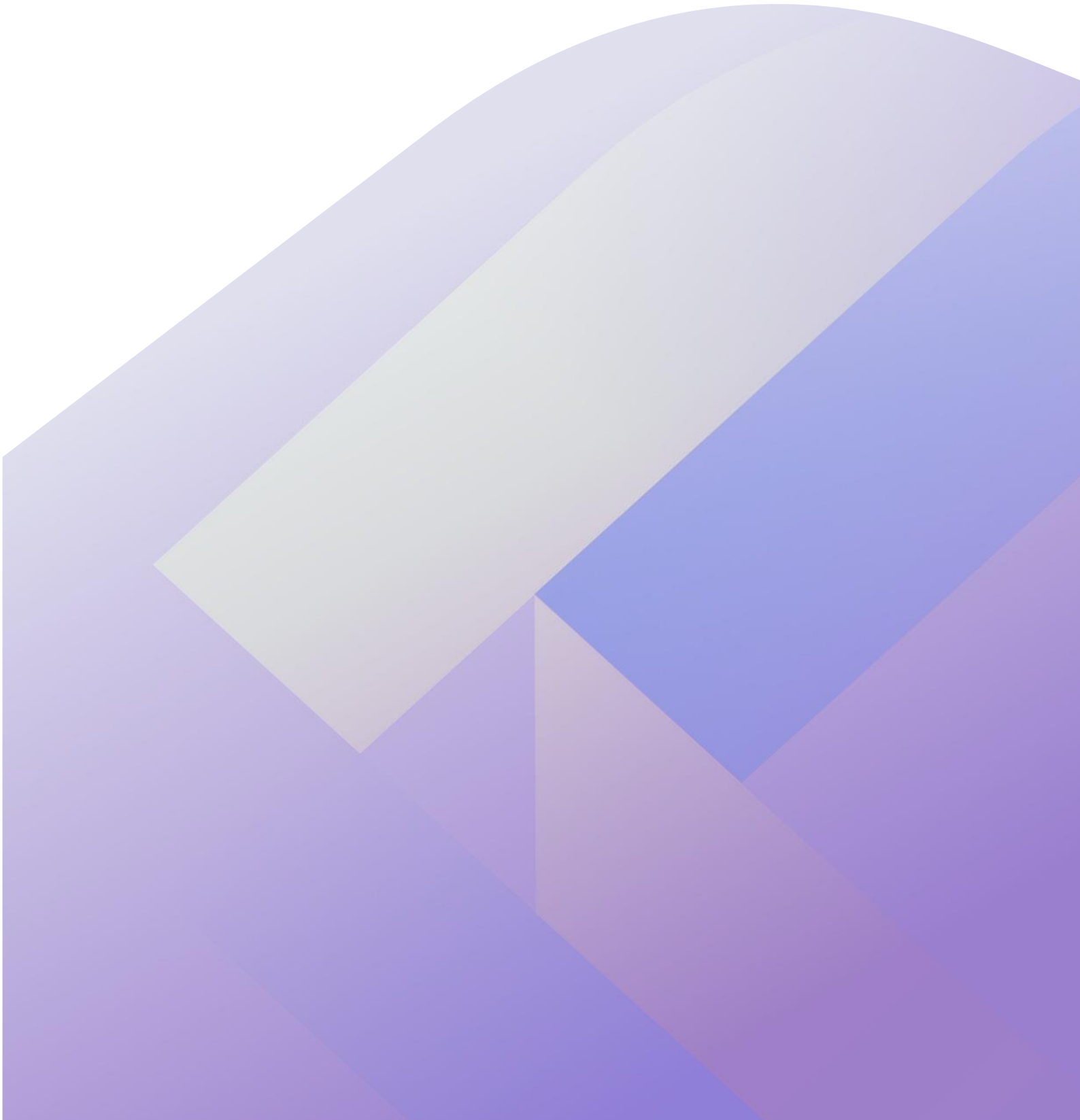
19 December 2024
ESMA80-1286971524-661

Consultation Paper

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



Responding to this paper

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

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

ESMA will consider all comments received by 18 March 2025**.**

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

Publication of responses

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

Data protection

Information on data protection can be found at www.esma.europa.eu under the heading 'Data protection'.

Who should read this paper?

This paper may be of interest to national competent authorities, other financial groups with a controlling participation in a Benchmark Administrator (BA), Credit Rating Agency (CRA), Data Reporting Service Provider (DRSP), Securitisation Repository (SR) or Trade Repository (TR) and firms considering applying to be a registered as a BA, CRA, DRSP, SR or TR.

Table of Contents

Executive summary

Reasons for publication

1. ESMA directly supervises all EU CRAs, SRs and TRs as well as certain BAs[1] and certain DRSPs[2] in accordance with the relevant Regulations. These Regulations include a number of requirements relating to the internal control system that supervised entities must have in place.[3]

2. ESMA published Guidelines on Internal Control for CRAs[4] on 30 September 2020. Those Guidelines set out the components and characteristics of an effective internal control system within a CRA.

3. This Consultation Paper proposes to build on and replace the Guidelines on Internal Control for CRAs and set out ESMA's views for all entities it directly supervises (except third-country central counterparties). It also revises ESMA's expectations considering the growing impact of technology on supervised entities' operations. This includes in terms of managing technology risk from external and internal sources, and the integration of new technologies into supervised entities' internal controls.

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

5. ESMA will apply proportionality in the application of 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.

Contents

6. The Consultation Paper is structured according to two main parts, establishing:

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

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

[1] ESMA supervises administrators of EU critical benchmarks and recognised third-country administrators.

Cost-benefit analysis

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

Next Steps

8. ESMA will consider the responses it receives to this CP and expects to publish a final report in Q4 2025.

[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. However, no CTP has been authorised yet.
[3] An internal control system includes both the internal control framework and internal control functions.
[4] Guidelines on Internal Control for CRAs, 30 September 2020 | ESMA33-9-371

Legislative 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
CRAR	Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit ratings agencies
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
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
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
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
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

Abbreviations

AI	Artificial intelligence
APA	Approved Publication Arrangement
ARM	Approved Reporting Mechanism
BA	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

Management Body	For the purpose of these Guidelines, 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 the '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
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 directly supervised by ESMA, namely: ▪ BAs ▪ CRAs ▪ DRSPs ▪ SRs ▪ TRs

Introduction

1. The Benchmark Regulation (BMR), the Credit Rating Agency 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 BAs, CRAs, DRSPs, SRs and TRs directly supervised by ESMA (hereinafter referred to as supervised entities). These regulations outline essential aspects such as governance, risk management, compliance, and operational controls, which the supervised entities must adhere to.

2. BMR includes governance and control requirements for BAs. These include requirements on conflicts of interest, oversight function, control frameworks, accountability and record keeping, complaints-handling mechanisms, outsourcing, input data, methodology and reporting of infringements.[5]

3. CRAR includes a number of requirements relating to the internal control system that a CRA must have in place in order to prevent or mitigate any possible conflicts of interest that may impact the independence of its credit rating activities. The need for a CRA to have a robust and appropriately resourced system of internal controls is set out in Article 6[6] and Annex I Section A of the CRA Regulation. EU-registered CRAs have already been subject to ESMA's Guidelines on Internal Controls for CRAs since 2020.[7]

4. EMIR, SFTR and SecR require TRs and SRs to have adequate internal control mechanisms, including sound administrative and accounting procedures, which prevent any disclosure of confidential information and to identify and minimise sources of operational risk through the development of appropriate controls and procedures.[8]

5. MiFIR requires DRSPs to implement governance arrangements that ensure effective and prudent management of the organisation, including the segregation of duties in the organisation and the prevention of conflicts of interest.[9] The organisational requirements that DRSPs need to comply with in order to be authorised by ESMA[10] include control arrangements (e.g., compliance and risk management controls embedded in IT systems) that are further specified in the applicable regulatory technical standards (RTS) on authorisation.[11]

---

[5] See Articles 4-10 of the Benchmark Regulation (OJ L 171, 29.06.2016, p.1)
[6] See Article 6(1), 6(2), 6(4) and Section A of Annex I of the CRA Regulation (OJ L 302, 17.11.2009, p.1).
[7] ESMA Publishes Final Report for Guidelines on Internal Control (europa.eu)
[8] See Articles 78 and 79 of EMIR (OJ L 201, 27.7.2012, p.1); Article 5(2) of SFTR (OJ L 337, 23.12.2015, p.1); Article 10(2) of SecR (OJ L 347, 28.12.2017, p. 35).
[9] See Article 27f(3) of MiFIR (OJ L 173, 12.6.2014, p.84).
[10] See Articles 27g(3), 27h(4), and 27i(2) of MiFIR.
[11] See COMMISSION DELEGATED REGULATION (EU) 2017/571 of 2 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards on the authorisation, organisational requirements and the publication of transactions for data reporting services providers.

6. However, the Regulations provide limited details on how the various components and characteristics of the internal control system should integrate and function together as complementary parts of a unified framework.

7. As ESMA has already communicated some of its expectations on internal controls bilaterally with supervised entities during supervisory engagements. 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. This reflects the importance that internal controls stay commensurate with the level of complexity in a supervised entity's business and first line activities. 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 resilience of supervised entities.

8. The proposed guidance in this paper has been developed with reference to a range of contributing sources, including the Regulations' provisions relevant to internal controls (as further specified in the respective RTS); ESMA's existing Guidelines[12], ESMA's supervisory experience and enforcement actions[13], and existing industry practices in supervised entities; EU approaches and guidance on internal control[14]; and internationally recognised internal control frameworks.[15] This has enabled ESMA to propose 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.

9. Nonetheless, ESMA has also taken the opportunity to expand and clarify some of its expectations related to technology given the growing risk and opportunities provided through its 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.

10. 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

[12] 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),
[13] 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).
[14] 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.
[15] COSO Internal Control – Integrated Framework, May 2013 © 2013, Committee of Sponsoring Organisations of the Treadway Commission (COSO), U.S.A.

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 and “Information and Communication Technology (ICT) General Controls” and “Information Security Management Function” of these Guidelines.

11. The present proposal aims to ensure that ESMA can take a consistent approach to its supervisory assessments of internal control practices across the entities it supervises.

12. The proposed guidance is structured in two key parts, that represent the internal control system]. The first part focuses on a supervised entity’s overall framework for internal controls (IC Framework), 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, is then further split into different components.

13. 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.

14. 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 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.

15. The proposed guidance on IC Functions is similarly 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; (iv) review function (for CRAs); (v) oversight function (for BAs). 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.

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

17. ESMA will apply proportionality in the application of 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.

Internal Control Framework – Component Parts and Characteristics

General - Internal Control Framework

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

19. The five components of this section are drawn from the COSO framework.[16] The approach of the guidance is to provide a general overview of ESMA's view on the importance of the role of each component within an IC Framework. Following this, the guidance describes the specific characteristics that ESMA would expect to see within a supervised entity's internal policies, procedures and practices.

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

21. Irrespective of name, format or classification, documented internal policies and procedures are important to ensure that the different components and characteristics of the IC Framework are embedded in a supervised entity's practices. In this regard, the Management Body should be accountable for overseeing and approving all components of the IC Framework as well as overseeing that they are subject to monitoring and regular update 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 and procedures and working practices.

22. There should be a clear, transparent and documented decision-making process for the monitoring and updating of these policies and procedures. These policies and procedures should include a clear allocation of roles and responsibilities within its IC Framework, which includes the business lines and IC Functions.

Component – Control Environment

23. The first component of the IC Framework is the control environment. The control environment is the set of standards, processes and structures necessary for carrying out

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

internal controls across an organisation. The control environment is the foundation on which an effective system of internal controls is built.

24. An effective control environment begins with the supervised entity's Management Body and executive senior management setting the right tone at the top of the supervised entity. In creating the conditions for an effective control environment, the supervised entity's Management Body is accountable for the adoption of a high level of ethical and professional standards relating to the conduct of the supervised entity's staff (and where relevant, external service providers). The supervised entity's executive senior management are subsequently responsible for the development and implementation of these standards and ensuring they consider the specific needs and characteristics of the supervised entity.

25. The supervised entity's executive senior management should be responsible for ensuring that the supervised entity's staff are aware of the potential internal and external disciplinary actions for not adhering to the supervised entity's policies and procedures as well as the applicable laws and regulations. The supervised entity's Management Body should be accountable for the oversight of these policies and procedures, this oversight should include assessing whether any transgressions have been properly addressed.

Part 1: Internal Control Framework		
Component	**1.1**	Control Environment
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 establish 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 ensure 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 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.
	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 – Risk Management

26. The second component of the IC Framework is effective risk management. This includes the identification, assessment, monitoring, management, mitigation and reporting of all risks relevant to the supervised entity that could materially impact the supervised entity's ability to meet its obligations under the Regulations or threaten its continued operation. Effective risk management enables a supervised entity to allocate its resources appropriately.

27. To ensure this is conducted effectively, the supervised entity's risk management processes should be carried out according to a defined and objective methodology. A high standard of risk management will ensure that the supervised entity is conscious of, and prepared for, the risks posed by its business activities. In turn, this will enable the supervised entity

to establish its risk appetite and allocate its internal control resources accordingly. This component of the Guidelines proposes that as part of their internal control framework, supervised entities should adopt an approach to risk management that encompasses all business lines and internal control functions.

28. These risk assessments should enable the supervised entity to make well-informed decisions as to whether the risks that it has identified across its business lines are within its risk appetite. In this regard, risks should be evaluated from both the bottom up and the top down, within and across business lines, using consistent terminology and methodologies.

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

Part 1: Internal Control Framework		
Component	**1.2**	Risk Management
Effective risk management framework should involve a dynamic and continuously evolving process for identifying, assessing and managing risks to the achievement of the supervised entity's main objectives. For example, this includes risks resulting from the supervised entity's use of new technologies and changes to its external risk landscape.		
Characteristics	**1.2.1**	The supervised entity should conduct its internal risk assessments in accordance with a defined and comprehensive risk assessment methodology. This methodology should define and identify in advance the criteria and objectives against which the supervised entity's risks are going to be assessed.
	1.2.2	The supervised entity should set its risk appetite and identify risk tolerance levels as part of the risk assessment process.
	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 – Control Activities

30. The third component of the IC Framework relates to the supervised entity's control activities. Control activities governing supervised entities' business activities help mitigate the impact of risks within an organisation. They are actions designed through policies, procedures, systems, mechanisms and other arrangements. This component is focused on ensuring that a supervised entity has appropriate controls and safeguards in place for the day-to-day business activities of its staff. It builds upon the presence of a strong control environment in which the risks to which the supervised entity is exposed to have been identified and its risk appetite appropriately defined.

31. Control activities may include approvals, reconciliations, monitoring, authorisations, verifications which are based on duly approved and communicated policies and procedures. For CRAs, these include methodology validation or credit rating approval. At the core of these activities lie the four-eyes review and segregation of duties principles. For BAs, control activities are covered by requirements on input data, methodology, record keeping, accountability, conflicts of interest, reporting of infringements and the code of conduct.

32. At CRAs, staff members in charge of carrying out the analytical work of a credit rating should not be responsible for the approval of that credit rating. In addition, staff members responsible for the development of credit rating methodologies[17] should not be involved in their implementation. Finally, staff members responsible for the development or implementation of credit rating methodologies should not be responsible for their review or validation.

33. The policies and procedures governing these activities should be documented with clearly designated responsibilities and only staff with the relevant authorisations are allowed to carry out sensitive tasks.

34. These control activities are applicable across the supervised entity's IC Functions and business lines, including the supervised entity's IT-related controls. For example, DRSPs, SRs, and TRs operate IT infrastructures through which they process sensitive information and disseminate it to the authorities and the public. The control activities should apply to those technological components that support the supervised entities' main objective to maintain the quality of the information they process end-to-end.

[17] For the purposes of these Guidelines the term 'methodology' is as described in Art 3 of the Proposed Revisions to Commission Delegated Regulation (EU) 447/2012 and Annex I of CRA Regulation.

35. These control activities also facilitate and contribute to the effectiveness of individual IC Functions in the fulfilment of their tasks by ensuring the presence of an effective audit trail for determining and assessing responsibility across the supervised entity's activities.

Part 1: Internal Control Framework		
Component	**1.3**	Control Activities
These 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: i. Staff members responsible for carrying out a task are not responsible for approving the outcome of its exercise; ii. Staff members responsible for the development, implementation or approval of a task/work item are not responsible for validating, assessing and reviewing it.[18] Where this cannot be avoided, this should be mitigated by staff members not being exclusively responsible for the activity.[19]
	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.
	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 relevant to the Regulations. The documentation of these controls should set out: i. A description of the control ii. The associated risk(s)

[18] 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 involved in their implementation; (iii) persons responsible for the validation, assessment or review of a credit rating methodology should not be involved in their development, implementation or approval.
[19] For instance, through a four-eyes check.

		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
	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 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 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 in all business activities to ensure that activities are approved and executed only by staff members acting within the scope of their authority.[20]
	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.[21]
	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

[20] For instance, for CRAs, only the persons with appropriate authorisation should carry out the credit rating process, the validation of methodologies and the review of the results of validation.
[21] This includes data validation and input controls, reviews of lists for authorised access to confidential information. For CRAs, such controls apply to, inter alia, credit rating activities and the processes underlying these activities such as credit methodology/model validation.

		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. 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 – Information and Communication

36. Building upon a strong compliance and information security culture, effective risk management and controls in business practices, the fourth element of the IC Framework concerns the internal and external communication of the supervised entities. Appropriate internal and external communication is critical to supervised entities meeting their regulatory obligations to the market, clients and staff. In this respect, the supervised entity should ensure its policies and procedures support appropriate upward (whistleblowing) and downward (announcements on activities and updates on new policies and procedures) communication within its organisation towards an effective level of communication with all stakeholders.

37. Internal communication involves ensuring that all staff are aware of new policies and procedures, business developments and training opportunities. Staff should be aware of their obligations, notably in relation to conflicts of interest declarations and information security.

38. Effective external communication involves timely communication with market, clients, users of its services and regulators.[22]

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

Part 1: Internal Control Framework		
Component	**1.4**	Information and Communication
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 on 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 services and regulators.
	1.4.2	The supervised entity should establish upward communication channels, including a whistleblowing procedure, to enable the escalation of 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 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

[22] In this context, external communication refers, but is not limited, to regulatory reporting requirements under the Regulations, general communication and interaction with clients as well as the notification and reporting of information to other regulators.

		security issues and presentations and training on policies and procedures.

Component – Monitoring Activities

40. The final component of the IC Framework concerns the effective monitoring of the supervised entities' activities and the adequacy of the IC Framework itself. Ongoing monitoring and thematic reviews of supervised entities' activities are necessary to ensure the continued adequacy and effectiveness of a supervised entity's internal control system. In this regard, there are a number of ways in which a supervised entity can and should monitor whether it is meeting its legal and regulatory requirements as well as adhering to its internal codes of conduct, policies and procedures. These are set out in detail in the proposed guidance and recommend measures that cover compliance planning as well as monitoring of outsourced business activities.

Part 1: Internal Control Framework		
Component	**1.5**	**Monitoring Activities**
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 is meeting its legal and regulatory requirements as well as 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 the 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.

Questions for Respondents

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

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

Internal Control Functions - Component Parts and Characteristics

General – Internal Control Functions

41. While the first part of the Guidelines addresses the components and characteristics of an effective IC Framework, the second part deals with specific IC Functions of the supervised entities and how these should be integrated into the organisational structure and business activities of the supervised entity.

42. As a starting point, it is important that each IC Function has sufficient resources and is staffed with individuals with sufficient expertise to discharge their duties. Staff working in IC Functions should have sufficient technical knowledge of the supervised entity's activities and the associated risks. In cases where supervised entities have 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 the 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, review (for CRAs) and oversight (for BAs) functions should be directly accountable to the Management Body and their performance should be reviewed by the Management Body.

43. 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, Characteristic 1.1.4 applies.

44. In addition, to ensure the independence of the IC Functions, supervised entities should consider the following principles when establishing the roles and responsibilities of their IC Functions:

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

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

    - The staff member in charge of an IC Function should not report to a person who has responsibility for managing the activities the IC Function monitors, audits or controls;

45. 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

46. While all supervised entities are expected to demonstrate the characteristics of effective internal control functions outlined in these Guidelines, ESMA will calibrate its expectations according to the nature, scale and complexity of a supervised entity.

47. When assessing the nature of 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.

48. When assessing the scale of the business, 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.

49. 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 regard to people, processes, technology, product offerings and interconnections.

50. This section sets out how ESMA will demonstrate proportionality in its supervision of compliance with these Guidelines.

Segregation of duties

51. Segregation of duties should be built into the development of control activities. There may however be some limited instances where segregation of duties is not practical due to a 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 eventually demonstrate that the arrangement does not impair the control environment.

Resource

52. In 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

53. 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. For example, in the supervised entities of a certain nature, scale and complexity, it may be appropriate to have dedicated monitoring or investigation teams within their compliance function.

Maturity of controls activities

54. 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, ESMA expects a higher degree of automated controls, and greater integration between the systems of control functions to optimise monitoring activities and a supervised entity's reporting management information to executive senior management and the Management Body.

55. The following sub-sections discuss key IC Functions and the characteristics that supervised entities should evidence to demonstrate the sufficient presence of each component within the supervised entity.

Internal Control Function - Compliance

56. ESMA is of the opinion that all supervised entities should establish a dedicated control function to manage compliance risk and related tasks. Supervised entities should appoint a person responsible for this function across the entire supervised entity who has the authority to report directly, on their own initiative, to the Management Body[23].

57. In line with the requirements of the relevant Regulations, the compliance function (or in the case of an exemption the delegated party or parties performing the compliance tasks) should be independent of the business lines and have sufficient authority, stature and resources. Staff within the compliance function should possess sufficient knowledge, skills and experience on compliance and procedures. The compliance function should have, in addition to the appropriate legal skills, also the technical competence to understand, evaluate and challenge risks and controls in the supervised entity core to its business. This includes controls in the IT environment and associated processes when these are important to ensure the supervised entity's compliance with the Regulations.

58. The compliance function should have unrestricted access to any records, documents, information and buildings/facilities of the supervised entity. This should include access to the management information systems and minutes of all committees and decision-making bodies.

59. The Management Body should oversee the implementation of a well-documented compliance policy which should be communicated to all staff.

Part 2: Internal Control Functions		
Component	**2.1**	Compliance Function
The compliance function of a 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 law and regulation 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 to 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, Independent Non-Executive Directors (INEDs).

[23] CRAs may receive an exemption from this requirement of the CRAR, if they can demonstrate there are sufficient safeguards in place and the provision is disproportionate.

	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 needs to 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 should assess, and where appropriate in conjunction with other relevant functions, 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.

Internal Control Function - Risk Management

60. ESMA is of the opinion that all supervised entities should establish a control function to develop and implement a risk management framework. The risk management function should have direct access to the supervised entity's Management Body and to all business lines and other internal units that have the potential to generate risks.

61. The staff within the risk management function should possess sufficient knowledge, skills and experience on risk management techniques and procedures and sufficient

understanding of the activities of the supervised entity and its products. The risk management function should provide relevant independent information, analysis and advice on risks identified as relevant to business lines or internal units and whether they are consistent with the supervised entity's risk appetite.

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

Part 2: Internal Control Functions		
Component	**2.2**	Risk Management Function[24]
The risk management function of a supervised entity is responsible for the development and implementation of the risk management framework. It should ensure that risks relevant to its obligations under the Regulations are identified, assessed, measured, monitored, managed and properly reported by the relevant departments/functions within the supervised entity.		
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 materially impact a supervised entity's ability to perform its obligations under the Regulation, or its continued operation, are identified, assessed, measured, 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.

[24] Where the supervised entity is part of a wider group, the group should ensure that its risk management function includes the activities of the EU-based supervised entities.

	2.2.5	The risk management function should recommend improvements to the risk management framework or/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.

Internal Control Function - Information Security Management Function (only for supervised entities not subject to DORA)

63. Supervised entities operate ICT infrastructures through which they process sensitive information and disseminate it to the authorities and the public. The overarching requirement for supervised entities is to have appropriate systems, controls, and procedures to ensure the quality of the information they process.

64. As part of that requirement, ESMA expects all supervised entities to establish an information security management function responsible for the development and implementation of the information security strategy resulting in sound and robust information security policies, practices and controls within the supervised entity and with regard to third parties.

Part 2: Internal Control Functions		
Component	**2.3**	Information Security Management Function[25]
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 an information security 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

[26] OJ L 171, 29.6.2016, p. 1.

		develop a broad understanding of the supervised entity's information security requirements.
	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).

Internal Control Function - Internal Audit

65. Supervised entities need to monitor and evaluate the effectiveness of their internal control system. ESMA considers that the most effective way of achieving this is through the establishment of an independent and effective internal audit function. However, not all supervised entities may have the resources to have such a dedicated function, and in these cases the internal audit activities should be carried out through other means. For example, the activities could be assigned to a group level internal audit function or an appropriate external party.

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

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

68. The internal audit function should adhere to national or international professional standards. The work of the internal audit function should be performed in accordance with an audit plan and detailed audit programs following a risk-based approach where appropriate. In this regard, an audit plan should be drawn up at least once a year based on the annual control objectives and be approved by the Management Body.

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

70. Finally, all audit recommendations should be subject to a formal follow-up procedure by the respective levels of management to ensure and report their effective and timely resolution. The staff member in charge of the internal audit function should be able to report directly, where appropriate and on their own initiative, to the Management Body on the implementation of the corrective measures decided upon.

Part 2: Internal Control Functions		
Component	**2.4**	Internal Audit Function
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 and leading practices.
	2.4.3	The internal audit function should independently review and provide objective assurance that the supervised entity's activities, including outsourced activities, are in compliance 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 and a detailed audit programme, 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.

Internal Control Function - Review (for CRAs)

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

72. ESMA has made two new additions to the expectations related to the review function.

73. Firstly, clarifying that the review function staff responsible for the validation and/or review of a methodology, who are also involved in its development phase, should not be solely responsible or have the majority of voting right in the approval committees (Characteristic 2.5.5). This separation of duties is essential to maintain impartiality and objectivity, ensuring that the methodology is thoroughly and independently reviewed before approval.

74. Secondly, that where the Review Function is outsourced, the CRA should take into account Characteristics 1.5.6 of Component 1.5 Monitoring Activities. This includes that the CRA should have suitable internal control mechanisms to ensure that the outsourced review function consistently adheres to the regulatory requirements and maintains appropriate analytical quality standards.

Part 2: Internal Control Functions		
Component	**2.5**	Review Function
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 validating 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 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.
	2.5.5	The Review function staff responsible for the validation and/or review of a methodology, who is also involved in its development phase, should not be solely responsible or have the majority of voting right in the approval committees.
	2.5.6	In case of outsourcing of the Review Function, the supervised entity should take into account Characteristics 1.5.6 of Component 1.5 Monitoring Activities. This includes that the CRA should have suitable internal control mechanisms to ensure that the outsourced review function consistently adheres to regulatory requirements and maintains appropriate analytical quality standards.

Internal Control Function - Oversight (for BAs)

Part 2: Internal Control Functions		
Component	**2.6**	Oversight Function
The oversight function covers the main aspects of the provision of their 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 benchmarks, 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 BA Oversight Function is independent from any Management Body or function of the BA and any external party of the BA. Independence assumes there are no conflicts of interest between the other activities of the members of the Oversight Function and their duties required by the membership within the Oversight Function. The BA

		should implement an internal control operating framework to prevent and mitigate any potential conflict of interests.
	2.6.2	The BA 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 BA Oversight Function should regularly perform a self-assessment to evaluate its effectiveness and the fitness of its members for the purpose of the function and to identify potential conflicts of interests and propose areas of improvement, if necessary.
	2.6.4	The BA Oversight Function should maintain a defined and regular communication channel with the Management Body, executive senior management and other key functions. The BA Oversight Function should be 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 BA Oversight Function should maintain a defined and regular communication channel with the relevant competent authorities, including but not limited to reporting any misconduct or violation by administrators or contributors.

Questions for respondents

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

Q4. Do you have any comments on ESMA's approach to proportionality for Internal Control Functions?

Q5. Are there any other comments you wish to raise on this section?

Annexes

Annex I

Cost-benefit analysis

Introduction

75. 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-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.

76. The purpose of these Guidelines is to ensure that ESMA's expectations are shared with all registered supervised entities and future applicants to ensure a level playing field and the adoption of consistent good practice. The means by which the Guidelines will achieve this is by making clear what components and characteristics ESMA considers should be evidenced within a 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.

77. Once implemented the Guidelines will be integrated into ESMA's supervisory assessment practices and guide how ESMA supervisors interact with supervised entities in relation to their internal controls systems.

The Impact of the Draft ESMA Guidelines

78. The approach of the Guidelines is to provide a framework of recommended practices against which supervised entities can compare and judge their own internal control systems and mechanisms.

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

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

Benefits

81. The benefits of these Guidelines to ESMA, supervised entities, and regulators 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 BA, CRA, DRSP, SR and TR market, the Guidelines will likewise provide them with clarity on the practical application of the Regulations internal control requirements. For users of the supervisory entities' services, these Guidelines will contribute to assuring more robust and effective services from the supervised entities. Finally, for regulators, the Guidelines will contribute to the improvement of the quality of the data they need to fulfil their mandates and responsibilities.

Costs

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

83. 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

84. 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 Regulations. As such, Guidelines which recommend a set of measures to ensure that supervised entities are better able to meet this objective are justified on the basis that the costs of implementation will be limited to compliance assessments, revisions to internal policies and procedures, and training for staff.

Annex II

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

Scope

Who?

1. These Guidelines apply to:

   (i) EU critical benchmark administrators established in the Union and authorised by ESMA, and third-country benchmark administrators recognised by ESMA, (together, “BAs") 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; and

   (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 BA’s effective compliance with Articles 4 to 10 of BMR; (ii) a CRAs’ effective compliance with Article 6(1),(2) and (4), 9 and Annex I, Section A, of CRAR; (iii) a DRSP’s effective compliance with Articles 27f to 27i of MiFIR; and (iv) a TR’s or SR’s effective compliance with Articles 78 and 79 of EMIR.

3. These Guidelines build on and replace the Guidelines on Internal Control for CRAs.

When?

4. These Guidelines apply from [three months after the Final Report is published].

1 References, abbreviations and definitions

1.1 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[26]
CRAR	Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit ratings agencies[27]
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
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[28]
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[29]
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[30]
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[31]

1.2 Abbreviations

AI	Artificial intelligence
APA	Approved Publication Arrangement
ARM	Approved Reporting Mechanism
BA	Benchmark Administrator
CP	Consultation Paper
CRA	Credit Rating Agency
DORA	Digital Operational Resilience Act
DRSP	Data Reporting Services Provider

[26] OJ L 171, 29.6.2016, p. 1.
[27] OJ L 302, 17.11.2009, p. 1.
[28] OJ L 201, 27.7.2012, p.1.
[29] OJ L 173, 12.6.2014, p.84.
[30] OJ L 347, 28.12.2017, p. 35.
[31] OJ L 337, 23.12.2015, p.1.

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

1.3 Definitions

Management Body	For the purpose of these Guidelines, 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 the '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
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 directly supervised by ESMA, namely: ▪ BAs ▪ CRAs ▪ DRSPs (excluding consolidated tape providers) ▪ SRs

	▪ TRs

2 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.

3 Compliance and reporting obligations

3.1 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.

3.2 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.

3.3 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 4.1 and 4.2 than those established at registration or recognition.

4 Guidelines

13. In order to demonstrate that supervised entities comply with the provisions referred to in paragraph 2 of these Guidelines, supervised entities should align their policies, procedures and working practices with Sections **4.1** (Internal Control Framework) and **4.2** (Internal Control Functions) of these Guidelines.

4.1 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 working practices.

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

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.

Characteristic

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 Regulation 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

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 managing risks to the achievement of the supervised entity's main objectives. For example, this includes risks resulting from the supervised entity's use of new technologies and changes to its external risk landscape.

Characteristic

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 as part of the risk assessment process.

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

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:

i. Staff members responsible for carrying out a task are not responsible for approving the outcome of its exercise;[32]

ii. Staff members responsible for the development, implementation or approval of a task/work item are not responsible for validating, assessing and reviewing it.[33] Where this cannot be avoided, this should be mitigated by these staff members not being exclusively responsible for the activity.[34]

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.

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 relevant to the Regulations. The documentation of these controls should set out:

i. A description of the control

ii. The associated 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

---

[32] For instance, staff members in charge of carrying out business requirements analysis activities or responsible for conducting commercial / business development activities should not be involved in client / regulatory support activities. In addition, staff members responsible for system development activities should not be involved in database administration, IT operations, and IT systems and network administration and maintenance.

[33] 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 involved in their implementation; (iii) persons responsible for the validation, assessment or review of a credit rating methodology should not be involved in their development, implementation or approval.

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

vi. The frequency of execution of the control

vii. A description of the testing procedure

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 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 in all business activities to ensure that activities are approved and executed only by staff members acting within the scope of their authority.[35]

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.[36]

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.

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,

[35] 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.
[36] This includes data validation and input controls, reviews of lists for authorised access to confidential information. For CRAs, such controls apply to, inter alia, credit rating activities and the processes underlying these activities such as credit methodology/model validation.

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

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 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 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

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 as well as 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.

4.2 Internal Control Functions

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

General Principles

18. 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, review (for CRAs) and oversight (for BAs) functions should be directly accountable to the Management Body and their performance should be reviewed by the Management Body.

19. 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 Characteristic 1.1.4 applies.

20. 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;

21. 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

22. 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.

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

Segregation of duties

24. 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

25. 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

26. 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

27. 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.

28. The following sub-sections discuss key IC Functions and the characteristics that supervised entities should evidence to demonstrate the sufficient presence of each component within the supervised entity.

Component 2.1 Compliance Function

29. 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, Independent Non-Executive Directors (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 needs to 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 should assess, and where appropriate in conjunction with other relevant functions, 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

30. The risk management function of a supervised entity is responsible for the development and implementation of the risk management framework. It should ensure that risks relevant to its obligations under the Regulations are identified, assessed, measured, monitored, managed and properly reported by the relevant departments/functions within the supervised entity.

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 materially impact a supervised entity's ability to perform its obligations under the Regulations, or its continued operation, are identified, assessed, measured, 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)

31. 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 requirements.

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

32. 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 and leading practices.

2.4.3 The internal audit function should independently review and provide objective assurance that the supervised entity's activities, including outsourced activities, are in compliance 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 and a detailed audit programme, 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)

33. 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 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 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.

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 right in the methodology approval committees.

2.5.6 In case of outsourcing of the review function, the CRA should take into account Characteristics 1.5.6 of Component 1.5 Monitoring Activities. This includes that 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 BAs only)[37]

34. The oversight function covers 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 BA Oversight Function is independent from any management body or function of the BA and any external party of the BA. Independence assumes there are no conflicts of interest between the other activities of the members of

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

the Oversight Function and their duties required by the membership within the Oversight Function. The BA should implement an internal control operating framework to prevent and mitigate any potential conflict of interests.

2.6.2 The BA 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 BA 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 interests and propose areas of improvement, if necessary.

2.6.4 The BA Oversight Function should maintain a defined and regular communication channel with the Management Body, executive senior management, and other key functions. The BA Oversight Function should be 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 BA Oversight Function should maintain a defined and regular communication channel with the relevant competent authorities, including but not limited to reporting any misconduct or violation by administrators or contributors.

4.3 Annex III

Summary of questions

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

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

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

Q4: **Do you have any comments on ESMA's approach to proportionality for Internal Control Functions?**

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