ABI Associazione Bancaria Italiana

ABI response to EBA consultation on revised Guidelines on internal governance

November 2025

POSITION PAPER

2025

The Italian Banking Association (ABI) would like to thank the European Banking Authority (EBA) for the opportunity to comment on revised Guidelines on internal governance.

*

General comments

- Some provisions of the draft revised Guidelines burden institutions with additional constraints that are not envisaged by the CRD VI Directive. These provisions – that go beyond the requirements of the CRD VI - set unjustified limits on banks' autonomy in defining their own governance mechanism. A particular example of these provisions is the cooling-off period of at least three years, during which the CEO cannot be appointed as Chair or member of the Board of Directors, as well as the specific mitigation measures for hypothetical and abstract conflicts of interest (see paragraph 107 b).
- The Draft Guidelines include very specific requirements on the mapping of duties, individual statements, reporting lines, and organisational structures. 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 seem to fit with the existing trend towards simplification in the EU.

So, we encourage the EBA to simplify the drafting of section 6. A more concise and principle-based text would achieve the intended supervisory objectives without introducing unnecessary prescriptiveness and would allow institutions to apply the Guidelines more effectively within their national governance frameworks.

Moreover, the detailed requirements set out in the draft Guidelines, for instance paragraphs 20, 68a, 68b, 68c and Annex II, will put an administrative burden on the institutions that will come at significant cost of implementation and maintenance. Due to, but not limited to, the application on a sub-consolidated and consolidated basis. Institutions should be given the option to comply through existing organizational charts, business allocation plans, lawful allocations of responsibilities, existing top management position descriptions, etc.

- The prescriptive nature of the proposed Guidelines may not lead to the development of a harmonised internal governance framework across the EU. This is particularly concerning given the possibility of divergent expectations among supervisors, which could lead to inconsistent implementation and increased compliance burden for banks.

This lack of harmonisation means that banks that provide services in multiple EU jurisdictions may face inconsistent (supervisory) expectations about, for example, who should have an individual statement of responsibilities and be included in the mapping of duties.

- CRD VI confirms that Key Function Holders 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 (if not part of the management body). 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.

*

Specific comments

Background and rationale

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. ~~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, we suggest 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 guidance into *de facto* binding requirements. Flexibility 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. It is essential that the Guidelines respect national company law frameworks, as envisaged in CRD.
In this sense, the removal of the following provisions in paragraph 8 should not take place:
"*When implementing these guidelines, competent authorities should take into account their national company law and specify, where necessary, to which body or members of*

the management body those functions should apply". This 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.
For the sake of clarity, it should be clarified in this paragraph and 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).

Paragraph 9 - Similarly, in connection with the variety of national governance regimes, paragraph 9 should maintain also the reference to the possibility of delegating a person or an internal executive body (e.g. executive committee, chief executive officer (CEO), management team or executive committee) as permitted under certain national laws. 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).
We suggest replacing by: "*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 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*".

Paragraph 13 – Definition of "*Chief Executive Officer (CEO)*"- It should be clarified 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). Therefore, we suggest amending as follow: "*means the person who is responsible for managing and steering the overall business activities of an institution* ***and represents the management body in its management function*** *or is part of it*".
Definitions of "*Head of Internal Control Functions*" and "*Key Function Holders*" - We would rather keep the definition of "*Head of Internal Control Functions*" and "*Key Function Holders*" which are core, and still, used in these guidelines and very often subject to misinterpretations. Some other definitions provided in this section are less vital than these ones in our opinion.
Moreover, 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.

Application date - we would expect the Guidelines to clarify their intended application date, especially because the CRD VI has not yet been transposed in most Member States. Without such clarification, the EBA risks getting ahead of the legislative process, which may create uncertainty for institutions regarding compliance expectations.

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

Paragraph 16 - Although guaranteed by Article 74 of the Directive, we feel that the general wording of the revised guidelines greatly softens the application of the principle of proportionality. We believe this principle to be fundamental.

Paragraph 22.c subpoint i – It is not clear the reasons for deleting the concept of independence of the compliance function, given that greater attention seems to be paid to this principle elsewhere.

Paragraph 22.c subpoint i(a) – It is not clear why concentration risk arising from exposures towards central counterparties (CCs) 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.o – It is not clear why concentration risk arising from exposures towards central counterparties is outlined here explicitly (there are processes for other material risks as well and 76 (2) of Directive 2013/36/EU also takes no explicit reference to CCs. Recommend deleting this sub bullet.

Paragraph 29a - 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. We suggest reformulating: "29a. *A member of the management body in its management function may the head of an internal control function as referred to in Title V, Sections 19.1 and 19.3, 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*."

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

Paragraph 51 – We suggest clarifying the wording if we do refer to 2 separate committees. Furthermore, we would like to have confirmed if the remuneration committee is concerned as well by this requirement. We suggest reformulating: "*The risk Committees and the nomination and remuneration committees should be composed of non-executive members of the management body in its supervisory function of the institution concerned.*"
Moreover, 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.
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 6**~~2~~3**.*"

Paragraph 61.c. - The illustrative list under bracket after "*operational*" is not very clear so we suggest keeping it to the current regulation (CRR definition of operational risk and the recently published RTS on Operational Risk Taxonomy) and to only refer to "*operational risks*". We it should not be included in operational risks "*fundamental rights and discrimination*" ***as these fall under compliance risks***.
It is therefore suggested to amend this recommendation as follows: "*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;".*

Paragraph 62: There is no legal basis in CRD VI for the risk committee to "*provide input*" to the remuneration committee regarding "*ESG risks and related targets or key performance indicators*", hence the proposed amendment should be cancelled. Indeed, CRD assigns the risk committee the very specific (and different) task of examining the incentives provided by the remuneration system to verify if they take into consideration "*risks, including those resulting from the impacts of ESG factors, capital, liquidity and the likelihood and timing of earnings*"[1]. Furthermore, assigning this additional task risks creating confusion about the different roles that these two committees have in the definition of remuneration policies and practices. Also, the reference to "*related targets or key performance indicators*" is ambiguous as these are terms typically used in the context of remuneration and incentive systems (especially "*key performance indicators*" which is

[1] Art. 76, par. 4, as amended by CRD VI, *"(…) In order to assist in the establishment of sound remuneration policies and practices, the risk committee shall, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration system take into consideration risks, including those resulting from the impacts of ESG factors, capital, liquidity and the likelihood and timing of earnings".*

never used by CRD VI with reference to ESG risks). This ambiguity increases the risk of potential confusion as to the tasks of each committee and reinforces the need to eliminate the proposed amendment.

Paragraphs 68a. – 68b. - Consider rephrasing and deleting any reference to 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 regarding the management body in its management function. Any setting of guidelines in this regard targeting the management in its supervisory function, e.g. paragraph 68.a.c. of the draft Guideline, is thus out of the EBA's competence. Moreover, provided that new requirements for institutions to draw up, maintain and update a mapping of duties have been introduced by the CRD VI Directive, the additional details included in the EBA Guidelines seem 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:

- clarify that the mapping of duties is not required for the management body in its supervisory function, whose roles are already widely described in the Corporate Governance Reports;
- 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 to the management body in its management function at least with respect to its direct reporting lines;
- delete the following references to roles and duties contained in the mapping of duties:
  - 68a (f) "iii. *the names of all members of the management body, senior management and KFH and a summary of their roles and duties ~~consistent with the individual statements of duties~~"* and
  - 68a (g) "*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~~*",

  because 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;
- specify that the individual statement is collected within the *fit & proper* assessment process for Key Function Holders (KFH) only, while this requirement does not apply to senior managers other than key function holders.

Moreover, as provided in article 88 CRD VI, the Guideline should specify that the mapping of duty and the individual statement is without prejudice to the collective responsibility.
In the end, we would appreciate if the EBA could clarify the terminology used in CRD VI regarding "*reporting lines*" and "*lines of responsibility/duty*": whether these terms refer to distinct concepts or if they are intended to represent the same idea.

Paragraph 68a (b) - Article 109 of the CRD provides for application either on an individual basis, at the sub-consolidated level or at the consolidated level, but not cumulatively at all levels: the provision should therefore be modified accordingly.
In any case, we request clarification on which entities must be included in the mapping of duties at a consolidated level. Specifically, for example, considering a Banking Group comprising a parent company that is a Significant Bank and other subsidiaries (including another Significant Bank, two asset management companies, one brokerage firm, two insurance companies, and financial intermediaries as per Article 106 of the Consolidated Law on Banking (TUB), it should be clarified that the consolidated mapping of duties should be carried out by the parent company only with reference to the group entities that individually fall within the scope of the Guidelines.

Paragraph 68a (e) – Second sentence should be deleted 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 68a (f) - As mentioned above, the reference to management body in supervisory function should be removed, as it is inconsistent with Article 88 (3) of Directive 2013/36/EU. Moreover, 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).
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 that 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 (g) - According to this paragraph, in two-tier-structures, the *"mapping of duties"* should be approved by the management body in its supervisory function. 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.
In any case, given the nature and level of detail of the document, in all corporate governance models, it seems more appropriate and in line with the division of responsibilities between the management body in its supervisory and management function, that the document (mapping of duties) is approved by the management body in its management function without prejudice to applicable national provisions. This may also be inferred from CRD VI Directive, which in recital 54 states, that the new tools "*statements of responsibilities*" and "*mapping of duties*" should ensure further accountability of the members of the management body in its management function, of senior management and of key function holders.

Paragraph 68b (d) - The requirement to submit the individual statement of duties together with all other documentation for each fit-and-proper assessment would create an excessive administrative burden, given that the documentation already required for such assessments is extensive.
This obligation appears to go beyond the standard set in CRD VI Article 88(3), 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.*"
Considering the above, we would outline that, where a fit-and-proper assessment is conducted before the individual formally takes up the position, it would be inconsistent to require a signed individual statement of duties at that stage, as the person may ultimately not be appointed.
The signature of the individual statement should therefore take place after formal appointment and should not be a mandatory component of the fit-and-proper submission package, but rather a document that remains available to the competent authority upon request once the appointment is confirmed.
We would also welcome clarification of the expressions "in due time" in Article 88(3) CRD VI to ensure consistent supervisory expectations across Member States.
In addition, it would be helpful for the EBA to specify, "in accordance with the RTS", whether any further procedural requirements are envisaged beyond the directive's "upon request" standard.

Paragraph 68c - 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. For these reasons this paragraph should be deleted.
In any case, 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). 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.

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

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 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 rationality behind it, we would suggest deleting it.

Paragraph 101a - We suggest specifying also that the selection of indicators should remain within the discretion of the institution, according to its specific organizational, dimensional and operational characteristics. In any case, we suggest that this matter should be addressed within the Guidelines, possibly also in footnote.

Paragraph 107a – This paragraph states "*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.*" The proposed restriction preventing a CEO of a subsidiary from simultaneously serving as Chair of the supervisory body of a parent undertaking appears to exceed the scope of Article 88(1) CRD, which states that "The Chair of the management body in its supervisory function of an institution shall not exercise simultaneously the functions of a chief executive officer within the same institution.". Hence, Article 88(1) CRD appears to be applicable only to a same institution.

Paragraph 107b – The provision envisaged by the EBA Guidelines of a cooling-off period of at least three years, during which the CEO cannot be appointed as Chair or member of the Board of Directors, 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"). The effect of this provision is to restrict the company's autonomy in appointing the Chair and non-executive directors. 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 provision of a colling-off period should be deleted and 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 171 – The phrase "*Institutions may establish a separate AML/CTF compliance function as an independent control function*" should be revised "*Institutions may establish a separate AML/CTF compliance function as an independent control function or may assign this function to the compliance function. It remains the appointment of a member of the management functions responsible for AML/CTF (with executive role)*".

Paragraph 172 - We think 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. On the other hand, paragraph 176 should deal 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 the senior person as provided under new paragraph 6 of article 76 of the Directive 2013/36/EU introduced by the CRDVI when conditions established thereto are met such as but not limited to there is no conflict interest. 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 the head of an internal control function performs other 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 174 (a) - We suggest to rephrase: "*In accordance with Article 76 paragraphs 5 and 6 of Directive 2013/36/EU -* ***and notwithstanding point 172*** *- institutions should have internal control functions independent of the operational functions and of the members of the management body in its management function and of senior management, allowing them to have direct access and report directly, as appropriate, to the management body in its supervisory function. This independence should be achieved by having appropriate and sufficient authority and stature, the ability to access directly and escalate any issue to the management body in its supervisory function where appropriate to fulfil their mission."*

Paragraph 176 - The new wording of the paragraph relating to the combination of internal control functions seems not very clear. 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*". Probably "***or***" should be replaced with "***and****"*.

Paragraph 201 – In accordance with (new) paragraph 29a and paragraph 172, also a member of the management body in its management function may be responsible for an internal control function. 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."***

Moreover, 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. 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 - 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.

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

Paragraph 230 - This paragraph 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.