18 December 2025
ESMA80-634726060-1762

Final Report

Guidelines on Internal Controls for Benchmark Administrators, Credit Rating Agencies and Market Transparency Infrastructures

Table of Contents

1 Executive Summary

Reasons for publication

ESMA directly supervises all EU Credit Rating Agencies (CRAs), Securitisation Repositories (SRs) and Trade Repositories (TRs) as well as certain Benchmark Administrators (BMAs)[1] and certain Data Reporting Services Providers (DRSPs)[2] in accordance with the relevant Regulations. These Regulations include requirements relating to the internal control system that these entities must have in place.[3]

On 19 December 2024, ESMA published a Consultation Paper (CP) for Guidelines on the Internal Controls for BMAs, CRAs and Market Transparency Infrastructures (MTI).[4] The CP proposed to build on and replace the Guidelines on Internal Control for CRAs[5] and set out ESMA's views for all entities it directly supervises (except third-country central counterparties and consolidated tape providers). It also revised ESMA's expectations considering the growing impact of technology on supervised entities' operations. This includes managing technology risk from external and internal sources, and the integration of new technologies into supervised entities' internal controls.

This final report summarises the feedback received to the public Consultation and includes the finalised Guidelines on Internal Controls. The finalised Guidelines will ensure that ESMA's expectations are shared with all supervised entities, as well as potential future applicants, in a comprehensive and cohesive way. These Guidelines will not only help ensure a level playing field but will also facilitate the adoption of consistent good practices across supervised entities, helping to strengthen the robustness of supervised entities' control system.

ESMA will use the principle of proportionality in implementing these Guidelines. This means that while all supervised entities are expected to demonstrate the characteristics of an effective internal control system, ESMA's expectations on implementation will be proportionate to the supervised entity's nature, scale and complexity.

Contents

This final report is split into three main sections. **Section 2** explains ESMA's overarching rationale for replacing the Guidelines, providing an overview of the main areas of revision and the reasons for any change in approach. **Section 3** summarises the feedback received to the Consultation and explains how ESMA has taken this into account in the final Guidelines. **Annex I** includes the updated cost and benefit analysis, and **Annex II** contains the final Guidelines on Internal Controls.

Next Steps

The Guidelines in Annex II will be published on ESMA's website. They will become effective on 1 October 2026. The entry into force of these Guidelines will repeal and replace the Guidelines on Internal Control for CRAs.

2 Overview of the Guidelines on internal controls

1. The Benchmark Regulation (BMR), the Credit Rating Agencies Regulation (CRAR), the European Market Infrastructure Regulation (EMIR), the Market in Financial Instruments Regulation (MiFIR), the Securitisation Regulation (SecR) and the Securities Financing Transactions Regulation (SFTR) (hereinafter referred to as the Regulations) establish the minimum requirements for internal control systems applicable to the BMAs, CRAs, DRSPs, SRs and TRs directly supervised by ESMA (hereinafter referred to as supervised entities). These regulations outline aspects such as governance, risk management, compliance, and operational controls, which the supervised entities must adhere to.
2. The purpose of these Guidelines is to ensure that ESMA's expectations are shared with all supervised entities, as well as potential future applicants, in a comprehensive and cohesive way. These Guidelines will not only help ensure a level playing field but will also facilitate the adoption of consistent good practices across supervised entities, helping to strengthen the robustness of their internal control system. The Guidelines aim to ensure that ESMA takes a consistent approach to its supervisory assessments of internal control practices across the entities it supervises.
3. ESMA developed the Guidelines taking into account the relevant Regulations' provisions relevant to internal controls, as further specified in the respective RTS. ESMA also considered its existing guidelines[6], supervisory experience and enforcement actions.[7]

[1] ESMA supervises administrators of EU critical benchmarks and recognised third-country administrators.
[2] MiFIR provides the following categories of data reporting services providers, namely approved reporting mechanisms (ARMs), approved publication arrangements (APAs), and consolidated tape providers (CTPs). ESMA does not supervise those APAs and ARMs that, by way of derogation from MiFIR on account of their limited relevance for the European Union (EU) market, are subject to authorisation and supervision by a competent authority of a Member State. MiFIR anticipates that ESMA will be the sole supervisor for CTPs, following the selection process for bond, equity and derivatives CTP.
[3] An internal control system includes both the internal control framework and internal control functions.
[4] Market Transparency Infrastructures (MTI) include Securitisation Repositories (SRs), Trade Repositories (TRs) and Data Reporting Services Providers (DRSPs).
[5] Guidelines on Internal Control for CRAs, 30 September 2020 | ESMA33-9-371
[6] For example, ESMA's Guidelines on Internal Controls for CRAs (which these guidelines will replace) and Guidelines on non-significant benchmarks under the Benchmarks Regulation (which must be read in conjunction with these guidelines),
[7] See Paragraphs 150 to 169 of the Scope enforcement decision of 22 March 2024; Paragraphs 101 to 166 of the S&P enforcement decision of 22 March 2023; Paragraphs 380 to 413 of the Moody's enforcement decision of 23 March 2021; Paragraphs 355 to 400 of the Fitch enforcement decision of 28 March 2019; Paragraphs 7 to 23 of the S&P enforcement decision of 20 May 2014; and pages 3 to 4 of the Fitch public notice of 21 July 2016. Please see Sanctions and Enforcement (europa.eu).

Finally, ESMA accounted for existing industry practices in supervised entities, EU approaches and guidance on internal control[8] as well as internationally recognised internal control frameworks.[9] This has enabled ESMA to define a set of practices that draw on existing good practices while taking into account the specificities of the Regulations and the business practices of supervised entities.

4. ESMA has also taken the opportunity to expand and clarify some of its expectations related to technology given the risks and opportunities arising from its growing use. For example, where a company uses artificial intelligence (AI), its internal control framework should be mature enough to assess and manage the risks of AI and to be integral to the AI lifecycle within a company. This includes the establishment of a supervised entity's AI strategy, ethics and principles, an appropriate governance and risk management framework, sufficient disclosures and system documentation, and controls around the design criteria, modelling, training, evaluation and deployment of AI systems.

5. For supervised entities subject to the Digital Operational Resilience Act (DORA), these Guidelines should be read in conjunction with its requirements. DORA lays down requirements on Information and Communication Technology (ICT) risk management, ICT third-party risk management, digital operational resilience testing, and the reporting of ICT-related incidents. As part of this, supervised entities will be required to have an ICT risk management framework as part of their overall risk management framework and to allocate the responsibility for managing and overseeing ICT risk to a control function with an appropriate level of independence. Supervised entities not subject to DORA should meet the expectations set out in the sections on 'Information and Communication Technology (ICT) General Controls' and 'Information Security Management Function' of these Guidelines.

6. The Guidelines are structured in two parts, each dealing with one pilar of the internal control system. The first part focuses on a supervised entity's overall framework for internal controls (IC Framework) while the second part focuses on the roles and responsibilities of different internal control functions within this framework (IC Functions). Under each part, the IC Framework and the IC Functions are then further split into different components.

7. 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.

8. Under the IC Framework, ESMA sets out its expectations as to what steps supervised entities should take to evidence the presence of each component in its internal control

[8] 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.

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

system. For example, with respect to the '*control environment*', the guidance outlines the actions the supervised entity's Management Body should take to establish a strong control environment and set the right tone at the top.

9. The guidance on IC Functions is split into components which match specific IC Functions, namely: (i) Compliance; (ii) risk management; (iii) information security management (only for supervised entities not in remit of DORA); (iv) internal audit; (v) Review Function (for CRAs); (vi) Oversight Function (for BMAs). 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.

10. ESMA will apply proportionality in implementing these Guidelines. This means that while all supervised entities are expected to demonstrate the characteristics of an effective internal control framework, ESMA's expectations on implementation will be proportionate to the supervised entity's nature, scale and complexity.

3 Feedback statement

11. This section provides a summary of the responses to the Consultation Paper (CP) on the Guidelines on Internal Controls for BMAs, CRAs and MTIs.

12. In total, 21 responses were received to the Consultation with eight of these provided on a confidential basis. Responses were received largely from market participants directly (six BMAs, seven CRAs, five MTIs) or via trade associations representing them. Respondents were mainly entities already supervised by ESMA but some entities that may become supervised by ESMA in the future also responded. Non-confidential responses are available on ESMA's website.

13. In providing this summary, ESMA explains the changes that it made in response to the comments provided during the consultation process. Although ESMA reviewed all responses to the Consultation, this feedback statement may not refer to all the comments made by respondents. In particular, this feedback statement does not cover some respondents' suggestions to provide more details on certain expectations when ESMA was of the view that the proposed Guidelines already provided sufficient details. In these cases, ESMA did not amend the proposed Guidelines to leave flexibility to the supervised entities on how to achieve the expected outcome. This ensures the Guidelines do not become overly prescriptive.

14. The feedback statement starts with a section addressing the general comments relevant to the entire Guidelines. It then follows the order of the sections as they were presented in the CP and as summarised below.

    - General - Internal Control Framework
        - Component – Control Environment

- Component – Risk Management
- Component – Control Activities
- Component – Information and Communication
- Component – Monitoring Activities

- General – Internal Control Functions
  - Proportionality – Internal Control Functions
  - Component - Compliance
  - Component - Risk Management
  - Component - Information Security Management Function
  - Component - Internal Audit
  - Component - Review (for CRAs)
  - Component - Oversight (for BMAs)

3.1 General remarks on the proposed Guidelines

3.1.1 Scope of the Guidelines

15. Some respondents commented on the types of supervised entities in scope of the draft Guidelines. One respondent mentioned that it was unclear how the draft Guidelines would apply to the EU legal representatives of third country recognised BMAs. Another respondent noted that ESMA did not comment on the application of the draft Guidelines to entities not yet supervised by ESMA but for which ESMA has been granted a supervisory mandate, such as EU Green Bond External Reviewers or ESG Rating Providers. This respondent suggested that, before subjecting new industries or actors to the Guidelines, ESMA should conduct a consultation so that the specifics of these activities are appropriately considered. Finally, a third respondent argued that the existing Guidelines for CRAs were not necessarily transferable or applicable to other supervised entities.

ESMA response:

16. ESMA would like to emphasise that these guidelines are applicable to all benchmark administrators which are authorised, registered or recognised with ESMA in accordance with BMR. As regards the EU legal representative, these guidelines are mainly applicable to the extent of legal representative's oversight function exercised together with the BMA and its duties under BMR . ESMA confirms that EU Green Bond External Reviewers or ESG Rating Providers are not in scope of the Guidelines. However, ESMA considers

that these Guidelines provide a good indication of ESMA's expectations to entities that it will supervise under future mandates. ESMA will consult again if and when it intends to expand the scope of these Guidelines to firms supervised under future mandates. In response to the comment about the transferability of the Guidelines applicable to CRAs to other supervised entities, ESMA stresses that, whilst the proposed Guidelines build on the currently applicable to CRAs, several adaptations were made so that they are relevant to all supervised entities in scope.

3.1.2 Costs and burden for supervised entities

17. Some respondents challenged the introduction of new guidelines on the basis that it could create undue costs and administrative burden which are not specifically required by the underlying EU regulatory frameworks. More specifically, some respondents argued that applying the proposed Guidelines to some s was not in line with the recent BMR review "*to reduce the administrative and regulatory burden imposed […] on EU benchmark administrators*". Some also argued that the proposed Guidelines are created during a period of significant regulatory and supervisory change for the BMA in scope. They suggested that ESMA delays the entry into force of the Guidelines.

ESMA response:

18. ESMA acknowledges that these Guidelines are issued during a period of significant regulatory and supervisory change for some of the supervised entities. However, ESMA notes that the BMR review did not amend any of the existing requirements regarding Internal Controls. ESMA also notes that these Guidelines have been designed to provide greater clarity on underlying EU regulatory frameworks and as such provide supervised firms with legal certainty by specifying how firms can satisfy the expectations set out in Level 1 texts. On that basis, ESMA does not believe these Guidelines introduce undue costs and administrative burden to the supervised entities in scope. In addition, ESMA would like to stress that the Guidelines also embed proportionality to ensure they work for smaller and less complex firms. By calibrating its supervisory expectations according to the nature, scale and complexity of a supervised entity, ESMA is of the view that the proposed Guidelines contribute to the overall policy objective of burden reduction. On that basis, ESMA confirms that the Guidelines will start to apply on 1 July 2026.

3.1.3 References to Management Body and Executive Senior Management

19. Several respondents commented on the use of the designations '*Management Body*' and '*Executive Senior Management*'. One respondent noted that '*Management Body*' is not a concept within the CRAR so the use of this term in the Guidelines should not inadvertently restrict the governance structures CRAs operate. The respondent suggested that the definition of Management Body should be wide enough to cater for

situations "*where the management function of the Board of Directors is delegated to a management committee*" (i.e. not the Board itself). Another respondent stressed the importance of ensuring consistency of terminology throughout ESMA's regulatory requirements and guidelines, notably with the Supervisory expectations for the Management Body.[10] The respondent saw a potential contradiction between both documents as they interpreted the Consultation Paper in a way which implies that Executive Senior Management is distinct from the Management Body.

ESMA response:

20. ESMA believes that, in line with the existing Guidelines for CRAs, it is important to continue to distinguish between the respective roles of the board and management. In particular, the role of the board is to monitor and oversee the elements of the IC Framework, while the role of management is to develop and implement the framework.

21. Considering the expanded group of firms the new Guidelines apply to, ESMA decided to replace the concepts of board and management by concepts that are defined under the relevant regulations or that are commonly accepted across industries. This is why ESMA uses the term '*Management Body*' instead of '*the board*'. Similarly, ESMA uses the term '*Executive Senior Management*' instead of '*management*'. ESMA chose not to use the term 'senior management' as this term is defined under Article 3(1)(n) of CRAR[11] and includes both management and members of 'the board'. ESMA uses the term '*Executive Senior Management*' to refer to the most senior persons directing the supervised entity on a day-to-day basis. This is typically the Chief Executive Officer (CEO) or equivalent and his/her direct reports. To clarify this, ESMA added a definition of '*Executive Senior Management*' for the purpose of these Guidelines. ESMA also aligned the definition of Management Body between the Guidelines and the Supervisory expectations for the Management Body.

22. ESMA acknowledges that, some members of the Executive Senior Management will typically be part of the Management Body. In particular, the Supervisory expectations for the Management Body envisages the scenario whereby the '*most senior executive managers*' are part of the Management Body together with the non-executive directors.

23. Because of this potential overlap, it is important to specify the expectation set out in Component 1.1, in particular that "*The Executive Senior Management is responsible for the development and performance of internal control and assessing the adequacy and effectiveness of the control environment*" and that "*The Management Body exercises oversight of Executive Senior Management in these areas*". When some members of the Executive Senior Management are part of the Management Body, it is the Management

[10] ESMA84-2131909211-9912 - Supervisory expectations for the management body
[11] 'Senior Management' means the person or persons who effectively direct the business of the CRA and the member or members of its administrative or supervisory board

Body in its supervisory function that is expected to oversee the Executive Senior Management.

3.1.4 Interactions between the Guidelines and DORA

24. One respondent noted that it understood mentions to 'new technologies' (1.2 Risk Management), 'information security' (1.4 Information and Communication), and 'relevant Regulations' (1.3 Control Activities) as referring to the implementation of DORA and that, as a result, the proposed Guidelines did not contain expectations stricter than those established in DORA.

ESMA response:

25. ESMA paid special attention to ensuring that the expectations set out in the Guidelines do not overlap with those in DORA. For instance, it noted that *"For supervised entities subject to the Digital Operational Resilience Act (DORA), these guidelines should be read in conjunction with its requirements."* However, the references to 'new technologies' (1.2 Risk Management), 'information security' (1.4 Information and Communication), and 'relevant Regulations' (1.3 Control Activities) go beyond the implementation of DORA. They have been added to reflect the growing impact of technology on supervised entities' operations, including in terms of managing technology risk from external and internal sources, and the integration of new technologies into supervised entities' internal controls.

3.2 Internal Control Framework – Component Parts and Characteristics

3.2.1 General - Internal Control Framework

26. One respondent suggested specifying that the supervised entity's Executive Senior Management's responsibilities relate to the internal control policies and procedures *"that support the components of the IC framework*". The respondent also suggested that the supervised entity's Executive Senior Management's responsibilities should be limited to *"policies and procedures"* and not extend to "*working practices*" as they think this would go beyond the scope of the internal control framework as set out in Paragraph 20 of ESMA's Consultation Paper.

27. One respondent argued that making the Management Body accountable for the internal control framework contradicts Article 5(3)(c) of the BMR which allocates such responsibility to the BMA's Oversight Function.

28. One respondent pointed out that this section may be interpreted in a way that the Management Body is required not only to approve internal policies and procedures but

also to approve and monitor the review cycle. They believe this may not be practical in many entities, where this authority has been delegated to the Internal Control function.

ESMA response:

29. ESMA amended the Guidelines to clarify that the supervised entity's Executive Senior Management's responsibilities relate to the internal control policies and procedures *"that support the components of the IC framework*". ESMA also aligned the scope of their responsibilities with the scope of the internal control framework as set out in Paragraph 20 in ESMA's Consultation Paper (i.e. "*policies, procedures and practices*").

30. ESMA notes that the BMR mandates that BMAs establish and maintain an effective Oversight Function to ensure the integrity and reliability of their benchmarks. While there are indeed, among others, some Internal Control Framework oversight elements attributed to the Oversight Function, ESMA is of the view that this does not conflict with the Management Body's accountability for the Internal Control framework.

31. ESMA's view is that the Management Body is accountable for the approval of internal policies and procedures and the monitoring of the review cycle. The Management Body can delegate the responsibility for this, including to Internal Control Functions. However, it remains accountable. On that basis, ESMA did not modify this section.

3.2.2 Component 1.1 – Control Environment

32. In relation to Characteristic 1.1.2, one respondent noted that there is no need for supervised entities to repeat in all policies and procedures that *"staff is expected to conduct themselves with honesty and integrity, perform their duties with due skill, care and diligence".*

33. In relation to Characteristic 1.1.3, one respondent suggested that it would be more accurate to reflect that internal control functions are responsible for updating and reviewing the policies and procedures, whilst the Executive Senior Management should approve and be accountable for the reviews.

ESMA response:

34. In relation to Characteristic 1.1.2, ESMA would like to clarify that supervised entities are not expected to repeat that "*staff is expected to conduct themselves with honesty and integrity, perform their duties with due skill, care and diligence*" in all policies and procedures. ESMA expects that these principles are covered in relevant policies and procedures but not necessarily in all. ESMA is of the view that the paragraph is already sufficiently clear. As such, it did not make any change to this characteristic. Beyond the inclusion in the relevant policies and procedures, supervised entities are expected to put these principles to life so that they become part of the firm's day-to-day operations.

35. In relation to the role of the Executive Senior Management set out in Characteristic 1.1.3, ESMA would like to stress that updating and reviewing the policies and procedures is not the sole responsibility of the internal control functions. Business functions, and more generally the first line of defence, may also be responsible for updating and reviewing certain policies and procedures. On that basis, ESMA did not make changes to Characteristic 1.1.3.

3.2.3 Component 1.2 – Risk Management

36. One respondent mentioned that the proposed Guidelines reflect a shift in supervisory approach to risk management and the types of risks that are in scope. The respondent noted that the proposed Guidelines appeared to capture all risks to a supervised entity's "*main objectives*" regardless of whether the objectives have any bearing on its ability to meet its obligations under the regulation. The respondent suggested keeping wording similar to that used in the existing Guidelines for CRAs and limit the scope to *"all risks that could materially impact the [supervised entity's] ability to meet its obligations under the [CRAR] or threaten its continued operation*".

37. In relation to Characteristic 1.2.2, one respondent asked ESMA to clarify their understanding of "*setting the risk appetite and identifying risk tolerance levels as part of the risk assessment process*".

38. In relation to Characteristic 1.2.3, one respondent suggested indicating that the supervised entity's risk assessment methodology should be informed by findings from the IC Functions of the supervised entity.

39. One respondent argued that Characteristics 1.2.3 and 1.2.4 place an excessive administrative burden on smaller BMAs while not accounting for lower complexity of operations and would be disproportionately resource-intensive relative to the actual risks being managed. The same respondent suggested a tiered approach to risk assessment requirements, where smaller firms with less complex operations could implement more streamlined risk management processes focused on material risks specific to their benchmark provision activities.

ESMA response:

40. ESMA agrees with the request to clarify and refine the types of risks that are in scope, and has therefore amended the relevant provision to clarify that supervised entities are expected to have in place a dynamic and continuously evolving process for identifying, assessing and measuring *"all risks that could impact a supervised entity's ability to perform its obligations under the Regulation, or its continued operation*". While ESMA believes that all risks should be identified, assessed and measured, and therefore these activities should not be limited to the risks that could "*materially*" impact the above objectives, ESMA agrees that only those risks with a material impact should be

monitored, mitigated and reported on. Therefore, ESMA introduced a materiality threshold for the types of risks that should be subject to these risk management activities (i.e. monitoring, mitigation, reporting). In making these amendments, ESMA ensured the final wording is aligned with that of Component 2.2 on the Risk Management Function.

41. In relation to Characteristic 1.2.2, ESMA amended the sentence to clarify that the expectation to "*set risk appetite and identify risk tolerance*" is independent from that of having a risk assessment process.

42. In relation to Characteristic 1.2.3, ESMA decided not to proceed with the suggested amendment. ESMA agrees with the respondent that the supervised entity's risk assessment methodology should be informed by findings from the IC Functions. However, the purpose of Characteristic 1.2.3 is rather to specify that all functions should be subject to the risk assessment, not only business lines. This is because risks can also originate from IC functions.

43. On the comment regarding administrative burden and a tiered approach for smaller BMAs, ESMA believes that a comprehensive assessment of risks across all business lines is a pre-requisite to any risk-based approach, including to risk management activities and the allocation of resources to areas where the risks are higher. On that basis, ESMA is of the view that supervised entities of all sizes and complexity levels should assess their risks across all their activities. This does not prevent firms from performing a more refined risk assessment in areas they consider more critical or complex. On that basis, ESMA does not deem it necessary to introduce a tiered approach to risk assessment.

3.2.4 Component 1.3 – Control Activities

44. In relation to Characteristic 1.3.1 on the segregation of duties, respondents pointed out that the Guidelines indicate a shift in the expectations for certain tasks within the scope of the CRA Regulation and that, more generally, they are excessively restrictive for staff involved in certain tasks whilst having a role in the approval, validation or review of those tasks unless it "*cannot be avoided*". These respondents suggested keeping the wording used in the existing Guidelines for CRAs. One respondent also noted that ESMA should provide alternative control measures for small firms with limited personnel that may struggle with strict segregation. Some respondents argued that the examples provided in the footnotes illustrating this characteristic were too prescriptive, while some of the activities described were too vague.

45. In relation to Characteristic 1.3.3, one respondent stated that the expectations about the documentation of controls and testing were unnecessarily prescriptive.

46. In relation to Characteristic 1.3.5, one respondent suggested focusing on '*key*' rather than '*all*' business activities.

47. In relation to Characteristics 1.3.6, two respondents suggested deleting the wording '*inter alia*' from footnote 36 to avoid broadening the section's scope of application.

ESMA response:

48. On the comments regarding the segregation of duties set out in Characteristic 1.3.1, ESMA confirms that it did not intend to amend the existing guidance. The final Guidelines have been amended to revert to the wording currently in place. ESMA has also provided an example of how smaller firms with limited personnel may ensure segregation of duties and refers to the section on proportionality where ESMA clarifies that its expectations on the level of segregation for internal control functions may be calibrated to each firm's nature, scale and complexity. On that basis, ESMA does not deem it necessary to specify additional alternatives to the segregation of duties. In relation to the footnotes illustrating Characteristics 1.3.1, ESMA modified the wording to remove the content that was considered too vague and, instead, focused on illustrating how the segregation of duties may be suitable for IT-related operations. ESMA also modified the examples specific to CRAs to align with the expectations in the Guidelines currently applicable to them.

49. Regarding the control documentation set out in Characteristic 1.3.3, ESMA followed the respondent's suggestion and made the characteristics more principle-based by removing the details of the control documentation. ESMA leaves it to each firm to decide on how to document their controls. Depending on their nature, scale and complexity, firms may consider documenting the following points: (i) a description of the control; (ii) the associated material risk(s); (iii) the role(s) or functions(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.

50. ESMA also agrees with a comment that the guidance set out in Section 1.3.3 may be addressed across multiple documents rather than consolidated into a single document.

51. Regarding Characteristic 1.3.5, while the suggestion to add '*mechanisms'* seems sensible as, indeed, '*processes'* are not the only methods that can be used to ensure appropriate authorisation or approval authority, ESMA considers no further amendment is necessary since ESMA's aim is that such '*processes'* and '*mechanisms'* apply to all business activities, not only key activities. Footnote 35 provides examples relevant to CRAs. It is not an exhaustive list of key business activities.

52. Regarding Characteristic 1.3.6, ESMA agrees with the suggested deletion and has reflected that in the final Guidelines.

3.2.5 Component 1.4 – Information and Communication

53. In relation to Characteristic 1.4.2, one respondent suggested to reinstate the materiality provision present in the existing Guidelines for CRAs for the escalation of internal control issues to the Management Body.

54. In relation to Characteristic 1.4.3, one respondent mentioned that the Management Body should not be involved in day-to-day operations, such as communications with staff. The respondent suggested an amendment so that only Executive Senior Management and the control functions should establish downward communication channels with staff.

ESMA response:

55. As regards Characteristic 1.4.2, ESMA followed the respondent's suggestion and amended the Guidelines to reinstate the materiality provision on the internal control issues that should be escalated to the Management Body and Executive Senior Management. As to the suggestion to clarify when a 'disagreement' requires escalation, ESMA agrees and added a materiality threshold.

56. As regards Characteristic 1.4.3, ESMA notes that communication from the Management Body to staff may be appropriate for certain objectives, notably to provide the right tone from the top. On that basis, ESMA did not amend this characteristic.

3.2.6 Component 1.5 – Monitoring Activities

57. In relation to Characteristic 1.5.6, one respondent noted that the provision related to outsourcing is too vague. They also noted that the requirement to allocate a member of staff with the specific task of monitoring that service should depend on the nature of the firm. Similar comments suggested that the existing Guidelines for CRAs should be kept to ensure that the outsourcing monitoring requirement is subject to a materiality threshold.

ESMA response:

58. ESMA expects supervised entities to implement monitoring controls for all outsourcing arrangements (i.e. not only important operational functions), including intragroup outsourcing. At the same time, ESMA recognises that the intensity of those monitoring controls should be commensurate to the risk and criticality of the outsourced activities. Supervised entities should consider ESMA's Principles for Third Party Risk Supervision[12] in the implementation of their outsourcing arrangements and controls.

[12] ESMA42-1710566791-6103 Principles on third-party risks supervision

3.3 Internal Control Functions - Component Parts and Characteristics

3.3.1 General – Internal Control Functions

59. In relation to Paragraph 18 of the proposed Guidelines, several respondents highlighted that the expectation that staff members in charge of IC functions "*should be directly accountable to the Management Body and their performance should be reviewed by the Management Body*" was somewhat vague, not proportionate and not in line with existing practices. One respondent suggested a clarification that this requirement pertains to the function, rather than any individual staff members.

60. In relation to Paragraph 18 and Paragraph 19, several respondents welcomed ESMA's acknowledgement that some supervised entities may "*outsource the operational tasks of an IC function to group level*". They stressed the importance of such intragroup outsourcing arrangement to build a centralised framework, achieve synergies and efficiencies.

61. Some respondents noted that ESMA's expectation that the supervised entity retains full responsibility applies to the outsourcing of "*operational tasks of an IC function*" whereas the corresponding expectations in the current Guidelines for CRAs only apply to the outsourcing of "*important operational tasks of an IC function".* They suggested re-introducing the materiality provision of "*important*" operational tasks.

ESMA response:

62. ESMA acknowledges that the expectation that staff members in charge of IC functions have "*their performance [….] reviewed by the Management Body"* did not directly serve the objective of this section which was to clarify the meaning of "*appropriate seniority*" and "*necessary authority*" for the staff in charge of IC functions. On that basis, ESMA removed this part of the paragraph. Similarly, ESMA modified the paragraph to clarify that it expects staff members in charge of IC functions to "*have direct access and report to Management Body on a regular basis*" rather than to "*be directly accountable to the Management Body*". ESMA confirms that these expectations, as amended, apply to the individual staff members and not to the function. For the avoidance of doubt, ESMA confirms that the IC Functions should also report to the Management Body, as stated in various sections of the document (e.g. Characteristics 2.1.1, 2.2.4, 2.3.4, 2.4.5, 2.5.1, 2.6.4).

63. Concerning the materiality criteria of "*important*" operational tasks, ESMA is of the view that the change compared to the current Guidelines for CRAs is justified. This is because the principle that supervised entities retain responsibility for outsourced activities is relevant to all types of outsourced activities. This principle is also included in ESMA's

Principles for Third Party Risk Supervision.[13] On that basis, ESMA does not deem it appropriate to re-introduce the materiality provision.

3.3.2 Proportionality – Internal Control Functions

64. Overall, a majority of respondents welcomed the clarification that ESMA provided on how it takes into account proportionality in its supervision of IC Functions. Several respondents asked for further clarification on its practical application

65. One respondent suggested that the assessment and calibration of relevant factors should not be determined by ESMA but through a self-assessment conducted by each entity.

ESMA response:

66. ESMA acknowledges the concerns expressed by respondents about proportionality and the request to add more details on how it applies proportionality into the Guidelines. ESMA will use its judgment based on its supervisory dialogue with supervised entities to understand each entity's situation and define and explain how it calibrates its expectations to their nature, scale, complexity and risks. As a result, ESMA did not make changes to this section.

67. ESMA agrees that firms should assess and calibrate their internal control framework and functions to their own risks. In line with Component 1.1, ESMA expects firms' Executive Senior Management to be responsible for assessing the adequacy and effectiveness of the firm's control environment. However, ESMA does not believe that this contradicts the idea that ESMA has its own expectations on the specific maturity that each firm needs to achieve.

3.3.3 Component 2.1 - Compliance

68. In relation to Characteristic 2.1.1, one respondent suggested specifying that the INEDs should receive the same information as the rest of the Board of Directors.

69. In relation to Characteristic 2.1.3, two respondents questioned whether expecting the Compliance function to exert oversight over IT processes was proportionate. This is because smaller or less complex firms tend to have small Compliance Functions and rely on other second line functions or the third line function to oversee IT processes. This comment was echoed by another respondent who argued that the Compliance Function is not the appropriate function to conduct monitoring activities on 'IT processes and systems'. This respondent suggested that these activities sit more naturally with the Risk Management Function, or, alternatively, with the ICT Risk Management Function as

[13] ESMA42-1710566791-6103 Principles on third-party risks supervision

established in DORA. Two other respondents argued that it is not appropriate to expect the Compliance Officer to have a full technical knowledge to cover processes and systems. The respondent would welcome a clarification in the final Guidelines that the scope of the Compliance programme may be based on risk-based assessments.

70. One respondent mentioned that many non-EU BMAs operate as part of global financial groups that have developed centralised governance, compliance, and risk management frameworks designed to ensure effective and consistent controls across jurisdictions. The respondent argued that the Consultation Paper remains unclear whether ESMA will allow firms to rely on these group-wide processes in practice.

ESMA response:

71. In relation to Characteristic 2.1.1, ESMA agrees with the comment that INEDs should receive at least the same information as other members of the Management Body. However, the INEDs may also require additional reports from the Compliance Function to fulfil their oversight responsibilities. ESMA amended Characteristic 2.1.1 to clarify that such additional reports may be provided directly to the INEDs when relevant.

72. In relation to Characteristic 2.1.3, ESMA would like to clarify that the second sentence does not aim to expand the scope of the Compliance Function but rather to specify that the existing scope includes IT processes and systems so long as they can affect the supervised entity's compliance. ESMA does not expect Compliance to be responsible for IT supervision. Instead, ESMA expects Compliance's activities (e.g. controls, testing, training) to also cover IT processes and systems when the latter could affect the supervised entity's compliance with the relevant Regulation. The Compliance Function may cooperate with other functions (including external ones) to carry out these tasks.

73. On the comment related to group functions, ESMA would like to highlight that the mentioned activities may be carried out at group level provided that the group structure does not impede the ability of a supervised entity to provide oversight and effectively manage its risks or ESMA's ability to effectively supervise the entity. In all cases Characteristic 1.1.4 applies. Moreover, ESMA would like to point out that all outsourcing (including intra-group) should be subject to monitoring and the intensity should be commensurate to the risk and criticality of the outsourced activities. ESMA invites supervised firms to also consider ESMA's Principles for Third Party Risk Supervision[14].

3.3.4 Component 2.2 - Risk Management Function

74. Following the comments made by some respondents on Component 1.2, ESMA removed the list of activities expected to be performed by the Risk Management Function

[14] ESMA42-1710566791-6103 Principles on third-party risks supervision

as this duplicated the expectation about the risk management activities set out in Component 1.2.

75. ESMA amended Characteristic 2.2.2 to specify to which activities the materiality provision applies. On the one hand, ESMA expects supervised entities to identify, assess and measure all risks that could materially impact their ability to perform their obligations under the Regulations, or their continued operation. This is because, until these activities have been performed, one cannot tell whether a risk may have material impact to the objectives or not. On the other hand, ESMA expects firms to monitor, manage, mitigate and properly report the material risks to these objectives.

3.3.5 Component 2.3 - Information Security Management Function (only for supervised entities not subject to DORA)

76. One respondent noted that it may not be proportionate to require all supervised entities to have a dedicated information security management function since information security can be an activity outsourced to group functions.

ESMA response:

77. ESMA would like to highlight that information security activities may be carried out at group level provided that the group structure does not impede the ability of the supervised entity to provide oversight and effectively manage its risks or ESMA's ability to effectively supervise the entity.

3.3.6 Component 2.4 - Internal Audit

78. In relation to Characteristic 2.4.2, one respondent expressed its concern that the reference to "*leading practices*" is ambiguous and could create uncertainty.

79. In relation to Characteristic 2.4.4, one respondent commented that the supervision over audit programs (i.e. approval, settlement of program, implementation) should be performed by the Head of Audit not by the Management Body.

80. Another respondent asked clarification on whether the proposed Guidelines precluded a model whereby the different internal control functions could rely upon each other's findings.

ESMA response:

81. In relation to Characteristic 2.4.2, ESMA removed the phrase "*leading practices*" to avoid ambiguity.

82. In response to the comment on Characteristic 2.4.4, ESMA amended the wording to clarify that it expects the Management Body to oversee the annual audit plan so that it can steer the use of resources to address the most pressing risks and receive assurance

where deemed necessary. ESMA removed the term "*detailed audit programme*" as the meaning was unclear.

83. As a third line of defence, the Internal Audit Function may evaluate the first line (i.e. business lines) and second line (i.e. other internal control functions). As a result, internal audit must be in a position to perform its functions independently from other internal control functions. This does not preclude an 'aligned assurance' model in which the lines of defence can rely upon each other's findings, subject to satisfying themselves of the robustness of the approach followed.

3.3.7 Component 2.5 - Review (for CRAs)

84. In relation to Paragraph 33, one respondent suggested specifying that a "*CRA's Review Function is also responsible for the validation and review of new methodologies, and any changes to existing methodologies*". The respondent also noted that this is how the expectation is set out in the current Guidelines applicable to CRAs.

85. In relation to Characteristic 2.5.4, one respondent noted that ESMA setting expectations on "*voting rights in a committee*" is prescriptive and inappropriate. Instead, the respondent believed that ESMA should leave CRAs free to decide how to produce and validate their methodologies according to the CRA Regulation.

ESMA response:

86. ESMA amended Paragraph 33 to specify that a "*CRA's Review Function is also responsible for the validation and review of new methodologies, and any changes to existing methodologies*", in line with the expectation set out in the current Guidelines applicable to CRAs.

87. ESMA notes that Characteristic 2.5.4 does not mandate the use of committees for approving methodologies. Based on supervisory experience, ESMA is aware that several CRAs use committees to this end. ESMA used Characteristic 2.5.4 to clarify its expectations when such a committee is being used. As a result, ESMA did not modify Characteristic 2.5.4.

3.3.8 Component 2.6 - Oversight (for BMAs)

88. Several respondents expressed concerns that the requirement for the Oversight Function to be independent from any function of the BMA would be overly burdensome and disproportionate and may conflict with the requirements of the Benchmark Regulation. One of these respondents mentioned that the Benchmark Regulation already establishes requirements for benchmark oversight and that the Guidelines' characteristics may generate increased administrative costs.

ESMA response:

89. While ESMA acknowledges that the Oversight Function's composition and structure may differ depending on the size and complexity of the BMA, ESMA's expectation for an Oversight Function and its members is that potential conflicts of interest are mitigated. ESMA amended the wording of Characteristic 2.6.1 to clarify that it expects BMAs to maintain the independence of the Oversight Function and its members irrespective of the size of and nature of the firm. The five characteristics in the Guidelines are set out to emphasise the above concept which is derives from the Benchmark Regulation and is applicable to all BMAs in scope of these Guidelines.

4 Annexes

Annex I - Cost-benefit analysis

Introduction

1. The need for supervised entities to have a robust and appropriately resourced system of internal controls is provided for in Articles 4-10 of BMR, Article 6 and Annex I Section A of CRAR, Articles 27f, 27g and 27i of MiFIR, Article 5(2) of SFTR and Articles 78 and 79 of EMIR (also applicable to SRs via Article 10 of SecR). The motivation for providing such guidance arose as a result of the identification of deficiencies in supervised entities' practices during ESMA's ongoing supervision.

    - The purpose of these Guidelines is to ensure that ESMA's expectations are shared with all registered entities and future applicants to ensure a level playing field and the adoption of consistent good practices. The Guidelines will achieve this by making clear what components and characteristics ESMA considers should be evidenced within a supervised entity's internal control system. Furthermore, the Guidelines clarify how ESMA's expectations are proportionate to the nature, scale and complexity of a supervised entity.
    - Once implemented the Guidelines will be integrated into ESMA's supervisory assessment practices and guide how ESMA interacts with supervised entities in relation to their internal controls systems.

Impact of ESMA Guidelines

2. The approach of the Guidelines is to provide a framework of practices against which supervised entities can compare and judge their own internal control systems and mechanisms. When firms identify that their internal control system falls short of the expectations set out in the Guidelines, they are encouraged to remediate such gaps.

3. The Guidelines have also been drafted in such a way that they do not recommend specific organisational structures. Rather they recommend principles that a supervised entity's internal control system should adhere to in order to demonstrate it meets the objectives of the relevant Regulations. As such, it is not expected that the Guidelines will require any supervised entity to fundamentally re-structure its internal organisation.

4. However, given that the guidance has drawn upon a wide range of standards and best practices, it is expected that even for supervised entities who are currently implementing well defined and sufficiently resourced internal control systems some revisions to current

practices may be necessary. These revisions could entail changes to existing work practices or delegation of internal reporting lines and responsibilities.

Benefits

5. The benefits of these Guidelines to ESMA and supervised entities are numerous. For ESMA, the Guidelines will help ensure consistency in how ESMA supervisors assess each supervised entity's internal control systems and mechanisms. For supervised entities, it will act as a resource against which they can assess the effectiveness and appropriateness of their existing internal control systems and mechanisms and provide clarity on ESMA's expectations as a supervisor. For any new entrants into the BMA, CRA, DRSP, SR and TR market, the Guidelines will likewise provide them with clarity on the practical application of the internal control requirements in the relevant Regulations. For users of the supervisory entities' services, these Guidelines will contribute to assuring more robust and effective services from the supervised entities. More mature internal control systems will result in greater operational efficiency as well as heightened capacity for error detection and prevention.

Costs

6. The expected costs arising from these Guidelines are potentially three-fold. First, supervised entities should assess the provisions against their existing internal control systems and mechanisms. Second, following this assessment, supervised entities may need to review their internal policies and procedures or internal control processes. Third, following any changes, supervised entities may need to inform and update all relevant staff as to the changes in the internal processes and provide training where necessary.

7. For CRAs, these costs are expected to be minimal given that they are already subject to the ESMA Internal Control Guidelines for CRAs and that most of the provisions in these Guidelines are the same.

Conclusions

8. Ensuring that supervised entities' activities are of a high quality and free from any conflicts of interest is one of the key objectives of the relevant Regulations. As such, ESMA Guidelines which provide a set of measures to ensure that supervised entities are better able to meet these objectives 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.

Annex II – Guidelines

Guidelines on Internal Controls for Benchmark Administrators, Credit Rating Agencies and Market Transparency Infrastructures

1 Scope

Who?

1. These Guidelines apply to:

   (i) benchmark administrators authorised, registered or recognised with ESMA (together 'BMAs') in accordance with BMR;

   (ii) credit rating agencies established in the Union and registered with ESMA (CRAs) in accordance with CRAR;

   (iii) data reporting services providers (excluding Consolidated Tape Providers (CTPs)) established in the Union and authorised by ESMA (DRSPs) in accordance with MiFIR;

   (iv) securitisation repositories established in the Union and registered with ESMA (SRs) in accordance with SecR;

   (v) trade repositories established in the Union and registered with ESMA (TRs) in accordance with EMIR;

   (vi) trade repositories established in the Union and registered with ESMA in accordance with SFTR (hereinafter together referred to as 'Supervised Entities').

What?

2. These Guidelines concern matters relating to the internal control structure and mechanisms necessary to ensure (i) a BMA's effective compliance with Articles 4 to 10 of BMR; (ii) a CRAs' effective compliance with Article 6(1),(2) and (4), Article 9 and Annex I, Section A, of CRAR; (iii) a DRSP's effective compliance with Articles 27f, 27g, 27i of MiFIR; and (iv) a TR's or SR's effective compliance with Articles 78 and 79 of EMIR.

When?

3. These Guidelines apply from 1 October 2026.

4. As of the date referred to in Paragraph 3, the Guidelines on Internal Control for CRAs (ESMA33-9-371) are repealed.

2 References, abbreviations and definitions

Legislative references

BMR	Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014[15]
CRAR	Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit ratings agencies[16]
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011[17]
EMIR	Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories[18]
MiFIR	Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012[19]
SecR	Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012[20]
SFTR	Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012[21]

Abbreviations

AI	Artificial intelligence
APA	Approved Publication Arrangement

[15] OJ L 171, 29.6.2016, p. 1.
[16] OJ L 302, 17.11.2009, p. 1.
[17] OJ L 333, 27.12.2022, p. 1.
[18] OJ L 201, 27.7.2012, p.1.
[19] OJ L 173, 12.6.2014, p.84.
[20] OJ L 347, 28.12.2017, p. 35.
[21] OJ L 337, 23.12.2015, p.1.

ARM	Approved Reporting Mechanism
BMA	Benchmark Administrator
CP	Consultation Paper
CRA	Credit Rating Agency
DORA	Digital Operational Resilience Act
DRSP	Data Reporting Services Provider
ESMA	European Securities and Markets Authority
EU	European Union
IC Framework	Internal Control Framework
IC Function	Internal Control Function
ICT	Information and Communication Technology
INED	Independent Non-Executive Director
MI	Management Information
RTS	Regulatory Technical Standards
SR	Securitisation Repository
TR	Trade Repository

Definitions

Executive Senior Management	This refers to the most senior persons directing the supervised entity on a day-to-day basis. This is typically the Chief Executive Officer (CEO) or equivalent and his/her direct reports.
Management Body	The body or bodies which are appointed in accordance with national law, which are empowered to set the entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making and include persons who effectively direct the business of the entity. This refers to the most senior governing bodies within an organisation. The term is defined in BMR, Article 3(1), point (20) and in MIFIR, Article 2(1), point (22). It covers the concepts of: ▪ 'administrative or supervisory board', of a CRA, being part of 'senior management', as defined in CRAR, Article 3(1), point n)] ▪ 'administrative or supervisory board, or both, in accordance with national company law', as defined in EMIR, Article 2(27)

Market Transparency Infrastructures	For the purpose of these Guidelines, this refers to: ▪ Data Reporting Services Providers, ▪ Securitisation Repositories and ▪ Trade Repositories
Relevant Regulations	For the purpose of these Guidelines, this refers to: ▪ BMR ▪ CRAR ▪ EMIR ▪ MiFIR ▪ SecR ▪ SFTR
Supervised entities	For the purpose of these Guidelines, this refers to the entities under ESMA's supervisory remit, namely: ▪ BMAs ▪ CRAs ▪ DRSPs (excluding consolidated tape providers) ▪ SRs ▪ TRs

3 Purpose

5. These 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 supervised entity.

4 Compliance and reporting obligations

Status of the Guidelines

6. This document contains Guidelines issued pursuant to Article 16 of the ESMA Regulation. In accordance with Article 16(3) of the ESMA Regulation, supervised entities must make every effort to comply with these Guidelines.

Reporting requirements

7. Financial market participants to which these Guidelines apply are not required to report whether they comply with these Guidelines. ESMA will assess the application of these Guidelines by the supervised entities through its ongoing supervision and monitoring of supervised entities' activities.

Proportionality

8. ESMA will apply proportionality in the application of these Guidelines. While all supervised entities are expected to demonstrate the components and characteristics of an effective internal control system outlined in these Guidelines, ESMA will calibrate its expectations under Section 4.2 according to the nature, scale, complexity and overall risk profile of a supervised entity and based how these characteristics may affect investor protection, orderly functioning of the market and financial stability.

9. When assessing the nature of a supervised entity, ESMA will consider the business and type of operations of the supervised entity, including its market role/mission, type, diversity and criticality of products and services offered by the supervised entity.

10. When assessing the scale of the business of a supervised entity, ESMA will have regard to relevant factors including headcount, revenue, number of clients and products, market share, interconnections with other industries/infrastructures, ancillary services and their relationship with core services and other factors specific to the size and market impact of the supervised entity.

11. When assessing the complexity of a supervised entity, ESMA will have regard to amongst other factors, its organisational structure and arrangements (group structure/relationships, shared services, outsourcing, etc.) as well as its operational characteristics in relation to people, processes, technology, product offerings and interconnections.

12. In calibrating its expectations, ESMA takes into account the conditions of a supervised entity's registration or recognition. A supervised entity's nature, scale and complexity may change after it is registered or recognised, and it is its responsibility to ensure that its internal controls stay commensurate with its nature, scale and complexity. ESMA will

communicate through its supervision if it has a higher threshold of expectations under Section 5.1 and 5.2 than those established at registration or recognition.

5 Guidelines

13. In order to demonstrate that supervised entities comply with Paragraph 2 of these Guidelines, supervised entities should demonstrate that their policies, procedures and working practices achieve the objectives of Sections **5.1** (Internal Control Framework) and **5.2** (Internal Control Functions) of these Guidelines.

5.1 Internal Control Framework

14. To ensure an effective IC framework, supervised entities should have the following components and characteristics in their policies, procedures and working practices.

General Principles

15. The Management Body of the supervised entity should be accountable for overseeing and approving all components of the IC Framework as well as overseeing that those components are subject to monitoring and are regularly updated by the Executive Senior Management. The supervised entity's Executive Senior Management should be responsible for establishing, implementing and updating the written internal control policies, procedures and practices that support the components of the IC framework.

16. As part of putting these policies and procedures in place, a supervised entity should have a clear, transparent and documented decision-making process and a clear allocation of roles and responsibilities within its IC Framework, including its business lines and IC functions.

Component 1.1 Control Environment

17. A supervised entity's Management Body and Executive Senior Management both contribute to establishing the tone at the top regarding the importance of internal control. The Executive Senior Management is responsible for the development and performance of internal control and assessing the adequacy and effectiveness of the control environment. The Management Body should exercise oversight of Executive Senior Management in these areas.

Characteristics

1.1.1 The supervised entity's Executive Senior Management should be responsible for establishing a strong culture of ethics and compliance within the supervised

entity through the implementation of policies and procedures that govern the conduct of the supervised entity's staff.

1.1.2 The supervised entity's Executive Senior Management should be responsible for ensuring that the supervised entity's policies and procedures:

i. Specify that the supervised entity's business should be conducted in compliance with the relevant Regulations and with the supervised entity's corporate values;

ii. Clarify that in addition to 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.

1.1.3 The supervised entity's Executive Senior Management should establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures.

1.1.4 The supervised entity's Executive Senior Management should retain responsibility for activities outsourced to external service providers or delegated to business partners.

Component 1.2 Risk Management

18. For the purposes of effective risk management, supervised entities should ensure that they have in place a dynamic and continuously evolving process for identifying, assessing and measuring all risks that could impact a supervised entity's ability to perform its obligations under the relevant Regulations, or its continued operation. For example, this includes risks resulting from the supervised entity's use of new technologies and changes to its external risk landscape. The process should enable the supervised entity to monitor, manage, mitigate and properly report material risks to these objectives.

Characteristics

1.2.1 The supervised entity should conduct its internal risk assessments in accordance with a defined and comprehensive risk assessment methodology.

1.2.2 The supervised entity should set its risk appetite and identify risk tolerance levels.

1.2.3 The supervised entity's risk assessment methodology should encompass all business lines and IC Functions of the supervised entity.

1.2.4 The supervised entity's risk assessment process should identify and assess changes that could significantly impact the system of internal control. This includes changes to its environment, organisation, activities and operations.

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

Component 1.3 Control Activities

19. The control activities should be preventative, detective, corrective or deterrent in nature.

Characteristics

1.3.1 *Segregation of Duties* – The supervised entity should ensure appropriate segregation of duties to manage risks of conflicts of interest, fraud and human error. The segregation of duties should ensure that staff members responsible for carrying out a task are not solely responsible for approving the outcome of its exercise. In particular, staff members responsible for the development, implementation or approval of a task/work item are not solely responsible for validating, assessing and reviewing it.[22] Where this cannot be avoided, this should be mitigated by staff members not being exclusively responsible for the activity. [23]

1.3.2 *Documentation* – The supervised entity should document its policies and procedures covering all areas of their business activities subject to the provisions of the relevant Regulations.

[22] For example, staff members responsible for system development activities should not be involved in database administration, IT operations, and IT systems and network administration and maintenance.For CRAs, (i) persons conducting the analysis of a credit rating should not be solely responsible for the approval of the credit rating, (ii) persons responsible for the development of credit rating methodologies should not be solely responsible for their approval; (iii) persons responsible for the validation, assessment or review of a credit rating methodology should not be solely responsible for the approval of the validation, assessment or review.

[23] For instance, through a four-eyes check.

1.3.3 *Documented Controls and Control Testing* – The supervised entity should document the key controls in place to ensure adherence to its policies and procedures established pursuant to the relevant Regulations.

1.3.4 *Designation of Responsibilities* – The supervised entity should designate in a clear and defined manner the roles or functions responsible for carrying out controls relating to the obligations under the relevant Regulations and specify their respective roles and responsibilities. In doing so, the supervised entity 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 supervised entity should have authorisation processes or mechanisms to ensure that only authorised individuals have access to information and tools on a need to know and least privilege basis. The supervised entity should also have processes or mechanisms in all business activities to ensure that activities are approved and executed only by staff members acting within the scope of their authority.[24]

1.3.6 *Verifications, validations, reconciliations and reviews* – The supervised entity should take measures to detect and act upon inappropriate, non-authorised, erroneous or fraudulent activities in a timely manner.[25]

1.3.7 *Information and Communication Technology (ICT) General Controls* (only for supervised entities not subject to DORA) – The supervised entity should implement strategies, policies and procedures that ensure the digital operational resilience of the ICT systems of the supervised entity in supporting the supervised entity's business processes.

The supervised entity should design its ICT controls and solutions proportionately. Therefore, ICT controls will vary among organisations depending on the nature, scale and complexity of the underlying business processes and of the relevant functions supported by those systems.

Supervised entities should ensure that they have sufficient controls to ensure data quality, in terms of availability, confidentiality and integrity of data, including data validation, processing controls and data file control procedures.

[24] For instance, for CRAs, only the persons designated as responsible for the respective tasks should carry out the credit rating process, the validation of methodologies and the review of the results of validation.
[25] This includes data validation and input controls, reviews of lists for authorised access to confidential information. For CRAs, such controls apply to, credit rating activities and to processes underlying these activities such as credit methodology/model validation.

The supervised entity should establish relevant information security management system and related control activities. As part of this, a supervised entity should determine the necessary controls to ensure the authenticity, confidentiality, integrity and availability of information as it is processed from source to ultimate user.

The supervised entity should establish and document all relevant ICT acquisition, development and maintenance processes control activities.

Component 1.4 Information and Communication

20. Supervised entities should establish procedures for the downward sharing of accurate, complete and good quality information to staff and external stakeholders. Supervised entities should also establish procedures for the regular reporting of information about the internal control system and activities to the Management Body and Executive Senior Management including information relating to behaviour and adherence to internal controls.

Characteristics

1.4.1 The supervised entity should ensure appropriate internal and external communication, sharing accurate, complete and of good quality information in a timely manner to the market, clients, users of its products and services and regulators.

1.4.2 The supervised entity should establish upward communication channels, including a whistleblowing procedure, to enable the escalation of material internal control issues to the Management Body and Executive Senior Management. The Management Body and Executive Senior Management should also receive regular updates about the internal control system and activities, including on information security. The supervised entity should have escalation procedures in case of material disagreement between IC Functions and operating units.

1.4.3 The supervised entity should establish downward communication channels from the Management Body, Executive 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 or information security issues and presentations and training on policies and procedures.

Component 1.5 Monitoring Activities

21. Supervised entities should ensure that they undertake monitoring activities that will help ascertain whether the components of a supervised entity's internal control system are present and functioning effectively.

Characteristics

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

1.5.2 Monitoring activities should be designed and carried out in a way that enables the supervised entity to check whether the supervised entity meets its legal and regulatory requirements, including adhering to its internal codes of conduct, policies and procedures. This includes the supervised entity's information security policies and procedures.

1.5.3 The evaluations of internal control systems should be carried out on a regular or thematic basis or through a mix of both.

1.5.4 The supervised entities should build ongoing evaluations into the business processes and adjust them to changing conditions.

1.5.5 The supervised entities should ensure that deficiencies identified from monitoring evaluations and the required remediation actions are reported to the Management Body and Executive Senior Management who should then monitor the timely implementation of corrective action(s).

1.5.6 In the case of outsourcing, the supervised entity should allocate the task for monitoring outsourced business processes to a member of staff. Supervised entities should ensure that sufficient information concerning objectives and delivery expectations is provided to the service provider, and that due diligence is conducted prior to the appointment of the provider.

5.2 Internal Control Functions

22. To ensure effective IC Functions, supervised entities should include the following components and characteristics in their policies, procedures and working practices.

General Principles

23. ESMA considers that supervised entities' IC functions should have sufficient resources and be staffed with individuals with sufficient expertise to discharge their duties. Staff working in IC Functions should have sufficient technical knowledge of the supervised entity's activities and the associated risks. Where a supervised entity has outsourced the operational tasks of an IC function to group level or to an external party, ESMA considers that the supervised entity retains full responsibility for the activities of the outsourced IC function. Supervised entities should ensure that staff in charge of IC functions should be of an appropriate seniority to have the necessary authority to fulfil their responsibilities. For example, staff members in charge of the Compliance, Risk Management, Internal Audit, Information Security Management, Review (for CRAs) and Oversight (for BMAs) Functions should have unfettered access and report to the Management Body on a regular basis.

24. Activities 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 supervised entity's Management Body to provide oversight, and the ability of Executive Senior Management to effectively manage its risks, or ESMA's ability to effectively supervise the supervised entity. In all cases Guideline 1.1.4 applies.

25. To ensure the independence of a supervised entity's IC functions, ESMA expects supervised entities to consider the following principles when 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 staff member in charge of an IC function should not report to a person who has responsibility for managing the activities the IC function monitors, audits or controls;

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

Proportionality – Internal Control Functions

27. While all supervised entities are expected to demonstrate the characteristics of effective IC Functions outlined in these Guidelines, ESMA calibrates its expectations according to

the nature, scale and complexity of a supervised entity, as described in Section 3.4 of these Guidelines.

28. This section sets out in more detail how ESMA takes into account proportionality in its supervision of IC Functions.

Segregation of duties

29. Segregation of duties should be built into the development of control activities. There may however be some instances where Union law does not require segregation of duties and such segregation is not practical considering the supervised entity's nature, scale and complexity. In this case, alternative controls may be more suitable. Where other controls are used, the supervised entities should document the rationale for the arrangement, identify the possible risks, implement compensating controls to address them and demonstrate that the arrangement does not impair the control environment.

Resources

30. For some supervised entities, it may not be proportionate to have full time staff in all functions given their nature, scale and complexity. In these instances, a supervised entity may choose to scale the hours of resource to match control activities or outsource the activity.

Specialisation within Functions

31. As a supervised entity grows, and its control environment matures, it should use staff specialisation to benefit from staff expertise in key processes or risk areas. Supervised entities of a certain nature, scale and complexity should have in place dedicated monitoring or investigation teams within their Compliance Function.

Maturity of control activities

32. The maturity of control activities (i.e. manual, hybrid, automated, and in some instances, incorporating Artificial Intelligence tools) should reflect the nature, scale and complexity and overall risk profile of a supervised entity. For supervised entities of a certain nature, scale and complexity, there should be a higher degree of automated controls as well as a greater integration between the systems of control functions to optimise monitoring activities and a supervised entity's reporting of Management Information to Executive Senior Management and the Management Body.

Component 2.1 Compliance Function

33. The Compliance Function of a supervised entity is responsible for monitoring and reporting on compliance of the supervised entity and its employees with its obligations under the relevant Regulation. The Compliance Function is responsible for following changes in the laws and regulations applicable to its activities. The Compliance Function is also responsible for advising the Management Body on laws, rules, regulations and standards that the supervised entity needs to comply with and assess, in conjunction with other relevant functions, the possible impact of any changes in the legal or regulatory environment on the supervised entity's activities.

Characteristics

2.1.1 The Compliance Function should perform its functions independently of the business lines and should provide regular reports to the supervised entity's Management Body and, where relevant, directly to the INEDs.

2.1.2 The Compliance Function should advise and assist staff members to comply with the obligations under the relevant Regulation. 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. The scope of Compliance activities should cover all the business and IT processes and systems that could affect the supervised entity's compliance with the relevant Regulation.

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 supervised entity's activities and communicate, as appropriate, with the Risk Management Function on the supervised entity's compliance risk in a timely manner.

2.1.5 The Compliance Function should ensure that compliance policies are followed and should report to the Management Body and Executive Senior Management on the supervised entity's 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 Management Body and Executive Senior Management as well as by the Risk Management Function within their risk-assessment processes.

Component 2.2 Risk Management Function

34. The Risk Management Function of a supervised entity is responsible for the development and implementation of the risk management framework.

Characteristics

2.2.1 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.

2.2.2 The Risk Management Function should ensure that all risks that could impact a supervised entity's ability to perform its obligations under the relevant Regulations, or its continued operation, are identified, assessed and measured. Material risks to these objectives should then be monitored, managed, mitigated and properly reported by and to the relevant units within the supervised entity in a timely manner.

2.2.3 The Risk Management Function should monitor the risk profile of the supervised entity against the supervised entity's risk appetite to enable decision-making.

2.2.4 The Risk Management Function should provide advice on proposals and risk decisions made by business lines and inform the Management Body as to whether those decisions are consistent with the supervised entity's risk appetite and objectives.

2.2.5 The Risk Management Function should recommend improvements to the risk management framework and amendments to risk policies and procedures where necessary. The Risk Management Function should revisit risk thresholds in accordance with any changes in the organisation's risk appetite.

Component 2.3 Information Security Management Function (only for supervised entities not subject to DORA)

35. The information security management function of a supervised entity is responsible for the development and implementation of information security within the supervised entity. A supervised entity should establish a function that promotes an information security culture within the supervised entity.

Characteristics

2.3.1 The Information Security Management Function should be responsible for reviewing and monitoring the supervised entity's compliance with the supervised entity's information security policies and procedures.

2.3.2 The Information Security Management Function should manage the supervised entity's information security activities.

2.3.3 The Information Security Management Function should develop and deploy an information security awareness program for personnel to enhance the security culture and develop a broad understanding of the supervised entity's information security framework.

2.3.4 The Information Security Management Function should report to and advise the Management Body and Executive 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 2.4 Internal Audit Function

36. An Internal Audit Function of a supervised entity 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

2.4.1 The Internal Audit Function should perform its functions independently of the business lines and other IC Functions. It should be governed by an internal audit charter that defines its role and responsibilities and is subject to oversight by the Management Body.

2.4.2 The Internal Audit Function should follow a risk-based approach and adhere to international internal audit standards.

2.4.3 The Internal Audit Function should independently review and provide objective assurance that the supervised entity's activities, including outsourced activities, comply with the supervised entity's policies and procedures as well as with applicable legal and regulatory requirements.

2.4.4 The Internal Audit Function should establish at least once a year, based on the annual internal audit control objectives, an audit plan which is subject to oversight by the Management Body.

2.4.5 The Internal Audit Function should provide regular reports to the independent members of the Management Body or to the Audit Committee, if in place.

2.4.6 The Internal Audit Function should communicate its audit recommendations in a clear and consistent way that allows the Management Body and Executive Senior Management to understand the materiality of recommendations and prioritise accordingly.

2.4.7 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.

Component 2.5 Review Function (for CRAs only)

37. The Review Function of a CRA is responsible for reviewing credit rating methodologies on at least an annual basis. The CRA's Review Function is also responsible for the validation and review of new methodologies, and any changes to existing methodologies.

Characteristics

2.5.1 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.

2.5.2 The CRA's shareholders or staff involved in business development should not perform the tasks of the Review Function.

2.5.3 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.

2.5.4 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.

2.5.5 The Review Function staff responsible for the validation and/or review of a methodology, and that are also involved in its development phase, should not

be solely responsible or have the majority of voting rights in the methodology approval committees.

2.5.6 In case of outsourcing of the Review Function, the CRA should take into account Guideline 1.5.6. Additionally, the CRA should have suitable internal control mechanisms to ensure that it consistently adheres to regulatory requirements and maintains appropriate analytical quality standards.

Component 2.6 Oversight Function (for BMAs only)[26]

38. The Oversight Function oversees the main aspects of the provision of benchmarks. This includes, but is not limited to, the review of the benchmark's definition and methodology, the management of third parties involved in the provision of the benchmark, assessing internal and external audits or reviews of the administrator's control framework, and reporting to the relevant competent authorities any relevant misconduct.

Characteristics

2.6.1 The BMA Oversight Function maintains its independence from any Management Body or function of the BMA and any external party of the BMA. Independence assumes that members of the Oversight Function are not subject to conflicts of interest between their activities as members of the Oversight Function and their other activities. The BMA should implement an internal control operating framework to prevent and mitigate any potential conflict of interests.

2.6.2 The BMA should have clear policies and procedures regarding the set-up and responsibilities of the Oversight Function and its members, including policies and procedures for benchmarks methodology updates and data integrity reviews.

2.6.3 The BMA Oversight Function should regularly perform a self-assessment to evaluate its effectiveness and the suitability of its members for the purpose of the function and to identify potential conflicts of interest and propose areas of improvement, if necessary.

2.6.4 The BMA Oversight Function should maintain a defined and regular communication channel with the Management Body, Executive Senior Management, and other key functions. The BMA Oversight Function should be

[26] Non-significant BMAs who apply article 26 of the BMR are expected to apply these Guidelines proportionally to the requirements of the article 26.

also able to access and challenge Management Information and receive updates regarding the status of remedial actions following internal and external audits, risk, and compliance reports.

2.6.5 The BMA Oversight Function should maintain a defined communication channel with the relevant competent authorities, including reporting any misconduct or violation by administrators or contributors.