Baker McKenzie.

Legal Update

November 2026

European Union: Revised EBA Governance Guidelines Balance Accountability with Flexibility

In brief

On 5 November 2026, the European Banking Authority (EBA) published its revised Guidelines on internal governance (EBA/GL/2026/10) under the Capital Requirements Directive ("**CRD**"), following the entry into force of Directive (EU) 2024/1619 ("**CRD VI**").

The revised Guidelines replace the previous EBA Guidelines on internal governance (EBA/GL/2021/05) and update the existing framework to reflect the changes introduced by CRD VI and broader regulatory developments, including in relation to digital operational resilience, environmental, social and governance (ESG) risks and risk management.

In particular, the revised Guidelines provide further clarity on the responsibilities of the management body; the mapping of roles and duties of members of the management body, senior management and key function holders; individual statements of roles and duties; organisational structures and the "know your structure" principle; conflicts of interest; and the internal control framework.

The revised Guidelines apply to:

- Credit institutions within the scope of the CRD, including central bodies referred to in Article 10 of Regulation (EU) No 575/2013;
- Investment firms subject to Title VII of the CRD, pursuant to Article 1(2) and (5) of Regulation (EU) 2019/2033;
- Financial holding companies and mixed financial holding companies that have been granted approval in accordance with Article 21a(1) of the CRD, having regard also to Article 3(3) of the CRD; and
- Third-country branches ("**TCBs**"), as defined in Article 47(3), point (1), of the CRD, in respect of the specific provisions of the Guidelines applicable to them.

The revised Guidelines apply on an individual, sub-consolidated and consolidated basis, in accordance with Article 109 of the CRD. They are intended to accommodate all existing board structures and do not advocate any particular governance model.

The Guidelines provide for application two months after their publication in all EU official languages.

Contents

In brief

Key takeaways

In more detail

- From allocation of responsibilities to demonstrable accountability
- Individual statements of roles and duties
- "Know your structure" and sufficient substance
- Stronger ownership by the management body
- Governance of ICT, ESG, AI and emerging risks
- Reinforced three-lines model and internal control functions
- More robust governance for new products and material changes
- Third-country branches and CRD VI
- Risk culture and responsible business conduct
- Proportionality and reduced prescriptiveness

Practical implications for institutions: what needs to be done?

Local implementation of the Guidelines

- Luxembourg
- The Netherlands
- Spain

Key takeaways

- Institutions will need to maintain a clear mapping of duties covering members of the management body, senior management and key function holders, supported by individual statements of roles and duties.
- Management bodies remain ultimately accountable for governance and risk oversight. The revised Guidelines reinforce expectations around effective challenge and oversight, including in relation to information and communication technology (ICT) and operational resilience, ESG risks, emerging technologies and other financial and non-financial risks.

- Governance structures must be transparent and supported by sufficient substance. Institutions and groups should be able to explain their organisational structures, intragroup dependencies and allocation of responsibilities, while avoiding unnecessarily complex structures or arrangements that could result in EU entities operating as “empty shells” or “letter-box entities”.
- The revised Guidelines extend governance expectations to areas such as ICT, ESG, AI, third-party arrangements and material business changes, while adopting a more principles-based approach that gives institutions flexibility as to how certain requirements are implemented and documented.
- A targeted implementation review is the practical next step. Institutions already complying with EBA/GL/2021/05 should not need to redesign their governance frameworks entirely, but should review their allocation of responsibilities, governance documentation, organisational charts, committee mandates, reporting lines and internal control arrangements against the revised requirements.

In more detail

The revised Guidelines build on the existing internal governance framework while introducing targeted changes to reflect CRD VI and the evolving risk and regulatory landscape. In particular, they place greater emphasis on clear and demonstrable accountability, effective management body oversight and robust organisational arrangements, while embedding considerations relating to ICTand operational resilience, ESG risks and emerging technologies more firmly within institutions' governance frameworks. At the same time, the final Guidelines retain a proportionate and principles-based approach, allowing institutions a degree of flexibility in how they implement and document the relevant requirements.

The EBA states that these Guidelines should be read in conjunction with other relevant guidelines, including its guidelines on the sound management of third-party risk, the joint EBA and European Securities and Markets Authority (ESMA) guidelines on the assessment of the suitability of members of the management body and key function holders, and the EBA guidelines on sound remuneration policies, the management of ESG risks and the supervisory review and evaluation process (SREP).

Against this background, in-scope institutions should pay attention to the following areas.

From allocation of responsibilities to demonstrable accountability

One of the most important developments is the introduction of a formal “mapping of duties”, in accordance with Article 88(3) of the CRD. Institutions must draw up, maintain and update a mapping of the individual duties of persons forming part of their governance arrangements. The mapping should be proportionate to the institution's size, nature, organisational structure and complexity, but sufficiently comprehensive to enable the institution to identify gaps in the allocation of responsibilities. The mapping must, among other things:

- Provide an overview of the roles and duties of members of the management body, senior management and key function holders;
- Explain how the management and supervisory functions and their committees contribute to decision-making;
- Identify relevant reporting lines and relationships with committees and, where applicable, other group entities; and
- Remain coherent with the individual statements of roles and duties.

The management body must approve the mapping, which must be available to the competent authority upon request.

Importantly, following concerns raised during the consultation regarding operational burden, the final Guidelines adopt a more principles-based approach. Institutions are not necessarily required to create one standalone document and may rely on a set of existing documents or a central repository, provided these collectively give a sufficiently clear and complete overview. This represents a significant practical shift compared with the 2021 framework: institutions must be able not only to describe their organisational architecture, but also to demonstrate clearly who is responsible for what and how individual responsibilities fit into the institution's overall governance structure.

For groups, implementation may require a broader review of the allocation of responsibilities between parent, subsidiary and group-level functions to ensure that local and group governance arrangements are reflected consistently in the mapping of duties.

Individual statements of roles and duties

The mapping is complemented by a significantly enhanced individual accountability framework. Each member of the management body in its management function, each member of senior management and each key function holder must have an individual statement of their roles and duties. The statements should be concise, but sufficiently detailed to establish clearly the individual's responsibilities. They must be kept up to date, align with the overall mapping of duties and be signed by the relevant individual. Where a person performs several roles within the same institution, a single statement may cover those roles. However, where that person performs roles in several institutions within a group, separate statements are required for each institution.

The EBA has included an optional template in Annex I to the Guidelines specifying, among other matters, the person's role, duties, effective dates, time commitment and any shared responsibilities.

The practical challenge for institutions will therefore be not only to prepare these documents initially, but also to establish a governance process to ensure that they remain aligned following reorganisations, changes to organisational charts or reporting lines, and appointments or departures.

“Know your structure” and sufficient substance

The revised Guidelines also reinforce the “know your structure” principle. The management body must fully understand the institution's legal, organisational and operational structure and ensure that it remains consistent with the institution's business strategy, risk strategy and risk appetite. For banking groups, this extends to understanding:

- The purpose and activities of individual entities;
- Relationships and dependencies between entities;
- Intragroup exposures;
- Funding, capital and liquidity dependencies;
- Group-specific operational risks; and
- The impact of the overall structure under both normal and adverse circumstances.

Institutions must avoid opaque or unnecessarily complex structures and be able to explain their rationale to supervisors. This is particularly relevant where institutions rely extensively on outsourcing, intragroup servicing or back-to-back arrangements. The Guidelines expressly emphasise that EU institutions must retain sufficient substance and should not effectively become “empty shells” or “letter-box entities”.

Stronger ownership by the management body

The Guidelines reinforce expectations regarding the management body's ultimate responsibility for internal governance. The management body must set, approve and oversee the institution's business and risk strategies and its internal governance and control framework, encompassing financial and non-financial risks, operational resilience, AML/CFT, ESG, remuneration, conflicts of interest and the integrity of financial and operational reporting. The supervisory function is expected to constructively challenge the management function and critically review proposals, information and decisions, rather than operate as a passive recipient of information.

In practice, institutions should therefore consider whether board and committee minutes, management information and escalation processes sufficiently evidence genuine challenge, discussion and follow-up.

Governance of ICT, ESG, AI and emerging risks

Another significant evolution from the 2021 framework is the express incorporation of newer and non-financial risks into mainstream governance expectations. The Guidelines reflect the interaction between CRD VI and the EU Digital Operational Resilience Act (DORA) and expressly include network and information systems within the governance framework. They also address the growing use of cloud services, artificial intelligence and other emerging technologies. ESG considerations are more deeply embedded into risk management, including the requirement under CRD VI to consider ESG risks over short-, medium- and long-term horizons, with the long-term horizon extending to at least 10 years.

These requirements reinforce an important supervisory message: cyber, ICT, ESG and technology risks should not be treated purely as specialist IT, sustainability or compliance topics. They form part of the institution's overall governance and management body responsibilities.

Reinforced three-lines model and internal control functions

The revised Guidelines provide a clearer articulation of the “three lines of defence” model:

- First line: business lines and other operational functions own and manage their risks;
- Second line: Risk Management and Compliance monitor, challenge and provide an institution-wide view of risk; and
- Third line: Internal Audit independently assesses the effectiveness of governance and of the first and second lines.

Internal control functions must have adequate authority, stature, resources, access to information and appropriate ICT capabilities. Their heads must have direct access to the management body in its supervisory function and be capable of escalating concerns directly. Independence should also be reflected in organisational separation: control staff should not perform the operational tasks they monitor, and heads of control functions should not be subordinate to persons responsible for the activities they oversee. Risk and Compliance may be combined where justified under the proportionality principle, subject to documented conflict-of-interest safeguards. Internal Audit cannot be combined with another internal control function.

More robust governance for new products and material changes

The revised Guidelines broaden governance expectations around the New Product Approval Policy beyond traditional product launches. The framework should capture material changes involving, among other things, new markets, services and products, material process or ICT changes, new third-party arrangements, M&A transactions, new entities or SPVs and significant changes to risk-management arrangements. Importantly, new products and significant changes should undergo a systematic prior assessment and a documented opinion from Compliance, with early involvement of Risk Management.

Third-country branches and CRD VI

The revised Guidelines also contain substantially more developed requirements for third-country branches, reflecting CRD VI. Among other requirements:

- At least two persons located in the relevant Member State must effectively direct the branch's business;
- Sufficient local presence, resources and internal controls must be maintained;
- Reliance on third-party and intragroup arrangements must not undermine effective local governance or regulatory compliance;
- ICT risks must be appropriately governed, including under DORA; and
- Risks connected with transactions having an EU nexus under back-to-back booking arrangements are expected to be managed from the EU.

These provisions will be particularly relevant for non-EU banking groups operating in the EU.

Risk culture and responsible business conduct

Institutions should promote an effective risk culture aligned with their risk appetite through clear management accountability, open communication and challenge, appropriate incentives and role-specific training. Risk management should remain embedded in the day-to-day responsibilities of business units. The management body should also promote ethical and professional standards through a code of conduct, supported by appropriate monitoring, escalation of breaches and regular reporting.

Proportionality and reduced prescriptiveness

The revised Guidelines reaffirm the principle of proportionality set out in Article 74(2) of the CRD. Internal governance arrangements should be appropriate to an institution’s size, internal organisation and the nature, scale and complexity of its activities, as well as its individual risk profile and business model. Accordingly, significant or more complex institutions are expected to maintain more sophisticated governance arrangements, while smaller and less complex institutions may adopt simpler arrangements.

Reflecting industry feedback during the consultation, the final Guidelines also take a more proportionate and principles-based approach to several new requirements. This flexibility does not, however, dilute the underlying governance expectations: institutions must remain able to demonstrate clearly how responsibilities and accountability are allocated and how their governance arrangements operate effectively in practice.

Practical implications for institutions: what needs to be done?

For institutions already operating in accordance with the 2021 framework, the revised Guidelines do not entail a complete redesign of their governance framework. They will, however, require a targeted review of existing governance arrangements and documentation.

In particular, institutions should assess whether their existing allocation of responsibilities can be translated into compliant individual statements and a consolidated mapping of duties, and whether these documents are consistent with existing governance policies, organisational charts, committee mandates, delegation arrangements and reporting lines.

For banking groups, particular attention should also be given to the allocation of responsibilities between parent, subsidiary and group-level functions, including the interaction between local and group reporting lines.

The revised Guidelines represent an important implementation exercise, particularly in terms of documenting and demonstrating individual accountability, even where the underlying governance structure itself does not require material change.

Local implementation of the Guidelines

Luxembourg

For Luxembourg institutions, the revised EBA Guidelines will have a further local implementation impact.

When CRD VI was transposed into national law, the CSSF expressly indicated that the new governance framework introduced into the amended Law on the Financial Sector ("**LFS**") would be supplemented by the revised EBA Guidelines and that Circular CSSF 12/552 would subsequently be updated to ensure maximum alignment with the European framework.

Accordingly, while the CRD VI requirements already introduced into the LFS apply directly, Luxembourg institutions should expect a forthcoming revision of Circular CSSF 12/552 reflecting the more detailed requirements of the revised Guidelines. This may require a further review and adjustment of existing Luxembourg governance arrangements and documentation once the revised Circular is published.

The Netherlands

For institutions authorised in the Netherlands, the revised EBA Guidelines will have a further local implementation impact.

The Netherlands has implemented CRD VI through amendments to the Dutch Financial Supervision Act ("**Wft**") and its implementing rules. These measures provide a binding legal basis for enhanced internal governance requirements, including rules on key function holders, allocation of management responsibilities, internal controls and third-country branches.

The Dutch Central Bank ("**DNB**") will apply the revised EBA Guidelines and use them as a benchmark in SREP reviews, governance assessments, fit-and-proper supervision and enforcement of the underlying Dutch CRD VI requirements. DNB has been very active and vocal on DORA compliance and it is expected that DNB will be similarly active in getting institutions to quickly incorporate the additional non-financial risks requirements under the EBA Guidelines into their governance and organisation.

Spain

For Spanish institutions, the revised EBA Guidelines will have both an immediate and a prospective impact.

As CRD VI has not yet been transposed into Spanish law, the new governance requirements introduced by CRD VI do not yet apply at national level. However, the revised Guidelines also reflect governance requirements stemming from other frameworks already applicable in Spain, including DORA and the existing AML/CFT and internal governance requirements.

This is particularly relevant in light of the Bank of Spain's 2026 supervisory priorities. These include a horizontal review of governance, focused on remedying deficiencies identified in internal control functions, and a horizontal review of the application of DORA, both of which are areas addressed by the revised Guidelines. Accordingly, Spanish institutions should assess their existing governance arrangements against the revised Guidelines, while also taking them into account as part of their forward-looking CRD VI implementation planning.

Contact us



Tim Alferink
Partner
tim.alferink@bakermckenzie.com



Paula De Biase
Partner
paula.debiase@bakermckenzie.com



Laurent Fessmann
Partner
laurent.fessmann@bakermckenzie.com



Jean-François Trapp
Partner
jean-francois.trapp@bakermckenzie.com



Ana Vazquez
Counsel
ana.vazquez@bakermckenzie.com

© 2026 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.