RegCORE – Client Alert

ESMA consults on draft guidelines on the internal control systems framework for some of its supervised entities

January 2025

Financial Services

ESMA consults on draft guidelines on the internal control systems framework for some of its supervised entities

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact the EU RegCORE Team
de_regcore@pwc.com

QuickTake

On 19 December 2024 the European Securities and Markets Authority (**ESMA**) published a consultation paper on draft guidelines[1] related to the internal control systems (**ICS**) framework of some of its supervised entities – specifically for benchmark administrators (**BA**s) and market transparency infrastructure provider (**MTIP**s) the latter being comprised of trade repositories (**TR**s), data reporting services providers (**DRSP**s) and securitisation repositories (**SR**s).

The proposed draft guidelines build on ESMA's existing Internal Control Guidelines currently in place for credit rating agencies (**CRA**s) and propose to extend those regulatory principles and supervisory expectations to the aforementioned body of BAs and MTIPs when operating in the EU. This extension means that the existing guideline would be replaced by this new comprehensive guideline proposed in the consultation paper and the draft guidelines to form one central set of rules applicable to all BAs, CRAs and MTIPs with respect to their ICS frameworks.

As assessed in this Client Alert, the draft guidelines outline ESMA's expectations for the components and characteristics of an effective ICS framework ensuring (i) a strong framework, detailing the internal control environment and informational aspects; and (ii) effective internal control functions, including compliance, risk management and internal audit (each an **ICF**). The draft guidelines equally reflect ESMA's supervisory expectations on how supervised entities reflect the impact and risk of information and communications technology (**ICT**) on business operations and the ICS framework. Welcomingly, the draft guidelines also explain in greater detail how ESMA applies proportionality in its expectations regarding the internal controls of a supervised entity.

[1] Available here.

The consultation is primarily addressed to national competent authorities (**NCA**s) as well as the body of CRAs, BAs and MTIPs within the scope of ESMA supervision as well as financial groups with a controlling participation in such persons. ESMA will review the stakeholder feedback received to this consultation by 18 March 2025 and expects to publish a final report containing the final version of the guidelines by fourth quarter of 2025. Following the publication of the final report, ESMA will translate the guidelines into the official languages of the EU and request clarifications from the NCAs, whether they will apply the guidelines.[2] This process takes up to three months so that the new guidelines in final form are likely to become applicable by early 2026 at the earliest.

Key takeaways from the draft guidelines

ESMA currently directly supervises all EU CRAs, SRs and TRs as well as certain BAs and DRSPs. The EU Regulations granting ESMA the mandate for direct supervision each contain a number of requirements relating to the ICS framework that supervised entities must maintain. There are slight differences between those requirements. Equally, as ESMA notes, these EU Regulations provide limited details on how the various components and characteristics of the ICS should integrate and function together as complementary parts of a unified framework.

In an effort to centralise and upgrade those requirements ESMA is using the consultation paper and proposed draft guidelines to build off but equally replace the existing ESMA-published Guidelines on

[2] As explored in other Client Alerts the term "should" in the context of a drafting of EU legislative but also other rulemaking instruments including supervisory guidance instruments such as guidelines, carries a specific connotation that is important to understand and how it differs to the use of the term "must". To recap: "Must": Indicates a mandatory requirement. It denotes an obligation that is legally enforceable and must be followed without exception. Failure to comply with a "must" requirement can result in legal penalties or sanctions. "Should": Indicates a recommendation rather than a mandatory requirement. It suggests that the action or standard being described is advisable and represents best practice, but it is not (necessarily) legally enforceable. Compliance with "should" is encouraged but not obligatory but can carry adverse supervisory consequences from ESMA. Equally, "should" carries only a limited amount of optionality – especially when contrasted with the word "may". In certain contexts, "should" can effectively mean "must" due to the following reasons:

1. **Regulatory interpretation:** If supervisory authorities interpret "should" as a de facto requirement, entities may feel compelled to comply to avoid regulatory scrutiny or reputational damage. In practice, this can make "should" functionally equivalent to "must."
2. **Industry standards:** In some cases, industry standards and best practices may evolve to the point where not following a "should" recommendation is seen as non-compliance. This can create a de facto obligation to adhere to the recommendation.
3. **Risk management:** Financial institutions and other entities may treat "should" as "must" in their internal policies and procedures to mitigate risk. By adhering to supervisory guidelines, they can demonstrate a commitment to best practices and reduce the likelihood of regulatory action.
4. **Supervisory pressure:** Supervisory authorities may exert pressure on entities to comply with "should" recommendations, especially in areas of high regulatory focus. This can create an environment where "should" is effectively treated as "must."
5. **Legal and compliance frameworks:** In some jurisdictions, national laws or regulations may incorporate EU supervisory guidelines by reference, making "should" recommendations legally binding. This can occur when NCAs seek to align local regulations with EU standards, which is effectively what ESMA does when asking NCAs to confirm whether they will or will not apply an ESMA guideline.

While the EU legislative and regulatory policymakers (and drafters) are slowly moving to adopting better use of "plain language conventions" to avoid ambiguous terms it is important to note that where a "should" is accompanied by rationale behind an outcome/recommendation or practical examples, this helps entities understand the importance and potential benefits of following the guideline.

Even if the above represents an English language and legal view of wording, the EU comprises multiple Member States with diverse legal traditions and languages. Using "must" instead of "should" or at the very least understanding when "should means must" would help harmonise the interpretation and application of rulemaking instruments across jurisdictions. "Must" is more likely to be consistently translated across different languages, maintaining the integrity of the legal requirement. "Should," on the other hand, may be translated in ways that imply varying degrees of obligation, leading to inconsistencies. As an example, "should" is often translated in German language versions of texts as "sollte" and in French as "devrait" both which have a higher degree of optionality implied in the respective term than may be the case in English.

Lastly, it is important to note that while the text of the guidelines set out the components and respective characteristics in the ICS and ICF parts with a heavy use of "should" the introduction to the guidelines clearly state (page 39 at para. 3.1 sub-para 6) that "…supervised entities must make every effort to comply with the guidelines." Thus, creating a framework where a "should" would be best interpreted as a "must" – subject to ESMA's application of proportionality where it deems it correct to do so.

Internal Control for CRAs. The proposed draft guidelines once finally approved will serve as a central, comprehensive and consistent set of rules on ICS frameworks applicable to all the entities ESMA directly supervises (except for non-EU i.e., third country central counterparties. As ESMA equally notes, the outcomes in the draft guidelines also aim to embed a number of its expectations that have been communicated bilaterally with certain entities during supervisory engagements. ESMA further notes that such an approach can help ESMA take a consistent approach to its supervisory assessment of ICS practices across all entities it supervises.

The harmonisation that ESMA is looking to achieve also extends to rolling out supervisory expectations on the use of artificial intelligence (**AI**) as well as ICT risk management for entities subject to the EU's Regulation known as the Digital Operational Resilience Act (**DORA**). This, in particular, concerns the mapping and managing of technology risk from external and internal sources and the integration of ICT solutions into supervised entities' ICS frameworks.

ESMA's proposed guidelines are structured in two key parts, namely:

1. a ***supervised entity's overall ICS framework*** – comprised of the following five components: (i) control environment; (ii) risk management; (iii) control activities; (iv) information and communication; and (v) monitoring activities – which should be present and reflected in the policies, procedures and working practices of supervised entities; and

2. the ***roles and responsibilities of different ICF within the ICS framework*** – comprised of a further five components which match the specific ICF designations: (i) compliance; (ii) risk management; (iii) information security management (only for those supervised entities not in the legislative remit of DORA); (iv) internal audit (which for CRAs is the "Review function"); and (v) the oversight function (which is relevant for BAs). ESMA sets out the actions a supervised entity's management body should take to establish a strong control environment and views on setting the right "tone from the top" as well as the role of individual ICFs, their reporting lines and whether such ICF roles can be merged or combined with other functions.

The text of the proposed guidelines is set out in Annex II to the consultation paper. Over the course of 17 pages the guidelines set out key outcomes that BAs, CRAs and MTIPs will need to observe the following components and characteristics under the proposed guidelines' two parts. These can be summarised as follows:

- ***Supervised entity's overall ICS framework***

    - **General principles:** the management body of the supervised entity is accountable for overseeing and approving all components of the ICF. The executive senior management is responsible for establishing, implementing and updating the written internal control policies, procedures and working practices. In summary, the management body and executive senior management have distinct but complementary roles in ensuring the effectiveness of the internal control framework. The management body focuses on oversight and accountability, while the executive senior management is responsible for the establishment, implementation and continuous improvement of internal control policies and procedures. Both are essential for maintaining a robust internal control environment that meets regulatory requirements and supports the entity's operational resilience.

    - **Control environment:** The control environment is foundational for an effective system of internal controls. The executive senior management must establish a strong culture of ethics and compliance through policies and procedures governing staff conduct. These policies should ensure compliance with relevant regulations and corporate values, clarify expectations for honesty and integrity and outline potential disciplinary actions for misconduct. Written internal control policies, mechanisms and procedures must be maintained and regularly updated. An entity (and its senior management) must retain responsibility for any (intragroup) outsourced activities.

    - **Risk management:** involves a dynamic process for identifying, assessing and managing risks that could impact the entity's ability to meet its objectives. This includes setting risk appetite and tolerance levels, conducting comprehensive risk assessments using a defined methodology and continuously evolving the risk assessment methodology and process. This includes identifying changes that could impact the ICS.

    - **Control activities:** are designed to mitigate risks through preventative, detective, corrective, or deterrent measures. Key characteristics include segregation of duties (in particular to manage

risks of conflicts of interest, fraud and human error), documentation of policies and procedures covering all business activities, documented controls and control testing, clear designation of responsibilities for carrying out controls and testing, authorisation processes and measures to detect and act upon inappropriate activities. For entities not subject to DORA, ICT general controls are also required to ensure digital operational resilience.

- **Information and communication:** are critical for ensuring that accurate, complete and high-quality information is shared internally and externally. This includes establishing upward communication channels, such as whistleblowing procedures and downward communication channels to keep staff informed about internal control objectives and responsibilities. Firms should document their communication processes, including the roles and responsibilities of staff involved in internal and external communication. Equally, clear escalation procedures should be in place for instances of disagreement between internal control functions and operating units. ESMA views this as crucial in timely resolution of conflicts and ensuring that critical issues are addressed promptly.

- **Monitoring activities:** involves regular evaluations of the (entirety as well as individual components of the) ICS conducted at different business levels, designed to check compliance with legal and regulatory requirements and include regular or thematic evaluations. Deficiencies identified should be reported to the management body and executive senior management, with timely implementation of corrective actions. The guidelines also highlight the importance of actively monitoring outsourced business processes.

- ***Roles and responsibilities of different ICF within the ICS framework***

  - **Compliance function:** is responsible for monitoring and reporting on the entity's compliance with regulatory obligations. This includes advising staff on compliance matters, proactively identifying risks and ensuring that compliance monitoring is carried out through a structured program. The compliance function should operate independently of business lines, provide regular reports to the management body and ensure a structured compliance monitoring programme. The function should also assess the impact of changes in the legal or regulatory environment and ensure compliance policies are followed.[3]

  - **Risk management function:** develops and implements the risk management framework, ensuring that all relevant risks are identified, assessed, monitored and managed. This function should operate independently of business lines, monitor the risk profile against the entity's risk appetite and recommend improvements to the risk management framework.

  - **Information security management function (for non-DORA firms):** is responsible for developing and implementing information security policies and practices. This includes promoting an information security culture and awareness program as well as reporting on the status of the information security management system and risks. The information security management system should include controls to ensure the authenticity, confidentiality, integrity and availability of information as it is processed from source to ultimate user. Firms should equally have controls in place to ensure the availability, confidentiality and integrity of data. This includes data validation, processing controls and data file control procedures.

  - **Internal audit function (which for CRAs is the "review function"):** provides independent assurance on the effectiveness of the ICS. This function should follow a risk-based approach, adhere to international standards and report regularly to the management body. Internal audit recommendations should be subject to formal follow-up procedures to ensure timely implementation. For CRAs, the review function is responsible for reviewing and validating credit rating methodologies. The review function should operate independently of business lines and ensure that methodologies are thoroughly reviewed before approval. The guidelines also address

[3] Horizon scanning, risk mapping and capturing changes to policies and procedures are all aspects that PwC Legal's Rule Scanner and trusted managed (legal) solutions are designed to help with.

the outsourcing of the review function, emphasising the need for suitable internal control mechanisms.

- **The Oversight function (relevant for BAs):** covers the main aspects of benchmark provision, including reviewing methodologies, managing third parties and reporting misconduct. This function should be independent and have clear policies and procedures for its responsibilities.

ESMA is clear that it will permit group functional lead concepts of ICF roles provided that the staff and designated holders of an ICF in a supervised entity have sufficient resources and that the entity is staffed with individuals with sufficient expertise plus technical knowledge of the supervised entity's activities and the associated risks to discharge their duties.

Where supervised entities have outsourced the operational tasks of an ICF to group level or to an external party, ESMA considers that the supervised entity retains full responsibility for the activities of the outsourced ICF. 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. As ESMA notes in an 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." Accordingly, 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 respective supervised entity. It should be noted with respect to the above that ESMA may apply greater supervisory scrutiny in respect of ICFs being outsourced outside of the EU and require the supervised entity to justify how the person to whom an ICF is outsourced can evidence sufficient expertise and technical knowledge of the supervised entity's EU operations.

Welcomingly, ESMA will apply proportionality in the application and thus supervision of the guidelines. While all ESMA supervised entities are expected to demonstrate the components and characteristics of an effective ICS framework, ESMA will "calibrate" its expectations on compliance with the roles and responsibilities of different ICF within the ICS framework. ESMA's decision to apply proportionality will be dependent on an evaluation of a supervised entity's conditions (including a recognition that these may have changed since ESMA's first review at authorisation/registration). Such evaluation will be according to the entity's nature (business and type of operations including criticality of its core and ancillary products/services), scale, complexity and overall risk profile of a given supervised entity as well its group structure/relationships, shared services/outsourcing and connectivity to the market and how such characteristics may affect investor protection as well as the orderly functioning of the market and financial stability.

Outlook

Given ESMA's drive towards centralisation and enhancement of ICS frameworks, entities under its supervision, including BAs, CRAs and MTIPs, should proactively review and adjust their ICS frameworks. The draft guidelines, which are expected to be finalised by late 2025 and become applicable by early 2026, emphasise a comprehensive and consistent approach to internal controls. Some entities may wish to review their policies, procedures and working practices to ensure they align with ESMA's more prescriptive expectations, in particular in areas such as risk management, compliance and internal audit functions. This may necessitate amendments to existing documentation and operational practices to demonstrate compliance and operational resilience. Some entities may wish to consider the potential need for changes in their documentation with suppliers, counterparties, clients and customers to ensure alignment with the new guidelines.

Furthermore, the guidelines' emphasis on proportionality means that ESMA will tailor its supervisory expectations based on the nature, scale, complexity and risk profile of each supervised entity. This approach requires entities to not only meet the baseline requirements as they will be reevaluated for compliance but also to be prepared for a nuanced evaluation of their ICS frameworks or to justify why proportionality should apply. Ultimately, early engagement with the consultation process and pre-emptive adjustments will be crucial for entities to navigate the upcoming regulatory landscape effectively and maintain compliance with ESMA's evolving standards.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from relevant related developments. We have assembled a multi-disciplinary and multijurisdictional team of sector experts to support clients to navigate challenges and seize opportunities as well as to proactively engage with their market stakeholders and regulators.

In order to assist firms in staying ahead of their compliance obligations we have developed a number of RegTech and SupTech tools for supervised firms. This includes PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from more than 2,000+ legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms' relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com