Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Comments

EBA Consultation Paper on
Draft revised Guidelines on internal governance under Directive 2013/36/EU (EBA/CP/2025/20)

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Thomas Lorenz
Function
Telephone: +49 30 1663- 3190
E-Mail: Thomas.lorenz@bdb.de

Berlin, 7 November 2025

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
https://die-dk.de
www.german-banking-industry.org

I. Basic principles

In the opinion of the German Banking Industry Committee (GBIC), the EBA's planned revision of the "Guidelines on internal governance" is generally to be welcomed, particularly with regard to the implementation of relevant CRD VI requirements. However, at the public hearing on 5 September 2025, the EBA also emphasised that the overarching objective of the guidelines was to provide guidance to institutions rather than to impose binding rules. Unfortunately, this objective has not been achieved: In effect, a binding and complex regulatory regime is being created that does not adequately take account of the principle of proportionality. Bureaucracy and unnecessary regulatory complexity are not being reduced but are continuing to increase. In addition, the planned requirements, some of which are very detailed, will at best create limited added value for both the entities subject to regulation and the supervisory authorities.

Take account of the principle of proportionality

Recital 60 of CRD VI states that, when developing standards and guidelines, the EBA should take due account of the principle of proportionality and ensure that those rules can also be applied by small and non-complex institutions without unnecessary effort. We do not consider this objective to have been achieved in this consultation paper. Instead of examining paths to more principle-based requirements and possible additional opening clauses for small and non-complex institutions (SNCIs), individual requirements – particularly those relating to the 'mapping of duties' and 'individual statements of roles and duties' (paras. 68a and 68b) – were formulated in excessive detail. These requirements, in particular, should be reviewed again in their entirety.

Regulate monitoring of ICT risks in line with DORA rules

In paragraph 25 of the section entitled 'Rationale and objective of the guidelines' on Regulation (EU) 2022/2554 (DORA), it states that the ICT risk management function should be organised in accordance with the three lines of defence model, taking into account the principle of proportionality. We recommend deleting this recital or, at the very least, aligning it with the different wording in Article 6(4) of DORA in order to avoid contradictions. There it states that, "Financial entities [...] shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model."

Clarification that additional control functions are permissible

According to the public hearing of Sept 5th, EBA understands risk management and compliance as mandatory functions within a second line. Institutions may set up additional control functions. However, the examples for the additional control functions can be currently misleading to interpret the formal exclusion from the second line of other functions, which also monitor and oversee risks (e.g. Human Resources, Physical Security). A clarification on this regard enhances transparency for institutions. Proposal: additional note on risk management and compliance being mandatory second line functions within a second line and in accordance with the proportionality principal.

Do not pre-empt upcoming EBA guidelines on third-party risk management

In section 8 (Third-party risk management policy), a reference to the planned EBA guidelines would be sufficient; a list of contents is dispensable. Irrespective of this, the transition/implementation periods provided for in the (final) TPRM guidelines should also be applicable to the policy.

II. Individual comments

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

No, we still see a need for changes/clarifications in this area.

Scope of application

Para. 8: Reference to national company law and the requirement for competent authorities to specify the relevant body under national law should remain ("*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.*"); it is unclear why this should be eliminated.

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

No, we still see a need for changes/clarifications in this area.

Application of the proportionality principle

Paragraphs 16 – 18: As the wording of the proportionality principle in Title I refers exclusively to institutions, we request clarification that this principle also applies to the now expanded scope of the guidelines, i.e. in particular to (mixed) financial holding companies.

Role and responsibilities of the management body

No. 20: Please refer to our comments on question 3 and paras. 68a – 68c and Annex II.

Supervisory function of the management body

Para. 22: In point c (i) ("*includes a clear organisational structure...*"), deletion of the term 'independent' is unnecessary, as it is in para. 206, particularly given the emphasis placed on the **independence of internal control functions** elsewhere in the guidelines (e.g. para. 174a in section 19.2, "Independence of internal control functions" or para. 176 in section 19.3 "Combination of internal control functions").

Since the independence of internal control functions (risk management, compliance and internal audit) is a fundamental principle of governance, as set out i.a. in Article 76(5) and (6) of CRD IV, we would welcome there being clarity and consistency within the guidelines on this, among other things. At the least, it should be made clear at the beginning of the guidelines that this principle must also be observed even if it is not explicitly mentioned in the context of internal control functions, to avoid any misunderstandings.

Para. 22: In point c i (a) ("*includes effective processes to …*"), we cannot understand why concentration risk from exposures to central counterparties should be explicitly mentioned here, especially since there are also procedures for other concentration risks. We recommend deleting the specific reference to central counterparties.

Para. 22: In point c. i. (b) ("*network and information systems...*"), the wording is linguistically/grammatically unclear and should be amended.

Para. 22: According to point o ("*specific plans and quantifiable targets...*"), requirements for specific plans and quantifiable targets with regard to concentration risks are to be established by central counterparties. However, there is no legal basis for this; Article 76(2) of Directive 2013/63/EU does not explicitly mention it. This requirement would also be excessive, particularly for smaller institutions with only minimal exposures to central counterparties and would lead to unnecessary administrative (documentation) effort. These requirements should therefore be removed and not replaced.

Para. 33: The **management body in its supervisory function** should include **independent members** in accordance with the provisions of Section 9.3 of the joint ESMA and EBA guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU. However, this requirement **still lacks a legal basis in CRD VI** and should therefore be removed.

Role of the chair of the management body

Para. 37: We understand the proposed deletion of sentence 2 ("*Where the chair...*") to mean that there should no longer be any exceptions to the principle set out in sentence 1 of para. 37 that the chair of the management body should not exercise any executive functions. However, in dualistic systems with separate management and supervisory functions (also taking into account national company law requirements), this would generally not be feasible or relevant anyway, especially since there are no uniform requirements for the chair of the management body. As a rule, the institutions also have suitable guidelines/measures in place to address potential conflicts of interest here.

The second sentence of paragraph 37 ("*Where the chair is permitted to assume executive duties, the institution should have measures in place to mitigate any adverse impact on the institution's checks and balances…")* should therefore not be deleted. At the very least, it needs to be clarified that this requirement only applies to monistic systems.

Role of the risk committee

Para. 61 point c ("*fundamental rights*"): Since the violation of fundamental rights by an institution is already covered by the 'legal risks' referred to in point c. the addition of 'fundamental rights' is not necessary. It should therefore be deleted. However, if ESG risks are involved here, the wording should be adjusted accordingly.

61 point c ("*discrimination*"): Please clarify the intended meaning of "discrimination" in this context and from which Article of the CRD VI this requirement is derived as it remains unclear.

Please consider that the Supervisory Board itself is better suited to allocating the topic of discrimination (including risks stemming from it) to a committee best equipped for it. This could be an ESG-Committee or the Audit Committee as it also handles whistleblowing reports. If discrimination risks arise, combined sessions with the Risk Committee would be better suited instead of allocating this topic exclusively to the Risk Committee.

Against this background, consideration should be given to deleting this passage.

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

No, we still see a need for changes/clarifications in this area.

Organisational framework

General comments on para. 20, paras. 68a – 68c and Annex II:
Given existing legislation, e.g. requirements in paragraphs 20, 22, 43 of the Guidelines, it is questionable why it needs these additional detailed provisions. Whilst the language of Article 88(3) Directive 2013/36/EU leaves room for the institutions to comply in a proportional way, the detailed requirements set out in the draft Guidelines will put an administrative burden on the institutions that will come at significant cost of implementation and maintenance. Therefore, in view of the principle-based requirement in Article 88(3) CRD VI, the level of detail in the planned additions to the 'mapping of duties' and the 'individual statements of roles and duties' appears excessive, even taking into account the proportionality criteria (Title I of the Guidelines).

Including the management body in its supervisory function under point c of para. 68a (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. In addition, it would not be practical as the management in its supervisory function does not have any reporting lines or any lines of responsibility. Any setting of requirements in this regard targeting the management body in its supervisory function is thus outside of the competence of the EBA. Please see also our detailed comments relating to paragraphs 68a lit c et seq., which can be found further below.

Furthermore, with particular regard to Article 88(3), we would like to expressly refer to the cost-benefit analysis as per chapter 5.1 here. 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. Furthermore, the draft guidance could conflict with national legislation, e.g., regarding the roles of Management Boards and Supervisory Boards as per German Public Companies Act.

Article 91(14) CRD VI contains a proviso that Articles 91 and 91a CRD VI apply without prejudice to member states' laws on the appointment of members of the management body in its supervisory function by regionally or locally elected bodies or by nomination in cases where the management body is not responsible for the selection and appointment of its members.

The EBA guidelines should also include this explicit proviso or refer to it explicitly, as they cannot go beyond their legal basis. In such cases, a 'mapping of duties' should be superfluous. In our view, there would otherwise be a risk that individual fit and proper assessments will have to be carried out, particularly under paragraphs 68b and 68c (individual statements/duties). Furthermore, it should be noted that there are also institutions that have no influence on the composition of the management body in its supervisory function, including gender-neutral composition. The above statements also apply to paragraph 101a of the draft accordingly.

If, despite our fundamental criticism, these requirements are to be retained, they would have to be significantly reduced overall, including by omitting unnecessary detailed specifications and duplications. For example, it is unclear why the mapping pursuant to paragraph 68a point (c) should also address individual duties if there are to be additional individual statements. Credit institutions already have extensive internal documentation defining tasks and duties (strategies, organisational charts, job/function descriptions, rules on powers and responsibilities, etc.). Therefore, if separate documents are deemed necessary for the purposes of Article 88(3) CRD VI, it should suffice to summarise the most important points therein. However, the requirements of paragraphs 68a and 68b give the impression that almost all of the content of the internal governance rules would have to be compiled again in new formats.

At the public EBA hearing on 5 September 2025, it was emphasised that the EBA's overriding concern was to provide guidance to institutions rather than to impose binding regulations. This should be made clearer in the guidelines, particularly in this area.

In particular, it should be noted that:

- **Para. 68a point c** ("*The management body should…*"): The provision to outline the duties for each role of the management in its supervisory function is not only redundant with para. 68b, but also disproportionate for a 2-tier-system as the members of the Supervisory Board only have this role. Extensive documentation of the backgrounds, skills and experiences of the members of a Supervisory Board already exists (e.g. CVs, competence matrix and documentation of experts of certain topics). This requirement goes beyond the stipulation in Art. 88 (3) CRD VI and therefore has to be deleted.

- **Para. 68a point f. (ii**) ("*how the management…*"): The competences of the management in its supervisory function (Supervisory Board) are derived directly from statutory company law and/or the Articles of Association of the legal entity. The duty to additionally draw up an explanation is disproportionate and redundant. This provision goes beyond the duties in Art. 88 (3) of Directive 2013/36/EU and this wording lies outside of the guiding-competence of the EBA. Against this background, the reference to the supervisory board should be deleted.

  In this context of **para. 68a point f. (ii)**, the following should be noted with regard to 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.

- **Para. 68a point f. (v)** *("a rationale for…"*): This requirement goes beyond the wording of Art. 88 (3) of Directive 2013/36/EU. Non-executive directors of the management board hold their function based on statutory law added by already public, clear and detailed provisions in the Articles of Incorporation as required by Company Law. Extensive documentation of the backgrounds, skills and experiences of the members of a Supervisory Board already exists (e.g. CVs, competence matrix, documentation of experts of certain topics). Against this background, at least the members of the supervisory board should be exempted from this requirement.

- **Para. 68a point g** ("*The Management Body…"*): This provision goes beyond what is required according to Art. 88 (3) of Directive 2013/36/EU. Art. 88 (3) of Directive 2013/36/EU only requires institutes to prepare documentation and keep it updated. No voting and approving necessity can be interpreted from the wording. An approving necessity by the Supervisory Board is unlawful under 2-tier company law, ineffective for its desired effect and simpler, yet more effective alternatives exist: (1) Roles, functions and duties need to retain flexibility, they will not be drawn up and then left unchanged for a long period of time; (2) A 2-tier supervisory board is not competent for allocation and supervision of duties and roles below the management level as this responsibility is strictly operational, and (3) The decision-making process, especially of a 2-tier-board would strongly delay any flexible reshaping and changing of company roles and responsibility. Against this background, at least the members of the supervisory board should be exempted from this requirement.

- **Para. 68b point b** ("*The allocation...*"): The indication of the expected time commitment should remain part of the Fit and Proper (FAP) - assessments and not be extended to members of the senior management which are not subject to FAP assessment.

- The requirement in the **second sentence of para. 68b point c** ("*the individuals should be able to...*") according to which members of the management and supervisory boards must prove to the supervisory authorities upon request that they have fulfilled their intended duties, also appears to us to be objectively unjustified. Credit institutions must in any case be able to provide evidence at any time that they comply with banking supervisory requirements (in Germany, for example, through supervisory audits in accordance with Section 29 of the German Banking Act (KWG) and as part of special audits in accordance with Section 44 KWG). This already includes appropriate disclosure obligations for the institutions and their bodies. Additional personal accountability of individual board members to the supervisory authority would constitute overregulation, particularly when applied to LSIs. If this requirement were also applied to supervisory board members, it could further reduce the willingness of suitable representatives of the regional economy to accept such mandates. The last half of paragraph 68c should therefore be deleted.

- **Para. 68b point d** ("*The individual statements..."):* 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. The signature requirement goes beyond

what is required according to Art. 88 (3) of Directive 2013/36/EU. Further, a signature requirement conflicts with national employment law as a change of contract.

- **Annex II**: The "*Optional template for individual statements of roles and duties*" provided for in Annex II should be omitted. There is a significant risk that this template could be (mis)interpreted as binding. If a supervisory authority considers it necessary to prescribe a specific format for the institutions it supervises, it should coordinate this with the relevant addressees.

- **Para. 68c sentence 2** *("The institutions should take appropriate…."*): It should be clarified that in this case "management body" is to be understood as "management body in its management function" (Article 3(1)(8a) CRD VI). A supervisory body's responsibility for assigning tasks below the management body would not be compatible with German (stock corporation) law.

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

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

No, we still see a need for changes/clarifications in this area.

Corporate Values and code of conduct

Para. 101a: In future, institutions are to be required to establish indicators to monitor gender diversity among their employees and, where necessary, take appropriate action in terms of human resource management. A number of example indicators are given for this purpose. This amendment should be rejected, as implementing this monitoring obligation on the basis of the examples given or similar indicators would create additional bureaucratic effort. This would be particularly inappropriate for small and medium-sized institutions with a relatively small workforce and would be of little benefit. Alternatively, the requirement should be expressly subject to the principle of proportionality. At the very least, any mention of example indicators should be removed, as otherwise a list is likely to create supervisory expectations. Even though these would only be non-binding examples, the institutions could in fact find themselves compelled to include at least some of them in their monitoring.

Conflict of interest policy at institutional level

Para. 107a („*In accordance with…*"): Article 88(1) CRD VI, referred to in paragraph 107a sentence 1, merely prohibits in paragraph 1, subparagraph 2 point e) the simultaneous exercise of the functions of chair of the supervisory body and of the CEO, which is not permitted in dualistic governance systems anyway. Further requirements regarding the simultaneous exercising of management duties in a parent company and supervisory duties in a subsidiary, as well as requirements in the event of non-compliance with a three-year waiting period between membership of the management and supervisory bodies (as outlined in paragraph 107b), are not included in CRD VI. Para. 107a should be amended accordingly.

Para. 107b ("*Where it is decided...*"): A cooling-off period of three years is indirectly proposed for the transition from CEO positions to the supervisory board. This requirement, which is not objectively justified, should be scrapped.

- There is no legal basis for this. Article 4a (4) of CRD VI only provides for a cooling-off period in the event of a member of the supervisory authority moving to an institution. This period only has to be between six and 12 months. However, in the case under consideration here, where the CEO is transferring to the supervisory board, there is no corresponding legal requirement in the CRD.

- With the planned indirect introduction of a cooling-off period of three years, the EBA would be exceeding its mandate under Article 74(3) CRD in conjunction with Article 16(1) EBA Regulation, according to which it may close loopholes within the CRD requirements but may not establish regulations that go beyond the CRD. The EBA's reference in the public hearing on 5 September 2025 to the existing EBA/ESMA guidelines on the assessment of the suitability of members of the management body and key function holders (fit and proper guidelines) is misguided since, according to these guidelines, previous membership of the management body merely leads to non-independence in the supervisory body (paragraph 89(a)), and even then only in principle (paragraph 90). To this extent, the fit & proper guidelines cannot be used to justify implementation of CRD VI with rules that go beyond the original intention of the directive.

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

No, we still see a need for changes/clarifications in this area.

Independence of internal control functions

Para. 175 point d: Consider revising to "remuneration system". It is incorrect that the "remuneration" should be directly overseen by the management function in its supervisory function. The supervisory function is only responsible for the "remuneration system" but not for the individual compensation package.

Compliance function

Paras. 209 – 210: The change in wording from "compliance risk" to "legal risk stemming from non-compliance events" raises significant questions regarding the distinction between compliance risk and legal risk. The proposed amendment appears to conflate the responsibilities of the compliance function with those of the legal department, which we consider neither practical nor appropriate. Furthermore, this wording change contradicts Article 76(5) point e CRD VI, which explicitly assigns responsibility for compliance risks to the compliance function ("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 decision"). We therefore recommend keeping the original wording.

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

---

* * * * *