06 November 2025

EBF COMMENTS ON THE EBA GUIDELINES ON INTERNAL GOVERNANCE

Main comments:

- **Need of respect for national governance frameworks and national laws:** certain provisions of the Guidelines may be overly prescriptive and detailed, which could risk transforming guidance into de facto binding requirements. Proportionality should therefore be interpreted broadly, considering not only the size, complexity and risk profile of institutions, but also the diversity of national governance frameworks and board structures across the European Union, which reflect deliberate choices by both national legislators and the EU legislator. **It is essential that the Guidelines respect national law frameworks, as envisaged in CRD**. In several Member States, national law provides for board systems where the supervisory and the management function are co-present in the body. In such systems, for instance, it is not feasible to individualise responsibilities as suggested in the draft Guidelines, for example by allocating duties to non-executive members or distinguishing between management and supervisory functions. The Guidelines should explicitly acknowledge this reality and avoid imposing expectations that conflict with national law. Moreover, the Guidelines should not undermine the principle of collective responsibility of the management body, irrespective whether it concerns a one-tier or two-tier board system. In this sense, **the removal of the following provisions in paragraph 8 of the Guidelines should not take place**: "*When implementing these guidelines, competent authorities should take into account their national law and specify, where necessary, to which body or members of the management body those functions should apply*". This removal is not coherent considering the changes introduced by the CRD VI. Furthermore, the legal nature of the CRD VI is that of a "*directive*" and, therefore, it has to be transposed by the Member States into the national law with the consequent room for any speciality under national law provided that it does not conflict with the CRD VI. Therefore, we do not understand the reason for removing said provisions of paragraph 8 which are already and currently existing under the EBA Guidelines on internal governance (2021). We believe it is important that the Guidelines explicitly recognise that the diversity of governance frameworks in the EU reflects deliberate choices by both national legislators and the EU legislator. While paragraph 26 of the Consultation Paper acknowledges this diversity, some provisions do not embed these principles, creating an intrinsic contradiction. The CRD framework was designed to accommodate different legal systems, and imposing a uniform governance model through soft law would undermine this balance. By preserving references to national law, the EBA can ensure that governance arrangements remain consistent with national legal environments while achieving sound risk management and effective oversight. Similarly, in connection with the variety of national governance regimes, paragraph 9 of the Guidelines should maintain the reference to the possibility of appointing an internal executive body (e.g. executive

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

committee, chief executive officer (CEO), management team or executive committee) as permitted under certain national laws.

- Article 88(1) of CRD, as last amended, unconditionally prevents the chair of the management body in its supervisory function from simultaneously exercising the functions of a CEO. However, CRD does not prevent the chair from exercising other executive functions within the institution and thus qualifying as an executive member of the management body. The executive chair role is also permitted under national laws of certain Member States and is expressly recognized in paragraph 62 of the Basel Committee on Banking Supervision's Corporate Governance principles for banks: "*[t]o promote checks and balances, the chair of the board should be an independent or nonexecutive board member. In jurisdictions where the chair is permitted to assume executive duties, the bank should have measures in place to mitigate any adverse impact on the bank's checks and balances, e.g. by designating a lead board member, a senior independent board member or a similar position and having a larger number of non-executives on the board.*" [emphasis added]. In light of the foregoing, **the recommendation to implement strong checks and balances where the chair assumes executive duties should not be removed from paragraph 37 of the Guidelines, as they have proven successful to avoid an excessive concentration of power and are aligned with relevant national laws**. Deleting this long-accepted recommendation throws unjustified and concerning doubts on its effectiveness within institutions with executive chairs that are not based on empirical evidence. **If these recommendations were to be deleted, the first sentence of paragraph 37 should be deleted in consequence.** The recommendation to have a non-executive chair is not justified or based on any reasoning or empirical evidence.[1] Moreover, recent supervisory experience and past financial crises have shown that institutions with different board structures (whether one-tier or two-tier, with executive or non-executive chairs) can be equally exposed to governance and financial failures. These arguments underline the importance of avoiding a one size fits all approach and instead focusing on ensuring that each institution has robust checks and balances, effective risk management and a strong culture of accountability, rather than imposing a uniform model across the Union.

- In the same vein, we are highly concerned with the risks of guidelines 107 a and b to limit the access of CEOs to the Board of directors within Groups. Those

[1] Several research and studies conclude that having an executive chair does not have a negative impact on the bank's governance or results. For instance:

- "Independent Chairman Research Spotlight" study points out that "most research finds no evidence that independence status impacts corporate outcomes on average" and concludes that "the evidence suggests that the independence status of the chairman is not a material indicator of firm performance or governance quality" (David F. Larcker and Brian Tayan. Corporate Governance Research Initiative. 2020. Stanford Graduate School of Business).
- In "Separation of Chair and CEO Roles", reference is made to American and Canadian studies which have concluded that non-executive chairs are not inherently more effective (Matteo Tonello. The Conference Board. 2011. Harvard Law School Forum on Corporate Governance).

guidelines are not envisaged by CRD and in direct contradiction with national corporate laws which do not provide for any such limitation and are not adapted to the specific models of company governance. It highly limits the organizational flexibility of banking institutions. It also creates legal uncertainty and risk of litigation. Hence we ask for the removal of guidelines 107a and 107b.

- **Mapping of duties and statements of roles:** the Draft Guidelines include very specific requirements on the mapping of duties, individual statements, reporting lines, and organisational structures. While transparency is important, this degree of prescription risks creating rigid compliance exercises rather than fostering effective governance. In practice, institutions may be forced to focus on producing documentation to satisfy supervisory checklists instead of tailoring governance arrangements to their specific size, complexity, governance and business model, which does not fit with the existing trend towards simplification in the EU and must be avoided. In any case the EBA Guidelines should clarify that the mapping of duties is not required neither for the management body in its supervisory function nor to be performed by the management body in its management functions with the level of detail envisaged in the Guidelines.

- CRD VI confirms that not all Key Function Holders, but the heads of the internal control functions and CFO, only remain subject to both internal (by the bank) and external (by the supervisor) fit and proper assessments. Art. 91a (5) explicitly limits the scope of external supervisory screening to the heads of internal control function and the CFO. This raises questions regarding the scope of the internal assessments. Based on the institution's definition of KFH, a broader group of people may fall within this category, which suggests that banks are expected to conduct internal assessments for a broader group than those subject to external supervisory screening. It is preferred that the scope of KFH for internal and external assessment is aligned and limited to the heads of internal control functions and CFO. In the absence of such alignment, there is a risk that national supervisors will interpret the scope of KFH differently and this would undermine the objective of a harmonised fit and proper framework across the EU.

- **Focus on ESG**: the proposed ESG related revisions seem to be rather disproportionately heavy on ESG and do not consider or mention other relevant developments and risk factors, such as for example geopolitical, cyber/AI, etc.

EBF COMMENTS

Background and rationale

Footnote 14 (p.16 of the draft guidelines) - it is unclear what the rationale of the addition in this footnote is (as well as of footnote 14 as a whole), considering that paragraph 6 refers to "all risks".

Paragraph 28 – it establishes that "*[i]n Member States where the management body appoints persons that effectively direct the business of the institution, those persons belong,* ***in accordance the Article 3(1)(8a) of Directive 2013/36/EU****, to the*

management function of the management body." [emphasis added]. Article 3(1)(8a) of the Directive 2013/36/EU defines "*management body in its management function*" without specifying the corporate body responsible for appointing the persons that effectively direct the business of the institution. In view of the above, it is suggested to amend paragraph 28 as follows:

> "*28.* ***~~In Member States where the management body appoints persons that effectively direct the business of the institution, those persons belong~~****,* *In accordance the Article 3(1)(8a) of Directive 2013/36/EU,* ***~~to the management function of~~*** *the "management body* ***in its management function" means the management body acting in its role of directing an institution and includes the persons who effectively direct the business of the institution****."*

Question 1: Are subject matter, scope of application, definitions and date of application appropriate and sufficiently clear?

Paragraph 7 - Points (8a) and (8) of Article 3(1) of Directive 2013/36/EU do not define the "management (executive) and supervisory (non-executive) functions" but the "management body in its management function" and the "management body in its supervisory function". Therefore, it is suggested that paragraph 7 be amended as follows:

> *"[…]The management body, as defined in point****~~s~~*** *(7)* ***~~and (8))~~****, of Article 3(1) of Directive 2013/36/EU, should be understood as having management (executive)* ***functions when acting as a "management body in its management function"*** *and as having supervisory (non-executive) functions* ***when acting as a "management body in its supervisory functions" as those terms are defined, respectively, in points (8a) and (8) of that article.****"*

Paragraph 8 – certain provisions of the Guidelines may be overly prescriptive and detailed, which could risk transforming Guidelines into de facto binding requirements. Flexibility should therefore be interpreted broadly, covering not only the size, complexity and risk profile of institutions, but also the diversity of national governance frameworks and board structures across the European Union. Moreover, EU law is framed with Regulations which apply directly in member states, but also with directives which need to be transposed by national law: institutions are bound by such national laws which may differ from one country to another. Institutions are also bound by laws which do not derive from EU law and have no other choice but to respect those laws. In this regard, the deleted last sentence of this paragraph should be reinstated. These guidelines should be implemented taking into consideration national company law. For the sake of clarity, it should be clarified in this paragraph and also throughout the whole document that the management body with management function may be, alternatively, a person (for example, CEO and/or General Manager) or a collegial body (for example, Management Board or Executive Committee). Please also see our comments above in the "Main comments" section.

Paragraph 9 - this paragraph should maintain the reference to the possibility of delegating the management function to an internal executive body, as it provides clarity and certainty in Member States where the law allows such delegation of management functions of the management body. In addition, the appointment of persons exercising the management function of the management body may differ across EU jurisdictions, as it is governed by national law. For instance, there are Member States where they may only be appointed by the management body in its supervisory function, and other Member States where they

may be appointed by shareholders (as is the case as regards the appointment of directors in one-tier systems). The reference to their appointment should therefore be removed (see also the comments to paragraph 28 above). The following wording is suggested: "*In Member States where the management body delegates, partially or fully, the executive functions to a person or an internal executive body (e.g. a chief executive officer (CEO), management team or executive committee), the persons / collegial body who perform those executive functions on the basis of that delegation should be understood as constituting the management function of the management body. Persons that exercise the management function of the management body, including those that effectively direct the business of the institution in accordance with Article 3(1)(8a) of Directive 2013/36/EU, are to be assessed for their suitability ~~in line with Article 91 of this Directive~~.*"

Paragraph 11 – it is important to maintain that definitions are purely functional and not intended to impose the appointment of those officers or the creation of such positions, unless prescribed by relevant EU or national law.

Paragraph 13 – the definition of "*operational resilience*" is consistent with the definition proposed in the draft Guidelines on the sound management of third-party risk (non-ICT related services), but it does not coincide with that of "digital operational resilience" introduced by the DORA Regulation. According to DORA Regulation, "*digital operational resilience*" means "*the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*". By contrast, the concept of "*operational resilience*" as described in the draft Guidelines under analysis refers to a financial institution's ability to perform critical or important functions in the event of a disruption. This capability enables a financial institution, directly or indirectly, including through the use of functions provided by third-party service providers, to identify and protect itself from threats and potential failures, to react and adapt, and to recover and learn from disruptive events, in order to minimize their impact on the performance of critical or important functions in the event of a disruption. In the context of the draft Guidelines under analysis, the concept of "*operational resilience*" is used mainly in relation to ICT and security risk management. Therefore, it would be preferable the definition adopted in the Guidelines be aligned with that contained in DORA Regulation.

Question 2: Are the changes made in Titles I (proportionality) and II (role of the management body and committees) appropriate and sufficiently clear?

General remark - although guaranteed by Article 74 of the Directive, we feel that the general wording of the revised guidelines greatly soften the application of the principle of proportionality. We believe this principle to be fundamental.

Paragraph 16 - While we welcome the EBA's intention to reinforce the role of proportionality in Titles I and II, we consider that the current drafting does not fully capture the breadth of this principle. In our view, proportionality should encompass not only the size, complexity and risk profile of institutions, but also the diversity of the different board structures permitted across the EU within the flexibility allowed by both EU and national

legislation. A clearer acknowledgment of these elements would help ensure that the Guidelines can be applied consistently and effectively across Member States. In connection with the above, a proposal for a new wording of paragraph 16 is suggested: "*16. The proportionality principle encoded in Article 74(2) of Directive 2013/36/EU aims to ensure that internal governance arrangements are consistent with the individual risk profile and business model of the institution, so that the objectives of the regulatory requirements and provisions are effectively achieved.* ***In applying this principle, competent authorities should take into account the diversity of governance frameworks and management body structures permitted across the EU within the flexibility provided by European Union and national company law***". In conclusion, we believe that Titles I and II should follow a more balanced and principle-based approach. Embedding a broader understanding of flexibility within the proportionality principle, and ensuring consistency with national company law frameworks, is essential to preserve legal certainty and accommodate the diversity of governance models across the EU. Clarifying paragraph 16 along the line suggested above would provide clearer guidance while avoiding prescriptive requirements that could conflict with national law and undermine the collective responsibility of the management body in one-tier systems.

Paragraph 18: - could the EBA clarify the difference between the use of third-party service providers (including the outsourcing of functions) and distribution channels (paragraphs 18 and 163)?

Paragraph 22.c - it seems that the numbering of the list needs to be adjusted (i.e. "i.(a)", "i.(b)" and "ii." should be, respectively, "ii.", "iii." and "iv").

Paragraph 22.c subpoint i - the removal of the term "*independent*" in paragraph 22.c subpoint i is not comprehensible, especially considering the emphasis placed on the independence of internal control functions elsewhere in the Guidelines (e.g., paragraph 174a under section 19.2 "*Independence of internal control functions*" or paragraph 176 under section 19.3 "*Combination of internal control functions*"). The independence of the compliance function is a fundamental principle of governance, and ensuring clarity and consistency within the Guidelines would be desirable.

Paragraph 22.c subpoint i(a) – we do not understand why concentration risk arising from exposures towards central counterparties is outlined here explicitly (there are processes for other concentration risks as well). Recommend deleting specific reference to central counterparties (CC) if at all it shall also read central clearing counterparties (CCPs).

Paragraph 22.c subpoint i(b) – this is not in line with DORA, which in article 5 states that the purpose of having in place an internal governance and control framework "*ensures effective and prudent management of ICT risk (…) in order to achieve a high level of digital operational resilience.*" Therefore, please delete paragraph 22.c subpoint i(b) and insert a new paragraph 22.d, which shall read as follows: "*(d.) an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with in accordance with Article 6(4) Regulation (EU) 2022/2554, in order to achieve a high level of digital operational resilience.*"

Paragraph 23 – for the sake of clarity: please define the terms "*traditional categories of financial and non-financial risks*" and "*potential materialisation of operational ~~and legal~~ risks*".

Paragraph 29.a - if the intention in this paragraph is to refer to segregation of duties, and mitigation of conflict of interest, we suggest expressing it differently. "*Mandate*" is not the adequate terminology if we want to address the case of a member of the management body in charge of private banking, credit, trading room or any other risk-taking function that would be incompatible with an ICF role. Additionally, new paragraph 29.a does not only refer to Section 19.1 ("*Heads of the internal control functions*") as it does the (deleted) paragraph 26, but also to Section 19.3 ("*Combination of internal control functions*"). We understand that it should refer to Section 19.1 (particularly paragraph 172) only but not to Section 19.3 (paragraph 176). Paragraph 172 describes the "*heads of internal control functions*" as such, with the possibility that the internal control function is headed by a member of the management body in its management function. On the other hand, Section 19.3 (paragraph 176) deals with the combination of internal control functions, which now does not only include the combination among internal control functions but also with other tasks performed by a senior person as provided under new paragraph 6 of article 76 of CRD introduced by the CRD VI when conditions established thereto are met such as but not limited to the absence of conflicts of interest. New paragraph 6 of article 76 of CRD does not refer to a member of the management body in its management function but to a "*senior person*", which should be understood in accordance with the new definition of "*senior management*" of article 3(1)(9) of the CRD as amended by the CRD VI, which specifically excludes members of the management body. In view of the above, we suggest reformulating: "*29a. A member of the management body in its management function may be the head of an internal control function as referred to in Title V, Sections 19.1, provided that the member does not have other responsibilities that would compromise the member's internal control activities and the independence of the internal control functions.*"

Paragraph 33: The requirement that the management body in its supervisory function should include independent members still lacks a legal basis in CRD VI. The provision should therefore be deleted.

Paragraph 37 - the Guidelines show a clear inclination towards governance choices that do not seem to be justified or supported by any reasoning or empirical evidence. Regarding the deletion of part of the text of paragraph 37, we consider that, when the chair is an executive director (in compliance with national legislation), what is particularly relevant is the existence of strong checks and balances that have proven successful to avoid an excessive concentration of power. In this respect, we believe such long-accepted mitigating measures should be maintained/reflected in the Guidance to provide certainty and to ensure alignment with national laws, previous Guidelines and the Basel Committee on Banking Supervision Corporate Governance principles for banks. Nowhere in CRD IV or CRD VI is there a point saying that the chair of the management body should be a non-executive member. Therefore, the text deleted in paragraph 37 should be maintained, as this goes against the existing law in several Member States. Otherwise, we ask to delete the first sentence of paragraph 37. Please also see our comments above in the "Main comments" section.

Question 3: Are the changes made in Title III (governance framework) section 6 appropriate and sufficiently clear?

Paragraph 51 - we notice that the draft Guidelines introduces a requirement for ESG related skills at the individual level of the members of the remuneration committee. This individual requirement seems excessive, not required under CRD VI and contrary to (i) the collective suitability criteria for members of the management body set out in the Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders and (ii) the collective knowledge requirement set out for the remuneration committee in section 2.4.1 of the EBA Guidelines on sound remuneration policies. In addition, to impose specific ESG requirements at the collective level also seems excessive as it involves a non-justified difference between ESG factors and other material factors with — potentially higher — impact on remuneration incentives, such as financial performance, capital and liquidity or management risk. Similarly, highlighting ESG risks among all the risks of an institution is not justified and throws concerning doubts on the importance of other risks when assessing remuneration incentives. It is therefore suggested to amend this recommendation as follows: "*Members of the remuneration committee should have, ~~individually and~~ collectively, appropriate knowledge, skills and experience to assess the impact of* ***different~~ESG~~*** *factors* ***(including ESG factors)****, and the consistency of the institution's risk appetite* ***~~regarding ESG risks~~*** *with, remuneration incentives, taking into account the assessment of the risk committee specified under paragraph 62."*

Paragraph 61.c. - the illustrative list under bracket after "*operational*" seems very random: We suggest keeping it to the current regulation (art 4.1 (52) CRR definition of operational risk and the recently published draft RTS on Operational Risk Taxonomy) and to only refer to '*operational risks*'. We disagree that we should include in operational risks "*fundamental rights and discrimination*" ***as these fall under compliance risks***: "*c. oversee the implementation of the strategies for capital and liquidity management as well as for all other relevant risks of an institution, such as market, credit, operational* ***~~(including legal and IT, fundamental rights, discrimination and ICT risks),~~*** *and reputational risks, in order to assess their adequacy against the approved risk strategy and risk appetite;".*

Paragraphs 68.a. – 68.b. - consider rephrasing and deleting any reference to the management in the supervisory function. Including the management in its supervisory function (e.g. the Supervisory Board in a 2-tier system or the non-executive directors in a 1-tier system) goes beyond what is required according to Art. 88 (3) of Directive 2013/36/EU. Art. 88 (3) of Directive 2013/36/EU in its wording clearly only requires institutions to prepare the mapping of roles with regard to the management body in its management function. Moreover, provided that new requirements for institutions to draw up, maintain and update individual statements on roles and duties and a mapping of duties have been introduced by the CRD VI Directive, the additional details included in the EBA Guidelines seems to burden institutions with additional constraints that are not envisaged by the Directive. Furthermore, the scope of application for the requirement is not fully clear, since governance documentation currently adopted by institutions in their internal governance framework, seems to meet the substance of this prescription. For this reason, the EBA Guidelines should:

- more explicitly state that the mapping of duties is not required for the management body in its supervisory function;
- clarify that the mapping of institution's activities and responsibilities of the management can be included in documents approved by the corporate bodies without the need for a specific format (for example, Organization Charts, Regulation on the Internal Control System, etc.) and without the

need to be approved by the management body, since the approval could be delegated at the institution's discretion (e.g. to the management body in its management function, or in one tier systems to senior management, at least with respect to its direct reporting lines);

- delete the following references to roles and duties contained in the mapping of duties:
  - "*consistent with the individual statements of duties*" (furthermore, the individual statements are only required to the members of the management body in its management function according to article 88(3) of CRD and, therefore, the summary of the roles and duties should be limited to them without including the members of the management body in its supervisory function and the consistency cannot be applied to the members of the management body in its supervisory function)
  - [The management body should approve the mapping of duties and institutions should timely update it as appropriate,] "*taking also into account the review of the individual statements*"

  these references appear (i) incoherent, since the mapping of duties should be updated first and only afterward should the individual statements be modified accordingly, and (ii) inconsistent with point 68(b)(d), which states with regard to the individual statements: "Institutions should review it on a regular basis, taking into account the review of the mapping of duties."
- clarify that individual statements requirement can be fulfilled simply through the acceptance of the position detailed in the mapping of duties;

Paragraph 68.a.c. - with reference to the introduction, the provision to outline the duties for each member of the management in its supervisory function is not in line with Article 88(3) of CRD VI and should therefore be limited to the management body in its management function only.

Paragraph 68.a.e. – please delete the second sentence in in its entirety, as it is overly prescriptive and detailed. As outlined in the introduction, such a prescriptive nature may turn guidance into de facto binding requirements. We propose to amend this paragraph as follows: "*The mapping of duties should be coherent with the individual statements of role and duties as referred to in paragraph 68b. ~~It should (i) provide a clear overview how roles and duties allocated in a particular statement fit into the overall management system and internal governance; and (ii) include sufficient information to enable a clear understanding of how the management and internal governance arrangements of the institution are structured and operate~~*".

Paragraph 68.a.f. –this paragraph should also expressly acknowledge the institutions' right to draw up and maintain the mapping of duties in a set of documents or a repository (vs. a single document) to avoid duplicities between internal documents and reduce the administrative burden that paragraph 68 entails, as most of the content provided therein is already reflected in existing documents (e.g. the board regulations, organizational charts, job descriptions, annual reports).

Paragraph 68.a.f.(ii). – firstly, the reference to management body in supervisory function and its sub-committees should be removed, as this provision is inconsistent with Art. 88 (3) of Directive 2013/36/EU and falls outside of the guiding-competence of the EBA. Secondly, the management body itself is the corporate body authorized to adopt decisions pursuant to local law (for instance in Dutch law). As such, there is no rationale for this

guideline. In addition, it should be noted regarding the Management Board in its Management Function, Senior Management and Key Function Holders: an online system (intranet) of the institution containing org-charts (with the respective reporting lines, rules of procedures and schedules of responsibilities) should be sufficient in order to meet this requirement. The mere copying compilation of existing tableaus, guidelines or procedures in another intranet location is an unnecessary administrative burden and has no additional value on its own.

Paragraph 68.a.f.(iii). - the EBA targets the same population as for individual statements and adds the board and its committees. These provisions go further than what is provided by the CRD VI Directive, which limits the scope to the management body in its management function (and not the full management body). Furthermore, point iii. requires the names and a summary of the roles and duties of all members of the management body (and not only of the members "*in its management function*"). Given that, as mentioned above, the mapping should be done only for the members of the management body in its management function, considering the link between names and roles is already ensured by internal management and communications system, providing only a summary of roles and duties should be sufficient to meet the requirement (without indicating names). Additionally, the acronym "*KFH*" in point iii. of letter f) should be defined or, alternatively, the full words "*key function holders*" should be stated. Therefore, we suggest point iii. of letter f) be amended as follows: "*iii. ~~the names of all members of the management body, senior management and KFH and~~ a summary of ~~their~~ roles and duties of the members* ***of the management body in its management function, senior management and key function holders*** *consistent with the individual statements of duties;*"

Paragraph 68a.f.(v). - this requirement may be administratively burdensome for smaller institutions. Smaller institutions typically have fewer employees, with individuals often performing multiple functions, reflecting a necessary proportionality in their organizational setup. This challenge does not necessarily indicate a deficiency in governance or accountability, but rather reflects the institution's natural organizational structure. Likewise, documenting responsibilities for third-party arrangements, including outsourcing (vi), may be unsuitable for some Member States. For instance, under Section 64c of the Danish Financial Business Act, an outsourcing manager is typically not a key function holder or part of actual management, meaning that institutions would need to document a person who is not otherwise captured under CRD. This may create ambiguities in the allocation of roles and impose additional administrative burdens without strengthening actual governance.

Paragraph 68.a.g. - this provision should be deleted because it goes beyond what is required according to Art. 88(3) CRD VI, which only requires institutions to prepare documentation and keep it updated. No voting and approving necessity can be interpreted from the wording.

Paragraph 68.b.a. - the indication of the expected time commitment should remain part of the FAP assessments and not be extended to members of the senior management which are not subject to FAP assessment. Furthermore, it is unclear why is referred to '*key duties*', rather than '*duties*', which is the terminology used throughout the Guidelines. Lastly, the acronym "*KFH*" should be defined or, alternatively, the full words "*key function holders*" should be stated. Also, the indication of the expected time commitment is

challenging in smaller institutions, as it is difficult to precisely allocate time to functions when individuals perform multiple roles concurrently. Documenting expected time commitments may therefore be challenging, as it reflects the practical realities of the institution's organisational framework rather than any lack of resources or insufficient governance. As a result, the institution may need to allocate additional resources to the affected roles or, in some cases, consider outsourcing certain functions.

Paragraph 68.b.b. – the first sentence should be rephrased to reflect the overarching principle of collective responsibility of the management body. We propose the following revision: "*The allocation in the individual statements of role(s) and duties to a member of the management body in its management function* ~~*does not exempt the respective individuals from their roles and duties as members*~~ ***is without prejudice to the collective responsibility*** *of the management body*." Furthermore, please delete the second sentence: "*All members of the management body in its management function are expected to have an appropriate understanding of, and contribute to, areas of the business, including for any other roles and duties not directly attributed to the respective member*". This sentence is unnecessary, as the suitability requirements already cover the expectation that members of the management body in its management function possess appropriate knowledge and contribute effectively. Repeating this here adds no substantive value and may lead to confusion or redundancy.

Paragraph 68.b.d. - 1) The requirement is disproportionate as any person could only assume the respective role after the passing of the suitability assessment. It conflicts with data privacy law (e.g. principle of data minimization (Art. 5 GDPR)) as sensitive personal data are concerned. 2) The signature requirement goes beyond what is required according to Art. 88 (3) of Directive 2013/36/EU which provides that: "*Member States shall ensure that the individual statements of duties and the mapping of duties are made available at all times and communicated, including to obtain authorization as set out in Article 8, in due time, upon request, to the competent authorities*". Further, a signature requirement conflicts with national employment law as a change of contract. 3) The acronym "RTS" should be defined or, alternatively, the full words should be stated. To sum up, we ask that this point is removed from the Guidelines.

Paragraph 68.c. - article 88(3) of Directive (EU) 2024/1619 only introduces an obligation to establish individual statements and map responsibilities; it does not set out a burden of proof framework in terms of establishing "*individuals*" not fulfilling these duties. Paragraph 68c appears to introduce such a regime at level 3, where it is not the competent authority, but the individual, that needs to evidence proper fulfilment of duties. This exceeds the mandate of the level 1 text because such provision is not included in the CRD VI and raises concerns. Moreover, the liability of board members and senior management is governed by national legislation. From a legal certainty perspective, the proposed wording is problematic due to vague and subjective expressions such as '*all actions that could reasonably be expected'*. Without clear benchmarks, individuals may be exposed to retrospective assessments based on evolving expectations, undermining predictability and fairness (the '*moving goalpost*' dilemma). There is also no explicit materiality threshold as to which issues are to be considered in scope. The draft guidelines read so that an individual is deemed to not have fulfilled their duties if "*an issue*" arises in their area of responsibility. In order to prove innocence, it is the individual who needs to establish to have taken actions that "*could reasonably be expected*" to prevent or stop "*the issue*". In varied organizational structures of EU banks, the ambiguity of grounds for liability may

deter qualified professionals from assuming key roles, where "*issues*" may rise at regular intervals, despite diligent efforts. Therefore, the current wording of paragraph 68c. creates a risk of chilling effect, and it can be seen as a matter of EU banking sector competitiveness as well. The obligation established by the CRD VI is limited to requiring the formalization of lines of responsibility. The proposed paragraph 68c is likely to create interpretative difficulties as regards what may be deemed an "*issue*" and the "*measures that could reasonably be expected*" in response. It is unclear what the supervisor's objective is in this regard and whether it is meant to characterize a breach that could justify a withdrawal of authorization. This would go beyond the CRD VI, as the latter does not provide for sanctions. In particular, the last half-sentence of para. 68c ("*the individuals should be able...*") according to which members of the management and supervisory boards must be able to prove to the supervisory authorities upon request that they have fulfilled their intended tasks, does not appear to be objectively justified and should be deleted. Credit institutions must in any case be able to prove at any time that the regulatory requirements have been met. This already entails appropriate information obligations for the institutions and their bodies. An additional personal accountability of individual board members to the supervisory authority would constitute overregulation, especially when applied to LSIs. If applied to supervisory board members, this requirement could also further reduce the willingness of suitable representatives of the regional economy to accept such mandates. The assessment and consequences of not fulfilling duties should be subject only to national company law and employment law. In addition, the legal regimes for statutory board members and senior managers who are '*ordinary*' employees differ. While the objective of enhancing and clarifying accountability is commendable, the current formulation proposed raises several legal and practical concerns. Therefore, we suggest the EBA to remove paragraph 68c entirely.

Question 4: Are the changes made in Title III section 7 (third-country branches) appropriate and sufficiently clear?

It is not clear enough in the guidelines what is applicable to the third-country branches (only this specific section, or other parts).

Paragraph 90c. - the prescription referred to persons effectively directing the business seems to go beyond what is required by CRD VI introducing new requirements. In particular, we would suggest deleting the following sentence: "*The position held in the third-country branch should be counted, where the conditions of Article 91 paragraphs (3) and (4) of Directive 2013/36/EU are met, as an executive directorship.*"

Paragraph 90j. - please note that article 48(g)(2) provides that third-country branches shall comply with articles 92, 94 and 95 of CRD which do not include article 93 and do not refer to "*the EBA Guidelines on sound remuneration policies under Directive 2013/36/EU, taking into account the risk appetite regarding ESG risks.*" We would therefore suggest the following changes: "*Third-country branches should comply with the remuneration principles set out in Articles 92, 94 and ~~to~~ 95 of Directive 2013/36/EU39 and the EBA Guidelines on sound remuneration policies under Directive 2013/36/EU, taking into account the risk appetite regarding ESG risks. [.../...].*"

Question 5: Are the changes made in Title IV (risk culture) appropriate and sufficiently clear?

Paragraph 94 - we suggest replacing the word "*equality*" with a word "*fairness*".

Paragraph 100 – it is not entirely clear what "*genetic features*" mean. It is not a commonly used term when addressing discrimination in the context of Diversity, Equity & Inclusion at the European or UK/US levels. Unless there was a strong rational behind it, we would suggest deleting it.

Paragraph 101a - we suggest specifying also that the selection of indicators to measure diversity (all types of diversity) should remain within the discretion of the institution, according to its specific organizational, dimensional and operational characteristics.

Paragraph 102 - the proposed drafting result in a slight broadening of scope and introduces the concept of "*professional standards*". While we understand this may be intended as a clarification, we would welcome further guidance from the EBA on the underlying objective: does this amendment aim to expand the range of aspects to be covered (e.g. beyond sustainability, responsibility and resilience), and how should "*professional standards*" be interpreted in this context?

Paragraph 107.a. – we ask for a removal of this paragraph which introduces a new recommendation that is not expressly foreseen in CRD VI: "*Similarly, within a group, the role of Chair of the management body in its supervisory function of a parent entity should not be held by the CEO of a subsidiary.*" As further explained in section Main comments above, EU law and several national laws allow for the board chair of an institution to assume executive functions other than the CEO's. This might result in the board chair having executive functions in a subsidiary. The prohibition under CRD VI is strictly limited to the roles of chair and CEO within the same institution. Extending the prohibition to all the entities within a group would go beyond national legislators' and EU legislator's choices and is not motivated or based on any evidence. Therefore, this new recommendation should be removed. Moreover, the third sentence of this paragraph goes far beyond the CRD VI Directive which does not prohibit for a member to have several directorships within the same group. Indeed, the privileged counting of directorships which provides notably that executive or non-executive directorships held within the same group shall count as a single directorship has been confirmed in the CRD VI Directive. Each entity has a suitability policy in place which covers conflicts of interests situations. In addition, the impact on "*the duty to oversee their own previous actions*" is not clear since the paragraph refers to functions exercised simultaneously.

Paragraph 107.b. – the provision envisaged by the EBA Guidelines of a cooling-off period of at least three years as well as the specific mitigation measures for hypothetical and abstract conflicts of interest, goes beyond the requirements of the Directive 2024/1619 ("CRD VI"). Specifically, the company's autonomy in appointing the Chair and non-executive directors results to be compromised. In this respect it should be taken into consideration that the role of non-executive board members may coexist with the position as non-independent member of the board. **For this purpose, the mentioned provisions under paragraph 107b of the EBA Guidelines should be deleted.** It should be instead clarified that an executive director who, at the end of his/her term, takes on the role of Chair or member of the management body with supervisory function, cannot be qualified

as an "*independent director*" for the period established by national regulations regarding the independence requirements for directors without any prejudice to the role as non-executive director. This approach is also consistent with the Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body. Having said the above, it should be also considered that the overall safeguards for managing specific conflicts of interest according to the ordinary rules of disclosure and abstention would remain in force, as these are already extensively regulated by corporate law, so the Guidelines should only defer to national law instead of illustrating situations of potential conflicts of interest and measures to mitigate them.

Paragraph 129ss - although the EBA Guidelines does not include amendments on this specific matter, the occasion may also be used as an opportunity to simplify the set of information required on exposures granted to related parties, making it more consistent with the information required in the context of the ECB's F&P Questionnaire, thereby reducing the compliance burden in the presence of non-significant exposures. In any case, it is suggested to raise the current threshold to determine the relevance of exposures for which additional information is required, currently set at euro 200.000.

Question 6: Are the changes made in Title V (internal control framework) appropriate and sufficiently clear?

Footnote 54 (p.62 of the draft guidelines) - the EBA Guidelines on the AML/CTF compliance function are no longer under development but in force since 21/11/2022.

Paragraph 152 - the added last sentence of this paragraph states as follows: "*The risk management framework should pay particular attention to [.../...] and to the channels through which they may drive their prudential risks, in particular through environmental physical and/or transition risks, and be compliant with the requirements set out in the EBA Guidelines on the management of ESG risks (EBA GL/2025/01).*" The end of this paragraph appearing in red is not part of article 74(1) of CRD, we would suggest its deletion. Otherwise, please include the full name of the Guidelines, i.e. "*Guidelines on the management of environmental, social and governance (ESG) risks (EBA GL/2025/01).*"

Paragraph 171 – as to how are reflected the concepts of "*compliance manager*" and "*compliance officer*" used in the Regulation (EU) 2024/1624[2] in the Guidelines - we understand that the "*member of the management body in its management function responsible for ensuring compliance with Regulation (EU) 2024/1624*" mentioned in the first sentence of paragraph 171 is the "*compliance manager*" prescribed under paragraph 1 of Article 11 of the Regulation (EU) 2024/1624 that establishes that the "[o]*bliged entities shall appoint one member of the management body in its management function who shall be responsible for ensuring compliance with this Regulation, Regulation (EU) 2023/1113 and any administrative act issued by any supervisor ('compliance manager')*." However, we are unclear whether the "*separate AML/CFT compliance function*" mentioned in the second sentence of paragraph 171 (i.e. "*Institutions may establish a separate*

[2] Please note that Regulation (EU) 2024/1624 (**AMLR6**) will enter into force and will apply as of 10 July 2027, except in relation to obliged entities referred to in Article 3, points (3)(n) and (o), to which it shall apply from 10 July 2029 (see art. 90 AMLR). Until 10 July 2027 national law implementing Directive 2015/849 will remain applicable.

AML/CFT compliance function as an independent control function") is the "*compliance officer*" mentioned in paragraph 204 (please see comments to paragraph 204, below) or the "*compliance officer*" prescribed under paragraph 2 of Article 11 of the Regulation (EU) 2024/1624. Should be the latter case, please note that, whereas the second sentence of paragraph 171 allows but it does not require to have it, the paragraph 2 of Article 11 of the Regulation (EU) 2024/1624 requires it (at least for "obliged entities") by establishing that the "[o]*bliged entities shall have a compliance officer, to be appointed by the management body in its management function and with sufficiently high hierarchical standing, who shall be responsible for the policies, procedures and controls in the day-to-day operation of the obliged entity's AML/CFT requirements, including in relation to the implementation of targeted financial sanctions, and shall be a contact point for competent authorities* […]." Therefore, the wording of this second sentence of paragraph 171 is not fully aligned with Regulation (EU) 2024/1624 (at least for "obliged entities" and, therefore, it is not optional). It would be advisable to adjust the second sentence of paragraph 171 accordingly and make a clear reference to Regulation (EU) 2024/1624 as in the first sentence of the same paragraph 171. As to the concept of "*compliance officer*", please see comments to paragraph 204, below.

Paragraph 172 - we understand that this paragraph 172 should be limited to describe the "*heads of internal control functions*" as such, with the possibility that the internal control function is headed by a member of the management body in its management function as provided under paragraph 29 (as commented and amended above). On the other hand, paragraph 176 - deals with the combination of internal control functions, which now not only includes the combination among internal control functions but also with other tasks performed by a senior person within the institution as provided under new paragraph 6 of article 76 of the Directive 2013/36/EU introduced by the CRD VI when conditions established thereto are met such as but not limited to the absence of conflicts of interest. Article 76 of CRD does not refer to a member of the management body in its management function but to a "senior person" which should understood in accordance with the new definition of "senior management" under of article 3(1)(9) of the CRD as amended by the CRD VI which specifically excludes members of the management body. Therefore, we suggest that the last sentence of paragraph 172 be deleted because the conditions regarding conflicts of interest, independence, etc… are specifically included in paragraph 176 for the cases where a senior person that performs other tasks within the institution may fulfil the responsibilities for the compliance or risk management functions by reference to Article 76(6) 3rd subparagraph of Directive 2013/36/EU: *"The heads of internal control functions should be established at an adequate hierarchical level that provides the head of the control function with the appropriate authority and stature needed to fulfil their responsibilities. Notwithstanding the overall responsibility of the management body, in accordance with Article 76(6) of Directive 2013/36/EU, the heads of internal control functions should be independent senior managers with distinct responsibility for the risk management, compliance and internal audit functions and be independent from the business lines or units they control. Where an internal control function is headed by a member of the management body in its management function, the institution should carefully ensure that appropriate safeguards and mitigants are in place to avoid conflicts of interest as referred to in paragraph 116, such as but not limited to, an independent mindset of the individual and appropriate key performance indicators, including objective appraisal and remuneration determination.* ~~***This also applies to cases where the head of an internal control function performs other functions pursuant to section 19.3.***~~*"*

Paragraph 175.d. - we would make the sentence, "*The remuneration of the heads of internal control functions should be directly overseen by the management body in its supervisory function or remuneration committee, as the case may be*.", a new e. as not linked to d. Moreover, consider revising to "*remuneration system*". It is incorrect that the "*remuneration*" should be directly overseen by the management function in its supervisory function. Additionally, in the event of one-tier structures, how can be overseen by the management body in its supervisory function when the (sole) management body is made up of executive and non-executive members?

Paragraph 176 - the new wording of the paragraph relating to the combination of internal control functions seems ambiguous to us. The revised version of the Guidelines indicates, as in the previous version, that "*the risk management function and compliance function may be combined*" while adding a nuance ("*may be combined under another senior person*"). But the penultimate sentence of the revised version mentions "*The decision to combine the risk management function or the compliance function under another senior person*". It is not clear if it means that either the risk management or the compliance function can be combined under another senior person or if the risk management and the compliance function can be combined under one senior person. Whereas paragraph 172 deals with the possibility that the internal control functions are headed by a member of the management body in its management function, paragraph 176 deals with the combination of internal control functions. We understand that the amendments to paragraph 172 are aiming at allowing not only the combination among internal control functions but also the combination of either such internal control functions with other tasks performed by a senior person within the institution as provided under new paragraph 6 of article 76 of the Directive 2013/36/EU introduced by the CRD VI. However, we understand that the conditions and measures of the new paragraph 6 of article 76 of the Directive 2013/36/EU are only applicable to cases where "*another senior person that performs other tasks within the institution may fulfil the responsibilities for the compliance or risk management functions"* in order to assess and prevent these other tasks, particularly when these are not of an internal control nature, from impairing these internal control functions. Paragraph 6 of article 76 does not regulate the case where there is a combination among the risk management and compliance functions held by a single senior person. Therefore, we suggest that paragraph 176 should be aligned with new paragraph 6 of article 76 of the Directive 2013/36/EU introduced by the CRD VI and, therefore, adjusted as follows:
"*Taking into account the proportionality criteria set out in Title I, the risk management function and the compliance function may be combined under* ***a single senior person. Where the nature, scale and complexity of the activities of the institution do not justify appointing a specific person for the risk management function or the compliance function,*** *another senior person* ***that performs other tasks within the institution may fulfil the responsibilities for the compliance or the risk management functions*** ~~***who may be a member of the management body in its management function as referred to paragraph 172***~~*, where the conditions in Article 76(6) 3rd subparagraph of Directive (EU) 2013/36 are met. In this case, institutions should be able to demonstrate that the nature, scale and complexity of the activities of the institution do not justify appointing a specific person for the risk management function or the compliance function, that the assessment of conflicts of interests required under Article 76 (6) 3rd subparagraph* ~~***and as further specified in paragraph 172***~~ *has been performed, and, if necessary, measures to address identified conflicts of interest have been taken. The decision to combine the risk management function* ***and***~~***or***~~ *the compliance*

function under ***a single senior person or to entrust the responsibilities for the compliance or risk management functions to*** *another senior person* ***that performs other tasks*** *should be documented. It should be ensured that the senior person fulfils the time commitment and suitability requirements laid out in Article 76(6) of Directive (EU) 2013/36. The internal audit function must not be combined with* ***any other business line or*** ~~***another***~~ *internal control function*."

Paragraph 187 – we note that the EBA Guidelines includes more than quantifiable targets. We suggest reformulating: "*The RMF should provide the management body with all relevant information to establish ESG risk-related strategies, policies and plans in line with the EBA guidelines on the management of environmental, social and governance (ESG) risks (EBA GL/2025/01), particularly section 6.*"

Paragraph 195 - it is not clear why ICT related information in particular is added to this specific paragraph, as one might also expect information on other risk types. Furthermore "*ICT-related information*" is not defined. Please remove the proposed part of the sentence ("*and ensure that ICT-related information is conveyed on a timely manner*").

Paragraph 201 – in accordance with (new) paragraph 29a and paragraph 172, a member of the management body in its management function may be responsible for an internal control function. In this event, as a member of the management body, it is presumed that it has sufficient independence (pursuant to paragraph 172) and sufficient seniority (as being a member of the management body. Therefore, paragraph 201 should be amended to contemplate this possibility as follows:

> "***As a general principle, ~~T~~t****he head of the RMF should be a senior manager with sufficient expertise, independence and seniority to challenge decisions that affect an institution's exposure to risks."* ***The head of the RMF may also be a member of the management body in its management function provided it complies with paragraphs 29a and 172.***

The notion of senior management being defined by Directive 2013/36/EU as "*[…] natural persons who exercise executive functions within an institution and who are responsible, and accountable to the management body, for the day-to-day management of the institution;".* These amendments strengthen the requirements for the head of the RMF by explicitly requiring this role to be held by a senior manager without prejudice to the possibility of being also a member of the management body in its management function pursuant to the paragraph 172. At the same time, the deletion of the previous wording removes the flexibility whereby another function could be designated as head of RMF with direct access to the management body in its supervisory function. This represents a more prescriptive approach. We would welcome clarification from the EBA on whether proportionality may still allow alternative governance models in smaller entities or subsidiaries.

Paragraph 204, paragraph 209 and paragraph 210 - we are totally opposed to the proposed amendment concerning the compliance function, extending its responsibility, beyond compliance matters, to the management of *'legal risk stemming from non-compliance events'*. We want to avoid the compliance function evolving to a function overseeing/overarching all regulation as applicable for a financial institution, which is absolutely not recommended and not feasible to be supported under the current circumstances. It is a delicate change to transform Compliance risks (in the market

generally similarly interpreted) to non- compliance events resulting on the institution legal risk stemming.

Paragraph 204 – all references to "*compliance risk*" have been deleted and replaced with reference to "*legal risk stemming from non-compliance events*". This new disposal would create confusion as the role of the compliance function with the role of the legal function, and furthermore it is not consistent with the provisions set in Level 1 of legislation (see par. 76.5 of Directive (EU) 2024/1619 (CRD VI) which provides that "*Member States shall ensure that: […] the compliance function assesses and mitigates compliance risk and ensures that the institution's risk strategy takes into account compliance risk and that compliance risk is adequately taken into account in all material risk management decisions*"). Therefore, should be replaced the previous references to compliance risk. Moreover, as to the use of the terminology "*the compliance officer or head of compliance*" - Please see comment to paragraph 171, above. According to article 11 of the Regulation (EU) 2024/1624 the "compliance officer" "*shall be responsible for the policies, procedures and controls in the day-to-day operation of the obliged entity's AML/CFT requirements, including in relation to the implementation of targeted financial sanctions, and shall be a contact point for competent authorities. The compliance officer shall also be responsible for reporting suspicious transactions to the FIU in accordance with Article 69(6)*". These functions do not fulfil all compliance functions under article 11 of the Regulation (EU) 2024/1624. By contrast, it seems that the functions of the "compliance officer" under paragraph 204 are broader than those of the "compliance officer" under Regulation (EU) 2024/1624. It should be clear that "compliance officer" should not be understood as the "*compliance officer*" under Regulation (EU) 2024/1624, and therefore we suggest to use the term "*head of compliance*" only when referring to the function described under paragraph 204. As to the compliance function being "*headed by an independent senior manager*". In accordance with (new) paragraph 29a and paragraph 172, a member of the management body in its management function may be responsible for an internal control function. In this event, as a member of the management body, it is presumed that it has sufficient independence (pursuant to paragraph 172) and sufficient seniority (as being a member of the management body). Therefore, paragraph 204 should be amended to contemplate this possibility as follows (without prejudice to the additional amendments which may result from the previous comment to this paragraph 204 on the "compliance officer"): " ***As a general principle, t****he compliance function should be headed by an independent senior manager responsible for this function across the entire institution (the head of compliance).* ***The head of compliance may also be a member of the management body in its management function provided it complies with paragraphs 29a and 172.***"

Paragraph 206 - the removal of paragraph 206 is not comprehensible, especially considering the emphasis placed on the independence of internal control functions elsewhere in the Guidelines (e.g., paragraph 174a under section 19.2 "*Independence of internal control functions*" or paragraph 176 under section 19.3 "*Combination of internal control functions*"). The independence of the compliance function is a fundamental principle of governance, and ensuring clarity and consistency within the Guidelines is absolutely necessary.

Paragraphs 209 and 210 – the draft language should be more specific on what the role of the compliance function is in delineation to the legal function. Reference is made to the

related discussion at the EBA public hearing on 5 September 2025 where we understood that the EBA will clarify this in line with our comments above.

Paragraph 215 - the removal of the last sentence in 215 is not comprehensible in line with the feedback on paragraph 176 (that '*The internal audit function must not be combined with any other business line or another (internal control) function*.'). As the IAF should not be combined with 1st or 2nd line responsibilities, the sentence should either be amended as follows '*Therefore, the IAF should not be combined with any other business line or other functions*' or (to avoid repetition) replaced by a reference to paragraph 176 '*Therefore, the IAF should be organised as set out in paragraph 176*'.

Question 7: Are the changes made in Title VI (business continuity management) appropriate and sufficiently clear?

Paragraphs 225, 228, 229 and 230 - in these paragraphs the term '*recovery*' and '*recovery plans*' are mentioned. It should be clarified in the text of these guidelines that the reference to '*recovery*' and '*recovery plans*' is not to the '*recovery*' and '*recovery plans*' relating to financial stress in accordance with the Bank Recovery & Resolution Directive (BRRD), but to '*disaster recovery*' as part of business continuity management.

Paragraph 230 - in the first sentence, the addition of the phrasing "...*and subject to internal audit review*" is unnecessary and should be deleted. Furthermore, the second sentence states: "*The documentation should be available to the staff involved in the execution of the plans and should be stored on systems that are physically separated and readily accessible in case of emergency.*" Although this is a formulation already present in the previous version of the Guidelines, it should be noted that the concept of "*physically separated systems*" is not reflected in either Regulation (EU) 2022/2554 (DORA), or the EBA Guidelines on ICT risk management and security (EBA/GL/2019/04). The current wording may generate interpretative uncertainty. It is not clear whether the expression should be interpreted as the obligation to keep the documentation exclusively on systems located in alternative sites or on backup media that are geographically separate and distinct from the production environment. Considering the above, it is proposed to reformulate or delete the reference to "*physically separated systems*", to ensure greater alignment with the current European regulatory framework, particularly with the DORA Regulation.

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere.

www.ebf.eu @EBFeu

For more information contact:

Blazej Blasikiewicz
Director of Legal, International & Public Affairs
b.blasikiewicz@ebf.eu