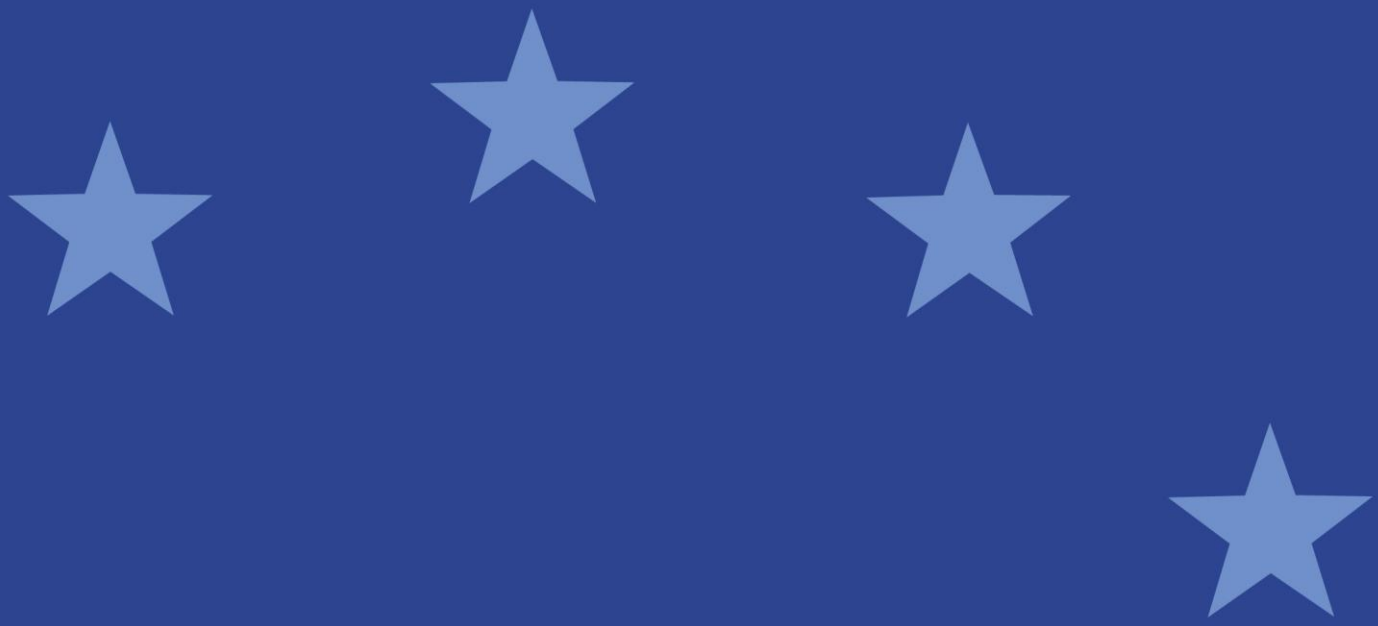
esma European Securities and Markets Authority

Guidelines

On Internal Control for CRAs



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

Table of Contents

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[1].

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.

[1] 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[2]
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.

[2] *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[3], 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.

[3] 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.