


POSITION PAPER



ESBG response to the EBA consultation on guidelines for internal governance

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

January 2017



As a general comment, ESBG is of the opinion that there is no analysis or description that identifies deficiencies that require a total revision of the previous EBA guideline number 44 on Internal Governance (GL44). The understanding of the guidelines and a proper implementation requires a well-defined rationale and a description of the material changes and the purpose for these. There are difficulties to see or discover where changes have been made because the structure has also been changed. In some cases just one word has been changed compared to GL44, and it is unclear if the new wording is meant to change the whole meaning of the requirement or if the scope should be the same, see for example subparagraph 106 where “management body shall” is changed to “management body should”.

In our view the most problematic issue is the independence requirements (Title I, Sections 3, 5.1 and 5.2) and the conflicts of interest (Title II, Section 9.3) for members of the management body. The framework regarding independence/conflicts of interest and the distinction between these two concepts is not sufficiently clear, is impractical and does not take into account the applicable national legal provisions. The applicability of the proposed independence criteria will impede in the future the election of suitable and high qualified members and will consequently significantly restrict the proper selection of members of the management body in its supervisory function.

As understood, the EBA has intended to take the BCBS corporate governance principles for banks and the “three-lines of defence model” into account (paragraphs 18 and 20). However, it is important that certain changes as outlined below are made, since there is a risk that the concept that the first line of defence is overall responsible for risk management, including internal control¹ could easily be misunderstood given the terminology used in the Draft Guidelines. The BCBS Guidelines defines internal control system as: “A set of rules and controls governing the bank’s organizational and operational structure, including reporting processes, and functions for risk management, compliance and internal audit”. Paragraph 114 of the draft guidelines describes this model well. However, other parts of the guidelines are less clear on this. Therefore and to underline more clearly that the first line is responsible for risk management and must also establish internal control systems, we suggest that the second and third line of defence (i.e. Risk Control, Compliance and Internal Audit), when referred to collectively is referred to as “Independent Control Functions” (rather than Internal Control Functions) to better underline that these functions are part of (and not the entire) internal control system of the institution. Consequently the defined term “Heads of Internal Control Functions” should be changed to “Heads of Independent Control Functions”. Also, the “Risk Management Function” should be renamed “Risk Control Function”. This is so because “Risk Management” shall be performed also in the first line (in accordance with what is stated in paragraph 20) and not only in a second line function. Risk Control is the terminology that should be used for the independent risk control performed in the second line.

Q1: Are the guidelines regarding the subject matter, scope, definitions and implementation appropriate and sufficiently clear?

Concerning the implementation date, ESBG would propose giving institutions sufficient time to implement these Guidelines as banks will have to modify their organisational structure, define processes or modify policies. We therefore consider that the earliest application date should be one year after its publication.

¹ The concept that “internal control” is a responsibility for the management and the first line (and something wider than only the work performed in the second and third lines of defence) is also described in e.g. item 93 of the Guidelines on Corporate Governance principles for banks issued by the Basel Committee in July 2015.



An institution's ability to assume risk should not only be assessed in relation to the institution's capital and liquidity base or level of risk management and control capabilities. It should also be compared to the level of competences that the institution possesses in order to secure the ability to understand, analyse, measure and manage the types and levels of risk exposures. Therefore, the definition of "risk capacity" should be amended as follows: Risk capacity 'means the maximum level of risk an institution is able to assume given its capital base, risk management and control capabilities, level of competences, as well as its regulatory constraints. Risk capacity is a new concept defined without any rationale and it is just mentioned a few times in the guideline. In subparagraph 83 it's used as interchangeable with risk appetite which is not correct and in subparagraph 84 b) the requirement for all staff to know and understand the risk capacity is to far reaching.

The definition of Compliance risk in GL44 is not included in the draft guideline and there is no explanation for this. It could be useful with a definition but the one provided for in GL44 is too wide since it includes violations and non-compliance with agreements.

In addition it should be clarified if any change is intended with the new more narrow definition of risk appetite instead of the definition in GL44 "Risk tolerance/appetite" which described both the absolute risks an institution is a priori open to take (which some call risk appetite) and the actual limits within its risk appetite that an institutions pursues (which some call risk tolerance).

According to paragraph 13, competent authorities shall determine other institutions as significant, based on an assessment of the institutions' size, internal organisation and the nature, the scope and the complexity of their activities. The identification of systemically important institutions already account for those criteria. A separate classification for the purpose of these Guidelines is not necessary. The definition should clearly be restricted to systemic relevance, and in the further requirements of the Guidelines, 'significant institutions' should be replaced by 'systemically important institutions'.

The definition of "key function holders" should be amended, as Article 91 of Directive 2013/36/EU (CRD IV) refers only to members of the management body, not to key function holders. There is no legal basis for setting the requirements for assessment on key function holders. The guidelines should limit to the harmonisation of the CRD IV-requirements. Additionally, the definition is so far clear ("persons who have significant influence over the direction of the institution"), as key function holders are the heads of internal control functions and the CFO, where they are not members of the management body. However, the addition "and other key function holders" is not sufficient and should therefore be deleted.

Q2: Are there any conflicts between the responsibilities assigned by national company law to a specific function of the management body and the responsibilities assigned by the Guidelines, in particular within paragraph 23, to either the management or supervisory function?

The draft guidelines claim not to advocate any particular structure and to embrace all existing governance structures (unitary, dual board). This claim does not seem to be clearly applied to all requirements and therefore an opening clause that makes this claim would improve clarity.

Additionally, ESBG would like to express our concern about the impact of the proposed Guidelines on the unitary board structure. In particular:



- Member States' company law allows for either a unitary and/or a dual board structure. EBA rightly explains that the guidelines do not advocate any particular structure and are intended to embrace all existing governance structures. However, those considerations have not been assigned accordingly in the consultation paper. We fear that that the recommendations of the guidelines result in reality in a mandatory dual board structure, due to the fact that some of the statements seem to propose the separation of the management body in its management function (with executive members) and the management body in its supervisory function (with non-executive members).
- A dual system is characterised by the fact that there are two separate boards of directors: (i) Management Board, and (ii) Supervisory Board. Each of these serves a particular purpose. However, we do not foresee how the unitary board structure will be able to comply with the EBA guidelines in particular with the proposal to clearly separate the management body in its management function and in its supervisory function, as it would not be legally possible in some Member States.
- One such example is paragraph 32, as there is a discrepancy with some national law. For example, according to Swedish law the “management body in its management function” and the “management body” in some cases must be interpreted as the CEO. The CEO shall as such make decisions as provided for by law as well as in accordance with the delegation from the management body. For this reason, ESBG would request that paragraph 32 is deleted.

ESBG would therefore request the EBA to adapt the guidelines in order to make it clear that both board structures (unitary and dual) are adequately contemplated, especially in view of the fact that some Member State's company law only allow for unitary Board structures.

According to the last sentence of para. 23 the management body in its supervisory function should “ensure” the integrity of financial information and reporting. “Ensure” could be interpreted as the supervisory functions exercising a more active role than would be allowed by law. For example, the Austrian Banking Act requires (§ 63a para. 4) the Audit Committee of the Supervisory Board to evaluate the independence of the external auditor as well as the annual financial statements and to supervise the accounting process, the effectiveness of the internal control system, internal audit and risk management as well as the audit of the financial statements. In our view, “evaluate” and “supervise” are not necessarily the same as “ensure” and we suggest aligning the wording, in order to ensure that these are in line with the applicable legal provisions.

ESBG would appreciate if section 3 – Role of the chair of the management body – could be clarified, as all paragraphs of section 3 (other than para. 27) mention the chair, without specifying whether this applies to the management body in its management or supervisory function (or both). In addition, para. 29 only applies to one-tier board structures (in two-tier boards, the allocation of responsibilities between executive and non-executive members results from the board structure with Management Board and Supervisory Board). This should be made clear in the text.

Q3: Are the guidelines in Title I regarding the role of the management body appropriate and sufficiently clear?

The requirement upon the management body regarding issues related to compliance, risk management, internal control, reporting, etc. are quite extensive. Such issues are clear and important conditions for running a credit institution. However, the large extent of such requirements must not



overshadow the board's important role and huge responsibility when it comes to establishing clear and realistic goals for the institution, establishing business strategies and business plans and following up on such goals, strategies and plans. It would be helpful if these guidelines also pointed out those important issues among the responsibilities of the board, as some Member State's company law include them as competences of the Board that cannot be delegated.

Paragraph 43 demands that each member of the committee individually has the required skills and level of competence. However, individual members are sometimes recruited due to specific skills in order to balance the profile of other committee members so that the collective competences of the committee are appropriate. It is our opinion that the individual requirements should instead be related to an expectation for a certain minimum insight into and understanding of risk management and internal control principles, for example by requiring that each member of the risk committee possess a basic understanding of the fundamental principles for risk management and internal control, and at the same time requiring the risk committee collectively to possess appropriate knowledge, skills and experience compared to the institutions business model, size, complexity and risk profile.

Paragraph 43 should also demand that members of the audit committee have the relevant and necessary accounting skills, proportionate to the institution's character, size and complexity as the wording "audit processes and practices" does not signal the need to understand relevant accounting principles and technicalities in order to carry out the duties of this committee.

ESBG believes that section 6.3 is not sufficiently clear. This chapter seems to address both the issue of complexity in an institution's own organisational structure and the complexity issues related to client activities. Both issues are relevant, but mixing those topics together is confusing. We would like to propose that section 6.3 is reserved for topics related to an institution's own organisational issues. Governance guidelines regarding client activities should be addressed in a separate chapter.

According to paragraph 34, the risk and nomination committee should advise the management body in its supervisory function "and prepare the decisions to be taken by this body". ESBG believes this requirement needs more clarity to allow committees the right to take decisions. Support means not only helping the management body to make decisions but means also to be able to make own or delegated decisions. The decision of the committee is therefore a decision of the management body in its supervisory function. Furthermore, the planned restriction would restrict the right to delegate certain duties and decisions to committees granted by German company law (Article 107 (3) Aktiengesetz). ESBG therefore believes that "and to prepare the decisions to be taken by this body" should be removed from the guidelines.

According to the draft guidelines (paragraph 37), committees should not be composed mostly of the same group of members which form another committee. In our experience, there are useful overlaps between committees regarding the flow of information and time spent understanding the work of all committees. For those institutions which have small management bodies in their supervisory function (under 10 people) it would not be possible to establish committees at all. This would also be the case for institutions with small management bodies in unitary structures. Therefore ESBG would appreciate if the final sentence of paragraph 37 could be removed.

Regarding paragraphs 37, 42 and 44, an appropriate number of independent members within the committees is proposed. In our opinion, it should be made clear that this requirement exists only if the management body in its supervisory function is obliged to form committees (risk, nomination or audit committee). These requirements should also contemplate unitary Board structures.



Some of the requirements in this section are too specific. For example, in paragraph 46 the risk and nomination committees should have ‘access to all relevant information and data including access to information and data where appropriate access to information and data from relevant corporate and control function (e.g. legal, finance, human resources, IT, risk, compliance, audit etc.)’. Giving these committees direct access would be problematic because of data protection issues, and is not necessary, as the board and committees receive regular reporting, ad-hoc information, communications or opinions from heads of internal control functions (see paragraph 46, part (b)).

Referring here to para. 47 (g) ESBG would like to point out that the requirement to “examine the alignment of all financial products and services offered to clients and the business model as well as the risk strategy” is impractical, as the risk committee will not review each product individually. Rather, the risk committee should review the policies and procedures in place to ensure that products and services are aligned to business and risk strategies as well as the risk appetite (e.g. the new product approval policies) and satisfy itself that these policies consider all relevant aspects are implemented throughout the organisation and function as intended (e.g. through a review of internal audit reports and supervisory examination reports related to the implementation of the policies). The risks associated with the offered products as well as the alignment of prices and profits can again not be examined at the granular level of each individual product. Rather, the risk committee should receive aggregate analytical information providing it with the necessary detail to decide whether the required alignment is in place.

Article 51 states that the audit committee has the responsibility to oversee the internal control on financial reporting. This is a useful clarification, but it also creates a possible source of uncertainty. The question that might be raised is if the audit committee also has the responsibility to oversee internal controls in other areas or if is that responsibility implicit is placed by any other committee. It would be helpful if the guideline could clarify the regulatory expectations regarding that issue.

In paragraph 51 of the draft guidelines, competent authorities may allow less significant institutions to establish a joint risk and audit committee. Since less-significant institutions are not required to form the above committees, it should be clarified that institutions should be able to form joint committees without permission from the competent authority.

The draft guidelines aim to embrace all existing governance structures (i.e. unitary, dual board), however this does not appear to apply to all requirements. For example, paragraph 53 requires the management body of an institution to ensure a suitable and transparent organisational and operational structure. In the German governance system, this is a responsibility of the executive directors only. In some Member States, this responsibility lies with the executive directors, therefore it has to be ensured that this provision is compliant with the existing national regimes.

Paragraph 57 should be amended as follows ‘should know and understand the main features of the organisational and operational structure of an institution’.

Para. 60 requires in its last sentence the management body to “ensure ... that the institutions within the group comply with all supervisory reporting requirements”. Firstly, we have the same reservations as to the use of the wording “ensure” as already outlined under our comment to para. 23 above. Thus, the wording should be reviewed and amended as appropriate. More importantly, however, is the fact that in our view it is rather the responsibility of the local management bodies of the subsidiaries within the group to ensure that supervisory reporting requirements are met. The management body of the consolidating institution is in our opinion responsible for supervising if adequate internal controls and sign-off procedures are implemented in its subsidiaries.



Q4: Are the guidelines in Title II regarding the internal governance policy, risk culture and business conduct appropriate and sufficiently clear?

ESBG is of the opinion that the value of these guidelines would be strengthened if they also clarify the division of roles, responsibilities and decision making power between the board of the mother company and the boards of subsidiaries.

Regarding paragraph 70 (Annex I), the aspects which should be taken into account when defining governance principles are too broad and do not allow the institutions enough scope. What a policy should contain has been mixed with actions taken or shortcomings noted by control functions. It is not reasonable to require a policy to include e.g. weaknesses identified by each control function (6 c) or recommendations made by the internal audit function (6 d). Even though recommendations by the control functions should be considered, these should not be included in a policy document. The aspects contained in the annex could, however, serve as a useful source for compliance teams in relation with these Guidelines.

Additionally for paragraph 70 (concerning Annex I), and in the case where these aspects are retained, ESBG would suggest that the exact weaknesses identified by each internal control functions are not included in the internal governance policy. While we support that the policies to identify such weakness should be included, we believe that the weaknesses themselves should be reported to the management body but are not part of the internal governance policy.

On a related note, we consider it doubtful whether the requirement that the management body should adopt a governance policy in itself serves to strengthen or clarify governance arrangements in institutions. Institutions should have suitable governance arrangements that should be reflected in steering documents adopted at various levels. A requirement that some of these arrangements should be set out in a policy adopted by the management body does not in itself contribute to clear and suitable governance arrangements. Moreover, we note that some of the topics mentioned in Annex 1 to the proposed guidelines concern matters that – in some Member States’ company law – fall within the ambit of the CEO. If a policy adopted by the management body addresses issues that are normally the responsibility of the CEO pursuant to applicable company law, this will not be conducive to clarifying governance arrangements in the institution.

Finally, para. 70 requires the implementation of a governance policy establishing “a clear organisational and operational structure with well-defined, transparent and consistent lines of responsibility”. Annex I establishes further the aspects to be taken into account when developing the internal governance policy. Most of these aspects are already implemented and laid down in the internal regulations and policies of the institutions. For example, the composition and functioning of the management body and the specialized committees of the management body in its supervisory function are already laid down in the Articles of Association and the Internal Rules of the committees. Aspects regarding key function holders are laid down in the Suitability Policy. The internal control framework is set in the internal regulations and policies of the internal control divisions (Audit, Compliance, and Risk Management). We therefore do not consider necessary to establish an internal governance policy to cover all these aspects mentioned in Annex I. We do believe that it would make more sense to require the institutions adapting their existing policies and regulations to the new aspects of the Internal Governance Draft GL.



Regarding paragraph 77, the assessment of independence of the members should comply with national laws in order to avoid conflicts with legal frameworks of savings banks including the cooperatives' one. For example, the criteria related to personal, professional or economic relationships with the owners of qualifying holdings in the institutions with the institution's or any subsidiaries is not compatible with legal provisions governing the French savings banks (e.g. Article L.512-106 of the French Monetary and Financial Code).

For paragraphs 85 and 87 (c), the requirement to define a catalogue of acceptable and unacceptable behaviour will be difficult to achieve. A single list of all acceptable and unacceptable behaviour would take up significant resources and time. Moreover, it is not possible to predict every possible scenario that could occur. The guidelines already contain various instruments to ensure compliance with legal and internal guidelines as well as ethically-correct behaviour and therefore a code of conduct should not be required for small institutions and thus the catalogue of acceptable and unacceptable behaviour should be deleted.

In paragraph 92, we would request clarification on the exact meaning of "other related parties". EBA Guidelines require that the conflict of interest policy of an entity should cover a list of relationships between an institution and, among others, "other related parties" (e.g. its parent company or subsidiaries). The meaning and possible connections with other EU legislation (e.g. Market Abuse) of this particular term are not sufficiently clear.

Additionally in paragraph 92, ESBG would appreciate clarification for part f, legal or natural persons closely linked to persons under points (a) to (e) above.

Para. 95 requires institutions to issue a statement in case of any identified conflict of interest. This could conflict with some Member States' company law, for example in Austria the legal framework (the Stock Corporation Act and the Corporate Governance Code but also the Banking Act) contains clear and sufficient provisions for dealing with conflicts of interests at the level of the management body (e.g. voting abstention of the concerned member, disclosure requirements). We therefore do not see the necessity of any additional legal requirements with this regard.

Regarding paragraph 101, even if the case should justify measures being taken against persons, such persons still should be protected against unjustified negative effects and should be protected by relevant confidentiality rules.

ESBG is concerned by the chosen approach in chapter 10. By inviting all employees to report possible breaches of laws and regulations to the authorities such authorities might end up by receiving a large amount of information with different value and quality. It is also a breach of the normal distribution of responsibilities within an institution and such reporting by single employees could create unnecessary confusion and workload both for the authorities and the board. However, we do of course see the need for a possibility to alert the authorities in situations where the board does not perform its duties. However, the regulatory framework requires a lot of control functions, and it should be clearly stated that the responsibility for reporting any breaches to the authorities primarily rests by the board and secondly by independent control functions such as external audit. If anybody else should be given such a responsibility or be motivated to perform such reporting, it should be the internal control functions like internal audit, risk management or the compliance functions and only after those control functions having requested the board to report the breaches themselves, but the board failing to do so.



Q5: Are the guidelines in Title III regarding the principle of proportionality appropriate and sufficiently clear?

ESBG agrees with the majority of the criteria listed in the application of the principle of proportionality, however believe that the provisions of Title III should be placed as an introduction to the Guidelines, with it being clearly stated that the principle of proportionality applies to all requirements.

In addition, ESBG strongly supports the subsidiarity principle recognised at EU level in order to respect the legal national frameworks of savings and retail banks, including the cooperative banking model.

Q6: Are the guidelines in Title IV regarding the internal control framework appropriate and sufficiently clear?

ESBG would like to point out that a clarification in these guidelines regarding the relationship between the required recovery plans according to Banking Recovery and Resolution Directive and the contingency and recovery plans according to these guidelines would have been very useful.

In paragraphs 144 and 145 the responsibility for ensuring internal compliance with the new product approval policy (NPAP) has been shared between the compliance function and the risk management function. A shared responsibility risks creating either overlap of work or allows issues to fall in-between the two functions. An institution should be able to assign the main responsibility to either of the functions, risk or compliance (see also paragraph 148). Furthermore, it would be desirable if all the requirements regarding the new product approval process could be subsumed under the same chapter (see for example paragraphs 158-160 regarding risk and 181 regarding compliance).

Para. 144 makes reference to the compliance function ensuring internal compliance with policies. ESBG does not believe that this has to be the responsibility of the compliance function. The compliance function is responsible for ensuring compliance with all applicable laws and regulations (which is set out in para. 181) and as such has a role in the product approval process, alongside risk management, which has to ensure all risks related to the products are appropriately addressed. However, it should be the decision of each financial institution's board if the compliance function also should be responsible for ensuring compliance with internal policies. Anyway, it is a core responsibility of the internal audit function to assess and verify the compliance with – among other things – the compliance with internal policies, on a risk based approach. Internal audit has to assess and verify if all required parties performed their duty during the product approval process, i.e. they also have to ensure that compliance undertook the relevant checks with respect to applicable laws and regulations.

Furthermore, we would like to mention that para. 145 seems to mix different concepts. The specific procedures for assessing compliance with policies should be part of the duties of internal audit. The assessment and approval by compliance needs to be part of the product approval process as set out under the previous comment. Para. 145 should be amended to clearly differentiate between these two aspects.

With regard to para. 156 it is unclear how the RMF would “test” the robustness and sustainability of the risk strategy and appetite. ESBG would appreciate if additional guidance could be provided to clarify this requirement.



Paragraphs 180 and 181 state, again, that cooperation should take place (see above paragraphs 144 and 145). Cooperation within an institution is fundamental to fulfil the requirement for authorisation in accordance with the legal requirements. If the guidelines address this requirement it means that the supervisory authority must be able to verify that such cooperation actually takes place, which in turn creates demand that the institutions can show a process for the cooperation. In total the requirement becomes vague and too far-reaching and should therefore be removed.

With regard to the section 15.3 on Internal Audit Function it would be desirable if all items related to the internal audit function could be gathered under the same section, for example para. 69 (structures and activities should be reviewed by the internal audit function).

We also believe that limitations to the risk-based approach that are to be applied by the Internal Audit function shall be limited to the greatest extent possible. Therefore, we suggest that the review described in paragraph 69 should be based on a risk-based approach and this should be reflected in the paragraph. A new wording of paragraph 69 could then be “All these structures and activities [...] should, *subject to a risk based approach*, be subject to review by the Internal Audit function”.

Q7: Are the guidelines in Title V regarding transparency of the organization of the institution appropriate and sufficiently clear?

No comments.

Q8: Are the findings and conclusions of the impact assessments appropriate; please provide to the extent possible an estimate of the cost to implement the Guidelines differentiating of one-off and ongoing costs?

It is crucial to maintain a neutral approach leaving the competent authorities the choice of implementing ex ante or ex post assessment in order to comply with national legal frameworks.

For instance, the ex-ante assessment cannot be implemented by the French savings banks. According to the provision of the French Monetary and Financial Code (Article L521.90), every 6 years, for all savings banks at the same time, the whole management body (in its supervisory function i.e. Conseil de Surveillance) is totally renewed by a general process of election including 5 different processes set up by the French law.



About ESBG (European Savings and Retail Banking Group)



European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ■ www.wsbi-esbg.org

Published by ESBG. [Date]