeting their regulatory obligations to the market, clients and staff. CRAs 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 of good quality information in a timely manner to the market, investors, clients and regulators.

[7] External communication in this context refers to but is not limited to regulatory reporting requirements under the CRA Regulation, general communication and interaction with clients as well as the notification and reporting of information to other regulators.

	1.4.2	The CRA should establish upward communication channels, including a whistle-blowing procedure to enable the escalation of internal control issues to the Board and senior management.
	1.4.3	The CRA should establish a downward communication channels from the Board, senior 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 – Monitoring Activities

29. The final component of the IC framework concerns the effective monitoring of the CRA's activities and the adequacy of the IC framework itself. In this regard, there are a number of ways in which a CRA can and should monitor whether it is meeting its legal and regulatory requirements as well as adhering to its internal codes of conduct. These are set out in detail in the proposed guidance and recommend measures that cover compliance planning as well as monitoring of outsourced business activities.

Part 1: Internal Control Framework		
Component	**1.5**	**Monitoring Activities**
Ongoing monitoring and thematic reviews of 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 business 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 real-time compliance checks[8], into the business processes and adjust them to changing conditions. This should include the periodic

[8] Real time compliance checks include monitoring of e-mails and interactions between analysts and issuers.

		participation of compliance in rating committees and periodic monitoring of interactions between analysts and issuers.
	1.5.4	The CRA should report deficiencies identified from monitoring evaluations and the required remediation actions to their Board and senior management who should then monitor the timely implementation of corrective action(s).
	1.5.5	In the case of outsourcing to an external party, the CRA should ensure staff have direct responsibility over the outsourced business processes. CRAs should ensure that external service providers are provided with clear directions on the CRA's objectives and its delivery expectations and that industry best practice such as the IOSCO principles on outsourcing[9] is taken into account prior to the appointment of the provider.

Questions for Respondents

Q1. Do you have any comments on the proposed Guidelines under the section on IC Framework? In providing your comments please refer to the general principle, component and/or characteristic that you are commenting on.

Q2. Are there any other comments you wish to raise on this section?

[9] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf

4. Internal Control Functions - Component Parts and Characteristics

General – Internal Control Functions

30. While the first part of the guidelines addresses the components and characteristics of an effective IC framework, the second part deals with CRA's specific IC functions and how these should be integrated into the organisational structure and business activities of the CRA.

31. This is an area where the EBA Guidelines on Internal Governance[10] have proven to be a useful reference point for establishing ESMA's views, given their detailed guidance on the roles and responsibilities of different IC functions. As a starting point, it is important that each IC function has sufficient resources and is staffed with individuals with sufficient expertise to discharge their duties.

32. Although some degree of role-sharing between IC functions can be accommodated within smaller CRAs, combinations of the internal audit function with another internal control function, such as compliance and the review function or risk management, should be ruled out.

33. In cases where CRAs have outsourced the operational tasks of an IC function to an external party or to a group level function within the CRA's group, the CRA retains full responsibility for the activities of the outsourced IC function or IC functions' responsibilities. More generally, CRAs should ensure that the staff in charge of IC functions should be of an adequate hierarchical level and have the necessary authority to fulfil their responsibilities. For example, the staff in charge of the compliance, risk management, review and internal audit functions should be directly accountable to the Board and their performance should be reviewed by the Board.

34. In addition, to ensure the independence of the IC functions, CRAs should consider the following when establishing the roles and responsibilities of their IC functions:

    - IC functions should be organisationally separate from the functions/activities they are assigned to monitor, audit or control;

    - 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;

    - The staff member in charge of an IC function should not be reporting to a person who has responsibility for managing the activities the IC function monitors, audits or controls.

[10] EBA Guidelines on Internal Governance

35. Staff performing responsibilities relating to internal control functions should have access to relevant internal or external training to ensure the adequacy of their skills to the tasks performed. The following sub-sections discuss key IC functions and the characteristics that CRAs should evidence in order to demonstrate the sufficient presence of each component within the CRA.

Proportionality

36. CRAs who have been granted exemptions from certain organisational requirements in accordance with Article 6(3) should ensure that where a stand-alone IC function is not present within that CRA's organisational structure, the responsibilities of that IC function should be allocated and assigned to an appropriate responsible party. In these cases, the administrative or supervisory board of the CRA retains responsibility for the conduct of these tasks. The CRA should ensure that the staffing and resources of its IC functions are appropriate to the nature, scale and complexity of its operations.

Internal Control Function - Compliance

37. ESMA is of the opinion that all CRAs should establish a dedicated control function in order to manage its compliance risk and related tasks. CRAs should appoint a person responsible for this function across the entire CRA who has the authority to report directly, on their own initiative, to the board. Nevertheless, it is possible to receive an exemption from this requirement of the CRA Regulation, if CRAs can demonstrate there are sufficient safeguards in place and the provision is disproportionate.

38. In line with the requirements of the CRA Regulation, the compliance function (or in the case of an exemption the delegated party or parties performing the compliance tasks) should be independent of the business lines and have sufficient authority, stature and resources. Staff within the compliance function should possess sufficient knowledge, skills and experience on compliance and procedures and have access to regular training. The administrative or supervisory board in its supervisory function should oversee the implementation of a well-documented compliance policy which should be communicated to all staff.

Part 2: Internal Control Functions		
Component	**2.1**	Compliance Function
The compliance function of a CRA is responsible for monitoring and reporting on compliance of the CRA and its employees with its obligations under the CRA Regulation. The compliance function is responsible for following changes on 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 assess 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 advise and assist staff members involved in credit rating activities to comply with the obligations under the CRA Regulation, it should be proactive in identifying risks and possible non-compliance through monitoring and assessment activities and follow-up on remediation.
	2.1.2	The compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance-monitoring programme.
	2.1.3	The compliance function 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.
	2.1.4	The compliance function should ensure that compliance policies are observed and report to the board and senior management on the CRA's management of compliance risk.
	2.1.5	The compliance function should cooperate with the risk management function to exchange information necessary for their respective tasks.
	2.1.6	The findings of the compliance function should be taken into account by the board and the risk management function within their decision-making processes.

Control Function - Review

39. The review function plays a key role under CRA Regulation in ensuring that there is appropriate review and validation of CRA's methodologies, models and key rating assumptions. Smaller CRAs who are able to demonstrate that this requirement is not proportionate in view of the nature scale and complexity of their business may be exempted from having a dedicated internal review function at the registration phase. However, as part of granting this exemption, the CRA would still need to implement measures and procedures to ensure effective compliance with the objectives of the regulation. For smaller CRAs this could be achieved by assigning the responsibilities to the group or parent company or an independent party with the relevant skills and expertise.

Part 2: Internal Control Functions		
Component	**2.2**	Review Function
The review function of a CRA is responsible for reviewing credit rating methodologies, models and key rating assumptions on at least an annual basis. The CRA's review function is also responsible for validating 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 be independent of the business lines that are responsible for credit rating activities and should report to the independent members of the Board
	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	Although analytical staff may participate in committees approving methodologies, analytical staff should not vote in committees approving methodologies, models and key rating assumptions they are responsible for applying themselves.
	2.2.4	The review function staff should have the majority of the voting rights in the committees that are responsible for approving methodologies, models and key rating assumptions.

Internal Control Function - Risk Management

40. While the establishment of a dedicated risk management function is not a requirement of the CRA Regulation, ESMA staff considers that the duties of a risk management function are nevertheless relevant for CRAs of significant scale and complexity. In these cases, whether acting as part of an existing function or on a standalone basis, the risk management function should have direct access to the CRA's Board and to all business lines and other internal units that have the potential to generate risks.

41. Where there is a dedicated risk management function, the staff within it should possess sufficient knowledge, skills and experience on risk management techniques and procedures and on the activities of the CRA and its products, and have access to regular training. The risk management function should provide relevant independent information, analysis and advice on risks identified as relevant to business lines or internal units and whether they are consistent with the CRA's risk appetite.

42. The risk management function should ensure all identified risks can be effectively monitored by the relevant business units and provide recommendations on improvements to the risk management framework and corrective measures to risk policies and procedures in accordance with any changes in the organisation's risk appetite.

Part 2: Internal Control Functions		
Component	**2.3**	Risk Management Function
The risk management function of a CRA is responsible for the development and implementation of the risk management framework. It should ensure that all risks 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 be independent 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 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 strategic goals and 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.

Internal Control Function - Information Security

43. As part of the broader requirement that CRAs have sound administrative and accounting procedures and effective procedures for risk assessment, the CRA regulation also requires that a CRA put in place effective control and safeguard arrangements for information processing systems.

44. While there is no requirement for a CRA to have a separate information security function, the proposed guidance will set out that ESMA expects larger CRAs with more credit rating activities of greater complexity to establish such a function. In the case of smaller CRAs while a stand-alone function is not required, the tasks outlined below should be carried out by an existing function.

Part 2: Internal Control Functions		
Component	**2.4**	Information Security Function[11]
The information security function of a CRA is responsible for the development and implementation of the information security strategy within the CRA and for relevant third parties. CRAs of significant scale and complexity should establish an information security function that promotes an information security culture within the CRA and takes the lead on the definition and implementation of the information security program and strategy. This function should be independent from operational functions and organisational structures, such as IT or other functions with operational duties.		
Characteristics	**2.4.1**	The information security function should be responsible for reviewing and monitoring the CRA's compliance with the CRA's information security policies and procedures.
	2.4.2	The information security function should collect, analyse and comment on information security metrics and incidents.
	2.4.3	The information security function should develop and deploy an information security awareness program for 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 report to and advise the board and senior management on the status of the information security management system and risks. This should include information about information security projects, information security incidents and the results of information security reviews.

Internal Control Function - Internal Audit

[11] This component relates to the responsibilities of the Information Security Function as opposed to the Information Technology function within a CRA, which has IT operational responsibilities.

45. The CRA Regulation requires that CRAs monitor and evaluate the effectiveness of their systems, internal control mechanisms and arrangements established in accordance with the CRA Regulation. ESMA staff considers that the most effective way of achieving this is through the establishment of an independent and effective internal audit function. However, not all CRAs may have the resources to have such a dedicated function, in these cases the internal audit responsibilities should be carried out through other appropriate means. For example, the responsibilities could be assigned to a suitably qualified Independent Non-Executive Director or an appropriate external party.

46. Whether it is carried out on a dedicated basis, or through other means, a CRA should ensure that the independent monitoring of the CRA's internal control mechanisms is carried out by a function or party that is independent of business lines and has sufficient resources and authority to carry out its tasks. The CRA should ensure that this internal audit function is independent from the audited activities. Therefore, the function or parties performing the internal audit function should not be combined with other functions.

47. The internal audit function should be responsible for independently reviewing the compliance of all the CRA's activities and units including outsourced activities, in line with the CRA's policies and procedures. The internal audit function should not be involved in designing, selecting, establishing and implementing specific internal control policies or mechanisms. However, this should not prevent the board in its management function from requesting input from internal audit on matters related to risk, internal controls and compliance with applicable rules.

48. The internal audit function should have access to any records, documents, information and buildings of the CRA. This should include access to the management information systems and minutes of all committees and decision-making bodies.

49. The internal audit function should adhere to national and international professional standards. The work of the internal audit function should be performed in accordance with an audit plan and detailed audit programs following a risk-based approach. In this regard, an audit plan should be drawn up at least once a year on the basis of the annual control objectives in line with the guidance of the administrative or supervisory board.

50. Finally, all audit recommendations should be subject to a formal follow-up procedure by the respective levels of management to ensure and report their effective and timely resolution. The head of the internal audit function should be able to report directly where appropriate and on his own initiative the administrative or supervisory board on the implementation of the corrective measures decided on.

Part 2: Internal Control Functions

Component	**2.5**	Internal Audit Function
An internal audit function 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 be governed by an internal audit charter that defines it role and responsibilities and is approved by the Board.
	2.5.2	The internal audit function should follow a risk-based approach and adhere to international internal audit standards and leading practices.
	2.5.3	The internal audit function should independently review and provide objective assurance that the CRA's activities, including outsourced activities, 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 approved by the Board
	2.5.5	The internal audit function should report directly to the independent members of the Board – 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 senior 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 ensure and report on their effective and timely implementation.

Questions for respondents

Q3. Do you have any comments on the proposed Guidelines under this section? In providing your comments please refer to the general principle, component and/or characteristic that you are commenting on.

Q4. Are there any other comments you wish to raise on this section?

Annex I Cost Benefit Analysis

Introduction

51. 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.

52. 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 means by which the guidelines will achieve this is by making clear what components and characteristics ESMA considers should be evidenced within a CRA's internal control system.

53. 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

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

55. The guidelines have also been drafted in such a way that they do not recommend 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.

56. 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

57. There benefits to ESMA, CRAs and the users of credit ratings. For ESMA, the guidelines will act not only as a supervisory handbook against which ESMA supervisors can assess each CRA's internal control systems and mechanisms. For CRAs it will act as a resource against which they can assess the effectiveness and appropriateness of their existing internal control systems and mechanisms and also provide clarity on ESMA's expectations as a supervisor. For any new entrants into the CRA market the guidelines will likewise

provide them with clarity on the practical application of the CRA Regulations 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 affected by any conflicts of interest.

Costs

58. 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

59. 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 a 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 training for staff.

Questions for respondents

Q5. Do you agree with the cost benefit analysis as it has been described?

Q6. Do you have any comments on the proportionality for smaller CRAs provided in the Guidelines?

Annex II Guidelines

Scope

Who?

1. These guidelines apply to credit rating agencies established in the Union and registered with ESMA (hereinafter "EU CRAs") in accordance with Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies[12] (hereinafter "CRA Regulation").

What?

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 Annex I Section A of the CRA Regulation.

When?

2. These Guidelines will be translated into all official EU languages and published on ESMA'S Website. ESMA will consider these Guidelines for the purpose of its supervision as of 1 October 2020.

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

Definitions, legislative references and acronyms

The following definitions apply:

CRA	Credit rating agency
CRAR	The Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit ratings agencies as amended by Regulation (EU) No 513/2011 of the European Parliament and of the Council of 11 May 2011, Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011, Regulation (EU) No 462/2013 of the European Parliament and of the Council of 21 May 2013, and Directive 2014/51/EU of the European Parliament and of the Council of 16 April 2014
IC Functions	Internal Control Functions
IC Framework	Internal Control Framework
ESMA	European Securities and Markets Authorities
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 (ESMA Regulation)
EU CRA	A credit rating agency registered with ESMA.

1 Purpose

3. The Guidelines set out ESMA's expectations regarding the components and characteristics of an effective internal control framework and the functions of different internal controls within a credit rating agency.

2 Compliance and reporting obligations

2.1 Status of the guidelines

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

2.2 Reporting requirements

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

3 Guidelines

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

6. In order to demonstrate that a CRA meets the objectives of Article 6(1)(2)(4) and Section A of Annex I of the CRA Regulation, ESMA expects that a CRA should be able to demonstrate that its policies, procedures and working practices are aligned with Sections **3.1** (Internal Control Framework) and **3.2** (Internal Control Functions) of these Guidelines.

7. In this context, the term "policies and procedures" should be understood as referring to any internal document that governs or directs how the CRA or its staff should perform activities or adhere to requirements of the CRA Regulation.

3.1 Internal Control Framework

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

General Principles

9. The administrative or supervisory board of the CRA should be accountable for all components of the IC framework as well as ensuring that they are subject to monitoring and regular update. CRA's senior management should be responsible for developing and implementing the written internal control policies, mechanisms and procedures supporting the components of the IC framework.

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

Component 1.1 Control Environment

11. 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.

12. The CRA's administrative or supervisory Board ('the Board') and senior management are accountable and responsible for establishing the tone at the top regarding the importance of internal control and exercises oversight of the development and performance of internal control. It is the Board that is also accountable for the adequacy and

effectiveness of the control environment. It is the Board that is ultimately accountable for the adequacy and effectiveness of the control environment.

Characteristic

1.1.1 The CRA's Board and senior management should be accountable and 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.

1.1.2 The CRA's Board and senior management should be accountable and 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.

1.1.3 The CRA's Board and senior management should be accountable and responsible for establishing, maintaining and regularly updating adequate written internal control policies, mechanisms and procedures.

1.1.4 The CRA's Board and senior management should retain ultimate accountability and responsibility for activities it has outsourced to external service providers or to a group level function within the CRA's group.

Component 1.2 Risk Management

13. Risk management involves the identification, assessment, monitoring and mitigation of all risks relevant to the CRA. 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, taking into account international standards and industry-leading practices.

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 an outcome 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

14. Control activities governing 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 areas of their business activities.

1.3.2 *Documented Controls* – CRAs should document the controls they put in place to ensure their business activities adhere to their policies and procedures. The documentation of these controls should set out:

i. A description of the control.

ii. The associated risk(s).

iii. The person(s) responsible for performing the control;

iv. The person(s) responsible for reviewing the control;

v. The evidence that it has been executed;

vi. The frequency of execution;

vii. A description of the testing procedure.

1.3.3 *Segregation of Duties* – The CRAs 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. Responsible for the development of credit rating methodologies, models or key rating assumptions are not involved in their implementation;

iii. Responsible for the validation, assessment or review of a credit rating methodology, model or key rating assumption are not involved in their development, implementation or approval.

1.3.5 *Designation of Responsibilities* – The CRA should designate and document the staff members responsible for carrying out controls and specify their respective roles and responsibilities. In doing so the CRA should distinguish between day-to-day 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 process of its credit rating methodologies, models and key rating assumptions. this should include the staff members responsible for their validation, and the review of validation results.

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 controls and reviews of lists for authorised recipients of confidential information

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

15. Appropriate internal and external communication is critical to CRAs meeting their regulatory obligations to the market, clients and staff. CRAs 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 of 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 internal control issues to the Board and senior management.

1.4.3 The CRA should establish a downward communication channels from the Board, senior 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

16. Ongoing monitoring and thematic reviews of 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 business 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 real-time compliance checks[13], into the business processes and adjust them to changing conditions this should include the periodic participation of compliance in rating committees and periodic monitoring of interactions between analysts and issuers.

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

1.5.5 In the case of outsourcing to an external party, the CRA should ensure staff have direct responsibility over the outsourced business processes. CRAs should ensure that external service providers are provided with clear directions on the CRA's objectives and its delivery expectations and that industry best

[13] Real time compliance checks include monitoring of e-mails and interactions between analysts and issuers.

practice such as the IOSCO principles on outsourcing[14] is taken into account prior to the appointment of the provider.

3.2 Internal Control Functions

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

General Principles

18. ESMA considers that 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 operational tasks of an IC function to group level or to an external party, ESMA considers that the 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 adequate hierarchical level to have the necessary authority to fulfil their responsibilities.

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

    i. IC functions should be organisationally 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 be reporting to a person who has 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

20. ESMA considers that CRAs who have been granted exemptions from certain organisational requirements in accordance with Article 6(3) of the CRA Regulation should ensure that where a stand-alone internal control function is not present within the CRA's organisational structure, the responsibilities of that IC function are allocated and assigned to an appropriate responsible party. In these cases, ESMA considers that the administrative or supervisory board of the CRA remains accountable for the conduct of

[14] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf

these tasks. The CRA should ensure that the staffing and resources of its IC functions are appropriate to the nature, scale and complexity of its operations.

Component 2.1 Compliance Function

21. The compliance function of a CRA is responsible for monitoring and reporting on compliance of the CRA and its employees with its obligations under the CRA Regulation. The compliance function is responsible for following changes on 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 assess 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 advise and assist staff members involved in credit rating activities to comply with the obligations under the CRA Regulation, it should be proactive in identifying risks and possible non-compliance through monitoring and assessment activities and follow-up on remediation.

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

2.1.3 The compliance function 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.

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

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

2.1.6 The findings of the compliance function should be taken into account by the board and the risk management function within their decision-making processes.

Component 2.2 Review Function

22. The review function of a CRA is responsible for reviewing credit rating methodologies, models and key rating assumptions on at least an annual basis. The CRA's review function is also responsible for validating 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 be independent of the business lines that are responsible for credit rating activities and should report to the independent members of the Board.

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 Although analytical staff may participate in committees approving methodologies, analytical staff should not vote in committees approving methodologies, models and key rating assumptions they are responsible for applying themselves.

2.2.4 Review function staff should 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

23. A risk management function of a CRA is responsible for the development and implementation of the risk management framework. It should ensure that all risks 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 be independent 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 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 strategic goals and 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

24. The information security function of a CRA is responsible for the development and implementation of the information security strategy within the CRA and for relevant third parties. CRAs of significant scale and complexity should establish an information security function that promotes an information security culture within the CRA and takes the lead on the definition and implementation of the information security program and strategy. This function should be independent from operational functions and organisational structures, such as IT or other functions with operational duties (e.g. rating or IT operations).

Characteristics

2.4.1 The information security function should be responsible for reviewing and monitoring the CRA's compliance with the CRA's information security policies and procedures collects.

2.4.2 The information security function should collect, analyse and comment on information security metrics and incidents.

2.4.3 The information security function should develop and deploy an information security awareness program for 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 report to and advise the board and senior management on the status of the information security management system and risks (e.g. information about information security projects, information security incidents and the results of information security reviews).

Component 2.5 Internal Audit Function

25. An 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 be governed by an internal audit charter that defines it role and responsibilities and is approved by the Board.

2.5.2 The internal audit function should follow a risk-based approach and adhere to international internal audit standards and leading practices.

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

2.5.5 The internal audit function should report directly to the independent members of the Board – 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 senior 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 ensure and report on their effective and timely implementation.

Annex III List of Questions

Q1	Do you have any comments on the proposed Guidelines under the section on IC Framework? In providing your comments please refer to the general principle, component and/or characteristic that you are commenting on.
Q2	Are there any other comments you wish to raise on this section?
Q3	Do you have any comments on the proposed Guidelines under this section? In providing your comments please refer to the general principle, component and/or characteristic that you are commenting on.
Q4	Are there any other comments you wish to raise on this section?
Q5	Do you agree with the cost benefit analysis as it has been described?
Q6	Do you have any comments on the proportionality for smaller CRAs provided in the Guidelines?